ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 2015
Seria: ORGANIZACJA I ZARZĄDZANIE z. 78 Nr kol. 1928

Tomasz GOŚCINIAK
Cisco Systems

ANALIZA SYGNAŁÓW Z PROCESU ZARZĄDZANIA INCYDENTAMI W SYSTEMACH IT I ICH WYKORZYSTANIE W PODEJMOWANIU DECYZJI Z UŻYCIEM METOD SZTUCZNEJ INTELIGENCJI

Streszczenie. Niezawodność systemów produkcyjnych coraz częściej zależy od niezawodności systemów IT, które nadzorują procesy produkcyjne oraz nimi sterują. Skuteczne wsparcie systemów IT pod względem naprawczym oraz utrzymania ich wysokiej niezawodności musi być optymalne kosztowo. Najczęstszym czynnikiem powodującym powstawanie błędów w procesie wsparcia są ludzie, stąd należy rozważyć możliwość wsparcia procesu decyzyjnego przy wykorzystaniu metod sztucznej inteligencji. W artykule przeprowadzono analizę sygnałów dostępnych w procesie naprawczym IT Zarządzania Incydentami oraz ich użyteczności w zastosowaniu w procesie komputerowo wspomaganych decyzji przy wykorzystaniu metod sztucznej inteligencji.

ANALYSIS OF SIGNALS FROM INCIDENT MANAGEMENT PROCESS IN IT SYSTEMS TO USE THEM IN DECISION MAKING USING ARTIFICIAL INTELLIGENCE METHODS

Summary. Reliability of production systems increasingly depends on performance of IT systems, which monitor and control production systems. Effective support of IT systems in the area of repair and maintaining of their high reliability must be performed at optimal costs. The most common factor of the support process errors are people and should consider the possibility of making decision in a different way. The article analyzes available signals from Incident Management process and their usability in the computer aided decision using artificial intelligence methods.

1. Wstęp

Aby uzyskać wysoki stopień niezawodności systemów produkcyjnych, należy zadbać o wysoki stopień niezawodności jego komponentów. Obecnie większość systemów produkcyjnych jest nadzorowana, sterowana oraz utrzymywana przez systemy IT[1]. W związku z tym niezawodność systemów IT przekłada się na niezawodność systemów produkcyjnych. Konkurencja rynkowa wymusza optymalizację koszów utrzymania systemów IT, co głównie implikuje ich większą automatyzację oraz ścisłą kontrolę wydatków na ich naprawy docelowe oraz ulepszenia.

2. Procesy wsparcia w IT

Na główne procesy wsparcia IT składają się:

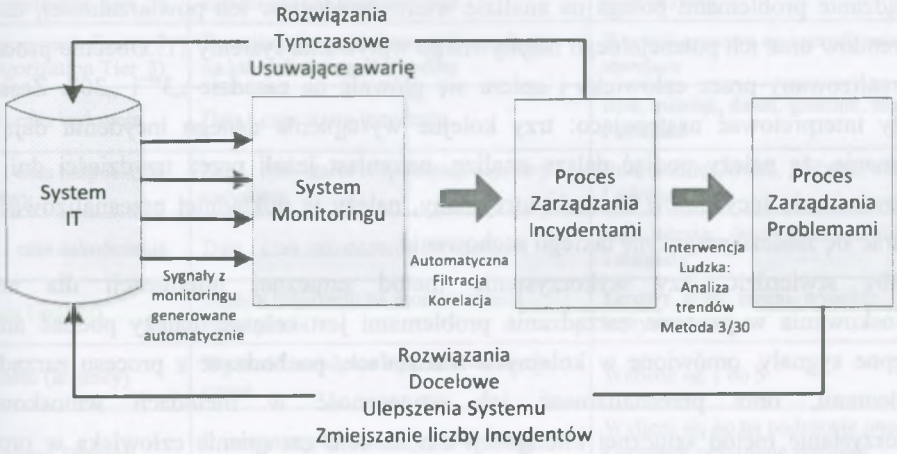
1. Monitoring sygnałów z systemów IT – główny cel to zebranie sygnałów oraz ich filtracja i korelacja. Większość procesów monitoringu obecnie jest dobrze oprogramowana i wykonywana automatycznie.
2. Zarządzanie incydentami – główny cel to usunięcie awarii przez zastosowanie szybkiego rozwiązania tymczasowego. Takie działanie, co prawda, przywraca funkcjonalność Systemu IT, jednakże nie usuwa przyczyny powstawania awarii.
3. Zarządzanie problemami – główny cel to zmniejszenie liczby incydentów oraz usuwanie przyczyn powstawania awarii, a także zmniejszenie negatywnego wpływu awarii na system IT. Ulepszenie systemu IT przez stosowanie rozwiązań docelowych poprawiających działanie systemu zmniejsza liczbę incydentów występujących w przyszłości, jednakże jest kosztowne i wymaga nakładów czasowych oraz pieniężnych.

