R G B WH GR BL Grey Scale #13 C M Y K
DANES-PICTA.COM
A 1 2 3 4 5 6 M 8 9 10 11 12 13 14 15 B 17 18 19

21

AKADEMIA
OBRONY
NARODOWEJ

mgr Halina ŚWIEBODA

ZAGROŻENIA INFORMACYJNE BEZPIECZEŃSTWA RP

Rozprawa doktorska

Biblioteka Główna
Akademii Obrony Narodowej
S/7594
05-007594-001-0

Warsza

75499

Colour Chart #13
Inches
Centimetres
Blue
Cyan
Green
Yellow
Red
Magenta
White
3/Color
Black
DANES-PICTA.COM

AKADEMIA OBRONY NARODOWEJ

WYDZIAŁ BEZPIECZEŃSTWA NARODOWEGO

BIBLIOTEKA GŁÓWNA - ARCHIWUM
Nr ewid. 75499
Akademii Obrony Narodowej

mgr Halina Świeboda

ZAGROŻENIA INFORMACYJNE BEZPIECZEŃSTWA RP

Rozprawa doktorska

Napisana pod kierunkiem
płk.w st.spocz.prof.dr.hab.inż.
Piotra Sienkiewicza

Praca naukowa zrealizowana w ramach projektu badawczego promotorskiego nr 0 N117 002934 finansowego przez Ministerstwo Nauki i Szkolnictwa Wyższego

[angl]

Warszawa **2009**

Spis treści

WSTĘP 5

Rozdział 1
PODSTAWY METODOLOGICZNE BADAŃ NAD ZAGROŻENIEMI INFORMACYJNYMI 11
1.1. Geneza problemu 11
1.2. Przedmiot badań 18
1.3. Cel badań 20
1.4. Problemy badawcze i hipotezy robocze 22
1.5. Metody, techniki i narzędzia badawcze 26
1.6. Ocena piśmiennictwa 33

Rozdział 2
WSPÓŁCZESNE ZAGROŻENIA INFORMACYJNE DLA BEZPIECZEŃSTWA PAŃSTWA 35
2.1. Wprowadzenie 35
2.2. Ewolucja technologii informacyjnych 37
2.3. Istota zagrożeń informacyjnych 40
2.4. Sytuacje zagrożeń dla bezpieczeństwa informacyjnego 50
2.5. Cyberterroryzm jako zagrożenie dla bezpieczeństwa narodowego 54
2.6. Współczesna walka informacyjna 61
2.7. Bezpieczeństwo informacyjne jako kategoria poznawcza 68
2.8. Bezpieczeństwo informacyjne jako czynnik bezpieczeństwa narodowego 69
2.9. Bezpieczeństwo informacyjne jako czynnik jakości życia 71
2.10. Teoria bezpieczeństwa informacyjnego 81
2.11. Wnioski 88

Rozdział 3
PROGNOZOWANIE ZAGROŻEŃ INFORMACYJNYCH 93
3.1. Wprowadzenie 93
3.2. Prognozowanie na podstawie szeregów czasowych 95
3.3. Sieci neuronowe 127
3.4. Analiza społecznej percepcji zagrożeń informacyjnych 138
3.5. Scenariusze zagrożeń informacyjnych 157
3.6. Wnioski 187

Rozdział 4
MODEL ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACYJNYM RP 193
4.1. Wprowadzenie 193
4.2. Zarządzanie ryzykiem 194
4.3. Model systemu zarządzania bezpieczeństwem informacyjnym 209
4.4. Wnioski 216

ZAKOŃCZENIE 219

LITERATURA **227**

Spis tabel 237
Spis rysunków 239
Streszczenie 243

ZAŁĄCZNIKI **245**
Załącznik I 245
Załącznik II 251
Załącznik III 254
Załącznik IV 257
Załącznik V 295
Załącznik VI 309
Załącznik VII 310
Załącznik VIII 312
Załącznik IX 314
Załącznik X 317

Problemy bezpieczeństwa w różnych dziedzinach są bardzo często tej samej natury i mogą zostać sformalizowane w ten sam sposób. Dało to początek temu, co teraz nazywane jest nauką o bezpieczeństwie".

W. J. Geysen

WSTĘP

Jednym z najważniejszych czynników rozwoju społecznego, ekonomicznego i technologicznego współczesnego społeczeństwa są zasoby informacyjne. Od zarania dziejów odgrywały ważną rolę, a na przełomie XX i XXI wieku stały się zasobem strategicznym państwa, jego gospodarki i sił zbrojnych. Obecnie informacja obok pracy, kapitału i ziemi jest podstawowym czynnikiem rozwoju gospodarczego. Przewaga informacyjna stała się jednym z głównych filarów powodzenia w walce i biznesie. Stało się to skutkiem dynamicznego rozwoju systemów informacyjnych: informatycznych, telekomunikacyjnych i masowej komunikacji. Oprócz niewątpliwych korzyści dla wyłaniającego się społeczeństwa informacyjnego, zmiany wywołane modernizacją przyniosły także wzrost zagrożeń. Rozwój systemów ICT (ang. *Information & Communication Technologies*) był jednym z czynników globalizacji i internacjonalizacji, lecz stworzył „niebezpieczną przestrzeń cybernetyczną".[1] Podniesienie informacji do rangi cechy określającej typ społeczeństwa wiąże się z przyspieszonym rozwojem ICT w drugiej połowie XX wieku.

Autorka zajmuje się problematyką rozwoju społeczeństwa informacyjnego od przeszło dziesięciu lat. Wyrazem tych zainteresowań był temat pracy magisterskiej: „Edukacja i praca w społeczeństwie informacyjnym"[2], w której poddano analizie zmiany w dziedzinie edukacji i pracy wywołane rozwojem ICT, w tym szanse i zagrożenia w kontekście pozycji Polski w rankingu państw pretendujących do miana społeczeństwa informacyjnego. Kolejnym etapem była praca wykonana w ramach Podyplomowych Studiów Bezpieczeństwa Narodowego w Akademii Obrony Narodowej poświęcona analizie wpływu edukacji na kulturę bezpieczeń-

[1] P.Sienkiewicz, H.Świeboda, *Niebezpieczna przestrzeń cybernetyczna*, Transformacje 1-4 (47-50) 2006, Wyd. Fundacja Edukacyjna Transformacje, Warszawa 2006.

[2] Praca została wyróżniona I nagrodą Rektora-Komendanta AON w konkursie na najlepszą pracę magisterską w roku akademickim 2002/2003.

stwa we współczesnym społeczeństwie przełomu XX i XXI wieku. Rozległość i różnorodność problematyki transformującego się społeczeństwa polskiego, pogłębiona zmianą systemową przełomu lat osiemdziesiątych i dziewięćdziesiątych XX wieku znalazła odzwierciedlenie w licznych artykułach oraz pracach naukowo-badawczych, które były moim udziałem.[3] Pod wpływem wyników badań, początkową fascynację możliwościami nowych technologii, zastąpiła krytyczna refleksja nad ryzykiem, niepewnością i zagrożeniami. Nie obniża to postrzegania wysokiej społecznej rangi zasobów informacyjnych i systemów ICT.

Głównym obiektem zainteresowania stały się problemy bezpieczeństwa informacyjnego i zagrożeń związanych z nowoczesnymi technologiami informacyjnymi, których wpływ na poziom bezpieczeństwa narodowego stale rośnie. Problematyka bezpieczeństwa narodowego do niedawna łączona była przede wszystkim z militarnymi zagrożeniami. Zmiany w środowisku bezpieczeństwa oraz zacieranie się granic pomiędzy nauką wojskową, a naukami „cywilnymi" przyniosła nowy wymiar problemów bezpieczeństwa wewnętrznego i zewnętrznego.[4]

Zaproponowany temat dysertacji osadzony jest w rozwijanej od początku lat 90. problematyce naukowej Wydziału Strategiczno-Obronnego, a następnie Wydziału Bezpieczeństwa Narodowego AON. W kontekście rozwoju globalnego społeczeństwa informacyjnego oraz współczesnej problematyki bezpieczeństwa systemów, przyjęto jako platformę metodologiczną analizę systemową wpływu zagrożeń informacyjnych na poziom bezpieczeństwa narodowego. Spowodowało to konieczność wyboru metod ewaluacji ryzyka i prognozowania zagrożeń, w tym analizę społecznej percepcji zagrożeń informacyjnych. Uznałam, że są to szczególnie istotne problemy poznawcze i praktyczne w kontekście współczesnej problematyki bezpieczeństwa. Nie budzi wątpliwości, że jednym z podstawowych, współczesnych wymiarów bezpieczeństwa narodowego jest bezpieczeństwo informacyjne, albowiem rozwój technologii informacyjnych spowodował powstanie nowych, w sensie jakościowym i ilościowym, zagrożeń informacyjnych dla bezpieczeństwa organizacji (instytucji) oraz bezpieczeństwa tzw. Krytycznej Infrastruktury Państwa (KIP). Analiza wpływu bezpieczeństwa informacyjnego na bezpieczeństwo narodowe (państwa) wraz z oceną ryzyka zagrożeń i prognozowaniem możliwych i prawdopodobnych zagrożeń informacyjnych stanowi nie tylko istotną,

---

[3] Przykładem mogą być prace realizowane w AON, np.: Modelownie rozwoju globalnego społeczeństwa informacyjnego. 2003, (kier. P.Sienkiewicz); Modelownie zagrożeń dla bezpieczeństwa informacyjnego państwa. Teoria walki informacyjnej. 2004, (kier. T.Jemioło); Modelownie procesów walki informacyjnej. „Model cyberwar". 2006, (kier. P.Sienkiewcz); Zarządzanie ryzykiem w sytuacjach kryzysowych (2006), (kier. P.Sienkiewicz).

[4] S.Zajas (red.), Nauki wojskowe a nauki o bezpieczeństwie i obronności. AON, Warszawa 2009.

lecz konieczną podstawę zarządzania bezpieczeństwem państwa (na różnych szczeblach struktury administracyjnej). W takim ujęciu badania dotyczące zagrożeń informacyjnych nie były podejmowane.

W trakcie badań i przygotowywania dysertacji miały miejsce wydarzenia, które potwierdzały zarówno rangę podjętej problematyki, jak i przyjętą postawę metodologiczną. Dotyczą one zarówno inicjatyw Unii Europejskiej i NATO, jak i inicjatyw krajowych.[5]

Ze względu na interdyscyplinarny charakter zagrożeń informacyjnych bezpieczeństwa w dysertacji przyjęto pewne ograniczenia, wynikające z określonego celu badań i charakteru oczekiwanych rezultatów. Przyjęte założenia i ograniczenia determinowały zaproponowany w rozprawie model postępowania badawczego.

Główny problem badawczy sformułowałam następująco: **w jakim zakresie (stopniu) zagrożenia informacyjne wpływają na poziom bezpieczeństwa narodowego RP oraz, za pomocą jakich metod naukowych (technik analityczno-ocenowych, diagnostycznych, prognostycznych) należy ocenić ryzyko zagrożeń informacyjnych i prognozować możliwe i prawdopodobne zagrożenia informacyjne dla bezpieczeństwa narodowego RP.**

Przyjęta metodologia rozwiązania głównego problemu wpłynęła na strukturę rozprawy. Dysertacja obejmuje cztery rozdziały: metodologiczny i trzy rozdziały merytoryczne zakończone wnioskami, wstęp i zakończenie, wykaz literatury, wykaz rysunków i tabel, a także streszczenie. Ponadto w pracy zamieszczono obszerne załączniki dotyczące zarówno kwestii ogólnych (klasyfikacja, typologia) jak i szczegółowej dokumentacji badań.

Rozdział pierwszy poświecono podstawom metodologicznym badań nad bezpieczeństwem informacyjnym oraz uzasadniono wybór tematu. W oparciu o analizę systemową skonkretyzowano przedmiot badań wyróżniając: zjawisko, system i proces. Określono przestrzeń badawczą oraz horyzont czasowy dla prognoz. Podkreślono złożoność i różnorodność badanych systemów wyznaczając cele rozprawy. Sformułowano problemy badawcze i hipotezy robocze w kontekście szeroko ujętej genezy problemu. Scharakteryzowano problem decyzyjny analizy systemowej i przedstawiono organizację badań.

Rozdział drugi jest próbą syntetycznej prezentacji współczesnych zagrożeń informacyjnych w kontekście bezpieczeństwa narodowego. Zawiera klasyfikację oraz typologię za-

---

[5] Np. powołanie przez Komisję Europejską 2004r. Agencji ENISA (*The European Network and Information Security Agency*), Rezolucja Parlamentu Europejskiego z dnia 19 lutego 2009 r. w sprawie europejskiej strategii bezpieczeństwa i europejskiej polityki bezpieczeństwa i obrony (2008/2202 (INI)); Rządowy Program Ochrony Cyberprzestrzeni RP na lata 2009-2011 (uchwalony 2009).

grożeń, których swoistym generatorem są współczesne systemy informacyjno-komunikacyjne. Scharakteryzowano istotę zagrożeń informacyjnych, podając wnikliwą ich taksonomię oraz wzajemne powiązania w szczególności stanowiące podstawę prognozowania, które jest treścią trzeciego rozdziału. Ponadto rozdział II wzbogacono o załącznik szczegółowo opisujący zagrożenia informacyjne, a także załącznik z opisem inicjatyw poprawy bezpieczeństwa informacyjnego, wspieranych programami ramowymi UE. W rozdziale tym zawarto zarówno informacje uzyskane z materiałów źródłowych, jak i liczne własne propozycje.

