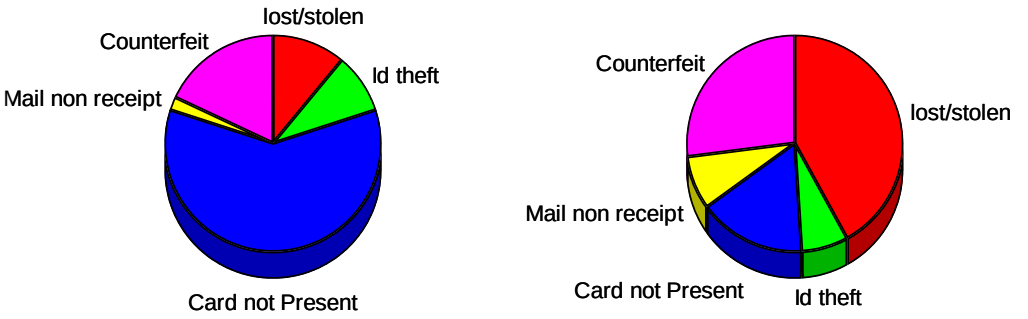
ZASTOSOWANIE SZTUCZNYCH SIECI NEURONOWYCH W DETEKCJI KARTOWYCH TRANSAKCJI OSZUKAŃCZYCH

Michał Grzywa, ALIOR BANK S.A.

Karty płatnicze są powszechnie stosowanym i bezpiecznym instrumentem płatniczym. W portfelach Polaków jest ich ok. 32 mln.; dokonano nimi w 2009 r. ok. 1,4 mld transakcji [10]. O ile teza o wygodzie płynącej z używania karty płatniczej zamiast gotówki nie wymaga dodatkowej argumentacji, o tyle - w kontekście tego artykułu - warto wspomnieć o przewagach w bezpieczeństwie obrotu kartowego nad obrotem gotówkowym. W porównaniu do gotówki dostęp do środków zgromadzonych na rachunku poprzez kartę wymaga, oprócz jej fizycznego posiadania, także znajomości kodu PIN, a w razie utraty karty istnieje możliwość jej natychmiastowego zastrzeżenia. Możliwe jest także zdefiniowanie dziennych, wartościowych limitów transakcyjnych, które ustawione na rozsądnym poziomie umożliwiają znaczne ograniczenie straty w razie utraty karty. Wiele banków oferuje klientom możliwość ubezpieczenia się od ewentualnej szkody powstałej w wyniku kradzieży karty. Transakcje kartowe są także monitorowane pod kątem bezpieczeństwa przez instytucje finansowe, co także pozwala uchronić klienta przed skutkami użycia karty przez osoby niepowołane. Pomimo powyższych przewag karty nad gotówką istnieje jednak ryzyko strat wynikających z transakcji oszukańczych (*fraud*). Ryzyko to jest ryzykiem operacyjnym wpisanym w działalność każdego banku - wydawcy kart płatniczych. Skuteczne zarządzanie tym ryzykiem obejmuje: prewencję, detekcję i obsługę incydentów fraud [11]. W ramach zarządzania ryzykiem banki stosują odpowiednie procedury bezpieczeństwa i procesy monitoringu transakcji. Z racji skali transakcji, które każdego dnia przechodzą przez systemy transakcyjne, ich monitoring wymaga zastosowania zaawansowanych, wydajnych systemów i metod analitycznych, a także specjalistycznej wiedzy pracowników, by skutecznie przeciwdziałać powstawaniu strat, a w razie ich wystąpienia ograniczać ich poziom.

Wyróżnia się kilka typów transakcji oszukańczych dokonanych przy użyciu kart płatniczych. Jednym z kryteriów podziału może być sposób, w jaki karta/dane znajdujące się na karcie zostały pozyskane przez przestępców. Podział przyjęty np. przez brytyjskie FFAUK (*Financial Fraud Action UK*) wyróżnia: transakcje dokonane kartami skopiowanymi (*counterfeit*/*skimming fraud*), transakcje kartami skradzionymi/zgubionymi (*lost*/*stolen fraud*), transakcje kartami przechwyconymi w drodze do adresata (*mail non receipt fraud*), transakcje kartami w środowisku CNP (*Card Not Present fraud*, np. transakcje w Internecie), transakcje fraud w wyniku przejęcia tożsamości (*account take over fraud*/*card id theft*) [7]. Zauważalną tendencją na rynku światowym w ostatnim czasie jest wzrost udziału

