И. В. Андрианов

ПРИМЕНЕНИЕ ИНТЕЛЛЕКТУАЛЬНОГО АНАЛИЗА ДАННЫХ ДЛЯ ВЫЯВЛЕНИЯ МОШЕННИЧЕСКИХ ТРАНЗАКЦИЙ ПО ПЛАТЕЖНЫМ КАРТАМ

Интеллектуальный анализ данных (ИАД) — это процесс обнаружения в сырых данных ранее неизвестных, нетривиальных, практически полезных и доступных интерпретации знаний, необходимых для принятия решений в различных сферах человеческой деятельности [1]. Отличительной особенностью data mining является то, что эта мультидисциплинарная область изначально направлена на конкретный, непосредственно применимый результат. Существуют несколько задач ИАД, в том числе классификация и прогнозирование. Процесс классификации заключается в разбиении объектов на классы с помощью некоего критерия, поиск которого и есть главная цель решения данной задачи. Если под классами понимать величину, принимающую не дискретные, а непрерывные значения, то аналогичная задача носит название «прогнозирование». Задачу классификации можно сформулировать следующим образом:

- имеется множество уникальных объектов, каждый из которых принадлежит одному из возможных классов;
- необходимо построить модель правил, которая определит, к какому классу будет принадлежать новый объект.

В случае задачи прогнозирования необходимо определить не класс, а конкретное значение зависимой переменной.

Рассмотрим возможность применения этих задач для формирования профилей несанкционированных операций по платежным картам. Введем множество всех возможных транзакций T, членами которого являются транзакции $t_k^i \in T$, где k — идентификатор карты, i — порядковой номер транзакции по карте с идентификатором k. Введём параметр l — глубина ретроспективы, определяющий количество предыдущих транзакций, подлежащих рассмотрению. Получаем последовательность транзакций $t_k^{i,l} = (t_k^i,\ t_k^{i-1},\ ...,\ t_k^{i-l}) \in T^{l+1}$.

Последовательности транзакций присваивается класс 1, если среди всех карт, по которым есть ретроспективные данные, число случаев (Q_1), где аналогичные последовательности, заканчивающиеся мошеннической операцией, превышают пороговое значение ρ. В противном случае последовательности присваивается класс 0 (число случаев, в которых результатом указанной последовательности является санкционированная операция владельца карты, обозначим Q_0). Таким образом, обобщаем последовательность $t_k^{i,l}$ на множество всех имеющихся карт и получаем последовательность $t_{(n)}^{i+1} = (t_{(n)}^{i+1},\ t_n^l,\ ...,\ t_n^1)$, где n — номер типа последовательности. Введя все необходимые обозначения, итеративно опишем подход к решению задачи классификации в данной сфере.

среди всех транзакций исходного представления выделяем первую мошенническую транзакцию t_k^i;

формируем последовательность $t_k^{i,l}$ и далее способом, описанным выше, обобщаем эту последовательность на все карты, записываем в таблицу последовательность $t_{(1)}^{l+1}$ и соответствующую метку $\in\{0,1\}$;

повторяем этот процесс для других мошеннических операций, формируем последовательности $t_{(2)}^{l+1},\ ...,\ t_{(n)}^{l+1}$ и сопоставляем им метки. Так как исходные последовательности обобщены на множество всех карт, то каждая последовательность встречается в таблице лишь один раз и, значит, метка определена однозначно.

Таким образом, получили представление данных, для которых известными методами (деревья решений, k-ближайшего соседа) может быть решена задача классификации. На вход модели

подается последовательность транзакций, выходом модели служит класс, определяющий, является ли данная последовательность транзакций потенциально опасной или нет. С помощью решения этой задачи, возможно сделать вывод о безопасности авторизации текущей транзакции.

Данные для решения задачи прогнозирования отличаются лишь меткой: бинарный вариант {0,1} неприменим, необходимо ввести непрерывную величину. Введем параметр $A = N_0*Q_0 - N_1*Q_1$, где N_1 — вес мошеннической транзакции, N_0 — вес законной транзакции ($N_1 > N_0$). На вход модели прогнозирования поступает последовательность транзакций (текущая + ретроспективные), на выходе — прогнозируемое число A, которое условно можно назвать риском транзакции, и далее эксперт (или другой алгоритм) может оценить, насколько разумной является авторизация данной транзакции. Этим алгоритмом может быть классификатор, на входе которого будет уже не последовательность транзакций, а число A. Такую задачу классификации решить проще, так как входное множество — не массив сложно структурированных данных, а конкретное число. Таким образом, последовательное решение задач прогнозирования и классификации также может быть применено для выявления несанкционированных операций.

Разработанный подход может в дальнейшем стать основой для модуля выявления мошеннических транзакций с использованием методов ИАД.

СПИСОК ЛИТЕРАТУРЫ:

1. Курс лекций Data Mining. Интернет-университет информационных технологий. URL: http://www.intuit.ru/department/database/datamining/.

А. А. Балаев, В. С. Горбатов

МЕТОДИКА АТТЕСТАЦИОННЫХ ИСПЫТАНИЙ PLC-СЕТЕЙ НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

В связи с принятием Федерального закона № 261-ФЗ «Об энергосбережении и о повышении энергетической эффективности и о внесении изменений в отдельные законодательные акты Российской Федерации» становится актуальной задача повышения эффективности управления системами информационной безопасности территориально-распределенных систем энергообеспечения. Для решения указанной задачи в системах электропитания представляется целесообразным применение распределенных систем передачи данных на основе технологии powerline communication (PLC) [1]. Однако в настоящее время никаких общих решений по вопросам обеспечения информационной безопасности таких сетей еще не предложено, что затрудняет оценку их защищенности.

В данной работе предлагается методика проведения проверки PLC-сети на соответствие требованиям безопасности информации, которая основывается на положениях руководящих документов ФСТЭК России [2] и типовых методиках испытаний объектов информатизации по требованиям безопасности информации и включает в себя:

1. Структурную модель PLC-сети;
2. Модель угроз и модель нарушителя;
3. Программно-аппаратную имитацию PLC-сети;