Rozdział trzeci poświęcono analizie prognostycznej zagrożeń informacyjnych, wykorzystując techniki ilościowe i jakościowe oraz metody scenariuszowe. W badaniach posłużono się modelami formalnymi stosownymi w prognozowaniu szeregów czasowych z dziedziny modeli adaptacyjnych. Wykonano również badania z zastosowaniem sztucznych sieci neuronowych, oraz badania opinii społecznej nt. postrzegania ryzyka zagrożeń informacyjnych w kontekście zmian wywołanych rozwojem ICT. Do przewidywania możliwych i prawdopodobnych zagrożeń informacyjnych zastosowano technikę budowania scenariuszy wraz z propozycją wykorzystania techniki eksperckiej.

W rozdziale czwartym poświęconym budowie modelu zarządzania bezpieczeństwem informacyjnym, uwzględniono zarządzanie ryzykiem zagrożeń informacyjnych w kontekście wyników badań otrzymanych w analizach rozdziału trzeciego. W modelu tym wykorzystano podstawowe ilościowe i jakościowe metody prognozowania oraz oryginalną metodykę ewaluacji ryzyka zagrożeń informacyjnych. Propozycja jest jednym z elementów wspomagania procesów decyzyjnych przy planowaniu polityki bezpieczeństwa. Proponowane procedury probabilistycznej analizy ryzyka, ich głównych konsekwencji dla bezpieczeństwa informacyjnego organizacji (instytucji) wraz z ich rangowniem i tworzeniem map ryzyka, zaprezentowano na przykładach. Zaproponowano model o strukturze dwu poziomowego sterownia z propozycją klasyfikacji sytuacji zagrożeń według ich ustrukturyzownia.

W zakończeniu rozprawy przedstawiono syntezę wniosków z poszczególnych rozdziałów, oraz nakreślono kierunki dalszych badań wraz z propozycjami rozwiązań metodologicznych i praktycznych.

Przyjęta struktura rozprawy sprawia, że znaczne jej części mogą być użyteczne w procesie dydaktycznym w uczelniach prowadzących studia na kierunku bezpieczeństwo narodowe, w szczególności zaś, w ramach przedmiotów: „bezpieczeństwo informacyjne", i „prognо-

zowanie zagrożeń dla bezpieczeństwa państwa".[6] Rozprawa może być pomocna w pracy analityków systemowych i planistów w procesie projektowania polityki bezpieczeństwa, a także w praktyce zarządzania bezpieczeństwem informacyjnym.

* * *

Pragnę podziękować wszystkim, których życzliwej pomocy doświadczyłam podczas opracowywania rozprawy i studiów doktoranckich.

Serdeczne podziękowania składam także moim przełożonym, za umożliwienie mi studiów doktoranckich w AON, a kolegom, koleżankom i przyjaciołom za cierpliwość i okazaną pomoc w zdobywaniu wiedzy, za ciekawe spostrzeżenia i dyskusje oraz krytyczne uwagi.

Szczególne podziękowania kieruję do najbliższej rodziny: męża i córek za pomoc, cierpliwość i wyręczanie w wielu obowiązkach domowych.

Profesorowi Piotrowi Sienkiewiczowi dziękuję nie tylko za kierownictwo merytoryczne, pomoc metodologiczną, lekcję analizy systemowej oraz udostępnianie unikalnych materiałów źródłowych, lecz także za umożliwienie aktywnego udziału w licznych konferencjach naukowych, dzięki którym nie tylko wzbogacałam wiedzę, ale również poznałam znakomitych przedstawicieli nauki.

* * *

[6] Autorka uczestniczyła w przygotowaniu programów tych przedmiotów oraz prowadziła zajęcia dydaktyczne w roku akademickim 2008/2009.

Rozdział 1

PODSTAWY METODOLOGICZNE BADAŃ NAD ZAGROŻENIEMI INFORMACYJNYMI

1.1. Geneza problemu

„Szczegóły nie stanowią nauki, jest ona zawarta w tym, co jest ogólne, w całości, w zespoleniu się wszystkich szczegółów"

D. Mendelejew

Warunki społeczno-polityczne pierwszej dekady XXI wieku są konsekwencją przemian systemowych końca minionego stulecia. Szczególną rolę w przemianach stosunków społecznych i politycznych spełniła rewolucja technologiczna - często stymulowana potrzebami bezpieczeństwa i obronności. Konsekwencją rozwoju technologii informacyjnych oraz wysokiej dynamiki dyfuzji wiedzy z obszaru mikroelektroniki, telekomunikacji i informatyki była transformująca się gospodarka i wyłanianie się społeczeństwa informacyjnego.[7] Efektem transformacji jest „nowa gospodarka" określana mianem gospodarki opartej na wiedzy (GOW), w której dostęp do informacji i wiedzy stał się równie istotny jak dostęp do innych zasobów mających strategiczne znaczenie. Efekty związane z pozyskiwaniem, przetwarzaniem i wykorzystaniem informacji mają wartość społeczną i ekonomiczną.[8] Istotną cechą wyłaniającego się społeczeństwa informacyjnego jest cyfryzacja technik i technologii informacyjnych (ICT) oraz usieciowienie systemów informacyjnych, a w konsekwencji struktur organizacyjnych. Wpłynęło to na przyspieszenie globalizacji gospodarki światowej i jej systemów finansowych, wzrost liczby relacji międzyludzkich, zwiększanie ich zasięgu i intensywności w sferze masowego komunikowania społecznego. Na szczególną uwagę zasługuje globalizacja systemów informacyjnych (telekomunikacja satelitarna i sieci komputerowe) a przede wszystkim powstanie Internetu (1990) i jego, w zasadzie niekontrolowany rozwój oraz integracja (konwergencja) systemów telekomunikacyjnych i systemów informatycznych (systemy teleinformatyczne) oraz systemów masowego komunikowania.[9]

---

[7] L.Zacher, Transformacje społeczeństw od informacji do wiedzy. Wyd. C.H.Beck, Warszawa 2007.

[8] P.Sienkiewicz, Wartość informacji w systemach zarządzania organizacja. AGH, Kraków 2009.

[9] P.Sienkiewicz, H.Swieboda, *Edukacyjne determinanty rozwoju społeczeństwa informacyjnego.* Zeszyty Naukowe WWSI, Nr 2, Warszawa 2007. Rośnie, z roku na rok, znaczenie Internetu oraz technologii internetowych, jak np. dostępu do stron WWW, poczta elektroniczna, coraz większe znaczenie ma jako infrastruktura dla telekomunikacji typu VoIP (*Voice over Internet Protocol*) telefonia internetowa, IP TV(*Internet Protocol Television)* przesyłanie sygnału telewizyjnego w sieciach opartych o protokół IP, telefonii komórkowej

Technologie informacyjne i komunikacyjne stały się podstawowym czynnikiem rozwoju cywilizacyjnego, silnie stymulującym wzrost gospodarczy i zatrudnienie. Obecnie technologie informacyjne odpowiadają za jedną czwartą wzrostu PKB i 40% wzrostu produktywności w Unii Europejskiej, bowiem udział ICT w unijnym PKB sięga 6,5%.[10] Całość polskiego rynku telekomunikacyjnego utrzymuje tempo wzrostu około 5% rocznie. Usługi internetowe stały się częścią gospodarki, charakteryzują się najwyższym współczynnikiem wzrostu (5,9 procent w okresie 2006-2007).[11] Zaletą sektora ICT są silne powiązania z innymi sektorami gospodarczymi, które generują dodatkowe korzyści. Warunkują w znacznym stopniu poziom jakości życia społeczeństwa (w ujęciu ekonomicznym, społecznym).[12] Są także przyczyną wielu zagrożeń wynikających z ich stosowania, ponadto w wielu przypadkach działają synergicznie w stosunku do klasycznych zagrożeń (kumulacja, amplifikacja). Szerokie ich stosownie spowodowało również zagrożenia w sferze psychospołecznej. [13]

Procesy modernizacyjne oparte na technologiach wspierane są instytucjonalnie, również finansowo w ramach unijnych programów sektorowych i narodowych, regionalnych i operacyjnych, tworzonych według zaleceń Komisji Europejskiej (załącznik I).[14] Aktualną procedurą wspierającą rozwój społeczeństwa informacyjnego w Polsce jest *Strategia rozwoju społeczeństwa informacyjnego w Polsce do roku 2013*.[15] Wśród zasad i postulatów prorozwojowych znalazły się propozycje zwiększające poczucie bezpieczeństwa poprzez eliminację zagrożeń cyfrowych (teleinformatycznych). Dla podniesienia poziomu bezpieczeństwa, a także świadomości społecznej i kultury bezpieczeństwa, podjęto inicjatywy takie, jak: *Ku europejskiej polityce w zakresie wyposażenia obronnego* (marzec 2003), Europejska Strategia

---

nowej generacji. Szczególne znacznie technologii internetowych wiąże się z efektywną realizacją połączeń wykorzystywanych przez repozytoria danych i aplikacje o znaczeniu krytycznym dla działania biznesu (banki, giełdy) i wojska.

[10] IP/07/453 roczne sprawozdanie z realizacji inicjatywy i2010.

[11] GUS, Wykorzystanie technologii informacyjno-telekomunikacyjnych w przedsiębiorstwach w 2007r., Warszawa.

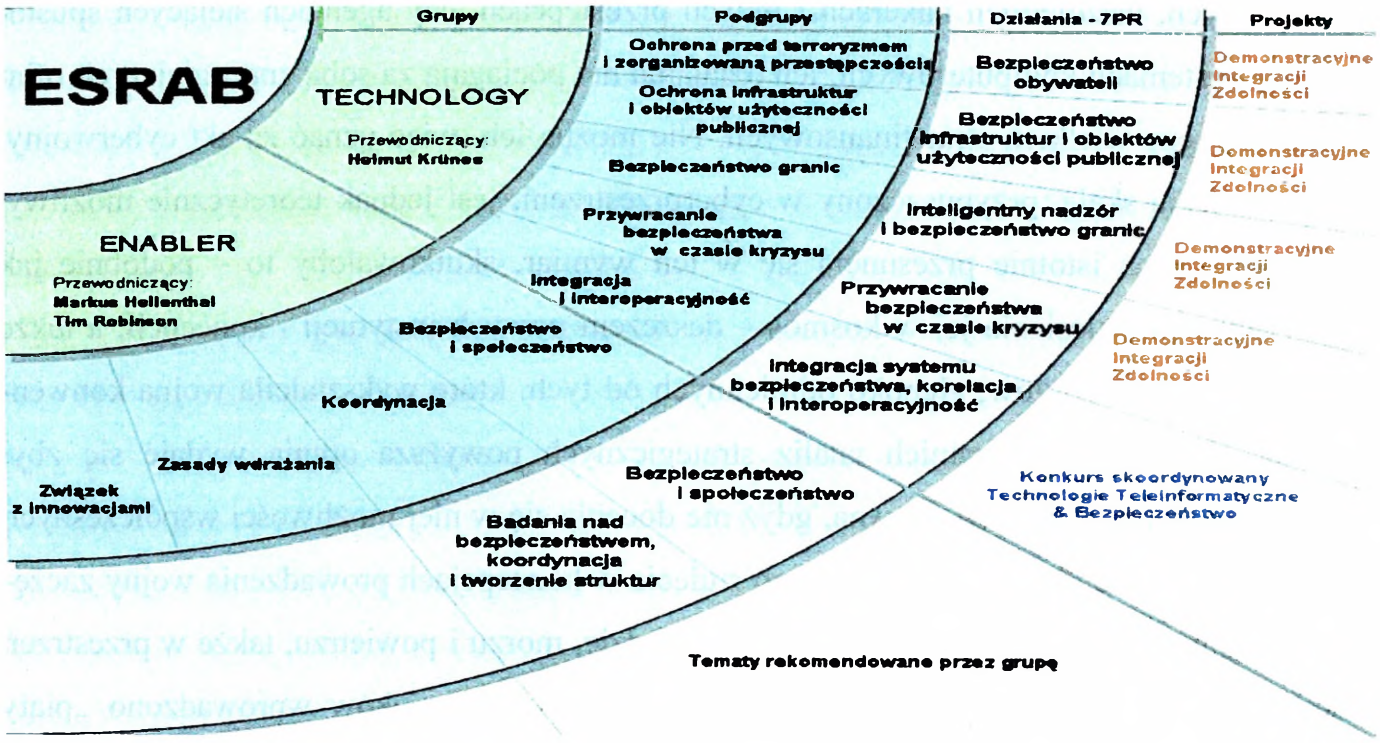
[12] P.Sienkiewicz, H.Świeboda, i in. *Bezpieczeństwo obywateli RP jako czynnik jakości* życia. AON, Warszawa 2009.