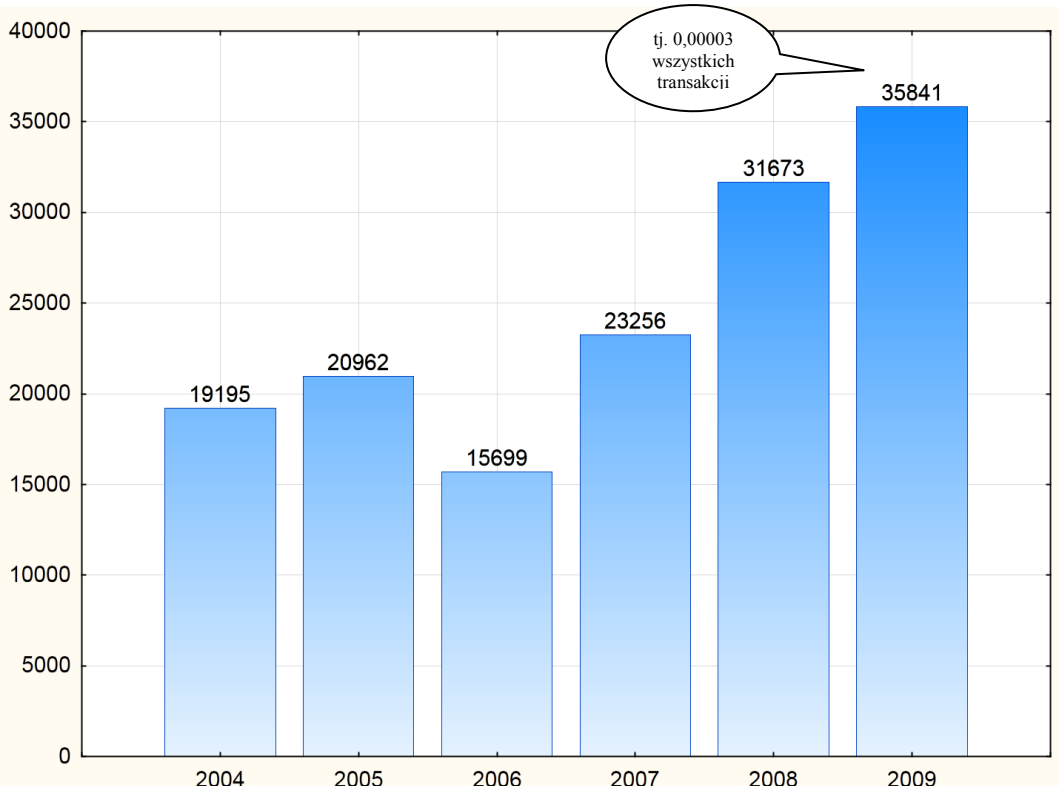
transakcji fraud typu CNP – przykładową zmianę struktury transakcji fraud dla rynku brytyjskiego w ciągu 10 lat przedstawia wykres 1.



2009 1999

Wykres 1. Struktura strat z tytułu kartowych transakcji oszukańczych wg typu fraud na rynku UK. Zmiana 1999-2009; źródło opracowanie własne na podstawie: http://www.ukpayments.org.uk/files/fraud_the_facts_2010.pdf.

Według danych Narodowego Banku Polskiego w 2009 roku liczba transakcji oszukańczych kartami płatniczymi wyniosła 35.841 [10]. Poziom strat z tytułu transakcji oszukańczych w Polsce jest na stosunkowo niskim poziomie w porównaniu do innych krajów UE. Podstawową miarą poziomu strat jest tzw. *Fraud Basis Point* (BP) – liczony jako wartość transakcji fraud do obrotu ogółem na danym portfelu kart x 10000. W 2009 roku zaraportowano do NBP straty o łącznej wartości 26.072.284 PLN, co daje wartość 0,79 BP.



Wykres 2. Liczba transakcji oszukańczych wg NBP w latach 2004-2009; źródło: oprac. własne na podstawie „Ocena funkcjonowania polskiego systemu płatniczego w II półroczu 2009. NBP Departament Systemu Płatniczego, III 2010".

Metody data mining w detekcji kartowych transakcji oszukańczych

Do wykrywania transakcji oszukańczych stosuje się rożne algorytmy. Najprostsze systemy monitoringu transakcji – FDS (*fraud detection system*) wykorzystują reguły (r*ule based systems*), których złamanie przez transakcję/grupę transakcji powoduje generowanie alertów. Systemy takie opierają się na wiedzy eksperckiej osób tworzących reguły i są od niej bezpośrednio zależne. Pewnym ograniczeniem tego typu podejścia jest dość wysoki poziom *false positive* i konieczność „ręcznego" budowania ciągle nowych reguł dostosowujących się do nowych zachowań fraud. Także liczba i złożoność reguł może być ograniczona przez wydajność systemu. Niewątpliwie do zalet systemów typu *rule based* należy ich prostota, szybkość i niski koszt wdrożenia, a także łatwa interpretacja wyników. Wszystko to sprawia, że ten rodzaj systemów ma zastosowanie również obecnie, choć często jest on ograniczony do kilku/kilkunastu „silnych" reguł, np. wystąpienie transakcji w dwóch rożnych lokalizacjach w czasie krótszym niż możliwy do pokonania dystansu między nimi.

Proces monitoringu transakcji kartowych stawia wiele wymagań dla systemów FDS. Do najczęściej wymienianych w literaturze przedmiotu i zaobserwowanych w praktyce zalicza się:

- skala transakcji podlegającej monitoringowi [5],
- ograniczony czas na rekcję systemu i operatora, tak aby ograniczyć straty[5],
- dysproporcja liczebności klas - transakcje *genuine*/*fraud* (np. zapewnienie wystarczającej liczby „złych" przypadków jako danych uczących model) [8],
- problem wysokiego poziomu *false positive* i różne koszty pomyłek dla *false positive* i *false negative* [12],
- wiele zmiennych pochodzących z rożnych źródeł danych analizowanych przy ocenie pojedynczej transakcji,
- zmieniający się w czasie charakter/typ transakcji fraud.

