[12] Lin Y.Y. i inni: *Path Selection in Streaming Video Over Multioverlay Application Layer Multicast*, IEEE Transactions on Circuits and Systems for Video Technology, vol. 20, no. 7, lipiec 2010
[13] Ni J. i inni: *Efficient and Dynamic Routing Topology Inference from End-to-End Measurements*, IEEE/ACM Transactions on Networking, vol. 18, no. 1, luty 2010
[14] Park K. i inni, *An Adaptive Peer-to-Peer Live Streaming System with Incentives for Resilience*, Elsevier Computer Networks, vol. 54, no. 8, czerwiec 2010,
[15] Cleju N. i inni: *Network Coding Node Placement for Delay Minimization in Streaming Overlays*, Proc. IEEE International Conference on Communications ICC, Kapsztad, RPA, maj 2010
[16] Chen Y. i inni: *Cooperative Peer-to-Peer Streaming: An Evolutionary Game-Theoretic Approach*, IEEE Transactions on Circuits and Systems for Video Technology, vol. 20, no. 10, październik 2010
[17] Huang F. i inni: *NAP: An Agent-Based Scheme on Reducing Churn-Induced Delays for P2P Live Streaming*, Proc. 10th IEEE International Conference on Peer-to-Peer Computing P2P, Delft, Holandia, sierpień 2010
[18] Xu K. i inni: *Proxy Caching for Peer-to-Peer Live Streaming*, Computer Networks, vol. 54, no. 7, maj 2010
[19] Smooth IT: *Simple Economic Management Approaches of Overlay Traffic in Heterogeneous Internet Topologies*, [Online] http://www.ict-smoothit.eu/

Artykuł recenzowany

(*Artykuł nadesłano do red. – luty 2011*)

Przemysław KUKIEŁKA, Zbigniew KOTULSKI***

Systemy wykrywania intruzów wykorzystujące metody sztucznej inteligencji

W ostatnich latach coraz więcej różnorodnych instytucji, przy prowadzeniu działalności, korzysta z sieci Internet. Powstają sklepy internetowe, większość firm udostępnia swoją ofertę lub informacje o rodzaju prowadzonej działalności na stronach WWW. Również coraz więcej osób korzysta z dobrodziejstw bankowości elektronicznej. W Internecie pojawiają się też nowe usługi, takie jak: telefonia **VoIP**, komunikatory internetowe, gry sieciowe albo usługi audio/wideo: radio internetowe, **IPTV**, **WEBTV**. Dodatkowo wiele instytucji ma oddziały na całym świecie, które wymieniają informacje pomiędzy sobą z wykorzystaniem ogólnodostępnej sieci Internet.

Niestety, rozwój Internetu wiąże się również ze zwiększoną liczbą przypadków naruszenia bezpieczeństwa systemów informatycznych. Dlatego bardzo ważną rolę odgrywa obecnie ich zabezpieczenie przed tego typu niepożądanymi działaniami. W celu ochrony systemów informatycznych pracujących w sieci lokalnej danej instytucji przed niepowołanym dostępem oraz działaniami mającymi na celu ograniczenie ich dostępności oraz niezawodności wykorzystuje się urządzenia lub oprogramowanie, pełniące rolę zapory sieciowej (*firewall*). Niestety, zapory sieciowe nie są w stanie wykryć i przeciwdziałać wszystkim atakom, ponieważ w stopniu bardzo ograniczonym sprawdzają treść przenoszoną przez pakiety IP. Z tego też powodu na przykład próby zainstalowania złośliwego oprogramowania typu robaki i konie trojańskie nie będą przez nie na ogół zauważone. Dlatego jest konieczne uzupełnienie zabezpieczeń o system wykrywania włamań **IDS** (*Intrusion Detection System*) umieszczony zazwyczaj jako druga linia obrony za systemem zapory sieciowej. Systemy IDS są użyteczne nie tylko do wykrywania ataków zakończonych sukcesem, ale również do monitorowania i rejestrowania prób złamania zabezpieczeń systemu informatycznego.

* **Instytut Telekomunikacji, Politechnika Warszawska, e-mail: Przemyslaw.Kukielka@telekomunikacja.pl**
** **Instytut Podstawowych Problemów Techniki Polskiej Akademii Nauk, e-mail: zkotulsk@ippt.gov.pl**

SYSTEMY IDS

Systemy wykrywania intruzów IDS można zdefiniować jako jeden z mechanizmów nadzorowania bezpieczeństwa, polegający na monitorowaniu i wykrywaniu ataków skierowanych przeciwko systemom informatycznym. Mają one za zadanie wykrywać ataki, polegające na przykład na nieautoryzowanym dostępie do zasobów, próbie zablokowania systemu komputerowego, próbie zainstalowania złośliwego oprogramowania typu robaki czy konie trojańskie. Istnieją dwa podstawowe sposoby podziału systemów IDS.

Podział systemów IDS ze względu na wykorzystywane techniki analizy

Systemy wykrywania nadużyć (*misuse*) **–** są wykorzystywane do wykrywania znanych ataków przy użyciu określonych, specyficznych dla nich cech-sygnatur.

Systemy wykrywania anomalii (*anomaly*) **–** których idea działania polega na monitorowaniu normalnej pracy systemu, w celu znalezienia anomalii, które mogą świadczyć o działaniu intruza. System IDS opierający się na wykorzystywaniu anomalii jest bardziej skuteczny od systemu wykrywania nadużyć przy stosowaniu nieznanych, nowych typów ataków.

Podział systemów IDS ze względu na źródła wykorzystywanych informacji

Lokalne systemy IDS – HIDS (*Host based IDS*) **–** systemy tego typu biorą pod uwagę informacje, jakie można pobrać bezpośrednio z chronionego hosta. Mogą to być na przykład logi systemowe, logi aplikacji korzystających z sieci IP lub informacje zawarte w plikach audytu systemu operacyjnego.

Sieciowy system IDS – NIDS (*Network Based IDS*) **–** analizuje on informacje w sieci, które przepływają pomiędzy hostami

połączonymi za pomocą różnych mediów i z wykorzystaniem różnych protokołów transmisji. Korzysta najczęściej ze zbioru sensorów, rozmieszczonych w różnych punktach sieci, które – oprócz zbierania danych – mogą przeprowadzać ich wstępne przetworzenie, a nawet lokalną analizę pod względem wykrycia ataków i przesyłają w takim przypadku raporty o podejrzanych zdarzeniach do centralnego systemu.

Jako początek rozwoju dziedziny nauki związanej z systemami IDS uważa się pracę Jamesa P. Andersona [3], który w roku 1980 zaproponował wykorzystanie informacji zawartych w plikach audytu do śledzenia zachowań użytkowników i wykrywania podejrzanych aktywności. Były to między innymi: informacje o przebiegu procesu logowania użytkowników, dostępie do plików systemowych i operacjach na nich wykonywanych, czynnościach wykonywanych przez użytkowników, wykorzystaniu czasu pracy procesora i operacjach wejścia/wyjścia. Do analizy danych zostały zaimplementowane mechanizmy statystyczne, wykorzystujące rozkład prawdopodobieństwa określonego parametru pobranego z rekordów audytu. W przypadku, gdy przyjęta wartość graniczna odchylenia od wartości średniej monitorowanego parametru zostanie przekroczona, fakt ten sygnalizuje podejrzane zachowanie użytkownika.

Początkowo systemy IDS do wykrywania włamań wykorzystywały zestawy reguł (systemy eksperckie), modele i analizę stanów. Tego typu systemy zostały określone w dalszej części pracy jako tradycyjne systemy IDS. Bardziej szczegółowe informacje na temat tradycyjnych systemów IDS można znaleźć w [21]. Niestety, wykorzystywane przez nie metody analizy mają pewne wady, szerzej omówione w dalszej części artykułu.

Własności systemów wykrywania nadużyć

Stworzenie odpowiedniego zestawu sygnatur do wykrywania ataków jest procesem skomplikowanym i wymaga dużej wiedzy eksperckiej.