[13] Badania prowadzone w cyklu dwuletnim od 2000-2007 roku: Diagnoza społeczna. Warunki i jakość życia Polaków. J.Czapińskiego (red); P.Sienkiewicz, H.Świeboda, Społeczna percepcja zagrożeń bezpieczeństwa obywateli w warunkach globalnego społeczeństwa informacyjnego. AON Warszawa 2009.

[14] W ramach promocji Społeczeństwa Informacyjnego Komisja Europejska wydała wiele dokumentów zawierających zalecenia, konkretne programy i rozwiązania mające na celu przyśpieszenie transformacji krajów Unii Europejskiej do społeczeństwa informacyjnego, w których często podawane były przybliżone daty ich wdrożenia.

[15] http://www.mswia.gov.pl/strategia/; Dokument ten spójny jest z kluczowymi dokumentami określającymi strategiczne kierunki rozwoju Polski, takimi jak: Strategia rozwoju kraju 2007-2015, Narodowymi ramami odniesienia 2007-2013; Strategicznym planem rządzenia. Strategia ta uwzględnia priorytety europejskiej polityki w dziedzinie SI wynikające z założeń Strategii Lizbońskiej i inicjatyw e-Europe – społeczeństwo informacyjne dla wszystkich oraz jej kontynuacji i2010 – europejskie społeczeństwo informacyjne na rzecz wzrostu i zatrudnienia. http://ukie.gov.pl .

Bezpieczeństwa: *Bezpieczna Europa w lepszym świecie* (grudzień 2003) i Raport Grupy Osobistości: *Badanie na rzecz Bezpiecznej Europy* (marzec 2004), przygotowano podwaliny pod 7 program ramowy badań nad bezpieczeństwem wprowadzany od 2007 roku (rysunek 1-1).



Rysunek 1-1. Zakres badań nad bezpieczeństwem w ramach europejskiego programu badań nad bezpieczeństwem realizowanych przez Polską Platformę Bezpieczeństwa Wewnętrznego

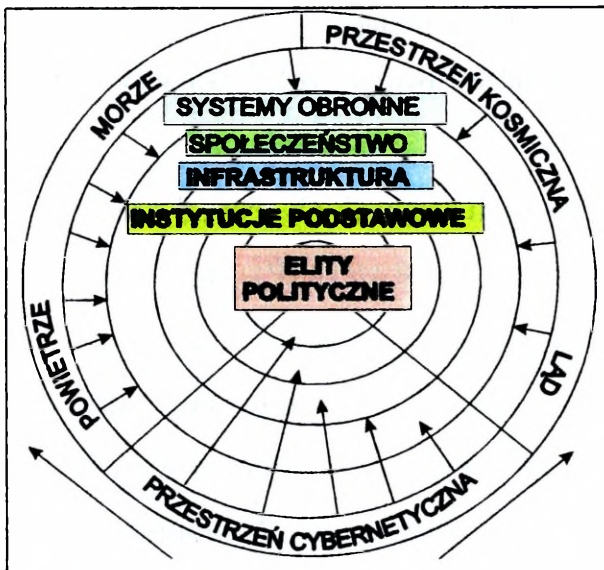
Źródło: Warsztaty, Polski Program Narodowych Badań Nad Bezpieczeństwem, WAT, Warszawa 28-29 listopada 2006.

Wraz z coraz większym uzależnieniem od technologii wszystkich niemal sfer życia społecznego, pojawiła się kategoria Krytycznej Infrastruktury Państwa (KIP), której naruszenie może spowodować istotne zagrożenia bezpieczeństwa państwa, obniżenie jego zdolności obronnych i rozwojowych.[16] W rezultacie globalizacji, państwa nie są w stanie istnieć i rozwijać się w izolacji, a gospodarki stają się coraz bardziej współzależne i podatne na wszelkiego rodzaju zaburzenia, co może sprzyjać powstawaniu sytuacji kryzysowych.[17] Nastąpiła zmiana charakteru zagrożeń oraz siły ich oddziaływania. Do katalogu już istniejących zagrożeń dla bezpieczeństwa, dołączają nowe, trudne do identyfikacji i interpretacji.

Dla nowego „pojałtańskiego ładu" (postmodernistycznego) oraz intensyfikacji procesów globalizacyjnych i wzrostu konfliktów o podłożu ekonomicznym, cywilizacyjnym (kulturowym), kategoria bezpieczeństwa informacyjnego stała się jednym z podstawowych elementów opisu sytuacji systemowych. Analiza sytuacji polityczno-gospodarczych w świecie oraz praktyka podejmowanych działań wykazują, że obecnie jak nigdy dotąd w historii, czynniki

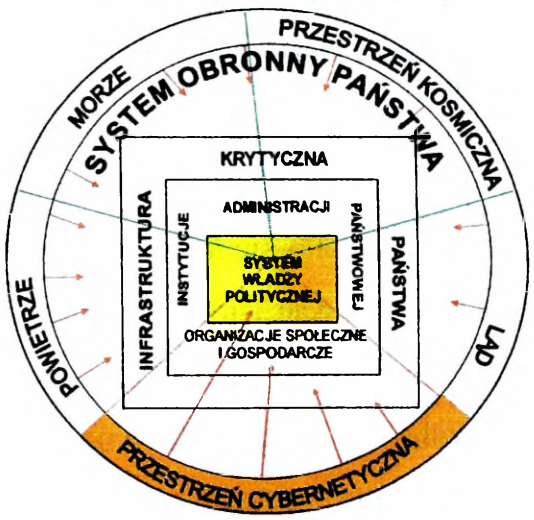
[16] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym. (Dz. U. Nr 89, poz. 590).
[17] G.Soros, *Nowy paradygmat rynków finansowych*, MT Biznes, Warszawa 2008.

informacyjne decydują o sile oddziaływania państw i ich bezpieczeństwie oraz stanie bezpieczeństwa międzynarodowego, a w szczególności o przewadze zarówno w biznesie jak i na polu walki. „Wojna wydaje się stać u bram cyberprzestrzeni. Choć ciągle słyszy się dziś o podstępnych, nastoletnich hakerach i innych przestępcach, czy agentach siejących spustoszenie w systemach komputerowych, ich działania nie pociągają za sobą znaczniejszych ofiar w ludziach, czy wielkich strat finansowych. Nie można ich, więc uznać za akt cyberwojny. Atak na wielką skalę, przypuszczony w cyberprzestrzeni, jest jednak teoretycznie możliwy, gdyby zaś wojna istotnie przesunęła się w ten wymiar, skutkowałoby to – podobnie jak w przypadku przeniesienia jej w kosmos – deszczem nowych instytucji i koncepcji, a także nowych typów konfliktów, głęboko odmiennych od tych, które wykształciła wojna konwencjonalna".[18] W świetle ostatnich analiz strategicznych powyższa opinia wydaje się zbyt ostrożna i cokolwiek konserwatywna, gdyż nie docenia się w niej możliwości współczesnych ICT. W ostatnim ćwierćwieczu ubiegłego stulecia w koncepcjach prowadzenia wojny zaczęto uwzględniać obok działań prowadzonych na lądzie, morzu i powietrzu, także w przestrzeń kosmiczną (koncepcja „gwiezdnych wojen"). Na przełomie wieków wprowadzono „piąty wymiar" konfliktów zbrojnych, a mianowicie „przestrzeń cybernetyczną" (rysunki 1-2, 1-3).



Rysunek 1-2. Przestrzeń zagrożeń militarnych w społeczeństwie informacyjnym

Źródło: J. Warden, *The Enemy as System*. 1995.



Rysunek 1-3. Przestrzeń zagrożeń bezpieczeństwa narodowego w społeczeństwie informacyjnym.

Źródło: P. Sienkiewicz, H. Świeboda, *Niebezpieczna przestrzeń cybernetyczna*. „Transformacje", 2006.

„Wpływ rewolucji informacyjnej na sferę militarną przejawia się w podstawowych obszarach: narzędziach wojny (technologii), prowadzeniu wojny (taktyka, operacje, organizacja sił zbrojnych) oraz charakterze wojny (strategia, cel, skala wojny)".[19]

---

[18] J.Baylis, J.Wirtz, C.Gray, E.Cohen, *Strategia we współczesnym świecie*. Wyd. UJ, Kraków 2009, s.168.

[19] Ł.Kamieński, Technologia i wojna przyszłości. Wokół nuklearnej i informacyjnej rewolucji w sprawach wojskowych. Wyd. UJ, Kraków 2009, s. 214.

Cyberprzestrzeń jest środowiskiem niezwykle złożonym, niedającym się zredukować wyłącznie do Internetu. To globalna przestrzeń służąca komunikacji „wszystkich ze wszystkimi". Świadomość możliwości zwiększania znacząco asymetrycznego działania, poprzez stworzenie swoich własnych sieci, by uzyskać przewagę informacyjną, skierowało uwagę na prace nad militarnym wykorzystaniem sieci, jako podstawy nowych koncepcji prowadzenia walki zbrojnej oraz działań innych niż wojna.[20] Technologie informacyjne umożliwiają szybsze zdobycie większej i bardziej szczegółowej wiedzy oraz wzrost tzw. świadomości operacyjnej, uzyskanie i utrzymanie dominacji informacyjnej, co przyjęto jako cel wyrażony w *Joint Vision 2020.* Połączenie sensorów, satelitów i radarów oraz sieci komputerowych i komunikacyjnych z nowoczesną bronią *high-tech* przyniosło „system systemów"[21].

Spowodowało to istotne zmiany w koncepcjach prowadzenia wojny, co przyniosło pojęcia „infowar", „cyberwar", „netwar", zaś jednym z ich przykładów jest tzw. sieciocentryczne pole walki (NCW).

Istotą tych koncepcji jest nie tylko silne uzależnienie efektywności bojowej (potencjału bojowego) sił zbrojnych od technologii teleinformatycznych, lecz założenie, iż możliwe jest osiągnięcie celów polityczno-militarnych w „cyberprzestrzeni" za pomocą środków informacyjnych. W szczególności, w wyniku „cyberataków" może nastąpić „paraliż" systemów łączności, rozpoznania i dowodzenia sił zbrojnych oraz innych komponentów systemu bezpieczeństwa narodowego, albo zakłócenie (destabilizacja, unieruchomienie) poszczególnych podsystemów krytycznej infrastruktury państwa (administracji służb publicznych, energetyki, bankowości, transportu i komunikacji, zaopatrywania w gaz, żywność, wodę).[22]

W celu uzyskania przewagi informacyjnej będą prowadzone działania w przestrzeni cybernetycznej dzięki powołanym w przyszłości wojskom informacyjnym. Wojska te będą integrowały siły i środki rozpoznania i walki elektronicznej, działań psychologicznych oraz działań w środowisku cybernetycznym. Implementacja w praktyce kształtujących się obecnie koncepcji sieciocentrycznego pola walki, w pełni usieciowi Siły Zbrojne RP, w perspektywie 20-25 lat. Systemy rozpoznania będą bazować na wielospektralnych aktywnych i pasywnych sensorach rozpoznawczych (cyfrowe kamery, skanery, radary, urządzenia elektroniczne).[23]

Również wyposażenie żołnierzy przyszłości będzie w coraz większym stopniu wykorzystywać elektronikę. Współcześnie armia jest wyposażona w sprzęt do komunikacji sateli-

---

[20] http://www.mon.gov.pl: Przewaga informacyjna będzie podstawowym warunkiem osiągnięcia sukcesu podkreśla się w Wizji Sił Zbrojnych RP 2030.

[21] W.Owens, *The Emerging U. S. System-of-System*. "Strategic Forum", No 63, 1996.

[22] P.Sienkiewicz, H.Świeboda, Sieci teleinformatyczne jako instrument państwa – walka informacyjna i szpiegostwo elektroniczne. PISM, Warszawa 2009.

[23] Wizja Sił Zbrojnych RP 2030.

tarnej, czujniki, mikroprocesory, wytrzymałe laptopy ze skomplikowanym oprogramowaniem.

Swoistość zagrożeń informacyjnych dla bezpieczeństwa polega na tym, że przeciwnik może być „niewidzialny", działający w przestrzeni wirtualnej, trudny do zidentyfikowania, wykorzystujący stosunkowo proste (ogólnie dostępne) środki techniczne itp.