Zarządzanie incydentami oraz zarządzanie problemami są to procesy ze sobą ściśle powiązane (rys. 1).

1. Zarządzanie incydentami stara się przywrócić normalne funkcjonowanie systemu nawet przy użyciu środków nie w pełni korygujących negatywne efekty powstałej awarii. Posługując się analogią medyczną, można to nazwać leczeniem objawowym.
2. Zarządzanie problemami rozwiązuje przyczyny wielu incydentów oraz usuwa przyczynę powstawania incydentów, a zarządzanie incydentami zakłada reagowanie na wystąpienie pojedynczej awarii.

[1] Gościniak T.: Zarządzanie procesami naprawczymi w systemach informatycznych operatorów telekomunikacyjnych. Zeszyty Naukowe Politechniki Śląskiej, s. Organizacja i Zarządzanie, z. 70, Politechnika Śląska, Gliwice 2014.

3. Zarządzanie problemami zajmuje się wykrywaniem przyczyny powstawania incydentów, a przez to przyczyny powstawania awarii systemu IT. Zarządzanie problemami przez wykrywanie źródeł powstawania awarii zajmuje się ulepszaniem systemów IT.
4. Problem to źródło oraz przyczyna powstawania incydentów i awarii, a incydent to pojedynczy negatywny efekt takiego wystąpienia.



Rys. 1. System wsparcia IT
Fig. 1. IT Support System
Źródło: Opracowanie własne.

Z badań DimensionData[2] wynika, że największą liczbę błędów w procesach utrzymania powodują ludzie, w sumie jest to 32% wśród wszystkich powodów występowania błędów w procesach wsparcia IT. W związku z tym tutaj należy upatrywać największej możliwości ich usprawnienia przez wprowadzenie metod automatyzacji.

Należy tu postawić pytanie: czy można zastąpić decyzję człowieka podejmowaną pomiędzy procesami zarządzania incydentami a zarządzania problemami przez wykorzystanie metod sztucznej inteligencji? Czy sztuczna sieć neuronowa może podejmować decyzje, w wyniku których incydenty mają być poddane dodatkowej analizie w celu usunięcia przyczyny powstawania awarii oraz czy proces ten może być równie efektywny jak wykonywany przez człowieka?

[2] DimensionData. Network Barometer Report 2014. Retrieved from www.dimension data.com; www.dimensiondata.com/Global/Global-Microsites/NetworkBarometer/Documents/assets/PDF/Network_Barometer_Report_2014.pdf.

3. Możliwości wykorzystania sztucznej inteligencji w procesach ulepszania systemów IT

W procesie wsparcia IT możemy zidentyfikować miejsce, gdzie interwencja człowieka jest szczególnie silna; jest to połączenie procesów zarządzania incydentami i problemami, czyli na styku naprawy tymczasowej oraz podejmowania decyzji, czy warto inwestować czas i pieniądze w poszukiwanie i zastosowanie, zwykle kosztownego, rozwiązania docelowego. Zarządzanie problemami polega na analizie wielu incydentów ich powtarzalności, analizie ich trendów oraz ich potencjalnego negatywnego wpływu na systemy IT. Obecnie proces ten jest realizowany przez człowieka i opiera się głównie na zasadzie „3" i „30". Zasadę tą należy interpretować następująco: trzy kolejne wystąpienia danego incydentu dają nam informacje, że należy podjąć dalszą analizę, natomiast jeżeli przez trzydzieści dni trend zachowania się incydentów zostanie utrzymany, należy je dokładniej przeanalizować oraz postarać się znaleźć przyczynę takiego zachowania.