W przypadku tworzenia sygnatur, opierających się na progach oddzielających normalny ruch i atak (np. ponad 10 000 połączeń pochodzących od tego samego adresu IP skierowanych do usługi **SMTP** – *Simple Mail Transfer Protocol* – w krótkim odstępie czasu może oznaczać atak – *mailbomb*), jest wymagane właściwe określenie wartości tych progów, zapewniające możliwie dużą dokładność wykrywania ataków przy małej liczbie fałszywych alarmów. Często nie jest to prosta sprawa i wymaga analizy ruchu przeprowadzonej dla konkretnej sieci, która ma być chroniona.

- Agresor, który pozna, jakie cechy ataków były brane pod uwagę podczas tworzenia sygnatury, może tak zmodyfikować swój atak, aby nie został rozpoznany przez system IDS.
- Systemy tego typu nie zapewniają wykrywania nowych ataków, których sygnatury nie zostały jeszcze w nich zaimplementowane.
- Sygnatury dla nowych typów ataków pojawiają się dopiero po pewnym czasie, potrzebnym do dokładnej analizy scenariusza ataku. W tym czasie hosty nie są przed nimi chronione.
- Bazy sygnatur wymagają ciągłych aktualizacji, a jeżeli administrator ich nie przeprowadza, systemy stają się mniej skuteczne i dodatkowo stwarzają niebezpieczeństwo mylącej pewności, że system jest dobrze chroniony.

Własności systemów wykrywania anomalii

- Trudności, związane ze zbudowaniem profilu, obejmującego wszystkie normalne zachowania użytkownika, chociażby ze względu na to, że zbiór tych zachowań jest znacznie większy od zbioru sygnatur związanych z atakami.
- System IDS, pracujący na zasadzie wykrywania anomalii, może generować znacznie większą liczbę fałszywych alarmów, ze względu na częste zmiany przyzwyczajeń lub zachowań użytkowników. Może to być na przykład próba użycia nowej usługi internetowej lub zainstalowanie nowego rodzaju oprogramowania korzystającego z sieci IP.
- Tego typu systemy wymagają dużej mocy obliczeniowej, ponieważ muszą analizować wiele różnorodnych profili i ponadto utrzymywać historie działalności użytkownika.
- Właściwy wybór wartości progu zgłaszania anomalii, tak żeby zachować równowagę pomiędzy poziomami błędów związanych z fałszywymi alarmami i niewykrytymi atakami, nie jest procesem łatwym.
- Wybór cech, które powinny podlegać monitorowaniu tak, żeby z dużą dokładnością wykrywać anomalie, również nie jest procesem łatwym. Ponadto nie ma uniwersalnego zbioru cech, który umożliwiłby wykrywanie wszystkich ataków. Jedne są bardziej istotne dla wykrywania określonego typu ataku, zaś inne do innego. Dodatkowo należy wziąć pod uwagę, że im większy zbiór cech, tym wymagana jest większa moc obliczeniowa systemu.
- W przypadku systemów IDS, wykorzystujących metody statystyczne, intruz może stopniowo – przez określone zachowania – tak modyfikować swój profil, że po pewnym czasie aktywność związana z atakiem będzie uznawana przez system jako normalny ruch.

Część przedstawionych powyżej ograniczeń dotyczących tradycyjnych systemów IDS może zostać wyeliminowana, dzięki zastosowaniu metod sztucznej inteligencji.

SZTUCZNA INTELIGENCJA

Sztuczna inteligencja AI (*Artificial Intelligence)* zgodnie z definicją R.J. Schalkoffa – obejmuje rozwiązywanie problemów sposobami wzorowanymi na naturalnych działaniach i procesach poznawczych człowieka za pomocą symulujących je programów komputerowych. W jej skład wchodzi wiele różnych metod, takich jak na przykład: sieci neuronowe, algorytmy genetyczne, metody grupowania danych, drzewa decyzyjne lub systemy immunologiczne. Szersze omówienie zasad działania poszczególnych metod zostało przedstawione między innymi w [35], [39].

Główną zaletą omawianych metod sztucznej inteligencji jest zdolność generalizacji, czyli klasyfikacji nie tylko danych prezentowanych podczas nauki, ale również wszelkich do nich podobnych. Dzięki tej własności metody te mogą pomóc w wyeliminowaniu ograniczenia tradycyjnych systemów IDS, związanego z trudnością w wykrywaniu nowych typów ataków (systemy wykrywania nadużyć) oraz z właściwą klasyfikacją nowego rodzaju ruchu, związanego z normalną aktywnością użytkowników (systemy oparte na anomaliach).

Metody sztucznej inteligencji w zadaniach związanych z klasyfikacją nie wymagają opisania zestawu reguł, na podstawie których zostanie podjęta decyzja o przypisaniu zebranych danych do określonej klasy. Reguły te są tworzone automatycznie w procesie nauki wykorzystywanej metody. Dzięki temu zastosowanie sztucznej inteligencji w systemach IDS rozwiązuje problemy tradycyjnych systemów związane z potrzebą budowy sygnatur do wykrywania określonych typów ataków oraz modeli charakteryzujących normalne zachowania użytkowników.

Inne zalety systemów sztucznej inteligencji, istotne z punktu widzenia systemów IDS, to możliwość szybkiej analizy dużych porcji danych pochodzących z wielu źródeł oraz prawidłowa klasyfikacja analizowanych danych nawet w przypadku braku kompletnej informacji wymaganej w tradycyjnych systemach IDS.

ZASTOSOWANIE SZTUCZNEJ INTELIGENCJI W SYSTEMACH IDS

Systemy IDS, wykorzystujące sztuczną inteligencję, mogą pracować, podobnie jak te tradycyjne, w trybie wykrywania anomalii lub nadużyć. W przypadku gdy dane wejściowe przeznaczone do nauki zawierają tylko zdarzenia związane z normalnym ruchem, system tego typu jest systemem wykrywającym anomalie od nauczonych wzorców. Taki system został przedstawiony na przykład w [27]. Wykorzystywana w nim sieć neuronowa **SOM** (*Self Organizing Map*) przypisuje analizowane dane do klas zdefiniowanych w procesie nauki. W przypadku gdy zdarzenie jest zlokalizowane daleko w wielowymiarowej przestrzeni analizy od każdej z klas może być uznane za anomalię. Zaletą zastosowania systemu uczącego się tylko normalnego ruchu jest możliwość wykrywania ataków bez potrzeby pozyskiwania i dodawania do procesu nauki wektorów reprezentujących te ataki. Ponieważ monitorowane zachowania użytkownika często się zmieniają, podobnie jak dla tradycyjnych systemów IDS, może to powodować dużą liczbę fałszywych alarmów. W takim przypadku nie ma jednak potrzeby, jak dla tradycyjnych systemów IDS, budowania nowych skomplikowanych profili zachowań. Wystarczy natomiast nauczyć sieć ponownie, z wykorzystaniem nowego rodzaju ruchu dodanego do zbioru uczącego.

W przypadku gdy do danych wejściowych, wykorzystywanych do nauki sieci neuronowej i reprezentujących normalny ruch, doda się również wzorce ataków, taki system można uznać za pracujący na zasadzie wykrywania nadużyć. Jednak – w odróżnieniu od tradycyjnych systemów IDS – ma on dużą zdolność generalizacji, więc może wykrywać również ataki, które są tylko podobne do nauczonych wzorców. Dodatkowo system wykorzystuje do nauki normalny ruch, więc w pewnym sensie pracuje również na zasadzie wykrywania anomalii. Do systemów wykrywających nadużycia należą między innymi opisane w [30], [31].