Powstanie państw demokratycznych, internacjonalizacja systemów gospodarki i ich globalizacja, oddziaływanie na stosunki międzynarodowe podmiotów niepaństwowych - korporacji, wzrost znaczenia handlu zagranicznego i rozwój naukowo-techniczny, przesunęły sferę rywalizacji państw ze sfery militarnej na sferę ekonomiczną. Do rywalizacji na tym polu w coraz większym stopniu można wykorzystać technologiczne środki zagrożeń informacyjnych. Między czynnikami politycznymi, wojskowymi, społecznymi, ekonomicznymi, a czynnikami informacyjnymi istnieją coraz wyraźniejsze zależności, zaś do badania ich stosowane są techniki analizy korelacji.[24]

Problem zagrożeń informacyjnych dostrzeżony został i przedstawiony w Strategii Bezpieczeństwa Narodowego Rzeczpospolitej Polskiej z 22 lipca 2003 r.: *...coraz bardziej realne stają się dla Polski zagrożenia w sferze teleinformatycznej. Rośnie zagrożenie operacjami mającymi na celu dezorganizację kluczowych systemów informacyjnych instytucji rządowych oraz niektórych sfer sektora prywatnego, oddziałujących na system bezpieczeństwa państwa, a także operacjami związanymi z penetracją baz danych i prowadzeniem działań dezinformacyjnych.*[25]

W Strategii Bezpieczeństwa Narodowego z roku 2007, wśród zdiagnozowanych zagrożeń dla państwa, wymieniono jako niebezpieczne oddziaływania w cyberprzestrzeni, skierowane w systemy i sieci teleinformatyczne infrastruktury krytycznej. Zawarto nie tylko wskazówki dla skutecznej obrony przed jakąkolwiek ingerencją w systemy teleinformatyczne, proponując wprowadzanie odpowiednich polityk bezpieczeństwa. Uznano, że krytycznym problemem dla bezpieczeństwa państwa jest zapewnienie efektywnego i bezpiecznego systemu łączności dla administracji rządowej, sił zbrojnych i innych kluczowych instytucji państwowych, opartego na najnowocześniejszych technologiach telekomunikacyjnych i najwyższych standardach bezpieczeństwa. Uważa się, że państwo powinno dysponować własnym system łączności satelitarnej, wykorzystując przyznane geostacjonarne pozycje orbitalne.[26]

---

[24] M.Piątkowski, Wpływ technologii informatycznych i telekomunikacyjnych na wzrost gospodarczy i rozwój przedsiębiorstw w krajach posocjalistycznych. Rozprawa doktorska. WSPiZ im. L.Koźmińskiego, 2004.
[25] Strategia Bezpieczeństwa Narodowego RP, Warszawa 2003.
[26] Strategia Bezpieczeństwa Narodowego RP, Warszawa 2007.

Nadmierna wiara w możliwości pozytywnego rozwoju, którego główną siłą sprawczą jest postęp naukowo-techniczny oraz „scjentystyczne" postawy wobec środowiska naturalnego, przyniosły zjawisko niedostrzegania lub bagatelizowania niszczycielskich sił przyrody, wywołanych np. naruszeniem równowagi ekologicznej. Były one i są istotną przyczyną zagrożeń dla bezpieczeństwa rozwoju społecznego. Ponadto pojawiły się nowe – obok dotychczasowych i nie do końca zidentyfikowanych – choroby cywilizacyjne, będące istotną przyczyną zagrożeń dla zdrowia i życia ludzi. Rozwój globalnych systemów informacyjnych, to społeczeństwo informacyjne i gospodarka oparta na wiedzy, ale również nowe zagrożenia (np. cyberterroryzm). Nadal istotnym źródłem zagrożeń dla bezpieczeństwa są sprzeczności ideologiczne, polityczne, religijne, ekonomiczne i kulturowe współczesnego świata (syndrom „zderzenia cywilizacji"[27]). Skłania to do zmiany paradygmatu w badaniach nad zjawiskiem bezpieczeństwa i podjęcia wyzwania poznawczego: odejścia od redukcjonistycznego (monodyscyplinarnego) ujęcia i przejścia do ujęcia holistyczno-systemowego (interdyscyplinarnego)[28].

Fascynacje nowymi technologiami oraz ich wpływ na społeczeństwo we wszystkich sferach aktywności ludzkiej, interesujący jest również ze względu na aspekt bezpieczeństwa personalnego, a także percepcję zagrożeń. Niepokojące informacje o nowych zagrożeniach związanych ze stosowaniem nowych technologii, a także ich kumulacja, pojawianie się nowych zagrożeń, były powodem, że problemem bezpieczeństwa informacyjnego stał się przedmiotem badań systemowych podjętych w rozprawie.

Istnieje potrzeba badań systemowych nad zagrożeniami informacyjnymi, bezpieczeństwem informacyjnym i jego wpływem na stan bezpieczeństwa państwa. Wobec szybkości następujących zmian, których kierunek trudny jest do przewidzenia, człowiek często jest bezradny. Stworzenie procedur postępowania w celu neutralizacji bądź redukcji zagrożeń, w tym informacyjnych oraz zarządzania ryzykiem stało się, zatem koniecznością. Zagrożenia informacyjne podlegają zmianom ilościowym i jakościowym, co utrudnia, a niekiedy wręcz uniemożliwia ich antycypację. Dążenie do doskonalenia mechanizmów zapewniających poczucie bezpieczeństwa, zmusza do wnikliwej identyfikacji zagrożeń informacyjnych.

Bezpieczeństwo w cyberprzestrzeni zależy od sposobów ochrony informacji stosowanych w każdym kraju, przez każdą firmę i każdego użytkownika korzystającego z sieci. Aby ochronić się przed wyrafinowanymi technikami specjalnie tworzonymi przez przestępców sie-

---

[27] S.P.Huntington, *Zderzenie cywilizacji*. Wyd. Spectrum, Warszawa 2008.

[28] P.Sienkiewicz, H.Świeboda, Wybrane metody naukowych badań nad bezpieczeństwem i obronnością. AON, Warszawa 2008, s.31.

ciowych, trzeba wytworzyć globalną kulturę bezpiecznych zachowań w cyberprzestrzeni. Będzie to wymagać nie tylko odpowiednich działań prewencyjnych i prawnych, ale także bardzo wysokiego poziomu świadomości istniejących zagrożeń oraz wdrożenia zdecydowanych środków zaradczych, opartych na cyfrowych technikach komunikacyjnych.[29] Stanowi to również wyzwanie dla edukacji dla bezpieczeństwa.

1.2. Przedmiot badań

Świadomość potrzeby podjęcia badań nad zjawiskiem, którego istota została wyrażona w tytule rozprawy spowodowała konieczność przyjęcia założeń wyjściowych, ograniczeń i wymagań, zgodnie z postulatami racjonalizmu metodologicznego.[30] Zakres pojęciowy wynikający z podjętego tematu i sformułowanego problemu badawczego, wymagał konkretyzacji i koniecznych redukcji dla określenia przedmiotu badań.

W celu określenia przedmiotu badań przyjęto swoistą hierarchię: zjawisko (byt, wyróżniony fragment rzeczywistości będący przedmiotem poznania), system (złożony obiekt, w którym zjawisko się realizuje, bądź stanowi siłę sprawczą mającą wpływ na sposoby przejawiania się zjawiska) i procesy (realizowany w systemie ciąg zdarzeń będących przyczyną bądź skutkiem zmian zjawiska).[31]

Tak pojmowany przedmiot badań znalazł w rozprawie następującą konkretyzację (rysunek 1-4):

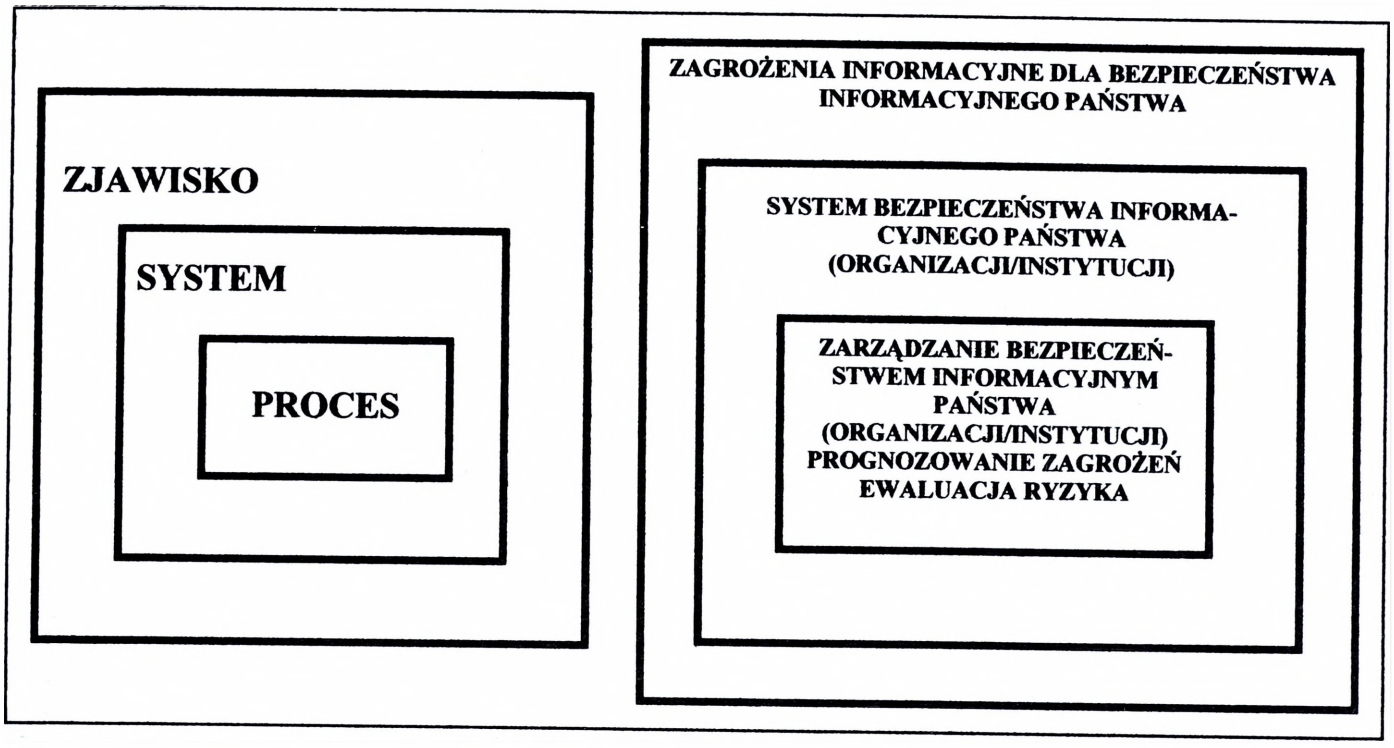
- zjawisko: ZAGROŻENIA INFORMACYJNE dla bezpieczeństwa państwa (organizacji, inwestycji);
- system: SYSTEM BEZPIECZEŃSTWA INFORMACYJNEGO państwa (organizacji, instytucji);
- procesy: ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACYJNYM państwa (organizacji, instytucji).

---

[29] Orędzie Yoshio Utsumi, Sekretarza Generalnego Międzynarodowego Związku Telekomunikacyjnego (ITU) z okazji Światowego Dnia Telekomunikacji 17 maja 2006.

[30] Według P.Sienkiewicza cechami konstytuwnymi racjonalizmu metodologicznego są: (1) Logiczne uporządkowanie (dziedzin myśli, pojęć, twierdzeń, argumentów). (2) Oparcie wiedzy na doświadczeniu. (3) Esencjalizm (wnikanie w „istotę", analiza, szukanie tego, co ważne). (4) Równowaga między wiedzą intersubiektywną, a indywidualnymi przekonaniami. (źródło: *Wybrane metody naukowych badań nad bezpieczeństwem i obronnością*. AON, Warszawa 2008, s.34).

[31] W trakcie dyskusji na seminarium doktoranckim przyjęto, jako kategorie opisu przedmiotu badań: zjawiska, systemy, procesy, zdarzenia.



Rysunek 1-4. Ogólny model przedmiotu (obiektu) badań i jego konkretyzacja
Źródło: opracowanie własne.

System bezpieczeństwa informacyjnego, w obszarze związanym z rozwojem ICT, jest ustawowo (w niektórych dziedzinach) uregulowanym prawnie elementem systemu bezpieczeństwa narodowego.[32] Zmieniające się uwarunkowania technologiczne i polityczno-gospodarcze sprawiają, że problem ten jest stale aktualny, a wydarzenia ostatnich lat sprawiły, że wzrosły obawy przed coraz częstszymi atakami z wykorzystaniem cyberprzestrzeni. Pojawił się cyberterroryzm jako realne zagrożenia bezpieczeństwa.[33] Zagrożeń informacyjnych przybywa, zaś formy klasycznych zagrożeń ewoluują stając się coraz bardziej wyrafinowanymi narzędziami (tabela 2-4 i inne oraz załącznik V).

Zagrożenia informacyjne jako przedmiot badań, eksplorowano z wykorzystaniem dwóch różnych metod i technik badawczych. Jedną grupę tworzą metody oparte na modelach formalnych (szeregi czasowe, sztuczne sieci neuronowe), natomiast drugą - techniki heurystyczne (scenariusze, oceny ekspertów). Ponadto, ze względu na społeczny aspekt zjawiska, zastosowano technikę wywiadów i ankietowania. W pierwszym etapie przyjętej procedury badawczej, skoncentrowano uwagę na zagrożeniach informacyjnych będących bezpośrednim skutkiem rozwoju ICT (prognozowanie ataków na bezpieczeństwo sieci teleinformatycz-

---

[32] Obszar ten regulują ustawy, np.: Ustawa z dnia 29 listopada 1990r. o łączności ze zmianami w 1995r. (Dz.U. 1995r., nr 117, poz.564, tekst jednolity); ustawa z dnia 29 grudnia 1992r. o radiofonii i telewizji (Dz.U. z 1993r., nr 7, poz. 34); Ustawa o prawie autorskim (Dz.U. 1994r., nr 24, poz. 83); Ustawa o ochronie danych (Dz.U.1997r., nr133, poz.883); ustawa o świadczeniu usług droga elektroniczną (Dz.U. 2002r., nr144, poz.1204); Ustawa o podpisie elektronicznym (Dz.U. 2001r., nr 130, poz.1450).