Przedstawione powyżej uwarunkowania procesu monitoringu sprawiają, że przydatne są zwłaszcza te systemy, które wykorzystują metody data mining. Od połowy lat 90. XX wieku w procesie detekcji fraud wykorzystuje się systemy angażujące ten typ metod. Stosuje się zarówno metody ukierunkowane (*supervised*) data mining, jak i metody nieukierunkowane (*unsupervised*) data mining. W podejściu ukierunkowanym model jest budowany w oparciu o zbiór transakcji „dobrych" (*genuine*) i transakcji *fraud* (znane są przypadki fraud z przeszłości i na ich podstawie model uczy się klasyfikować przyszłe transakcje). W podejściu nieukierunkowanym, zwanym często „modelami behawioralnymi", wykorzystuje się analizę bieżących zachowań transakcyjnych użytkownika karty i porównanie ich w stosunku do profilu transakcyjnego klienta - budowanego w oparciu o dane historycznie. Do najczęściej stosowanych metod data mining w systemach FDS należą: sztuczne sieci neuronowe, SVM (*support vector machine*) metoda wektorów nośnych, CBR (*case based reasoning*) wnioskowanie na bazie przykładów, regresję logistyczną, drzewa klasyfikacyjne, drzewa wzmacniane [2][4]. Szczegółowy przegląd metod stosowanych w FDS można znaleźć w pracy Phua, Lee, Smith, Gayler 2005 [13]. Pewnym ograniczeniem ich stosowania może być prędkość działania i wydajność niektórych z tych metod, zwłaszcza jeśli są one adaptowane do zadań w trybie *real online* [12] - czyli odpowiedź systemu autoryzacyjnego na zapytanie autoryzacyjne jest uzależniona od odpowiedzi systemu FDS.

W ostatnich latach buduje się też systemy hybrydowe – w których łączy się tradycyjne metody, np. oparte na regułach i metodach data mining. Połączenie takie może dawać lepszą skuteczność i obniżać poziom *false positive*. Architektura hybrydowego systemu może zakładać sekwencyjne ułożenie metod w procesie klasyfikacji lub równoległe ich działanie, a potem agregację wyników, np. poprzez głosowanie modeli. Innym stosowanym w praktyce podejściem jest równoległe działanie dwóch systemów: np. *rule based*, który wykazuje wyższą skuteczność dla znanych już schematów fraud, i system oparty na modelu behawioralnym (data mining nieukierunkowany), który okazuje się skuteczniejszy dla nowych typów fraud [8].

Sztuczne sieci neuronowe znajdują szerokie zastosowanie w systemach FDS i jako jedne z pierwszych zostały w nich zaimplementowane. Przykładem może być zgłoszony już w roku 1998 w USA patent nr 5819226 na „Fraud detection using predictive modeling" przez firmę HNC Software Inc. Sieci neuronowe mogą być wykorzystywane w systemie jako jedyna metoda, np. opracowany przez E. Aleskerova i in. system Cardwatch [2], lub występować w systemach hybrydowych i uzupełniać działanie innych metod [3]. O wysokiej skuteczności sieci w detekcji fraud mogą świadczyć wyniki przedstawione np. przez Ghosh and Reily [6] - zastosowanie sieci pozwoliło ograniczyć straty z tytułu transakcji fraud o ok. 20-40%.

Do głównych zalet sieci neuronowych jako metody w zadaniach klasyfikacyjnych należą m.in. [15]:

- brak hipotez, założeń co do postaci funkcji klasyfikacji,
- możliwość wykorzystania wielu zmiennych o charakterze jakościowym i ilościowym,
- szybkość działania,
- zdolność sieci do uczenia się i do generalizacji wyników.

Najczęściej wykorzystywanym typem sieci w detekcji fraud są sieci MLP i RBF – zaliczane do metod uczenia z nauczycielem. W literaturze spotyka się także sieci Kohonena typu SOM (*self organised map*), które wykorzystują uczenie bezwzorcowe [9][14][16]. Sieci takie stosuje się do segmentacji transakcji, grupowania ich w podobne skupiska. Niektóre z tych skupisk po analizie eksperckiej mogą być zidentyfikowane jako transakcje fraud, również transakcje, które na mapie topologicznej powstałej z sieci SOM są nietypowe i nie „pasują" do żadnego skupiska, mogą być transakcjami o podwyższonym ryzyku. W pracy Quah, Sriganesh [14] zaproponowano użycie sieci SOM jako warstwy filtrującej transakcje, dopiero transakcje ze skupisk „podejrzanych" zostały poddane właściwemu scoringowi. Podejście takie pozwoliło w sposób znaczący ograniczyć czas potrzebny na liczenie dodatkowych charakterystyk (np. liczenie agregatów) używanych jako zmienne już w samym scoringu.