Systemy wykorzystujące metody sztucznej inteligencji, podobnie jak tradycyjne systemy IDS, mogą używać dwu źródeł danych poddanych analizie. System sieciowy (NIDS), korzystający z informacji pobranych z nagłówków pakietów IP przepływających w analizowanej sieci, został zaprezentowany przez Cannady w [5]. Dane do nauki i testowania zebrano za pomocą monitora *Real Secure*, ataki były symulowane z wykorzystaniem narzędzia *Internet Scanner*. Wiele prac związanych z systemami sieciowymi wykorzystywało gotowe dane, dostarczone przez projekt zrealizowany przez agencję **DARPA** (*Defense Advanced Research Projects Agency*), a następnie przetworzone w roku 1999 w ramach projektu **KDD** (*Knowledge Discovery and Data Mining Competition*) na wektory reprezentujące poszczególne połączenia, tworzące zbiór około 5 milionów rekordów. Połączenie jest rozumiane jako sekwencja pakietów, rozpoczynająca się i kończąca w zdefiniowanym czasie, podczas którego dane przepływają pomiędzy adresem źródłowym i docelowym przy wykorzystaniu określonego protokołu. Każde połączenie jest opisane za pomocą 41 cech. Dane KDD zawierają symulacje normalnego ruchu oraz ataków należących do czterech grup: **DoS** (*Denial of Service*), **U2R** (*User to Root*), **R2L** (*Remote to Local*) i ataki rozpoznawcze (*probe*). Szczegółowe informacje na temat obu projektów można znaleźć miedzy innymi w [18], [29], [24].

Identycznie jak w przypadku tradycyjnych systemów IDS dla systemów HIDS źródłem danych poddawanych analizie są informacje pobrane bezpośrednio z chronionego hosta. Przykładowo mogą to być komendy wydawane przez użytkownika w czasie korzystania z systemu informatycznego. Tego rodzaju system IDS, wykorzystujący rekurencyjną sieć neuronową, został opisany w 1992 r. przez Debar w pracy [11]. Wchodząca w jego skład sieć neuronowa uczy się przewidywania następnej komendy na podstawie sekwencji komend wydanych przez użytkownika w przeszłości. Przewidziana komenda jest porównywana z aktualnie wydaną i wszelkie odchyłki są uznawane za atak. Istotną kwestią w tej technice jest wielkość okna zawierającego ostatnio wydane komendy. Zbyt krótkie okno generuje fałszywe alarmy, zbyt długie może sprawiać problemy z wykryciem niektórych ataków.

W literaturze można znaleźć wyniki badań nad zastosowaniem wielu różnych metod sztucznej inteligencji do wykrywania włamań. Próby wykorzystania systemów immunologicznych przedstawiono w [13], [19]. W pracy [41] zawarto analizę efektywności zastosowania w IDS, opartym na systemach immunologicznych, różnych metod generowania przeciwciał oraz kodowania danych pobranych z sieci IP. W pracy [32] przedstawiono wykorzystanie systemu **MARS** (*Multivariate Adaptive Regression Splines)* do wykrywania intruzów. Zastosowanie programowania genetycznego o liniowym genomie **LGP** zaproponowano w [34]. Oba wymienione systemy jako wektory wejściowe wykorzystywały zbiór danych KDD. Proces testowania został przeprowadzony nie dla całego zbioru danych testowych, ale dla wybranych 6890 połączeń. Zarówno MARS, jak też LGP, w wyniku przeprowadzonych badań okazały się skutecznymi metodami do wykrywania ataków z każdej z czterech klas oraz do klasyfikacji normalnego ruchu.

Zastosowanie algorytmów genetycznych w IDS przedstawiono w [25]. Jako dane wejściowe wykorzystano wektory złożone z podstawowych informacji zawartych w nagłówkach pakietów (np. port i adres IP). Zadaniem algorytmu była nie samodzielna klasyfikacja, ale wygenerowanie zbioru reguł, które w przyszłości będą wykorzystywane do wykrywania ataków. Wadą rozwiązania, związaną ze sposobem doboru cech wektora wejściowego, jest problem klasyfikacji złożonych ataków, które składają się z wielu połączeń rozłożonych w czasie.

Również sieci Bayesa znalazły zastosowanie przy wykrywaniu intruzów. Praca [37] przedstawia system wykorzystujący tę metodę do analizy logów audytu. W publikacji [7] sieć Bayesa została wykorzystana do analizy danych z projektu KDD. Oprócz grupy ataków R2L, w której dokładność klasyfikacji była na poziomie 60%, pozostałe grupy ataków oraz normalny ruch dla pełnego wektora KDD zawierającego 41 cech zostały rozpoznane z ponad 99% skutecznością. Testy przeprowadzono nie dla całego zbioru testowego, ale dla wybranego losowo podzbioru liczącego 6890 wektorów.

Szeroko stosowano w systemach IDS metody wykorzystujące drzewa decyzyjne [2], [20], [26]. W większości przypadków wykorzystywano algorytm C4.5 do tworzenia drzewa. Systemy tego typu wykazywały dużą skuteczność, ale ich wadą jest problem dostosowania do nowej sytuacji, gdy pojawiają się nowe ataki lub nowy rodzaj normalnego ruchu. W takim przypadku drzewo decyzyjne musi być tworzone lub modyfikowane. Lepiej z takimi sytuacjami radzą sobie sieci neuronowe, które wystarczy wtedy nauczyć ponownie, z wykorzystaniem nowego zbioru danych [44].

Zastosowanie systemu hybrydowego złożonego z algorytmu genetycznego oraz drzewa decyzyjnego przedstawiono w pracy [43]. Rolą algorytmu genetycznego był wybór najważniejszych cech wektora KDD, natomiast drzewo decyzyjne pełniło rolę klasyfikatora. Jak pokazały wyniki badań, zastosowanie wcześniejszej selekcji najważniejszych cech poprawiło dokładność klasyfikacji. Zarówno drzewa decyzyjne, jak też system hybrydowy, miały największy problem z wykrywaniem ataków z grupy R2L (tylko 81% sklasyfikowano poprawnie).

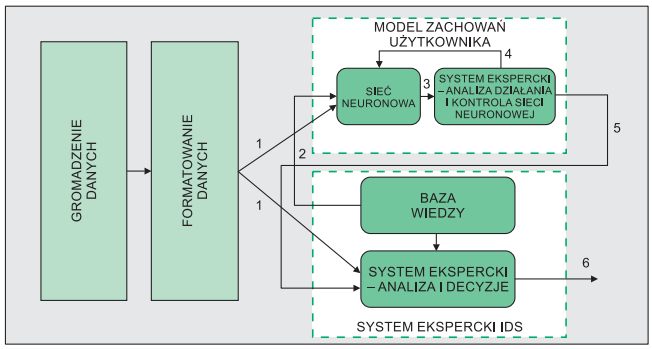
Z metod odkrywania wiedzy (*data mining*) korzysta system **ADAM** (*Audit Data Analysis and Mining*) przedstawiony w [10]. Kombinacja reguł oraz algorytmów klasyfikacji służy do wykrywania ataków na podstawie analizy danych w formacie *tcpdump*. System w fazie nauki tworzy bazę wiedzy, zawierającą wzorce

znanych ataków. Następnie, z wykorzystaniem algorytmu czasu rzeczywistego, ostatnie połączenia są porównywane z bazą wiedzy i wyłaniane są jedynie połączenia reprezentujące podejrzany ruch. Równocześnie uczony jest też moduł klasyfikatora. W fazie detekcji klasyfikator analizuje podejrzane dane, w celu zaliczenia ich do trzech klas: normalny ruch, atak oraz nieznany ruch (w przypadku ataku, którego system nie jest w stanie prawidłowo zaklasyfikować).

Jedną z metod sztucznej inteligencji najczęściej stosowanych do wykrywania ataków jest użycie sieci neuronowych. W literaturze przedstawiono dwa podejścia do wykorzystania sieci neuronowych w systemach IDS.

- Sieć neuronowa identyfikuje podejrzane zdarzenia i przekazuje je do systemu eksperckiego do dalszej analizy.
- Sieć neuronowa jest samodzielnym systemem uczącym się sygnatur ataków lub normalnych zachowań użytkowników. Na podstawie przeprowadzonej analizy decyduje o wygenerowaniu alarmu lub podjęciu innej reakcji na wykryty atak. Jest to rozwiązanie znacznie częściej spotykane w literaturze.