[33] Por. T.Jemioło (red.) Cyberteroryzm nowe wyzwania XXI wieku. Warszawa 2009; E. Lichocki, Model systemu zarządzania kryzysowego w warunkach zagrożeń cyberterrorystycznych dla bezpieczeństwa informacyjnego Sił Zbrojnych Rzeczypospolitej Polskiej. rozprawa doktorska, AON, Warszawa 2009.

nych). Drugi eksperyment odnosi się do prognozowania poziomu zagrożeń (opinia społeczna, eksperci) w kontekście tzw. „społecznego wzburzenia"[34].

Przestrzeń badawczą zredukowano do obszaru Polski, chociaż nie można było uniknąć analizy bliższego i dalszego otoczenia RP. Czas analizy wyznaczają pierwsze przejawy zagrożeń informacyjnych, w kontekście społeczeństwa informacyjnego i „nowej przestrzeni bezpieczeństwa", które są skutkiem rozwoju ICT, oraz przyjęty horyzont prognozowania (do roku 2015). Czas ten przyjęto jako racjonalny dla prognozowania możliwych i prawdopodobnych zagrożeń, aczkolwiek ze świadomością, że ze względu na trafność prognoz (błędy, dokładność), sens mają przede wszystkim prognozy krótkookresowe (horyzont: miesiąc, kwartał, rok, 2-3 lata).

Na konkretyzację przedmiotu badań niewątpliwy wpływ miały, wspomniane we wstępie, inicjatywy UE[35] i NATO[36] oraz przyjęta *Strategia Rozwoju Polski do roku 2030*, a także założenia *Rządowego Programu Ochrony Cyberprzestrzeni RP na lata 2009-2011* z marca 2009 roku.

1.3. Cel badań

Badania naukowe w obszarze bezpieczeństwa państwa, ze względu na rozległość powiązań strukturalno-funkcjonalnych oraz prawnych ograniczeń działających w niej systemów, są niezwykle złożone. Wynika to ze złożoności i różnorodności tych systemów, które charakteryzują się:

- wielofunkcyjnością wynikającą z faktu, że ze względu na zasady bezpieczeństwa formułuje się zbiory różnorodnych wymagań, które grupuje się stosownie do obszaru przyszłego, planowanego funkcjonowania systemów;
- złożonością struktury systemów działania (organizacji, instytucji, państwa);
- dużą liczbą podsystemów wchodzących w skład badanych systemów, pozostających w różnych relacjach (stosunkach, sprzężeniach) oraz dużą liczbą wielorakich relacji z bliższym i dalszym otoczeniem;
- specyfiką i dynamiką procesów zachodzących w systemach oraz zewnętrznych oddziaływań (wymuszeń), o charakterze losowym (stochastycznym):

---

[34]Pojęciem tym, za P.Sandamnem, (*Responding to Community Outrage: Strategies effective Risk Communication*, American Industrial Hyguene Association Fairfax. 1997), posługuje się J.Wolanin (*Zarys teorii bezpieczeństwa obywateli*. Warszawa 2005).

[35] Warto wspomnieć o Konwencji o cyberprzestępczości. Budapeszt, 23.11.2003r.

[36] Zmiany w podejściu do cyberterroryzm zapowiedziano na nieformalnym spotkaniu ministrów obrony państw NATO, które odbyło się w lutym 2009 roku w Krakowie. Zapowiedziano włączenie zagrożenia cyberterroryzmem i bezpieczeństwa informatycznego do przygotowywanej nowej koncepcji strategicznej Sojuszu. (słowa Jaapa de Hoop Scheffera).

- dużym zasięgiem przestrzennym systemów, brakiem jednoznaczności;
- rozproszonym systemem sterowania procesami informacyjno-decyzyjnymi (np. wiele ośrodków decyzyjnych, brak jasnego zakresu odpowiedzialności itp.);
- rozwiniętą, otwartą i rozległą teleinformatyczną infrastrukturą, znajdującą się w stanie permanentnego rozwoju.

Podjęte badania miały także zapewnić osiągnięcie typowych celów eksploracji, a mianowicie:[37]

- zaspokojenie ciekawości badacza i jego pragnienia lepszego zrozumienia przedmiotu badań;
- zbadanie możliwości podjęcia szerszych badań;
- opracowanie metod, które zostaną użyte w dalszych badaniach.

Z tak określonych celów eksploracji, wynikają zgodnie z ogólną procedurą przedsięwzięć badawczych, dwa podstawowe cele badawcze: poznawczy i utylitarny.

Cel poznawczy dotyczy analizy obserwowanych zjawisk: poziomu zagrożeń informacyjnych i ich negatywnych skutków rozpatrywanych w aspekcie aktualnej polityki bezpieczeństwa informacyjnego, a także poziomu społecznej percepcji zagrożeń informacyjnych w kontekście tzw. „społecznego wzburzenia". W obszarze poznawczym lokalizują się badania nad przydatnością metod prognozowania zagrożeń informacyjnych (modeli prognozowania), a w szczególności wykorzystania analizy szeregów czasowych, sztucznych sieci neuronowych, scenariuszy i badań sondażowych opinii społecznej, a także ocen ekspertów.

Cel utylitarny wiąże się z potrzebą określenia kierunków i sposobów kreowania i wdrażania metod prognozowania i ewaluacji ryzyka do polityki bezpieczeństwa informacyjnego na różnych poziomach struktury państwa.

Główny cel badań to opracowanie modelu systemu zarządzania bezpieczeństwem informacyjnym, wykorzystującego analizę systemową sytuacji zagrożeń informacyjnych, wraz z metodami prognozowania zagrożeń i ewaluacji ryzyka.

Z celu głównego wynikają cele szczegółowe, a mianowicie:

- identyfikacja zagrożeń bezpieczeństwa informacyjnego;
- określenie relacji między bezpieczeństwem informacyjnym a bezpieczeństwem państwa (narodowym);
- określenie poziomu percepcji ryzyka zagrożeń informacyjnych;
- opracowanie metodyki diagnozowania i prognozowania zagrożeń informacyjnych;

---

[37] E. Babbie, *Badania społeczne w praktyce*. Wydawnictwo Naukowe PWN, Warszawa 2005, s.111.

- opracowanie metodyki analizy i oceny ryzyka zagrożeń informacyjnych;
- opracowanie ogólnego modelu systemu zarządzania bezpieczeństwem informacyjnym na potrzeby systemu zarządzania bezpieczeństwem narodowym RP.

Powyżej przyjęte cele pracy stanowią podstawę do sformułowania szczegółowych problemów badawczych, które określają obiekty analiz empirycznych oraz determinują wybór technik badawczych, oceny jakości metod prognozowania zagrożeń, oraz formułowanych propozycji modelowych.

1.4. Problemy badawcze i hipotezy robocze

Podstawowym warunkiem podejmowania wszelkich badań naukowych jest uświadomienie sobie problemów oraz hipotez roboczych, określających w sposób możliwie precyzyjny cel i zakres planowanych przedsięwzięć badawczych. Bez wyraźnie sformułowanych problemów i hipotez trudno byłoby o postęp lub nowe odkrycia w dziedzinie interesujących nas faktów i zjawisk.[38]

Problem jest rodzajem zadania (sytuacji), którego podmiot nie może rozwiązać za pomocą posiadanego zasobu wiedzy. Jego rozwiązanie jest możliwe dzięki czynności myślenia produktywnego, które prowadzi do wzbogacenia wiedzy podmiotu.[39] Problem badawczy – to tyle, co, pewne pytanie lub zespół pytań, na które odpowiedzi ma dostarczyć badanie.[40] Sformalizowane w formie pytań problemy powinny wyczerpywać zakres naszej niewiedzy, zawarty w temacie badań i spełniać warunki precyzyjnego określenia obszaru, przedmiotu badawczego oraz zdefiniowanie zależności między zidentyfikowanymi zmiennymi.

Główny problem badawczy sformułowano następująco:

Jaki model systemu zarządzania bezpieczeństwem informacyjnym zapewni właściwą identyfikację, diagnozę i prognozowanie zagrożeń informacyjnych bezpieczeństwa RP oraz racjonalne przeciwstawianie się im?

Zdefiniowany problem badawczy pozwolił na wyodrębnienie obszarów badań, w których zlokalizowano szczegółowe problemy badawcze określające kierunki i zakres badań:

1. **Współczesne zagrożenia informacyjne dla bezpieczeństwa państwa**
   - Jaka jest istota zagrożeń informacyjnych?
   - Jakie realne sytuacje stanowią zagrożenia informacyjne dla bezpieczeństwa narodowego?

---

[38] Por. M.Łobocki, *Metody badań pedagogicznych*, Warszawa 1982, s. 55.
[39] Por. J.Kozielecki, *Rozwiązywanie problemów*, Warszawa 1969.
[40] S.Nowak: Metodologia badań socjologicznych, Warszawa 1970.

- W jakich sytuacjach cyberterroryzm może stanowić zagrożenie bezpieczeństwa narodowego?
- Czy w społeczeństwie istnieje świadomość zagrożeń informacyjnych dla bezpieczeństwa narodowego?
- Czy zagrożenia bezpieczeństwa obywateli wpływają na jakość ich życia?
- Jak jest postrzegany wpływ bezpieczeństwa na jakość życia?
- W jakim zakresie (stopniu) zagrożenia informacyjne wpływają na poziom bezpieczeństwa narodowego RP?

2. **Prognozowanie zagrożeń informacyjnych**
   - Jakie procedury analityczno-ocenowe i decyzyjne należy stosować dla rozpoznawania zagrożeń dla bezpieczeństwa informacyjnego państwa?
   - Czy analiza szeregów czasowych może być skuteczną metodą prognozowania zagrożenia (typu wirusy, trojany, spam)?
   - Które z modeli prognozowania są adekwatne i w jakich warunkach oraz jaki horyzont czasowy jest właściwy dla wyznaczanych prognoz zagrożeń informacyjnych?
   - Jakie warunki muszą być spełnione, by można było stosować w praktyce zarządzania bezpieczeństwem, przyjęte modele prognostyczne?
   - Jaka jest skala świadomości zagrożeń informacyjnych w społeczeństwie?
   - Czy metoda scenariuszy jest właściwą (racjonalną) metodą i czy może być stosowana w prognozach zagrożeń informacyjnych?
   - W jakich warunkach należy stosować technikę scenariuszy i jakie może być praktyczne ich zastosowanie?
3. **Zarządzanie ryzykiem zagrożeń informacyjnych dla bezpieczeństwa narodowego**
   - Jakie interpretacje oraz metody (modele) ewaluacji ryzyka należy stosować?
   - Czy jest możliwe stworzenie map ryzyka zagrożeń informacyjnych na potrzeby różnych szczebli zarządzania bezpieczeństwem?
   - Jaka jest użyteczność opracowanych metodyk (metod) prognozowania zagrożeń informacyjnych i ewaluacji ryzyka w sytuacjach zarządzania bezpieczeństwem informacyjnym państwa?

- Czy przyjęte metodyki prognozowania zagrożeń informacyjnych i ewaluacji ich ryzyka mogą znaleźć zastosowanie w analizach bezpieczeństwa informacyjnego KIP?

4. **Model zarządzania bezpieczeństwem informacyjnym państwa**
   - Czy w oparciu o dokonane analizy możemy w wybranych obszarach zbudować model zarządzania bezpieczeństwem informacyjnym państwa?
   - Czy metodyki prognozowania zagrożeń informacyjnych mogą być zastosowane w systemie zarządzania bezpieczeństwem informacyjnym RP?

Przedstawione powyżej problemy i kwestie szczegółowe nie wyczerpują wszystkich zagadnień, które należało podjąć realizując projektowane badania. Uzyskanie odpowiedzi na powyższe pytania (problemy) wiązało się z:

- dokonaniem analizy występujących zagrożeń informacyjnych w obszarze militarnym i niemilitarnym środowiska bezpieczeństwa narodowego RP;
- przeprowadzeniem badań z wykorzystaniem pakietu Statistica i Excel w celu:
  - określenia świadomości zagrożeń informacyjnych w społeczeństwie „społeczne wzburzenie" (jako uogólniony wskaźnik społecznej percepcji zagrożeń informacyjnych);
  - weryfikacji metod prognozowania zagrożeń informacyjnych;
- stworzeniem spójnej metodyki ewaluacji ryzyka zagrożeń informacyjnych dla bezpieczeństwa narodowego.

Sformułowane problemy skłaniają do przyjęcia określonych hipotez. Hipotezy stanowią stwierdzenia, co do których istnieje pewne prawdopodobieństwo, że są właściwym rozwiązaniem sformułowanych poprzednio problemów badawczych. Inaczej mówiąc, są oczekiwanymi przez badacza wynikami planowanych badań.[41] Tworzy się je określając związek między zmiennymi zależnymi i niezależnymi. Hipotezy badawcze powinny być: (1) jasno sformułowane, (2) konkretne (specyficzne), (3) poddawać się weryfikacji empirycznej za pomocą metod badawczych oraz (4) nie zawierać sądów wartościujących.[42]

Sformułowano następujące hipotezy:

---

[41] „Hipotezą nazywa się wszelkie twierdzenia częściowo tylko uzasadnione, przeto także wszelki domysł, za pomocą, którego tłumaczymy dane faktyczne, a więc też i domysł w postaci uogólnienia, osiągniętego (...) na podstawie danych wyjściowych". T.Kotarbiński, *Elementy teorii poznania, logiki formalnej i metodologii nauk*. Wrocław 1961.