Aby stwierdzić, czy wykorzystanie metod sztucznej inteligencji dla analizy i wnioskowania w procesie zarządzania problemami jest celowe, należy poddać analizie dostępne sygnały, omówione w kolejnych rozdziałach, pochodzące z procesu zarządzania incydentami, oraz przeanalizować ich użyteczność w metodach wnioskowania. Wykorzystanie metod sztucznej inteligencji ma na celu zastąpienie człowieka w procesie decyzyjnym, a przez to wyeliminowanie czynnika ludzkiego z procesu podejmowania decyzji, jako przyczyny dużej liczby błędów w procesie wsparcia IT[3]. Na wyjściu z procesu decyzyjnego wspomaganego metodami sztucznej inteligencji chcemy uzyskać informacje co do kwalifikacji incydentu do dalszej analizy w procesie zarządzania problemami; obecnie decyzja ta jest podejmowana przez człowieka.

4. Sygnały i informacje wejściowe z procesu zarządzania incydentami

Incydent to opis niekorzystnego zdarzenia od początku jego zanotowania do jego rozwiązania. W zależności od systemu obsługi incydentów informacje zbierane na ich temat mogą się różnić. Najczęściej występujące informacje zbierane o incydentach w systemach monitoringu IT zostały przedstawione w tabeli 1.

[3] Ibidem.

Tabela 1

Informacje o incydencie

Nazwa	Opis	Przybierane wartości
Liczba wystąpień alarmu (Alarm_Count)	Liczba wystąpień alarmu	Wartość liczbowa całkowita od 1 zwykle do kilkuset
Kategoryzacja Grupa_1 (Categorization Tier_1)	Pierwszorzędny opis kategorii urządzeń, na których wystąpił incydent	Wartość opisowa np.: urządzenia telekomunikacyjne
Kategoryzacja Grupa_2 (Categorization Tier_2)	Drugorzędny opis kategorii urządzeń, na których wystąpił incydent	Wartość opisowa np.: urządzenia transmisyjne
Kategoryzacja Grupa_3 (Categorization Tier_3)	Trzeciorzędny opis kategorii urządzeń, na których wystąpił incydent	Wartość opisowa np.: urządzenia sterujące
Data i czas wykrycia	Data i czas startu incydentu	Rok, miesiąc, dzień, godzina, minuta i sekunda
Data i czas rozpoczęcia naprawy	Data i czas startu rozpoczęcia naprawy incydentu	Rok, miesiąc, dzień, godzina, minuta i sekunda
Data i czas zakończenia	Data i czas zakończenia incydentu	Rok, miesiąc, dzień, godzina, minuta i sekunda
Wpływ (impact)	Wpływ incydentu na monitorowane rozwiązanie	Zerowy, niski, średni, wysoki, krytyczny
Ważność (urgency)	Ważność incydentu z punktu widzenia czasu	Wartość od 1 do 5
Wyliczony Priorytet	Priorytet, z jakim należy potraktować incydent	Wylicza się go na podstawie *impact* i *urgency*, przyjmuje wartości od 1 do 4
Identyfikator urządzenia	Nazwa urządzenia – tekst	Tekstowy opis lub nazwa urządzenia
Częstotliwość występowania	Liczba wystąpień identycznego incydentu w przeszłości	Wartość liczbowa od 0 zwykle do kilkuset
Root_cause_known	Informacja, czy przyczyna występowania incydentu jest znana, czy też należy ją zidentyfikować	Wartość 1 lub 0 (1 – tak, 0 – nie)
Wpływ na usługi klienckie (Service_Impacting)	Informacja, czy incydent miał negatywny wpływ na usługi świadczone dla klienta	Wartość 1 lub 0 (1 – tak, 0 – nie)
Submitter	Kategoryzacja zgłaszającego incydent	Czy zgłoszenie pochodzi z: Monitoring automatyczny (własny, firm trzecich), użytkownik końcowy
Escalation	Czy incydent był eskalowany?	Wartość 1 lub 0 (1 – tak, 0 – nie)
Escalation level	Na jakim poziomie zakończyła się eskalacja incydentu?	Poziom do którego został wyskalowany incydent w celu rozwiązania: wartości od do 4
Service Impacting	Czy incydent miał negatywny wpływ na usługi dostarczane klientowi końcowemu?	Wartość 1 lub 0 (1 – tak, 0 – nie)
Time in Pending	Czas w sekundach, w którym incydent oczekiwał na interwencje	Ilość sekund, które incydent spędził w stanie Pending