Przykład systemu IDS, będącego kombinacją sieci neuronowej i systemu eksperckiego, został opisany przez Debar w [11]. W tym rozwiązaniu system ekspercki ma za zadanie podejmowanie ostatecznej decyzji o wygenerowaniu alarmu na podstawie informacji z sieci neuronowej oraz analizy danych audytu polegającej na porównaniu ich ze znanymi scenariuszami ataków zgromadzonymi w bazie wiedzy. Architekturę tego systemu IDS przedstawiono na rys. 1.



Rys. 1. Schemat blokowy systemu IDS (opracowano według [11])

System składa się z następujących bloków:

- **gromadzenie danych** – blok odpowiedzialny za zbieranie danych audytu,
- **formatowanie danych** – blok przetwarzający zebrane dane audytu do postaci przyswajalnej przez sieć neuronową i system ekspercki,
- **sieć neuronowa** – **blok** odpowiadający za analizę danych audytu; oprócz samej sieci zawiera moduł kodujący do postaci numerycznej i dekodujący dane audytu,
- **system ekspercki: analiza działania i kontrola sieci neuronowej** – moduł analizujący wyjście sieci neuronowej i tłumaczący do postaci najbardziej odpowiedniej do wykrywania intruzów; dodatkowo odpowiada za nadzór procesu nauki,
- **system ekspercki: analiza i decyzje** – korzystający z bazy wiedzy, zawierającej znane scenariusze ataków; moduł generuje alarmy, gdy pojawiają się znaczne odchyłki w zachowaniach przewidzianych przez sieć neuronową lub gdy zostanie wykryty jeden ze scenariuszy ataków.

Zalety podejścia wykorzystującego kombinację sieci neuronowej i systemu eksperckiego w IDS to między innymi zmniejszenie liczby fałszywych alarmów, dzięki adaptacji progów opartych na zdarzeniach dostarczanych przez sieć neuronową. Ponadto do systemu eksperckiego są przekazywane wyłącznie podejrzane zdarzenia, co poprawia znacznie jego wydajność i dokładność klasyfikacji. Wadą tego podejścia jest potrzeba aktualizacji systemu eksperckiego w sytuacji, gdy sieć neuronowa wykryje nowy atak. W przeciwnym przypadku ten alarm zostanie zignorowany.

W przypadku drugiego podejścia, gdy sieć neuronowa działa samodzielnie, między innymi takie architektury sieci neuronowych, jak: **MLP** (*Multi-Layer Perceptron*), **SOM**, **ART** (*Adaptive Resonance Theory*), sieci neuronowe rekurencyjne, radialne **RBF** (*Radial Basis Function*), **SVM** (*Support Vector Machine*), były badane w przeszłości pod względem ich wykorzystania w systemach wykrywania włamań. Poniżej przedstawiono wybrane przykłady tych badań.

Sieci neuronowe rekurencyjne są wykorzystywane w przypadku danych prezentowanych jako szeregi czasowe, w których sygnał wejściowy zależy od odpowiedzi systemu w poprzednich chwilach. W przypadku systemów IDS może to być zbiór komend wydanych przez użytkownika w pewnym przedziale czasu lub zbiór zapytań języka **SQL**. Takie zastosowanie sieci neuronowych rekurencyjnych *Elmana* do analizy zestawu komend użytych w systemie operacyjnym *Unix* zostało opisane w pracy [12]. Badania nad zastosowaniem sieci rekurencyjnych *Jordana* i *Elmana* do wykrywania ataków przeciwko bazom danych wykorzystujących język SQL przedstawiono w [42]. Sieć rekurencyjna Hamminga w zastosowaniu do wykrywania ataków zawartych w zbiorze KDD została opisana w [16].

Wykorzystanie sieci samoorganizujących się SOM *Kohonena* przedstawiono w pracy [38]. Nauczona sieć pokazuje odległość pomiędzy wektorem reprezentującym normalny ruch a wektorem związanym z atakiem. W przypadku gdy przekracza ona pewien próg, zostaje wygenerowany alarm informujący o działaniu intruza. Również w pracy [28] zastosowano sieć neuronową SOM. Składała się ona z dwóch warstw: pierwsza zawierała 6 różnych sieci SOM pracujących oddzielnie dla każdej cechy wektora wejściowego. Mają one za zadanie analizę zmienności każdej z 6 cech dla pewnego przedziału czasowego. Dzięki temu sieć może reagować na wzorce związane z kolejnością występowania połączeń o określonych cechach. Zadaniem drugiej warstwy jest jednoczesna analiza wektora złożonego ze wszystkich 6 cech.

Wyniki testów z zastosowaniem zbioru KDD nie były zadowalające. Dla takiej architektury 15 308 ataków z 250 399 nie zostało wykrytych, dodatkowo przy dużej liczbie 20 588 fałszywych alarmów. Podobne podejście z zastosowaniem hierarchicznej sieci SOM zbudowanej z dwóch warstw zostało opisane w [27]. Pierwsza warstwa jest złożona z trzech odrębnych sieci SOM, odpowiedzialnych za analizę kolejności występowania określonych wartości następujących cech: lokalizacja źródła, z którego nawiązano połączenia, nazwa konta użytkownika oraz typ połączenia.

W celu powiązania tych cech z czasem rozważono dwa podejścia: pierwsze z rejestrem przesuwnym **FIFO**, w którym są tracone odniesienia do pory dnia oraz odstępów czasu pomiędzy kolejnymi zdarzeniami oraz drugie, w którym są wykorzystywane znaczniki czasowe dla każdego zdarzenia. Badania pokazały, że pierwsza metoda lepiej potrafi odseparować od siebie poszczególne grupy użytkowników oraz odnaleźć potencjalne anomalie. Druga warstwa analizuje wyniki z warstwy pierwszej i tworzy na ich podstawie sumaryczny opis profilu użytkownika. Profile należące do różnych typów użytkowników są grupowane w kilka klas, rozmieszczonych w przestrzeni analizy, blisko środka każdej z nich, natomiast aktywność związana z działalnością agresora jest rozpoznawana, ponieważ jest znacznie oddalona od każdej z wyodrębnionych grup. Opisane powyżej przykłady zastosowania sieci neuronowych SOM były wykorzystywane do analizy *off-line* wcześniej zgromadzonych danych. Takie podejście uniemożliwia jednak natychmiastową reakcję na atak,

a jedynie wykrywa fakt jego zaistnienia. Architektura systemu IDS **RT-UNNID** (*Real-Time Unsupervised Neural-Net-based Intrusion Detektor*), działającego w czasie rzeczywistym, została opisana w pracy [1].

Proces nauki sieci neuronowej odbywa się w opisanym poniżej porządku. W pierwszym kroku sieć uczy się i klasyfikuje wektory do określonych grup, opierając się na ich podobieństwie. Po zakończeniu procesu grupowania jest ustalany neuron wyjściowy, reprezentujący każdą z grup. Etykieta dla każdej z nich jest ustalana na podstawie największej liczby wektorów danego typu, zaklasyfikowanych do danej grupy. Na przykład jeżeli ponad 50% wektorów należy do grupy *normal,* to cała grupa jest uznawana jako *normal*. W przypadku gdy wyjściowy neuron nie wskazuje na żadną z grup, powinien być usunięty.

W pracy [1] zawarto również porównanie zastosowania sieci neuronowych ART i SOM jako modułu *UNN Engine* odpowiedzialnego za klasyfikację. Lepsze wyniki uzyskano dla sieci ART, która zapewniła osiągnięcie dokładności wykrywania ataków na poziomie 97%, przy fałszywych alarmach na poziomie 2%. Wyniki, jakie uzyskano dla sieci SOM, to 95% wykrytych ataków przy 3,5% fałszywych alarmów. Sieci ART są również bardziej stabilne, dzięki czemu wektory wejściowe nie oscylują wokół różnych grup oraz umożliwiają naukę nowych wzorców na każdym jej etapie. Dodatkowo przeprowadzono porównanie wydajności obu rodzajów sieci, które pokazało, że sieć ART uczy się szybciej i jest w stanie również szybciej klasyfikować wektory podawane na wejście, niż sieć SOM.