Jako zarzut przeciw stosowaniu sztucznych sieci neuronowych w detekcji fraud pojawia się stwierdzenie, że są one „czarną skrzynką" i brakuje w tej metodzie prostego wytłumaczenia odpowiedzi wygenerowanej na wyjściu sieci. Cała „wiedza" sieci i ich zdolność do rozwiązywania zadań jest ukryta w wagach połączeń między neuronami, które to ustalane są w procesie uczenia sieci. Sztuczne sieci neuronowe, które są uproszczonym odwzorowaniem działania biologicznej struktury mózgu, pozwalają wychwycić i uwzględnić w wyniku interakcje między zmienną objaśnianą a zmiennymi objaśniającymi. Jeżeli porównać proces myślowy, jaki zachodzi w mózgu osoby sprawującej nadzór nad transakcjami do działania sztucznej sieci neuronowej, to inwestygujący transakcje człowiek również musi odpowiednio „zważyć" wszystkie za i przeciw, zanim podejmie decyzję o klasyfikacji danej transakcji jako fraud. To „ważenie" za i przeciw jest tym skuteczniejsze, im większą wiedzę i doświadczenie posiada człowiek. Często spotykanym w praktyce przy inwestygacji transakcji jest stwierdzenie inwestygującego specjalisty: że „coś w tej transakcji mi nie pasuje", ale nie potrafi on dokładnie wskazać, co, która zmienna

o tym decyduje, jaki jej poziom etc. Mówi się wtedy, że o poprawnej decyzji o wstrzymaniu transakcji zaważyła intuicja kontrolującego. Sieci - być może choć w uproszczonym stopniu - symulują tę „intuicję" i między innymi dlatego dobrze sprawdzają się w systemach FDS.

Budowa modelu

Celem biznesowym opisywanego projektu pilotażowego było sprawdzenie przez ALIOR BANK S.A., czy sztuczne sieci neuronowe skutecznie mogą wykrywać kartowe transakcje oszukańcze, przy jakim poziomie *false positive*, a także jaka architektura sieci sprawdzi się najlepiej. Budowa i ocena przydatności modeli data mining do detekcji fraud prezentowanych w literaturze dokonywana jest najczęściej w oparciu o dane sztucznie wygenerowane, celem projektu była więc także weryfikacja skuteczności SSN na danych rzeczywistych. Do budowy modelu i jego oceny wykorzystano narzędzie *STATISTICA Data Miner* + *Zestaw Skoringowy STATISTICA* (metodyka skoringu kredytowego wykazuje znaczną analogię do detekcji fraud). Skuteczność stosowania narzędzi *STATISTICA* w detekcji fraud potwierdza ich wykorzystanie w pracach: [1][4][9]. Dane na niektórych wykresach i tabelach zostały celowo ukryte lub pominięte.

Przygotowanie danych

Proces przygotowania danych uczących do sieci był najbardziej pracochłonnym etapem. Obejmował on przygotowanie zbioru zawierającego transakcje fraud (F) i transakcje genuine (G). O ile zgromadzenie wystarczającej liczby (kilku tysięcy) przypadków genuine nie stanowiło problemu - wylosowano je z historycznej bazy transakcji, o tyle o reprezentantów klasy fraud było trudniej. W okresie ponad dwóch lat działalności Banku zgromadzono ich niewiele. Zbiór ten obejmuje w przeważającej większości transakcje, które nie doszły do skutku – nie zostały pozytywnie zautoryzowane, czyli np. otrzymały odmowy z powodu wcześniejszej blokady karty przez Bank w wyniku monitoringu. Liczebność klasy fraud wydaje się jednak wystarczająca w porównaniu do innych prac tego typu oraz zaleceń co do liczebności klas, np. przy skoringu kredytowym.

Wychodząc z założenia, że wiedza jest w danych, przy budowie modelu konieczne jest zadbanie o wysoką jakość danych. Przygotowanie danych to także uzupełnienie braków, „czyszczenie" danych, np. usunięcie zdublowanych rekordów, usunięcie danych odstających (np. błędnie wprowadzona w systemie kwota autoryzacji itp.), przekształcanie zmiennych (np. daty na dzień tygodnia), zmiana kodowania niektórych z nich (np. format czasu transakcji) itp. Do modelu wykorzystano także zmienne profilowe; aby wyliczyć te zmienne pochodne dla każdej z kart występującej w modelu konieczne było także przygotowania zbioru wszystkich transakcji (w tym transakcji genuine dla kart, dla których odnotowano później transakcje fraud).

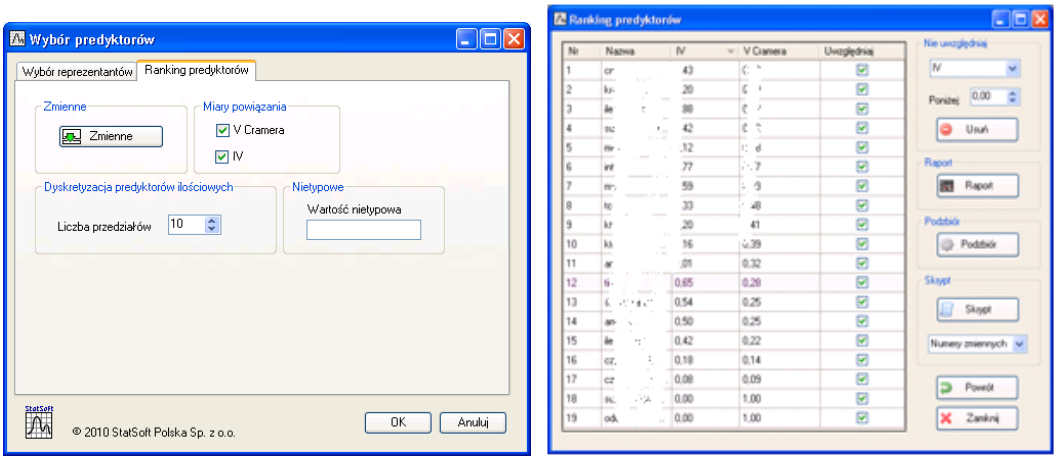
Przy budowie modelu SSN konieczny jest podział na zbiory: uczący, testowy i walidacyjny, by kontrolować wyniki sieci na zbiorze walidacyjnym i przeciwdziałać „przeuczeniu