cd. tab. 1

Team Involved (Bouncing)	Liczba transferów incydentu pomiędzy różnymi zespołami w celu rozwiązania	Liczba transferów: wartość od 0 do zwykle kilkudziesięciu
Problem Management	Informacja, czy incydent został zakwalifikowany przez człowieka do dalszej analizy w procesie zarządzania problemami	Wartość 1 lub 0 (1 – tak, 0 – nie)

Źródło: Opracowanie własne.

Powyższe dostępne sygnały należy rozpatrzyć pod kątem wykorzystania ich w analizie za pomocą metod sztucznej inteligencji. Sygnały, które można wykorzystać do analizy za pomocą metod sztucznej inteligencji, muszą być kwantyfikowalne oraz zostać poddane normalizacji[4].

Tabela 2 zawiera podział dostępnych sygnałów i informacji z procesu zarządzania incydentami na dwie grupy:

- kwantyfikowalne, których wartości można ująć ilościowo,
- opisowe (jakościowe), których nie da się bezpośrednio ująć ilościowo.

Tabela 2

Podział sygnałów z procesu zarządzania incydentami

Nazwa	Opis	Kwantyfikowalny/opisowy
Liczba wystąpień alarmu (Alarm_Count)	Ilość wystąpień alarmu	Kwantyfikowalny
Kategoryzacja Grupa_1 (Categorization Tier_1)	Pierwszorzędny opis kategorii urządzeń, na których wystąpił incydent	Opisowy
Kategoryzacja Grupa_2 (Categorization Tier_2)	Drugorzędny opis kategorii urządzeń, na których wystąpił incydent	Opisowy
Kategoryzacja Grupa_3 (Categorization Tier_3)	Trzeciorzędny opis kategorii urządzeń, na których wystąpił incydent	Opisowy
Data i czas wykrycia	Data i czas startu incydentu	Kwantyfikowalny
Data i czas rozpoczęcia naprawy	Data i czas startu rozpoczęcia naprawy incydentu	Kwantyfikowalny
Data i czas zakończenia	Data i czas zakończenia incydentu	Kwantyfikowalny
Wpływ (impact)	Wpływ incydentu na monitorowane rozwiązanie	Kwantyfikowalny
Ważność (urgency)	Ważność incydentu z punktu widzenia czasu	Kwantyfikowalny
Wyliczony priorytet	Priorytet, z jakim należy potraktować incydent	Kwantyfikowalny
Identyfikator urządzenia	Nazwa urządzenia – tekst	Opisowy
Częstotliwość występowania	Liczba wystąpień identycznego incydentu w przeszłości	Kwantyfikowalny

[4] Korbicz J., Obuchowski A., Uciński D.: Sztuczne sieci neuronowe. Podstawy i zastosowania. Akademicka Oficyna Wydawnicza, Warszawa 1994.

cd. tab. 2

Root_cause_known	Informacja, czy przyczyna występowania incydentu jest znana, czy też należy ją zidentyfikować	Kwantyfikowalny
Wpływ na usługi klienckie (Service_Impacting)	Informacja, czy incydent miał negatywny wpływ na usługi świadczone dla klienta	Kwantyfikowalny
Submitter	Kategoryzacja zgłaszającego incydent	Kwantyfikowalny
Escalation	Czy incydent był eskalowany?	Kwantyfikowalny
Escalation level	Na jakim poziomie zakończyła się eskalacja incydentu?	Kwantyfikowalny
Service Impacting	Czy incydent miał negatywny wpływ na usługi dostarczane klientowi końcowemu?	Kwantyfikowalny
Time in Pending	Czas w sekundach, w którym incydent oczekiwał na interwencje	Kwantyfikowalny
Team Involved (Bouncing)	Liczba transferów incydentu pomiędzy różnymi zespołami w celu rozwiązania	Kwantyfikowalny
Problem Management	Informacja, czy incydent został zakwalifikowany przez człowieka do dalszej analizy w procesie zarządzania problemami	Kwantyfikowalny

Źródło: Opracowanie własne.