Zaletą zastosowania sieci SOM jest to, że może się ona uczyć bez nauczyciela, więc nie wymaga procesu wstępnego etykietowania wektorów jako normalnego ruchu lub ataku. W przypadku gdy takie etykietowanie jest wymagane (np. dla omówionego wcześniej systemu RT-UNNID), odbywa się ono już po pogrupowaniu danych, co znacznie przyspiesza cały proces. Istnieje jednak także wada zastosowania sieci SOM. Z powodu bowiem całkowitej automatyzacji procesu nauki istnieje zagrożenie, że agresor może nauczyć sieć rozpoznawania ataku jako normalnego ruchu. Można co prawda zastosować dodatkowy system ekspercki, który dobrze rozpozna znane ataki, jednak w przypadku nowych może się on okazać nieskuteczny. Inną wadą sieci SOM jest wpływ liczby neuronów na wydajność sieci. Zwiększenie liczby wyjść sieci zwiększa rozdzielczość klasyfikacji, ale czas potrzebny do analizy znacznie wzrasta.

W pracy [46] przedstawiono rozwiązanie, które zachowując tę samą dokładność wykrywania ataków jak SOM, umożliwia skrócenie czasu potrzebnego do wykonania analizy. Ponadto zwiększenie liczby neuronów wyjściowych, jak pokazały testy, nie wpływa na czas analizy. Proponowany algorytm **ICLN** (*Improved Competitive Learning Network)* zmienia tradycyjny sposób aktualizacji wag neuronów przez zastosowanie dodatkowej funkcji jądra (o argumentach związanych z odległością pomiędzy neuronami), od której zależy wartość aktualizacji wag. Dla zbioru KDD ograniczonego tylko do 7 ataków oraz normalnego ruchu uzyskano dokładność klasyfikacji na poziomie 98%.

Duża liczba publikacji zawiera również wyniki prac nad wykorzystaniem sieci MLP do wykrywania intruzów. W badaniach przedstawionych przez Cannady w [5] została wykorzystana sieć neuronowa MLP o 4 warstwach, signoidalnej funkcji aktywacji, 9 wejściach i dwóch wyjściach reprezentujących atak „1", „0" lub normalny ruch „0", „1". Badania wykazały wysoką skuteczność w wykrywaniu prezentowanych trzech typów ataków.

Wykorzystywana sieć neuronowa miała jednak zbyt złożoną architekturę, stąd długi czas nauki i testowania.

W pracy [30] Mahdi Moradi i Mohammad Zulkemine przedstawili również koncepcję zastosowania sieci neuronowej MLP jako klasyfikatora do wykrywania włamań. Wykorzystywana sieć umożliwia określenie, jakiego rodzaju atak nastąpił. Dzięki temu było możliwe podjęcie właściwej akcji zaradczej. Klasyfikator przedstawiony w pracy rozpoznawał tylko dwa typy ataków: *satan* i *neptune* oraz ruch związany z normalną aktywnością użytkownika. Do testów i nauki użyto zbioru zawierającego około 15 000 połączeń wybranych z projektu KDD. Przy zastosowaniu dwóch warstw ukrytych uzyskano dokładność klasyfikacji wektorów *normal* oraz dwóch typów ataków na poziomie 91%, natomiast przy jednej warstwie ukrytej – około 87%. Minusem przedstawionej implementacji był długi czas nauki (po zastosowaniu algorytmu wczesnego zatrzymania w celu uniknięcia efektu przetrenowania sieci wyniósł on około 5 godzin). Autorzy tłumaczą tak długi czas dużą liczbą danych wejściowych. Również mogła na to wpłynąć zbyt duża komplikacja architektury sieci, która zawierała aż 35 neuronów w każdej z ukrytych warstw. Inne przykłady zastosowania sieci MLP to [6], [40].

Bardzo dobre wyniki detekcji ataków uzyskano z wykorzystaniem sieci SVM. Charakteryzują się one dużą szybkością nauki i działania oraz mogą się uczyć znacznie większego zbioru wzorców niż inne sieci neuronowe. System IDS wykorzystujący sieci SVM został przedstawiony przez Mukkamala [31] w roku 2002. Wykorzystując zbiór KDD wykazano, że przy zachowaniu podobnego poziomu skuteczności klasyfikacji (około 99%) sieć SVM uczyła się i pracowała w procesie testowania znacznie szybciej, niż sieć MLP o dwóch warstwach ukrytych. Pewną niewielką wadą systemu IDS opartego na sieciach SVM może być możliwość jego wykorzystania tylko do klasyfikacji problemów binarnych, czyli określenia, czy dany wektor jest związany z atakiem czy też z normalnym ruchem. W przypadku potrzeby rozpoznania, do jakiej grupy należy lub jakiego typu atak został wykryty, muszą zostać wykorzystane odrębne sieci SVM dla każdej z klas [31].

Porównanie wyników zastosowania architektur sieci neuronowych, takich jak: MLP, SOM oraz RBF, do wykrywania ataków zawartych w zbiorze KDD przedstawiono w [22]. W tej publikacji dokonano również porównania zastosowania różnych wariacji metody propagacji wstecznej do nauki sieci MLP. Najlepszą dokładność klasyfikacji przy najkrótszym czasie nauki uzyskano dla sieci MLP. Natomiast algorytmem, który umożliwił najszybszą naukę tej sieci, okazał się **RPROP** (*Resilient backpropagation*).

Sieci neuronowe znalazły też zastosowania w systemach hybrydowych, które oprócz sieci wykorzystują jeszcze inne metody sztucznej inteligencji. Sieci RBF oraz SOM posłużyły do budowy hybrydowego systemu IDS opisanego w pracy [14]. Jako dane wejściowe wykorzystano cechy dotyczące nagłówka pakietu **TCP**/**IP** pobrane ze zbioru DARPA. Dane były przetwarzane do postaci **ASCII** za pomocą oprogramowania *Snort.* Wykorzystano symulacje następujących ataków**:** *back, dictionary, guest, ipsweep, nmap, warezclient*. Dla każdego z nich opisano skuteczność klasyfikacji oraz zidentyfikowano cechy, które są najbardziej istotne do jego detekcji. Wadą rozwiązania jest dłuższy czas nauki, niż przy wykorzystaniu jedynie sieci RBF przy podobnych lub nieco lepszych wynikach klasyfikacji dla sieci RBF-SOM.

W pracy [45] przedstawiono system hybrydowy złożony z sieci SVM oraz systemu wykorzystującego logikę rozmytą. Sieć SVM w procesie nauki dostarcza wektory podtrzymujące, z których są tworzone reguły rozmyte. Następnie zestaw reguł jest poddawany działaniu funkcji rozmytych i w wyniku tego powstaje klasyfikator rozmyty lub rozmyta granica decyzyjna. Testy oraz nauka proponowanego rozwiązania zostały przeprowadzone z wykorzystaniem losowo wybranych połączeń ze zbioru KDD. Ich wyniki pokazały wysoką skuteczność klasyfikacji na poziomie 99% przy czasach testowania poniżej jednej minuty (dla zbioru 10 000 połączeń). Przedstawione rozwiązanie, w odróżnieniu od innych wykorzystujących statyczny klasyfikator, ma dynamiczną granicę klasyfikacji, która dostosowuje się do aktualnych potrzeb. Granica ta jest sterowana przez wybór współczynnika γ funkcji jądra o postaci radialnej w sieci SVM. Przy jego

małej wartości liczba generowanych wektorów podtrzymujących jest mała, dokładność wykrywania mniejsza, ale też mniejsze wymagania dotyczące mocy obliczeniowej. Przy dużej wartości γ rośnie dokładność, ale też rosną koszty obliczeniowe.