się sieci". Podziału na zbiory uczący, testowy i walidacyjny w proporcjach odpowiednio (70%/15%/15%) dokonano poprzez losowanie przypadków do poszczególnych kategorii.

Zgodnie z metodologią SSN liczebności klas użyte do budowy sieci powinny być zrównoważone. Autor przetestował kilkanaście sieci, zarówno przy układzie zrównoważonych liczebności klas, jak i przewagi klasy genuine (G). Dla każdego wariantu analizowana była macierz klasyfikacji. O ile poziom prawidłowych klasyfikacji dla klasy fraud był na bardzo zbliżonym poziomie, o tyle przy niezrównoważonej liczebności (na korzyść klasy genuine) model wykazywał mniejszą skłonność do pomyłek dla klasy genuine, czyli niższy poziom false positive (FP). Właściwość ta miała duże znacznie, gdyż niski poziom FP oznacza niższe koszty procesu. Poniżej w pracy analizie poddano model, który uczony był przez zbiór w proporcji liczebności 90%(G),10%(F).

Wybór zmiennych

Lista zmiennych dostępnych z systemu autoryzacyjnego, które charakteryzują każdą transakcję jest obszerna; jeśli doliczyć do tego zmienne profilowe, to liczba ta może dojść do kilkudziesięciu. Zmienne pochodne/profilowe pozwalają ograniczyć *false positive*. Przykładowymi zmiennymi profilowymi może być średnia kwota transakcji i odchylenie standardowe dla transakcji genuine dla każdej z kart; informacja, czy klient wcześniej mylił się w PIN, czy klient wcześniej miał odmowy z powodu braków środków, która jest to z kolei transakcja w ciągu 1 godziny etc. Warto w tym miejscu zaznaczyć, że wdrożenie modelu SSN w trybie *real online* nakłada ograniczenie czasowe w wyliczeniu niektórych zmiennych agregatowych.

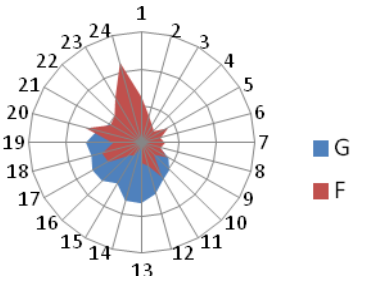


Rysunek 1. Moduł *Wybór* i *Ranking Predyktorów* w *Zestawie Skoringowym STATISTICA*.

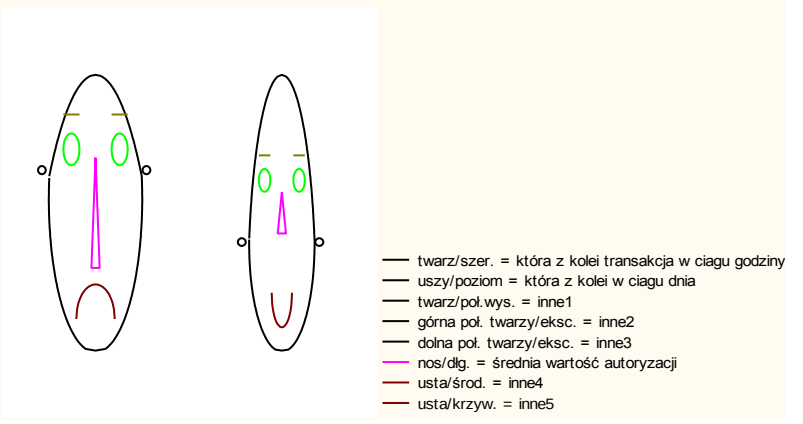
Przy budowie modelu należy liczbę zmiennych ograniczyć, by z jednej strony uprościć model (liczba zmiennych przekłada się bezpośrednio na liczbę wag w sieci, a to z kolei wymusza odpowiednią liczbę danych uczących), a z drugiej strony wybrać te zmienne, które niosą jak najwięcej informacji - wpływając na zmienność zmiennej objaśnianej. Przydatnym narzędziem w procesie wyboru zmiennych może być moduł *Zestaw*

Skoringowy/Wybór Predyktorów w *STATISTICA*, który umożliwia analizę siły wpływu poszczególnych zmiennych na zmienną zależną (mierzoną poprzez *Information Value* i *V Cramera*) i stworzenie tym samym rankingu predyktorów.