[42] C.Frankfort-Nachmias, D.Nachmias, *Metody badawcze w naukach społecznych*, Wyd. Zysk i S-ka, Poznań 2001, s.78.

Hipotezy ogólne:

1. Wzrost zagrożeń informacyjnych może powodować obniżenie poziomu bezpieczeństwa informacyjnego państwa.
2. Obniżenie poziomu bezpieczeństwa informacyjnego państwa może powodować obniżenie poziomu bezpieczeństwa narodowego.
3. Bezpieczeństwo informacyjne jest istotnym czynnikiem jakości życia obywateli.[43]

Hipotezy dotyczące diagnozy polskiego systemu bezpieczeństwa informacyjnego:

4. W polskim systemie bezpieczeństwa informacyjnego pomimo wprowadzanych zmian legislacyjnych, strukturalnych, organizacyjnych i technicznych, nadal występują liczne dysfunkcjonalności, a także braki w świadomości społecznej zagrożeń w tym obszarze.
5. Stosunkowo duża liczba stwierdzonych naruszeń bezpieczeństwa informacyjnego świadczy o braku lub niskiej efektywności technologii bezpieczeństwa, ochrony, bądź metod analizy zagrożeń oraz mechanizmów ich wprowadzania.

Hipotezy dotyczące możliwości wdrożenia narzędzi wspomagających politykę bezpieczeństwa informacyjnego państwa:

6. Zastosowanie nowoczesnych metod pomiaru, analizy i oceny jakości bezpieczeństwa informacyjnego stwarza możliwość prowadzenia racjonalnej polityki bezpieczeństwa oraz zapewnienia pożądanego poziomu bezpieczeństwa informacyjnego państwa.

Hipotezy dotyczące zakresu i sposobu realizacji przedsięwzięć zapewniających bezpieczeństwo informacyjne państwa:

7. Upowszechnienie nowoczesnych metod i narzędzi pomiaru, analizy i oceny zagrożeń bezpieczeństwa informacyjnego, przy jednoczesnym właściwym doborze treści, form i środków kształcenia i szkolenia jest jednym z podstawowych warunków zapewnienia bezpieczeństwa informacyjnego państwa.

Ze względu na wielowątkowość badań, doboru i kwalifikowania zmiennych dokonano, kierując się zasadą stosowalności i skuteczności w przyjętej sytuacji problemowej oraz zgodnie z metodologią określającą, *że* „przez zmienne niezależne rozumie się czynniki powodujące określone zmiany w innych czynnikach (zmiennych), a przez zmienne zależne – czynniki, podlegające wyraźnym wpływom ze strony zmiennych niezależnych".[44]

---

[43] W znanych badaniach jakości życia nie uwzględnia się *explicite* wpływu bezpieczeństwa.
[44] M.Łobocki, *Metody,...*, 1978, op.cit., s.48.

Zdefiniowanie przedmiotu badań i zinterpretowanie charakteru zależności pomiędzy zagadnieniami określonymi jako szczegółowe problemy badawcze, pozwalają wyróżnić jako zmienną zależną: bezpieczeństwo narodowe. Ponieważ założono, że zagrożenia informacyjne są przyczyną zmian w poziomie bezpieczeństwa narodowego, jako zmienną niezależną przyjęto zagrożenia informacyjne, będące przedmiotem analizy zagrożeń i prognozowania. Za zmienną pośredniczącą, uznano ryzyko negatywnych skutków dla bezpieczeństwa narodowego, występowania zagrożeń informacyjnych.

Złożony, interdyscyplinarny charakter problemu badawczego, wymusza przyjęcie jednolitej podstawy metodologicznej w postaci „metametody" - analizy systemowej, gwarantującej spełnienie warunków założonych w hipotezach.[45]

1.5. Metody, techniki i narzędzia badawcze

W obszarze nauk społecznych, do których należą nauki wojskowe, od dawna stosowano podejście (ujęcie) systemowe, choć nie zawsze świadomie i konsekwentnie.[46] Korzysta się również z dorobku innych nauk dostosowując narzędzia badań do potrzeb, np. statystyki, modelowania matematycznego, technik sondażowych, ankiet, itp.

Tabela 1-1. Różnice między ujęciem systemowym a ujęciem tradycyjnym

UJĘCIE ANALITYCZNE (REDUKCJONISTYCZNE)	UJĘCIE SYSTEMOWE
• Wyodrębnienia: koncentruje się na elementach • Bada charakter relacji • Opiera się na danych szczegółowych • Modyfikuje precyzyjne i szczegółowe, ale trudne do zastosowania parametry • Uwzględnia oddziaływania liniowe i słabe • Znajomość szczegółów, cele słabo określone • Prowadzi do działania „zalgorytmizowanego" wykorzystującego znajomość szczegółów • Prowadzi do nauczania monodyscyplinarnego"	• Łączy: koncentruje się na relacjach między elementami • Bada efekty relacji • Opiera się na ogólnym modelu • Modyfikuje grupy parametrów • Modele ogólne, ale dające się wykorzystać przy podejmowaniu decyzji • Uwzględnia oddziaływania nieliniowe i silne • Znajomość celów, szczegóły płynne • Prowadzi do działania celowego • Prowadzi do nauczania „multi i interdyscyplinarnego"

Źródło: P.Sienkiewicz, H.Świeboda, *Metodologia badań nad bezpieczeństwem*. AON, Warszawa 2008.

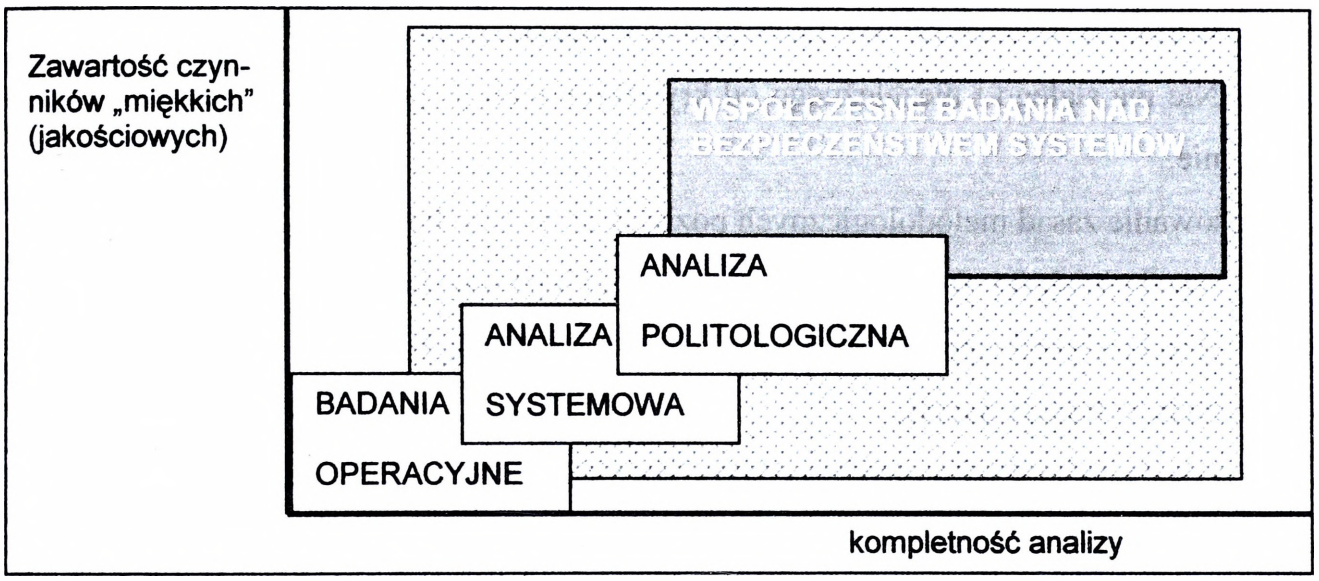
Współczesne badania systemowe wywodzą się z niejednego źródła. Kluczową kategorią jest kategoria SYSTEMU, czyli takiego obiektu, który rozpatrywany jest jako CAŁOŚĆ, tworzoną przez zbiór ELEMENTÓW i RELACJI między nimi. Istotnym postulatem badań

[45] P.Sienkiewicz, *Analiza systemowa*. Bellona, Warszawa 1995.

[46] P.Sienkiewicz, Współczesne badania systemowe. Cz.II – teorie, analiza, inżynieria. Transformacje (w druku).

systemowych jest HOLIZM zakładający, że rzeczywistość postrzegana jest w sposób całościowy i, że badanie całości ma sens.

Badanie sytuacji charakteryzujących się niepewnością i ryzykiem, a w szczególności sytuacji kryzysowych i konfliktowych, odbywało się w ostatnim półwieczu na różnych poziomach ogólności (konkretności). W latach 40 ubiegłego wieku nadzieje wiązano z badaniami operacyjnymi, których rozwinięciem stała się następnie analiza systemowa (w ujęciu RAND), a z ich dorobku czerpie inspiracje współczesna analiza politologiczna (rysunek 1-5).[47] Nie oznacza to rezygnacji z ujęć tradycyjnych (tabela 1-1).[48]



Rysunek 1-5. Metody badań nad bezpieczeństwem (konfliktami, zagrożeniami) politycznym
Źródło: na podstawie P. Sienkiewicz, *Metodologia badań nad bezpieczeństwem* [w:] *Wybrane metody badań nad obronnością*. AON, Warszawa 2008, s.36.

Grupa problemów związanych z bezpieczeństwem jest bezpośrednio warunkowana wzrastającą złożonością, swoistym „splątaniem" różnych podmiotów dążących do często bardzo różnych celów. Analiza politologiczna, której przedmiotem jest bezpieczeństwo narodowe (międzynarodowe), korzysta np. z modeli teorii gier i symulacji komputerowej, metod analizy ryzyka, techniki scenariuszy itp. – twórczo rozwijanych w ramach badań operacyjnych i analizy systemowej. Podobne zależności i wpływy bez trudu można dostrzec analizując współczesne badania nad bezpieczeństwem ekonomicznym i biznesowym, ekologicznym, informacyjnym itp.[49]

---

[47] P.Sienkiewicz, H.Świeboda, *Wybrane,...*,2008, op.cit., s.37.
[48] P.Sienkiewicz, H.Świeboda, Perspektywy badań systemowych nad bezpieczeństwem. Międzynarodowa konferencja naukowa nt. Bezpieczeństwo wymiar współczesny oraz perspektywy badań. Kraków 2008.
[49] P.Sienkiewicz, *Analiza,...*,1995, op.cit., s.22.

Założenia i ograniczenia

Podstawę metodologiczną badań systemowych stanowią następujące zasady:[50]

1. Badane są pewne zorganizowane całości, dobrze wyodrębnione ze środowiska (otoczenia). Całości te są określane jako systemy.
2. System może być podzielony na części (podsystemy) i ich relacje na wiele różnych sposobów - nie ma podziału uniwersalnego.
3. Każdy podział systemu na części daje pewien jego obraz. Podział zależy, więc od tego, które cechy systemu lub jego elementy stanowią przedmiot badań.
4. Własności składników systemu nie mogą być badane niezależnie od systemu, w którym występują. Nie ma własności niezależnych od środowiska (otoczenia). Nie ma stałego i niezależnego od kryterium analizy, podziału na system i otoczenie.