System hybrydowy złożony z sieci neuronowej MLP i algorytmu C4.5 drzew decyzyjnych opisano w [36]. Proces nauki i testowania został przeprowadzony z wykorzystaniem danych KDD. W zbiorze związanym z nauką znalazły się: normalny ruch oraz po jednym reprezentancie ataków z każdej z czterech grup (DoS, R2L, U2R, *probe*). Sieć neuronowa wykazała się większą skutecznością dla wykrywania ataków z grupy *probe* i DoS, natomiast drzewo decyzyjne lepiej wykrywało ataki z pozostałych grup. Dzięki połączeniu obu metod uzyskano system łączący najlepsze cechy każdej z nich i charakteryzujący się dzięki temu wyższą skutecznością klasyfikacji. System IDS, będący połączeniem sieci neuronowej MLP oraz grupowania danych **FCM** (FUZZY C-MEANS) opisano w [17]. Zadaniem FCM jest podział wektorów wejściowych na dwie klasy: normalny ruch oraz atak. Dane należące do tej drugiej klasy są dodatkowo podawane na wejście sieci neuronowej MLP, która odpowiada za ich przydzielenie do jednej z 4 kategorii ataków zawartych w zbiorze KDD.

Oprócz zadań klasyfikacyjnych, metody sztucznej inteligencji były wykorzystywane do redukcji zbioru danych, na podstawie których odbywa się rozpoznawanie ataków. Dane wejściowe, pochodzące z pakietów IP lub plików audytu, muszą być przetworzone do postaci wektorów numerycznych przyswajalnych przez sieci neuronowe. Dodatkowo, w związku z tym, że zbiór danych do analizy jest bardzo duży, system IDS musi się charakteryzować dużą wydajnością. Dlatego metody redukcji danych wejściowych niepogarszające dokładności klasyfikacji, lecz wpływające pozytywnie na wydajność systemu IDS, są bardzo istotne, zwłaszcza w przypadku systemów czasu rzeczywistego. W literaturze przedstawiono dwa główne sposoby redukcji wymaganego zasobu danych wejściowych.

Pierwszy polega na tym, że przed podaniem na wejście sieci neuronowej dane mogą być wcześniej grupowane w zbiory o podobnych właściwościach. Umożliwia to między innymi ograniczenie liczby analizowanych danych przez rozpatrywanie grup o podobnych cechach, a nie indywidualnych wektorów. Do tego celu były wykorzystywane między innymi sieci SOM. W przypadku publikacji [6] umożliwiło to stworzenie wektorów wejściowych dla sieci neuronowej, uwzględniających serię zdarzeń składających się na dany atak. Praca [4] natomiast zawiera opis wykorzystania sieci SOM dla wstępnego przetworzenia danych wejściowych w celu wyodrębnienia stałej liczby grup o zbliżonej intensywności ruchu w sieci IP.

Drugim sposobem poprawienia wydajności systemów IDS jest ograniczenie liczby cech analizowanego wektora wejściowego. W tym celu w pracach [8], [9] zaproponowano wybór najistotniejszych cech dla każdej grupy ataków. Do tego celu wykorzystano algorytm **FNT** (*Flexible Neural Tree*). Jego zastosowanie zapewnia zredukowanie liczby cech wektora KDD dla poszczególnych klas do 4 (*normal*), 12 (*probe*), 12 (DoS), 8 (U2R) i 10 (R2L). W pracy przedstawiono również wyniki symulacji, w której osiągnięto dokładność wykrywania włamań na poziomie 98,39% do 99,7 %, przy liczbie fałszywych alarmów na poziomie od 0,1 do 0,8 %. Zredukowanie liczby cech wektora wejściowego do 12 poprawiło dokładność klasyfikacji sieci neuronowej dla ataków z grupy DoS oraz R2L. Wykorzystanie modelu *Markov blanket* do wyznaczenia najbardziej istotnych cech wektora KDD opisano w [7]. Przy zastosowaniu sieci Bayesa jako klasyfikatora dla zredukowanego zbioru danych (wektor o 17 najważniejszych cechach) wykazano, że czas nauki i testowania sieci uległ skróceniu przy nieznacznym zmniejszeniu dokładności klasyfikacji w porównaniu do pełnego wektora KDD o 41 cechach. W pracy [18] wyznaczono najważniejszą cechę dla każdego z 22 zawartych w zbiorze *10%KDD* typów ataku oraz normalnego ruchu. Dodatkowo zlokalizowano 9 cech najmniej istotnych dla wykrywania ataków. W tym celu wyznaczono przyrost informacji (*information gain*) dla każdej z nich. Do wyboru najważniejszych cech ze zbioru DARPA, związanych z nagłówkiem TCP/IP, były również wykorzystywane algorytmy genetyczne [14]. Redukcja danych wejściowych z wykorzystaniem metody **PBRM (***Performance-based Ranking Metod)* oraz sieci neuronowych SVM została opisana w [33]. W pracy dokonano wyboru najważniejszych cech wektora wejściowego umożliwiających jego przypisanie do jednej z pięciu klas (4 grupy ataków, normalny ruch) zbioru danych KDD. Idea działania metody PBRM jest następująca: z danych wejściowych usuwa się jedną z cech, następnie zostaje przeprowadzony proces nauki i testowania, a w ostatnim kroku podlega ocenie dokładność klasyfikacji oraz czas trwania procesu nauki i testowania w porównaniu do klasyfikatora uczonego z wykorzystaniem wszystkich 41 cech. Na zakończenie dla każdej klasy otrzymano trzy podzbiory cech: ważne, drugorzędne i nieistotne. Natomiast wykorzystanie metody wektorów wspierających do wyboru najważniejszych cech dla każdej z klas (metoda *Support Vector Decision Function Ranking*) polega na obliczeniu wag z zastosowaniem funkcji decyzyjnej wektorów podtrzymujących. O istotności każdej z cech decyduje wartość bezwzględna wag. Wyniki uzyskane dla obu metod pokrywały się przy wyborze najważniejszych cech dla wszystkich klas z wyjątkiem *normal* oraz U2R. Następnie przedstawiono wyniki klasyfikacji, przeprowadzonej za pomocą sieci SVM wektorów wykorzystujących tylko najważniejsze cechy w porównaniu z wektorami zawierającymi cechy ważne i drugorzędne oraz wszystkie 41 cech. Jak pokazały badania, dokładność klasyfikacji była dla wszystkich przypadków bardzo podobna, natomiast dla wektorów o mniejszej liczbie cech uległ skróceniu czas nauki i testowania systemu.

* * *

Jak pokazały wyniki badań, systemy IDS oparte na metodach sztucznej inteligencji zapewniają skuteczne wykrywanie nauczonych ataków oraz ich zmodyfikowanych nowych wersji przy niewielkim poziomie fałszywych alarmów. Systemy tego typu częściowo eliminują również problem tradycyjnych systemów IDS związan z wykrywaniem nowych nieznanych ataków. Tylko częściowo, ponieważ – jak pokazują badania przedstawione w [21] oraz [15] – nie wszystkie typy nowych ataków są poprawnie klasyfikowane bez konieczności ponownej nauki systemu IDS. Natomiast ponowna nauka wymaga zdobycia wzorców nowych ataków, co często nie jest proste. Propozycja sposobu pozyskania takich wzorców z wykorzystaniem dedykowanej do tego celu architektury systemu IDS została opisana w [23].

Systemy IDS, wykorzystujące metody sztucznej inteligencji, w odróżnieniu od tradycyjnych systemów IDS, nie wymagają budowy skomplikowanych zbiorów sygnatur odrębnych dla każdej instancji ataków oraz profili normalnych zachowań użytkowników, ponieważ są one tworzone automatycznie w procesie nauki sieci. Dodatkowo znika problem związany z określeniem wartości progów oddzielających normalny ruch i atak, ponieważ progi te są tworzone automatycznie w procesie nauki i mogą się zmieniać w zależności od zawartości zbioru uczącego, podanego na wejście sieci. W przypadku tradycyjnych systemów IDS stworzenie takich progów wymaga przeprowadzenia szczegółowej i czasochłonnej analizy ruchu w chronionej sieci. Dodatkowo taka analiza musi odbywać się dość często, aby zapewnić prawidłowe działanie systemu IDS w przypadku zmian zachowań użytkowników.