Wyboru zmiennych dokonano także w oparciu o analizę ekspercką, przy wykorzystaniu analizy graficznej rozkładu zmiennych w klasie F i G (np. wykres 3 i 4) i analizę macierzy korelacji. Ostatecznie do modelu przyjęto 5 zmiennych ilościowych i 7 jakościowych. Niektóre zmienne jakościowe miały bardzo liczne kategorie, co wymagało kodowania ich na wejściu do sieci na typ 1 z N. Przydatnym narzędziem do oceny post fatum słuszności wyboru poszczególnych zmiennych może być globalna analiza wrażliwości. Wszystkie wybrane zmienne miały wartość powyżej 1 (co oznacza stratę na jakości sieci, gdyby zmienne te wyłączono z modelu), choć ich ranking był w części zaskoczeniem dla ekspertów.



Wykres 3. Rozkład wg godzin dokonania transakcji w grupie F i G.



Wykres 4. Twarze Chernoffa (twarz z lewej to „profil" transakcyjny F, twarz z prawej dla profilu „G"). O poziomie, wielkości, kształcie poszczególnych elementów twarzy decyduje poziom wybranych zmiennych.

Architektura sieci

Korzystając z modułu automatycznego projektanta sieci zbudowano ok. 20 różnych sieci, w tym sieci o architekturze MLP i RBF; o różnej liczbie neuronów w warstwie ukrytej

i różnych funkcjach aktywacji. Każdą z sieci oceniono pod względem poziomu błędu (jakość sieci), jego stabilności w zbiorach: uczącym, testowymi walidacyjnym, a także wyników macierzy klasyfikacji. Najlepszą charakterystykę miała sieć typu (MLP) perceptron trójwarstwowy o 13 neuronach w warstwie ukrytej z funkcją aktywacji *tanh* w warstwie ukrytej i funkcją *softmax* w warstwie wyjściowej.

Tabela 1. Parametry sieci.

Podsumowanie sieci				
	Id sieci	**Nazwa sieci**	**Aktywacja (ukryte)**	**Aktywacja (wyjściowe)**
	1	MLP 265-13-2	Tanh	Softmax

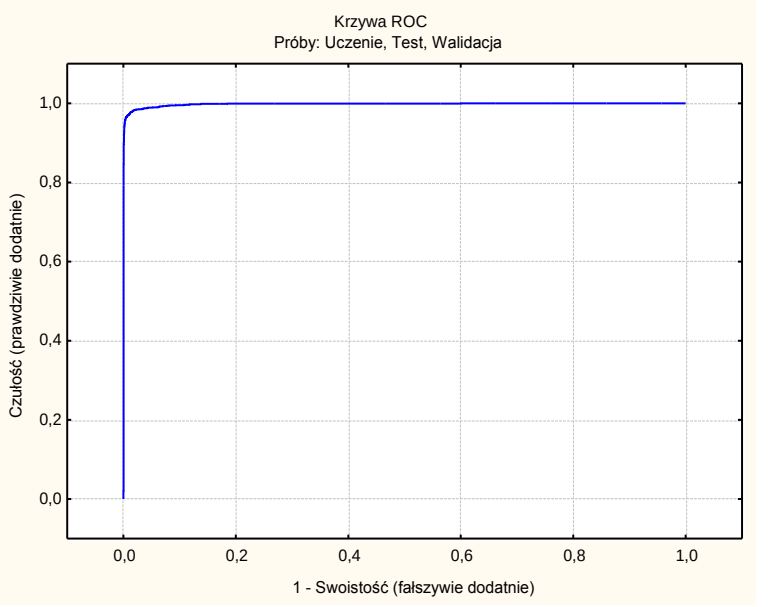
Ocena jakości sieci

Wybrana sieć poprawnie sklasyfikowała ponad 95% transakcji fraud (dane dla zbioru uczącego, testowego i walidacyjnego), popełniając przy tym błąd *false positive* na poziomie ok. 0,3%. O Ile wynik *true positive* jest zaskakująco dobry, to poziom *false positive* przy większej dziennej skali transakcji może okazać się za wysoki, konieczne jest wtedy odpowiednie ustawienie punktu odcięcia.

Tabela 2. Macierz klasyfikacji sieci.

F/G (Podsumowanie klasyfikacji)				
		F/G-F	**F/G-G**	**F/G-Wszystkie**
1.MLP 265-13-2	Razem			
	Poprawne			
	Niepoprawne			
	Poprawne (%)	95,622	99,71	99,26
	Niepoprawne (%)	4,378	0,29	0,74

Kolejną miarą jakości sieci jako klasyfikatora jest krzywa ROC (R*eceiver Operating Characteristic*). Pokazuje ona na jednej osi skumulowaną wartość TP, a na drugiej skumulowaną FP. Im pole pod krzywą (AUC) jest bliższe jedności, tym lepsza jakość klasyfikatora. Jak widać z przebiegu ROC i wartości AUC, wyniki uzyskane przez sieć są bardzo dobre.