Z danych zawartych w tabeli 2 wynika, że większość sygnałów, które są dostępne z procesu zarządzania incydentami, ma wartości kwantyfikowalne, co skłania do wykorzystania w ich analizie metod sztucznej inteligencji opierających się na sygnałach kwantyfikowalnych, nie na rozmytych[5]. Jedną z metod sztucznej inteligencji, która może zostać wykorzystana w tym przypadku, jest metoda sztucznych sieci neuronowych, wykorzystującą sygnały dostępne w procesie zarządzania incydentami.

5. Przykłady zbiorów danych

System monitoringu IT dostaje w sposób ciągły informacje o awariach. Informacje te są przetwarzane i zamieniane w opis incydentu zawierający dane jak w przykładzie w tabeli 3. Sieć neuronowa zostanie użyta do ciągłej analizy informacji o przychodzących incydentach z monitoringu systemów IT. Na podstawie wybranych sygnałów z procesu zarządzania incydentami sieć neuronowa będzie podejmować decyzję, czy dany incydent należy zakwalifikować do dalszej analizy w celu znalezienia przyczyn powstawania danej awarii oraz wypracowania rozwiązania docelowego usuwającego przyczyny, a nie skutki.

[5] Żurada J., Barski M., Jędruch W.: Sztuczne sieci neuronowe. PWN, Warszawa 1996.

Dane w tabeli 3 zawierają informacje, które będą poddawane analizie przez sieć neuronową (wszystkie wiersze z wyjątkiem „Problem Management"), oraz informacje kontrolne, które zostaną wykorzystane w procesie uczenia sieci neuronowej oraz weryfikacji wyników jej działania (wszystkie wiersze, wiersz „Problem Management" stanowi informację kontrolną porównującą działanie sieci neuronowej z działaniem człowieka).

Tabela 3

Przykład informacji o incydentach

Nazwa	INC0001	INC0002	INC0003	INC0004
Liczba wystąpień alarmu	2	3	17	1
Kategoryzacja Grupa_1 (Categorization Tier_1)	1	1	1	1
Kategoryzacja Grupa_2 (Categorization Tier_2)	0	1	0	0
Kategoryzacja Grupa_3 (Categorization Tier_3)	0	0	1	0
Data i czas wykrycia	2013-04-30 20:41	2013-05-01 11:11	2013-05-01 13:21	2013-05-01 21:23
Data i czas rozpoczęcia naprawy	2013-04-30 20:43	2013-05-01 11:14	2013-05-01 13:22	2013-05-01 21:45
Data i czas zakończenia	2013-04-30 23:11	2013-05-01 12:01	2013-05-01 13:59	2013-05-02 14:47
Wpływ (impact)	3	2	1	3
Ważność (urgency)	3	3	2	4
Wyliczony priorytet	3	2	1	3
Identyfikator urządzenia	ahdpcr01	kollamc7s02	chnarhcis01	kollamc7s02
Częstotliwość występowania	1	1	1	5
Root_cause_known	1	0	0	0
Wpływ na usługi klienckie	1	1	1	0
Submitter	Customer	Monitoring	Monitoring	Monitoring
Escalation	0	0	1	0
Escalation level	0	0	1	0
Time in Pending	0	0	0	1800
Team Involved (Bouncing)	1	1	6	1
Problem Management	0	1	1	0

Źródło: Opracowanie własne.

Aby poprawnie wykorzystać dane zebrane w procesie zarządzania incydentami oraz użyć ich w analizie sieci neuronowych, należy poddać je normalizacji[6], aby zakres zmienności wszystkich sygnałów na wejściu sieci neuronowej był taki sam i zawierał się w przedziale od 0 do 1.

[6] Ibidem.