Systemy IDS wykorzystujące sztuczną inteligencję są w stanie również analizować z dużą szybkością dane pochodzące z różnych źródeł. Dzięki temu znika ograniczenie tradycyjnych systemów IDS, związane z dużymi wymaganiami na moc obliczeniową potrzebną do analizy wielu różnych profili zachowań użytkowników. Ponieważ metody sztucznej inteligencji mogą

podejmować decyzje, wykorzystując niekompletne dane wykrywają ataki opierając się na mniejszej liczbie informacji, niż wymagają tego tradycyjne systemy IDS. Analogiczna próba analizy takich danych z wykorzystaniem metod algorytmicznych (np. reguł, modeli lub profili zachowań użytkowników znanych z tradycyjnych systemów IDS) jest bardzo skomplikowana, a często wręcz niemożliwa.

Trzeba jednak pamiętać , że zastosowanie metod sztucznej inteligencji ma oczywiście sens w przypadkach, gdy stworzenie odpowiedniej reguły wykrywającej atak jest procesem skomplikowanym. Na przykład ataki polegające na niewłaściwej fragmentaryzacji pakietów IP można w prosty sposób wykryć, sprawdzając dwa pola nagłówka IP: offset oraz długość pakietu. To samo dotyczy wszelkich ataków, polegających na wysłaniu pakietów zbudowanych niezgodnie ze standardem. Dlatego wydaje się słuszne, że pełne rozwiązanie systemu IDS powinno być kombinacją systemu wykorzystującego metody sztucznej inteligencji oraz tradycyjnego systemu wykrywania nadużyć. W przypadku analizy skomplikowanych ataków oraz danych pod względem wykrywania zmodyfikowanych wersji dobrze znanych albo wybranych nowych typów ataków, można wykorzystać metody sztucznej inteligencji. Natomiast za detekcję dobrze znanych prostych ataków może odpowiadać tradycyjny system wykrywania nadużyć.

Zgodnie z przytoczonymi publikacjami, oprócz klasyfikacji, metody sztucznej inteligencji można wykorzystać również w celu ograniczenia liczby danych poddawanych analizie. Dzięki temu systemy IDS mogą działać oraz uczyć się szybciej, co jest istotne szczególnie w przypadku systemów podejmujących decyzje w czasie rzeczywistym.

LITERATURA

[1] Amini M., Jalili R., Shahriari H. R.: *RT-UNNID: A practical solution to real-time network-based intrusion detection using unsupervised neural networks*, Computers & Security 25, May 2006

[2] Amor N. B., Benferhat S., Elouedi Z.: *Naive Bayes vs decision trees in intrusion detection systems*, In Proc. ACM Symp. on Applied Computing, 2004

[3] J. P. Anderson: *Computer Security Threat Monitoring and Surveillance*, Fort Washington, Pa., 1980.

[4] Bivens A., Palagiri C., Smith R., Szymanski B., Embrechts M.: *Network-Based Intrusion Detection using Neural Networks*, ASME Press, vol. 12 , New York 2002

[5] Cannady J.: *Artificial neural networks for Misuse Detection*, National Information Systems Security Conference, 1998

[6] Cannady J., Maheffey J.: *The application of artificial neural networks to misuse detection. Initial results*; In: Proc. of the 1st International Workshop on Recent Advances in Intrusion Detection (RAID), Louvain-la-Neuve, Belgium, 1998

[7] Chebroluа S., Abrahamа A., Thomasа J. P.: *Feature deduction and ensemble design of intrusion detection systems,* Computers & Security, 2004

[8] Chen Y., Abraham A., Yang B.: *Hybrid Flexible Neural-Tree Based IDS, International Journal of Intelligent Systems*, vol. 22, no. 4, 2007

[9] Chen Y., Abraham A.: *Feature selection and intrusion detection using Hybrid Flexible Neural Tree*, In Proc. of Second International Symposium on Neural Networks (ISNN-05), LNCS 3498, 2005

[10] Barbara D., Couto J., Jajodia S., Popyack L., Wu N.: *ADAM: Detecting Intrusions by Data Mining*, In Proc of the 2001 IEEE Workshop on Information Assurance and Security, T1A3 1100 United States Military Academy, West Point, NY, 5-6 June 2001

[11] Debar H., Becke M., Siboni D.: *A neural network component for an intrusion detection system*, In Proc. of the IEEE Computer Society Symposium on Research in Security and Privacy, 1992

[12] Debar H., Dorizzi B.: *An Application of a Recurrent Network to an Intrusion Detection System*, In Proc. of the International Joint Conference on Neural Network, 1992

[13] Hofmeyr S. A., Forrest S.: *Immunity by Design: An Artificial Immune System*, In Proc. of the Genetic and Evolutionary Computation Conference (GECCO), Morgan-Kaufmann, San Francisco, CA, 1999

[14] Horeis T.: *Intrusion Detection with Neural Networks-Combination of SOM and RBF networks for human Expert integration*, available online in http://ieeecis.org/_files/EAC_Research_2003_Report_Horeis.pdf, 2003

[15] Hwang T. S., Lee T.-J., Lee Y.-J.: *A three-tier IDS via Data Mining Approach*, In: Proc. of the 3rd Annual ACM Workshop on Mining Network Data (MineNet), San Diego USA, June 12 2007

[16] Jawhar M. M. T., Mehrotra M: *Anomaly Intrusion Detection System using Hamming Network Approach.* International Journal of Computer Science & Communication, Vol. 1, No. 1, January-June 2010

[17] Jawhar M. M. T.: *Design Network Intrusion Detection System using hybrid Fuzzy-Neural Network*, International Journal of Computer Science and Security, Volume 4

[18] Kayacik H.G., Zincir-Heywood A.N., Heywood M.I.: *Selecting Features for Intrusion Detection: A Feature Relevance Analysis on KDD99 Intrusion Detection Dataset*, In Proc. of the Third Annual Conference on Privacy, Security and Trust (PST-2005), October 2005

[19] Kim J., Bentley P., Aickelin U., Greensmith J., Tedesco G., Twycross J.: *Immune System Approaches to Intrusion Detection – A Review*- Natural Computing, vol. 6, no. 4, December 2007

[20] Kruegel C., Toth T.: *Using decision trees to improve signature-based intrusion detection*, In Proc. of the 6th Symposium on Recent Advances in Intrusion Detection (RAID), 2003

[21] Kukiełka P.: *Wykrywanie ataków na systemy informacyjne z wykorzystaniem metod adaptacyjnych*, rozprawa doktorska, Politechnika Warszawska Wydział Elektroniki i Technik Informacyjnych, Warszawa 2010

[22] Kukielka P., Kotulski Z.: *Analysis of different architectures of neural networks for application in Intrusion Detection Systems*. IMCSIT 2008

[23] Kukielka P., Kotulski Z.: *Adaptation of the neural network-based IDS to new attacks detection*, CoRR abs/1009.2406: (2010)

[24] Lee W., Stolfo S. J.: *A Framework for Constructing Features and Models for Intrusion Detection System*, ACM Transactions on Information and System Security (TISSEC), 3(4) 2000

[25] Li W.: *Using Genetic Algorithm for network intrusion detection*, In Proc. United States Department of Energy Cyber Security Group 2004 Training Conference, Kansas City, Kansas, May 24–27, 2004

[26] X. Li, Ye N.: *Decision tree classifier for computer intrusion detection*, Journal of Parallel and Distributed Computing Practices, 2001

[27] Lichodzijewski P., Zincir-Heywood A. N., Heywood M. I.: *Host-based intrusion detection using self-organizing maps*, In Proc. of the 2002 IEEE World Congress on Computational Intelligence, 2002

[28] Lichodzijewski P., Zincir-Heywood A. N., Heywood M. I.: *Dynamic Intrusion Detection Using Self-Organizing Maps*, In Proc. of the IEEE International Joint Conference on Neural Networks. IEEE, May 2002

[29] Lippmann R., Haines J.W., Fried D.J., Korba J., Das K.: *The 1999 Darpa Off-Line Intrusion Detection Evaluation*, Computer Networks: The International Journal of Computer and Telecommunications Networking 34 (2000) 579–595, 2000.