Stosowanie zasad metodologicznych pozwala na wyodrębnianie systemu wg założeń:

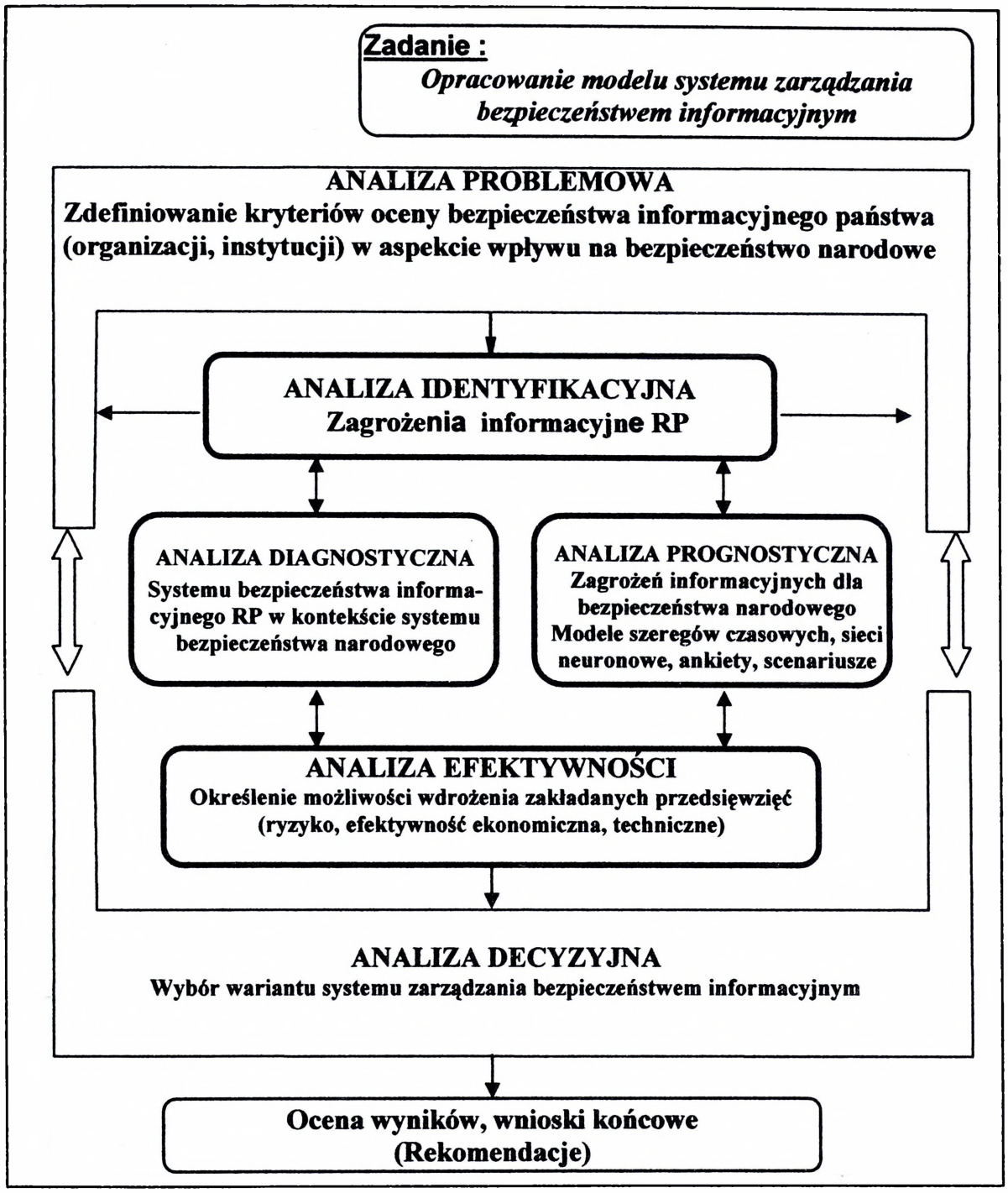
1) zasada ścisłości określania granic systemu i jego otoczenia;
2) zasada niezmienności dokonanego rozróżnienia między systemem a jego otoczeniem w trakcie badań;
3) zasada zupełności podziału systemu (na podsystemy);
4) zasada rozłączności rozpatrywanych systemów (i ich podsystemów);
5) zasada funkcjonalności, czyli podziału systemu na podsystemy ze względu na rodzaj spełnianych przez nie funkcji w całości.

Zaletą zastosowania analizy systemowej jest wprowadzenie znacznej dozy obiektywizmu do badania procesu bezpieczeństwa informacyjnego, który jest w znacznej mierze subiektywny, uwzględnianie szerszego kontekstu badań, a także uwzględnianie czynnika niepewności i ryzyka. Ponadto analiza systemowa pozwala skoncentrować uwagę na skutkach działania, co może sprzyjać ujawnieniu nieprzewidzianych następstw analizowanego zagrożenia.

Złożoność i obszerność badań wymagała zastosowania analizy systemowej jako meta metody spinającej poszczególne etapy badań. Przyjęto, że analiza systemowa jest zbiorem metod i technik analitycznych, oceanowych i decyzyjnych służących racjonalnemu rozwiązywania systemowych sytuacji decyzyjnych przede wszystkim w warunkach niepewności i ryzyka.[51] Dlatego dla zrealizowania głównego celu badawczego przyjęto schemat postępowania przedstawiony na rysunkach 1-6, 1-7 i 1-8.

---

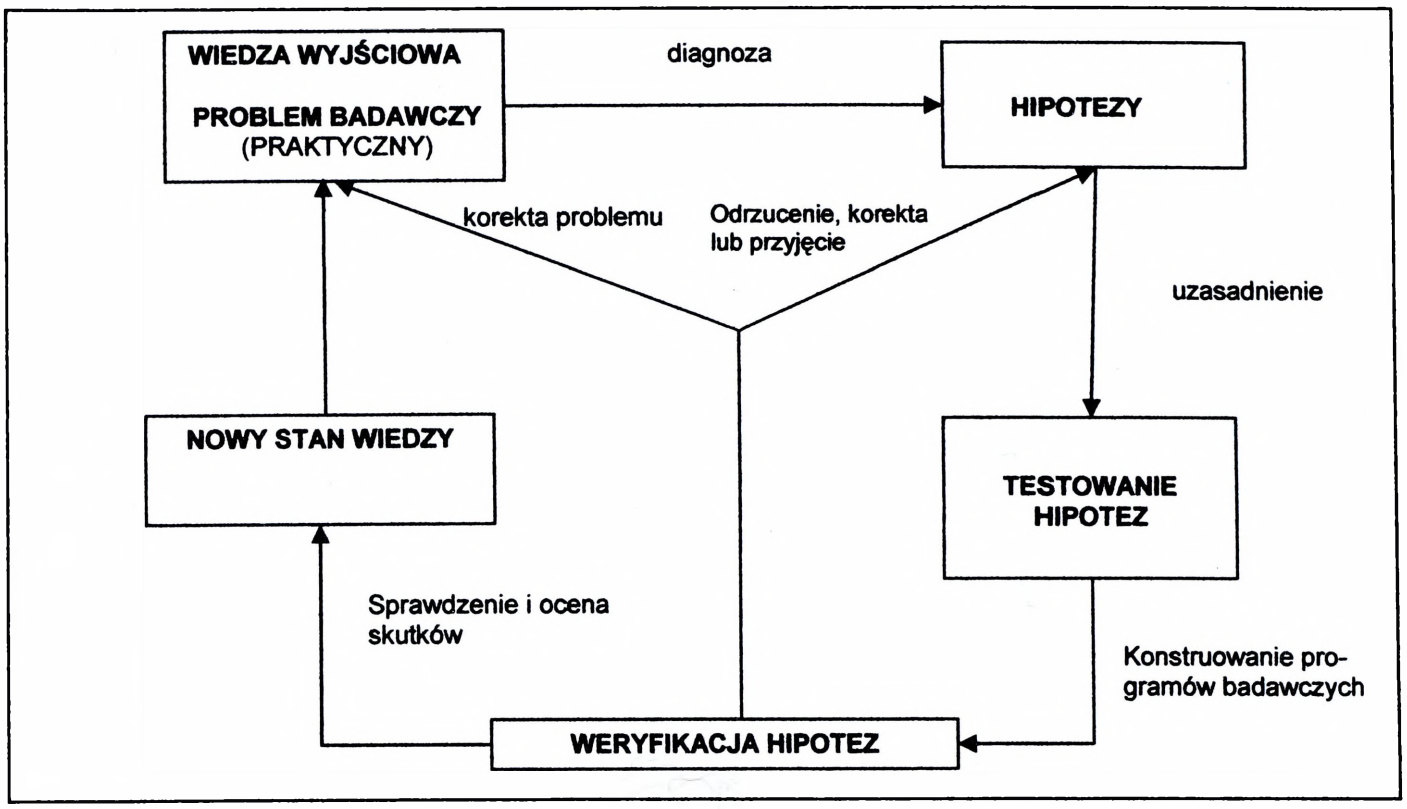
[50] Ibidem, s.38.
[51] P.Sienkiewicz, *Analiza,...*, 1995, op.cit., s.37.



Rysunek 1-6. Analiza systemowa sytuacji problemowej

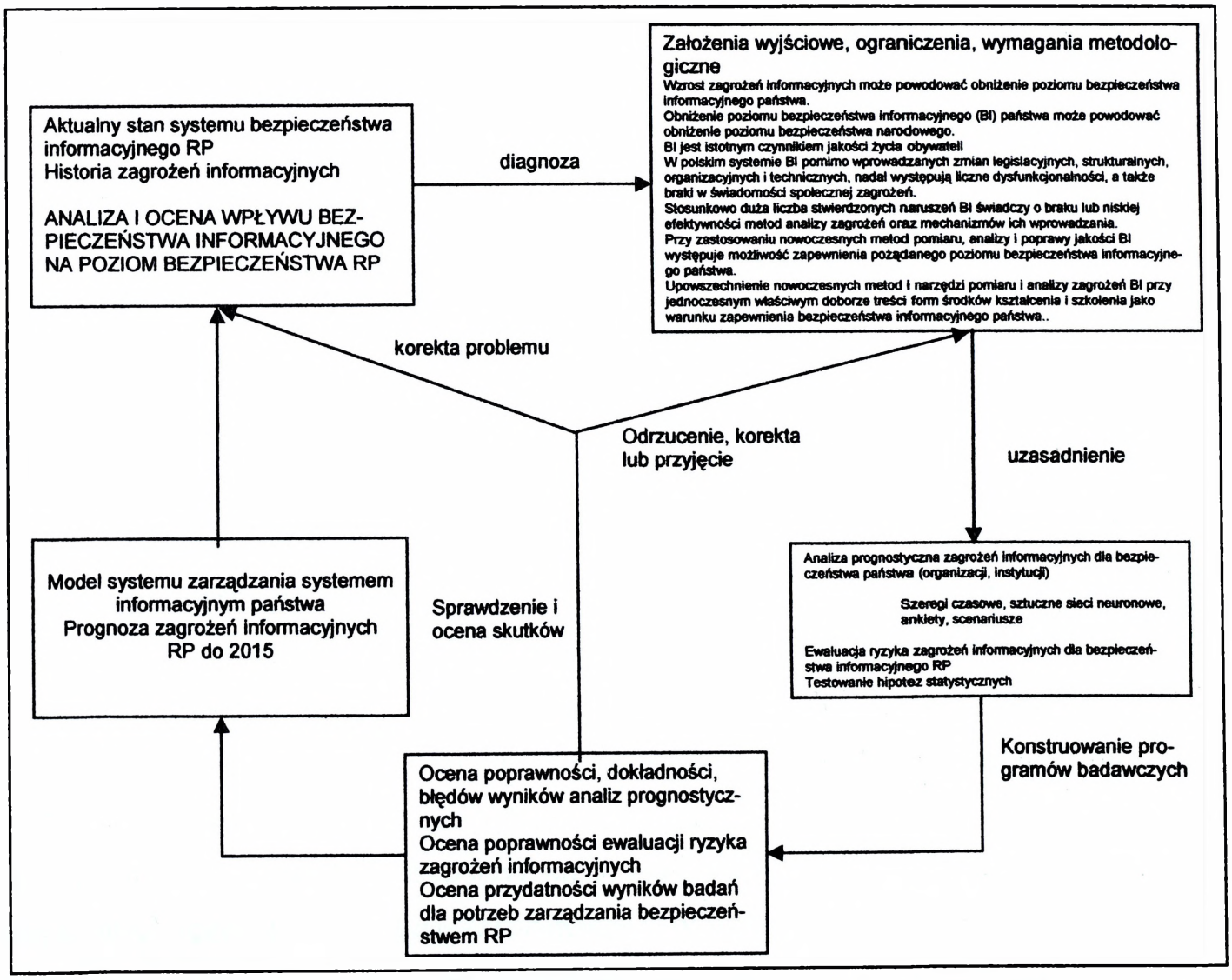
Źródło: opracowanie własne na podstawie: D. Mąka, *Ryzyko w systemie bezpieczeństwa informacyjnego państwa w aspekcie standardów NATO i Unii Europejskiej*. Rozpraw doktorska, AON, Warszawa 2004.

Pozwoliło to wybrać adekwatne techniki analityczno-ocenowe dla rozwiązywania poszczególnych problemów badawczych. W obszarze identyfikacji zagrożeń odwołano się do analizy zarówno literatury przedmiotu, jak i ustaw regulujących obszar związany z technologiami infokomunikacyjnymi. Stosowano metody teoretyczne, jak: analizę, syntezę, indukcję, redukcję itd. W obszarze badań empirycznych zaś zastosowano analizy szeregów czasowych, natomiast w badaniach społecznych odwołano się do metody sondażowej, której wyniki opracowano statystycznie. Uogólnienie postępowania badawczego stanowi ogólnym model procesu badań naukowych (rysunek 1-7) oraz jego konkretyzacja odniesienia do głównego problemu badawczego rozprawy (rysunek 1-8).



Rysunek 1-7. Ogólny model procesu badań naukowych

Źródło: opracowanie własne.



Rysunek 1-8. Ogólny model procesu badań naukowych nad bezpieczeństwem informacyjnym RP

Źródło: opracowanie własne.

Organizacja badań

Konsekwencją przedstawionych ustaleń, założeń i ograniczeń jest ostateczna procedura badawcza przedstawiona w postaci modelu procesu badawczego (tabela 1-2).