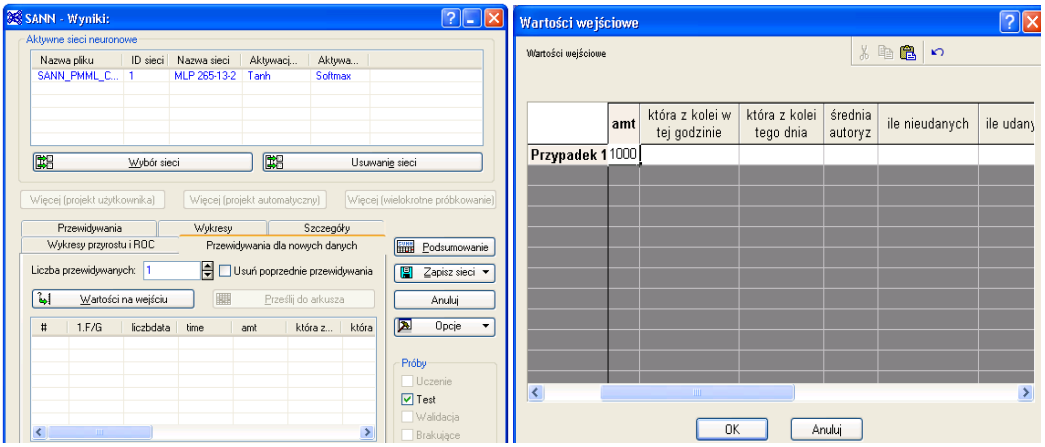


Wykres 5. Krzywa ROC dla wybranej sieci.

Tabela 3. AUC dla wybranej sieci.

Powierzchnia i próg ROC	
	1. MLP 265-13-2
Powierzchnia ROC	0,997802

Przydatnym narzędziem w module sieci neuronowe w *STATISTICA* jest możliwość natychmiastowego sprawdzenia, jak zbudowana sieć zachowałaby się dla nowych danych (np. wpływa nowe zgłoszenie reklamacyjne dotyczące transakcji fraud). Prawidłowy wynik działania sieci dla nowych danych świadczy tak naprawdę o jej zdolności do generalizacji wyników i potwierdza zasadność jej wdrożenia.

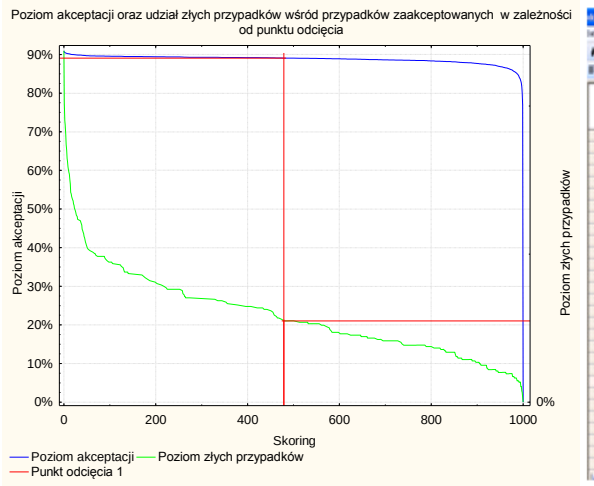


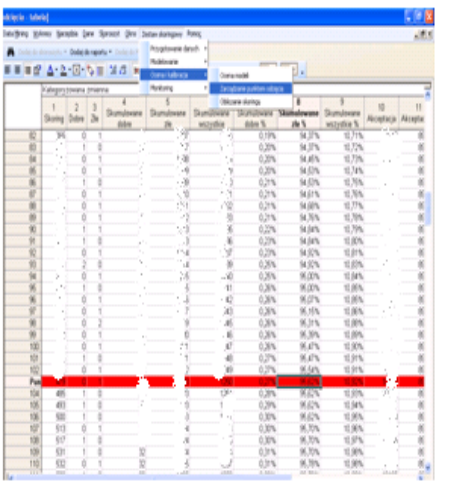
Rysunek 2. Moduł do przewidywania wyjścia sieci dla nowych danych.

Zarządzanie puktem odcięcia

Mając na uwadze, że liczebności klas F i G wykazują w rzeczywistości skrajną dysproporcję, należy uwzględnić to w interpretacji wyników macierzy klasyfikacji dla danej sieci. Sieć klasyfikuje przypadki do klasy F i G w oparciu o poziom p na każdym z 2 neuronów na wyjściu sieci. Wyniki prezentowane w macierzy klasyfikacji zakładają, że dany przypadek trafia do klasy G, jeżeli P(G)>0,48. Przy tak ustawionym poziomie granicznym być może poziom *false positive* 0,3% jest za wysoki i należy wyznaczyć inny graniczny poziom, którego przekroczenie będzie powodować zmianę przynależności do klasy. Ustalanie tego poziomu granicznego określane jest jako zarządzanie optymalnym punktem odcięcia (*cut-off*). Aby zoptymalizować działanie modelu pod kątem kosztów przy ustalaniu poziomu *cut-off*, konieczna jest wiedza o kosztach błędnych klasyfikacji (dla F i G).

Przykładowym podejściem do ustalenia poziomu odcięcia w systemie FDS może być uwzględnienie ograniczeń wydajności obsługi alertów z systemu FDS. Można więc wyznaczyć taką wartość skoringu na wyjściu sieci, która zapewni dostateczną zdolność do detekcji fraud przy zadanym poziomie *false positive*. Zakładając, że planowany wolumen autoryzacji dziennej wynosi np. 1 mln transakcji, a możliwości operacyjne obsługi alertów z systemu FDS to np. 500 dziennie, to szukany punkt odcięcia to taka wartość skoringu (wyjścia sieci), dla której wartość *false positive* nie przekroczy 500/1 000000=0,0005= =0,05%. Ustalenie nowego punktu odcięcia obniżającego poziom FP - co zrozumiałe - spowoduje spadek skuteczności systemu w detekcji transakcji fraud - w wypadku analizowanej sieci do poziomu ok. 84%.