[30] Moradi M., Zulkernine M.: *Neural Network Based System for Intrusion Detection and Classification of Attacks*, IEEE International Conference on Advances in Intelligent Systems – Theory and Applications, Luxembourg-Kirchberg, Luxembourg, November 15–18, 2004

[31] Mukkamala S., Janoski G., Sung A H.: *Intrusion Detection Using Neural Networks and Support Vector Machines,* In Proc. of the IEEE International Joint Conference on Neural Networks, IEEE Computer Society Press, 2002

[32] Mukkamala S., Sung A. H., Abraham A., Ramos V.: *Intrusion Detection Systems using Adaptive Regression Splines.* In Proc. of ICEIS-04 – 6th Int. Conf. on Enterprise Information Systems, Porto, Portugal, April 14–17, 2004

[33] Mukkamala S., Sung A. H.: *Feature selection for Intrusion Detection using Neural Networks and Support Vector Machines*, Journal of the Transportation Research Board (of the National Academies), 2003

[34] Mukkamala S., Sung A. H., Abraham A.: *Modeling Intrusion Detection Systems Using Linear Genetic Programming Approach*, In Proc. of the 17th International Conference on Innovations in Applied Artificial Intelligence, Ottawa, Canada, 2004

[35] Osowski S.: *Sieci neuronowe do przetwarzanie informacji*, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2006, ISBN 83-7207-615-4

[36] Pan Z. S., Chen S. C., Hu G. B.: *Hybrid neural network and C4.5 for misuse detection*, In Proc. of the Second International Conference on Machine Learning and Cybernetics (ICMLC'03), 2003
[37] Puttini R. S., Marrakchi Z., Mé L.: *A Bayesian Classification Model for Real-Time Intrusion Detection*, In Proc. of the 22th International Workshop on Bayesian Inference and Maximum Entropy Methods in Science and Engineering, 2002
[38] Rhodes B. C., Mahaffey J. A., Cannady J. D.: *Multiple self-organizing maps for intrusion detection*, In Proc. of the 23rd National Information Systems Security Conference, 2000
[39] Rutkowski L.: *Metody i techniki sztucznej inteligencji*, Wydawnictwo Naukowe PWN, Warszawa 2006, ISBN-13 978-83-01-14529-3
[40] Ryan J., Lin M J., Miikkulain R.*: Intrusion detection with neural networks*, Advances in Neural Information Processing Systems, vol. 10, Cambridge, MA: MIT Press; 1998
[41] Seredynski F., Bouvry P.: *Some Issues in Solving the Anomaly Detection Problem using Immunological Approach*, In Proc. of 19th International Parallel and Distributed Processing Symposium (IPDPS), Denver, USA, 2005
[42] Skaruz J., Seredynski F.: *Recurrent neural networks towards detection of SQL attacks*, IEEE International Parallel and Distributed Processing Symposium – IPDPS, 2007, 26–30 March 2007
[43] Stein G., Chen B., Wu A. S., Hua K. A.: *Decision Tree Classifier For Network Intrusion Detection With GA-based Feature Selection*, In Proc. of the 43rd Annual Southeast Regional Conference, Kennesaw, Georgia, March 2005
[44] Xu Q., Pei W., Yang Li, Zhao Q.: *An Intrusion Detection Approach Based On Understandable Neural Network Trees*, International Journal of Computer Science and Network Security, November 2006, v6 i11
[45] Yao J.T., Zhao S.L., Saxton L.V.: *A Study on fuzzy intrusion detection*, In Proc. of SPIE Vol. 5812, Data Mining, Intrusion Detection, Information Assurance, And Data Networks Security, Orlando, Florida, USA, 28 March – 1 April 2005
[46] Zhong J., Ghorbani A.: *Network Intrusion Detection Using an Improved Competitive Learning Neural Network*, In Proc. of the Second Annual Conference on Communication Networks and Services Research, 2004

Artykuł recenzowany

(*Artykuł nadesłay do red. – luty 2011*)

*Andrzej ZIELIŃSKI**

Rynek komunikacji elektronicznej w Polsce w 2010 roku
Część I

Rok 2010 niewątpliwie upływał w Polsce pod znakiem zmian w dziedzinie mediów elektronicznych. Zostały podjęte kolejne próby uporządkowania ich sytuacji prawnej, a w konsekwencji wyprowadzenia mediów publicznych z długo trwającego kryzysu w obszarze zarządzania (głównie w TVP SA), a także ekonomiki.

Proces przełączenia cyfrowego telewizji naziemnej w drugiej połowie roku nabrał pewnego przyspieszenia, chociaż trudno powiedzieć, że zostały już usunięte wszystkie ważne przeszkody na drodze do pełnego sukcesu. Niestety, bardzo ważna dla tego procesu tzw. ustawa cyfryzacyjna, na temat której poważną dyskusję rozpoczęto już na początku 2009 roku ([1] i [2]), nadal znajduje się w stadium przygotowań. Oznacza to, że jako akt obowiązujący może się ona ukazać dopiero w połowie 2011 roku.

W sektorze telekomunikacji na podkreślenie zasługuje uchwalenie ustawy o wspomaganiu inwestycji sieciowych, co może przyspieszyć modernizację infrastruktury telekomunikacyjnej i rozwój Internetu szerokopasmowego. Znane już od kilku lat tendencje zmniejszania się zakresu usług telefonii stacjonarnej utrzymują się, pogłębia natomiast dominacja telekomunikacji komórkowej (mobilnej).

Niniejszy artykuł jest komentarzem, dotyczącym przede wszystkim mediów elektronicznych, a następnie telekomunikacji. Ponieważ większość danych statystycznych, związanych z sektorem komunikacji elektronicznej w 2010 r., nie jest jeszcze znana, autor będzie posługiwać się danymi odnoszącymi się do 2009 roku. Niekiedy dane na temat roku 2010 będą antycypowane lub przytaczane na podstawie doniesień prasowych.

* **Instytut Łączności, Państwowy Instytut Badawczy, Warszawa, e-mail: A.Zielinski@itl.waw.pl**

PRAWNE I EKONOMICZNE ASPEKTY FUNKCJONOWANIA RYNKU MEDIÓW ELEKTRONICZNYCH

Jak o tym wielokrotnie pisano, w tym w [2], co pewien czas podejmuje się próbę uchwalenia nowej ustawy o radiofonii i telewizji, modernizującej podstawową ustawę dotyczącą tej dziedziny z roku 1992 [23].

Pierwszą poważną próbę podjęła w 2002 r. rządząca wówczas koalicja SLD-PSL. Zakończyła się ona skandalem, znanym jako *rywingate*, chociaż – z perspektywy wielu już lat – projekt, wypracowany wtedy z udziałem grupy wybitnych specjalistów, można ocenić jako udany. Wskutek powiązań z aferą korupcyjną i politycznymi rozgrywkami projekt ten upadł – po prostu został zaniechany. Przez kilka lat nie podejmowano poważnych prób całościowego oglądu sytuacji prawnej tego sektora. Stały temu na przeszkodzie kolejne wybory parlamentarne w roku 2005 i 2007 oraz prezydenckie w 2005, a także przyspieszone w 2010. Zmiany w prawie dotyczącym mediów elektronicznych (radiofonii i telewizji), mniej lub bardziej zasadnicze, zostały przedstawione przez autora niniejszej publikacji m.in. w [2], a także w [14] .

Do ważnych inicjatyw z tego zakresu z pewnością należy zaliczyć projekt z lat 2008–2009, powstały w czasach rządzącej koalicji PO – PSL, uzgodniony z SLD. Upadł on formalnie w maju 2009 r., w wyniku weta Prezydenta, jednak w rzeczywistości w wyniku wycofania się PO z uzgodnień dotyczących finansowania mediów przez budżet państwa zamiast abonamentu radiowo-telewizyjnego [2]. Wówczas w środowiskach twórczych powstała społeczna inicjatywa [2] opracowania ustawy niezależnie od środowisk politycznych (partii, Sejmu, Senatu). Postanowiono przedstawić projekt, który gwaranto-