Tabela 4

Przykład znormalizowanych informacji o incydentach

Nazwa	INC0001	INC0002	INC0003	INC0004
Liczba wystąpień alarmu	0,1	0,15	0,85	0,05
Kategoryzacja Grupa_1 (Categorization Tier_1)	1	1	1	1
Kategoryzacja Grupa_2 (Categorization Tier_2)	0	1	0	0
Kategoryzacja Grupa_3 (Categorization Tier_3)	0	0	1	0
Data i czas wykrycia	0,631635465	0,631644684	0,631646069	0,631651178
Data i czas rozpoczęcia naprawy	0,631635487	0,631644721	0,631646078	0,631651402
Data i czas zakończenia	0,631637058	0,631645213	0,631646466	0,631662237
Wpływ (impact)	0,5	0,333333333	0,166666667	0,5
Ważność (urgency)	0,5	0,5	0,333333333	0,666666667
Wyliczony priorytet	0,5	0,333333333	0,166666667	0,5
Częstotliwość występowania	0,01	0,01	0,01	0,05
Root_cause_known	1	0	0	0
Wpływ na usługi klienckie	1	1	1	0
Submitter	0	1	1	1
Escalation	0	0	1	0
Escalation level	0	0	1	0
Time in Pending	0	0	0	0,020833333
Team Involved (Bouncing)	0,05	0,05	0,3	0,05
Problem Management	0	1	1	0

Źródło: Opracowanie własne.

Oczekiwanym działaniem sieci neuronowej jest wskazanie, które z analizowanych incydentów mają być poddane dalszej analizie inżynierskiej w procesie zarządzania problemami w celu wykrycia przyczyn powstawania awarii oraz wypracowania rozwiązania docelowego.

6. Zastosowania w praktyce

Podejmowany temat zastosowania sieci neuronowych w celu podejmowania decyzji w procesie wsparcia IT jest umiejscowiony w powszechnie rozumianej automatyzacji procesów i narzędzi. Przy odniesieniu się do rys. 1 praktyka tematu pokazuje, że następujące metody automatyzacji są stosowane w różnych obszarach procesów wsparcia omawianych w niniejszym artykule:

1. zbieranie zdarzeń z systemów IT:
   - filtracja niepotrzebnych zdarzeń na podstawie głównie ich pozytywnej lub negatywnej selekcji („whitelist" lub „blacklist"),
   - korelacja zdarzeń pomiędzy systemami monitoringu, np. ukrycie awarii aplikacji i podanie jako przyczyny awarii serwera, na którym działa dany system,

- korelacja pod kątem czasowego występowania zdarzeń, np. 10 kolejnych błędów urządzenia występujących w ciągu określonego odcinka czasu,
- korelacja zdarzeń pod kątem symulacji topologii systemów IT, np. awaria typu Single Point of Failure;

2. zarządzanie incydentami:
   - wzbogacanie informacji w incydentach na podstawie danych z innych systemów, np. CRM/ERP,
   - wykonywanie automatycznych akcji naprawczych w ograniczonym zakresie;
3. zarządzanie problemami:
   - analiza ilościowa incydentów oraz zdarzeń występujących w systemach IT,
   - analiza trendów incydentów w systemach IT,
   - analiza jakościowa dotycząca grup incydentów.

Zastosowanie sieci neuronowych w podejmowaniu decyzji o kwalifikacji incydentu do dalszej analizy w procesie zarządzania problemami powinno dać kilka z poniższych korzyści:

1. eliminację najsłabszego ogniwa – człowieka – w procesie wsparcia IT[7],
2. zwiększenie wydajności systemu analizy w procesie zarządzania problemami; obecnie większość analizy jest robiona w sposób ręczny lub przy wykorzystaniu podstawowych narzędzi, takich jak arkusz kalkulacyjny,
3. ujednolicenie podejmowanych decyzji przez wprowadzenie automatyzacji,
4. szybkość w podejmowaniu decyzji: obecnie część decyzji jest podejmowana na podstawie 30-dniowych trendów, które wymagają miesięcznych danych historycznych, żeby móc podjąć skuteczną decyzję,
5. obniżkę kosztów przez wprowadzenie automatyzacji w podejmowaniu decyzji oraz częściowe lub całkowite wyeliminowanie człowieka z procesu.