Wykres 6. Wartość skoringu, dla którego skuteczność detekcji fraud wynosi 95%, a FP 0,3%. Aby umożliwić analizę w module *Zarządzanie punktem odcięcia* w *Zestawie Skoringowym STATISTICA*, *p* na wyjściu sieci pomnożono przez 1000.

Decyzją biznesową pozostaje już, czy korzystniejszy jest nieznaczny wzrost poziomu niewykrytych transakcji fraud na skutek słabszej czułości systemu czy też korzystniejsze jest zwiększenie nakładów na zasoby potrzebne od obsłużenia wyższego poziomu FP.

Tabela 4. Klasyfikacja przy nowym punkcie odcięcia.

Skoring	Procent złych	Procent dobrych
(-inf;x>	**84,60%**	**0,05%**
(x;inf)	15,40%	99,95%
Ogół	100,00%	100,00%

Podsumowanie

Systemy FDS mogą skutecznie przeciwdziałać kartowym transakcjom oszukańczym, a w razie ich wystąpienia ograniczać poziom strat. Zbudowany przez ALIOR BANK S.A. model sieci typu MLP bardzo dobrze sprawdził się w detekcji transakcji fraud i potwierdził skuteczność tej nowoczesnej metody data mining. Poziom skuteczności ok. 84% przy poziomie FP 0,05% można uznać za bardzo dobry wynik. Oprogramowanie *STATISTICA* umożliwia zapisanie modelu sieci jako skrypt PMML i przetestowanie jego działania na nowych danych. Faktycznym wyznacznikiem skuteczności modelu będzie więc jego aplikacja w przyszłości do nowych przypadków. Szybko zmieniająca się rzeczywistość, w tym modus operandi przestępców, wymaga jednak, by sieć była uczona co pewien czas, zwłaszcza gdy zmieni się zasadniczo charakter transakcji fraud. Wyzwaniem w stosowaniu metod data mining w detekcji fraud nadal pozostaje utrzymanie wysokiej skuteczności przy niskim poziomie FP; być może połączenie SSN z innymi metodami lub włączenie

dodatkowych zmiennych pozwoliłoby uzyskać jeszcze lepsze wyniki. Możliwym dalszym kierunkiem prac jest także budowa osobnych sieci dla różnych typów fraud.

LITERATURA

1. Abbott D.W., Matkovsky I.P., Elder IV J.P, Ph.D, *An Evaluation of High-end Data Mining Tools for Fraud Detection*, 1998 IEEE International Conference on Systems, Man, and Cybernetics, San Diego, CA, October 12-14, 1998.
2. Aleskerov E., Freisleben B., Rao B., *CARDWATCH a neural based data mining system for credit card fraud detection*, Proceedings of the Computational Intelligence for Financial Engineering, 1997.
3. Chen R.C. , Luo S.T., Liang X., Lee V.C.S., *Personalized approach based on SVM and ANN for detecting credit card fraud*, Proceedings of the IEEE International Conference on Neural Networks and Brain, October 2005.
4. Demski T., *Tworzenie i stosowanie modelu data mining za pomocą przepisów STATISTICA Data Miner na przykładzie wykrywania nadużyć*, Statsoft Polska, 2009.
5. Dorronsoro J.R. , Ginel F., Sanchez C., Cruz C.S., *Neural fraud detection in credit card operations*, IEEE transactions on neural networks 8 July 1997.
6. Ghohs S., Reilly D.L., *Credit card fraud detection with a neural network*, Proceedings of the annual International Conference on System Science, 1994.
7. http://www.financialfraudaction.org.uk/Financial-card-fraud.asp.
8. Kriviko M., *A hybrid model for plastic card fraud detection system*, Expert Systems with Applications 37, 2010.
9. Kujilen T., Migut G., *Wykrywanie nadużyć i prania brudnych pieniędzy*, Statystyka i Data Mining w Praktyce, Statsoft Polska, 2004.
10. *Ocena funkcjonowania polskiego systemu płatniczego w II półroczu 2009*. NBP Departament Systemu Płatniczego, III 2010.
11. Ogsts K., *An innovative approach to fraud management*, Card Technology Today p. 9, October 2008.
12. Panigrahi S. , Kundu A., Sural S., Majumdar A.K., *Credit card fraud detection: A fusion approach using Dempster -Shafer theory and Bayesian learning*, Information Fusion nr 10, 2009.
13. Phua C., Lee V., Smith K., Gayler R., *A Comprehensive Survey of Data Mining-based Fraud Detection Research*, School Of Business Systems, Faculty of Information Technology, Monash University, 2005.
14. Quah Jon T.S., Sriganesh M., *Real-time credit card fraud detection using computational intelligence*, Expert Systems with Applications nr 35, 2008.
15. Tadeusiewicz R., Wójtowicz P., *Sieci neuronowe, Materiały Kursowe*, StatSoft Polska, 2010.
16. Zaslavsky V., Strizhak A., *Credit card fraud detection using self organizing maps*, Information and Security nr 18, 2006.