7. Wnioski oraz potencjalne problemy badawcze

Przeprowadzone w niniejszym artykule rozważania mogą prowadzić do stwierdzenia, że istnieją przesłanki do zastosowania sieci neuronowych do analizy sygnałów przychodzących z procesu zarządzania incydentami oraz że mogą one zostać wykorzystane do wsparcia decyzji człowieka w procesie zarządzania problemami. Aby jednak uzyskać poziom pewności co do takich możliwych zastosowań sieci neuronowych, należy ukierunkować badania na[8]:

[7] DimensionData..., op.cit.
[8] Tadeusiewicz R.: Sieci neuronowe. Akademicka Oficyna Wydawnicza, Warszawa 1993.

1. analizę sygnałów pochodzących z procesu zarządzania incydentami. Problem ten należy podzielić na następujące główne obszary badawcze, które dotyczą:
   - liczby sygnałów, które należy zanalizować, aby uzyskać wystarczająco dokładną odpowiedź sieci neuronowej. W tym obszarze badania skupią się na wyborze minimalnej liczby sygnałów oraz odniesieniu tego do jakości uzyskiwanych wyników,
   - jakości sygnałów. Obszar jakości sygnałów jest ściśle powiązany z obszarem ich liczby na wejściu, jednakże analizuje, które sygnały mają istotniejszy wpływ na jakość działania sieci neuronowej, a które sygnały wejściowe mają pomijalny wpływ na wynik analizy. Połączenie tych dwóch obszarów powinno wskazać optymalny dobór liczby oraz jakości sygnałów do analizy;
2. budowę oraz strukturę sieci neuronowej – w tym obszarze należy poddać analizie budowę i strukturę sieci neuronowej[9]:
   - liczba wejść w sieci neuronowej; ten obszar jest ściśle uwarunkowany liczbą oraz analizą dostępnych sygnałów z procesu zarządzania incydentami,
   - liczba wyjść z sieci neuronowej – w obecnej chwili należy się skłaniać ku tezie, że sieć neuronowa zastosowana w tym przypadku powinna mieć jedno wyjście pokazujące, czy dany incydent należy skierować do procesu zarządzania problemami, czy też nie, jednakże nie należy wykluczyć innych potencjalnych sygnałów wyjściowych, np. priorytet, ważność itp.,
   - złożoność wewnętrzną sieci neuronowej, czyli ilość warstw ukrytych oraz ilość neuronów w tych warstwach. Wynik tych analiz będą podyktowane głównie skutecznością uczenia się sieci neuronowej, które będzie się ocenić przy pomocy bieżącej analizy funkcji oraz wyników na podstawie próby kontrolnej,
   - wybór sieci neuronowej: z sprzężeniem zwrotnym oraz bez sprzężenia zwrotnego,
   - parametry funkcji zastosowanych w neuronach;
3. proces uczenia oraz weryfikacji wyników, w którym należy ustalić zestaw danych treningowych w celu uzyskania optymalnego procesu uczenia, a także odpowiedzieć na pytanie, w jaki sposób porównać osiągane wyniki z procesem decyzyjnym podejmowanym przez człowieka.

[9] Ibidem.

Bibliografia

1. DimensionData. Network Barometer Report 2014. Retrieved from www.dimension data.com; www.dimensiondata.com/Global/Global-Microsites/NetworkBarometer/ Documents/ assets/PDF/Network_Barometer_Report_2014.pdf.
2. Gościniak T.: Zarządzanie procesami naprawczymi w systemach informatycznych operatorów telekomunikacyjnych. Zeszyty Naukowe Politechniki Śląskiej, s. Organizacja i Zarządzanie, z. 70, Politechnika Śląska, Gliwice 2014.
3. Korbicz J., Obuchowski A., Uciński D.: Sztuczne sieci neuronowe. Podstawy i zastosowania. Akademicka Oficyna Wydawnicza, Warszawa 1994.
4. OGC. ITIL Service Operations. TSO, London 2007.
5. Tadeusiewicz R.: Sieci neuronowe. Akademicka Oficyna Wydawnicza, Warszawa 1993.
6. Żurada J., Barski M., Jędruch W.: Sztuczne sieci neuronowe. PWN, Warszawa 1996.

Abstract

Publication is presenting analysis of available signals from incident management process. According to research humans are the weakest link in IT support process thus giving a huge potential of improvements when replaces by computer aided decision process. This article is describing potential use of available signals as an input to neural networks aided decision process. Summary section is outlining potential further research areas.