Tabela 1-2. Etapy realizacji badań

I ETAP BADAŃ: „diagnoza wstępna"

(1) ANALIZA AKTÓW PRAWNYCH
dotyczących bezpieczeństwa informacyjnego

(2) ANALIZA DZIAŁALNOŚCI INSTYTUCJI I ORGANIZACJI
zajmujących się bezpieczeństwem informacyjnym

(3) ANALIZA DOSTĘPNYCH DANYCH STATYSTYCZNYCH
dotyczących zagrożeń

(4) ANALIZA DOROBKU NAUKOWEGO Z ZAKRESU BEZPIECZEŃSTWA INFORMACYJNEGO
dotyczącego metod m.in. prognozowania, przewidywania zagrożeń

↓

II ETAP BADAŃ: „diagnoza społeczna"

(5) badanie opinii społecznej

(6) badanie opinii ekspertów
na temat zagrożeń informacyjnych

↓

III ETAP BADAŃ: „analiza prognostyczna"

(7) zastosowanie modeli formalnych z obszaru ekonomii do prognozowania zagrożeń informacyjnych

(8) prognozowanie zagrożeń z zastosowaniem sztucznych sieci neuronowych

↓

IV ETAP BADAŃ: „weryfikacja badań"

(9) ILOŚCIOWE I JAKOŚCIOWE BADANIA WERYFIKUJĄCE HIPOTEZY
etapu II badań opinii społecznej i badań opinii ekspertów oraz etapu III – badań eksploracyjnych

↓

V ETAP BADAŃ: „prezentacja wyników badań"

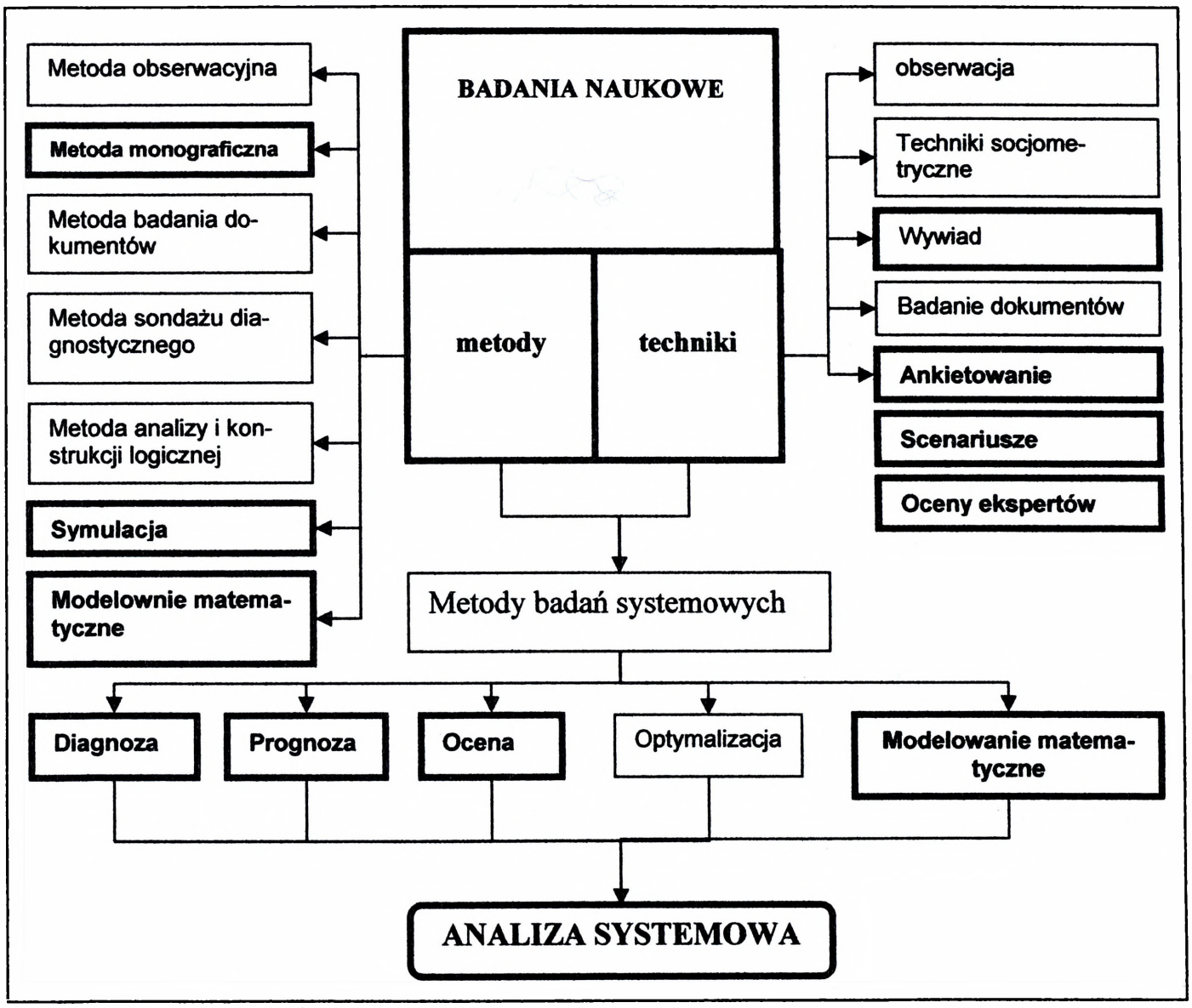
(10) UPOWSZECHNIANIE WYNIKÓW I WNIOSKÓW
z wszystkich etapów analiz i badań przez: (1) konferencje, (2) publikacje obejmujące: identyfikację zagrożeń, badanie percepcji zagrożeń, ewaluacji ryzyka, zarządzania bezpieczeństwem

(11) OPRACOWNIE DYSERTACJI WRAZ Z REKOMENDACJAMI
projektów skierowanych do poprawy bezpieczeństwa informacyjnego

Źródło: opracowanie własne.

Należy pokreślić, że w zasadzie każdy złożony przedmiot badań oraz interdyscyplinarny i mulitidyscyplinarny charakter problemu badawczego wymaga właściwego stosowania przede wszystkim metody indukcyjnej typowej dla badań empirycznych (realnych), ale także – w znacznie mniejszym stopniu – metody dedukcyjnej, która odnosi się do nauk apriorycz-

nych (formalnych, dedukcyjnych).[52] Ponadto proces badawczy wymaga takich operacji myślowych, jak: analiza i synteza, porównywanie i przeciwstawianie, uogólnianie i wnioskowanie. Natomiast wykazanie metod badań systemowych (rysunek 1-9) miało sens ze względu na to, że w obszarze metodologii holistyczno-systemowej rozwijają się metody i techniki dotyczące zagadnień szczegółowych takich, jak np.: ewaluacja (analiza i ocena), komparatystyka (wielokryterialna lub wielowariantowa analiza porównawcza), taksonomia, czy liczne metody i techniki optymalizacji (optymalnego sterowania) itp. Z kolei, analiza systemowa nie jest szczegółową techniką postępowania, lecz raczej zbiorem technik analityczno-ocenowych użytecznych we wspomaganiu decyzji, zwłaszcza w warunkach niepewności i ryzyka.[53]



Rysunek 1-9. Typologia metod i technik badań naukowych

Źródło: opracowanie własne z wykorzystaniem J.Apanowicz (2003), *Metodologia nauk*. Wyd. „DOM ORGANIZATORA", Toruń 2003.

---

[52] W zasadzie po indukcje sięgamy, gdy posługujemy się formalizacją, tworząc np. modele matematyczne obiektów (systemów, procesów).

[53] W.Findeisen, (red.), *Analiza systemowa – podstawy i metodologia*. WNT, Warszawa 1985; P.Sienkiewicz, *Teoria efektywności systemów*. Ossolineum, Wrocław 1987; *Analiza,...*, 1995, op.cit.

1.6. Ocena piśmiennictwa

Literatura przedmiotu, w mniejszym lub większym stopniu dotycząca przyjętego w rozprawie problemu badawczego jest bardzo obszerna. Aczkolwiek brak jest zwartych opracowań wprost dotyczących tematu rozprawy, to bez trudu odnajdzie się prace oryginalne i wartościowe, które bądź dotyczą szczegółowych zagadnień, bądź proponują bardzo ogólne spojrzenie na przedmiotową problematykę.

Z punktu widzenia tematu rozprawy i sposobu jego realizacji ze szczególną uwagą potraktowano wydawnictwa, które ukazały się po 1990 roku, czyli po powstaniu Internetu, natomiast z wcześniejszych – te prace, które można obecnie traktować jako „klasykę". Do nich można zaliczyć, np. inspirująca publicystykę A.Tofflera, czy M.McLuhana. [54]

Literaturę, którą uwzględniono w przygotowaniu dysertacji umownie podzielono na grupy takie, jak:

a) Problemy społeczeństwa informacyjnego, do której zaliczono zarówno „klasykę światową (A.Toffler, M.Castells), jak i prace Autorów poznanych podczas konferencji i sympozjów (L.Zachera, K.Krzysztofka, L.Habera, T.Gobana-Klasa, A.Szewczyk, Siwik, J.Lubacza i innych).[55]
b) Problemy bezpieczeństwa informacyjnego w ujęciu politologicznym (prace np. M.Madeja, A.Bógdał-Brzeźińskiej i M.Gawryckiego, P.Bączka),[56]
c) Problemy bezpieczeństwa informacyjnego ujęcie techniczne (np. A.Białasa, J.Stokłosa, T.Bilski, T.Pankowski, A. Barczak, T.Sidoruk, K.Liderman).[57]

---

[54] A.Toffler, Szok przyszłości. Wyd. KRUPISZ, 2007; A.Toffler, Trzecia fala. PIW, Warszawa 1997; A.H.Toffler, Wojna i antywojna. Jak przetrwać na progu XXI wieku. WWL Muza SA, Warszawa 1997; M.McLuhan, Zrozumieć media. WNT, Warszawa 2004.

[55] L.Zacher, *Gry o przeszłe światy*. Komitet prognoz Polska 2000 Plus, PAN, Warszawa 2006; L.Zacher, *Transformacja społeczeństw, od informacji do wiedzy*. C.H.Beck, Warszawa 2007; *Społeczeństwo sieci*. Wyd. Naukowe PWN, Warszawa 2007; M.McLuhan, *Zrozumieć media*. WNT, Warszawa 2004; *Zagrożenia asymetryczne bezpieczeństwa państwa obszaru transatlantyckiego*. Wyd. PISM, Warszawa 2007; L.Haber *Społeczeństwo informacyjne. Wizja czy rzeczywistość?* (red.), wyd. Uczelniane Wydawnictwa Naukowo–Dydaktyczne, Kraków 2004; L.Haber, *Od robotnika do Internetu – w kierunku społeczeństwa informacyjnego*. AGH, Kraków 2008; T.Goban-Klas, *Media i komunikowanie masowe – teoria i analizy prasy, radia, telewizji i Internetu*. Warszawa 2004; A.Szewczyk, *Społeczeństwo informacyjne – problemy rozwojowe*. Difin, Warszawa 2007; Siwik (red.), *Od społeczeństwa industrialnego do społeczeństwa informacyjnego*. AGH, Kraków 2007.

[56] M.Madej, Zagrożenia asymetryczne bezpieczeństwa państw obszaru transatlantyckiego, PISM, Warszawa 2007; A.Bógdał-Brzeźińska, M.F.Gawrycki, Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie. Wyd. Fundacja Studiów Międzynarodowych, Warszawa 2003; P.Bączek, Zagrożenia informacyjne a bezpieczeństwo państwa polskiego, Wyd. A. Marszałek, Toruń 2005.

[57] A.Białas, Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie. WNT, 2006; T.Pankowski, Bezpieczeństwo w systemach informatycznych. Wyd. Naukowe PWN, Warszawa 2001; A.Barczak, T.Sidoruk, Bezpieczeństwo systemów informatycznych. Wyd. Akademii Podlaskiej, Siedlce 2002; K.Lideerman, Analiza ryzyka i ochrona informacji w systemach komputerowych. PWN, Warszawa 2008; K.Liderman, Analiza ryzyka i ochrona informacji w systemach komputerowych. Wyd. Naukowe PWN, Warszawa 2008; K.Liderman, Bezpieczeństwo teleinformatyczne. WAT, Warszawa 2001.

d) Problemy walki informacyjnej i wojskowego wykorzystania ICT: (L.Ciborowski, R.Szpyra, R.Kwećka, J.Kręcikij J.Posobiec Z.Mierczyk, A.Campen, M.Libicki, J.Garstka).[58]

Na osobną uwagę zasługują pozycje z serii TAO (Tajemnica-Atak-Obrona) Wydawnictwa Naukowo-Technicznego – D.Dening, E.Yourdon, D.Pipkin, R.Anderson,[59] także z oczywistych powodów uwagę przyciągnęły kolejne raporty RAND Corporation – począwszy od J.Arguilla[60], a kończąc na analizach z roku 2009[61]. Ogromną liczbą informacji w tym, np. danych o incydentach terrorystycznych, dysponują zasoby Internetu.

---

[58] L.Ciborowski, Walka informacyjna. Toruń 1999; R.Szpyra, Militarne operacje informacyjne. AON, Warszawa 2003; R.Szpyra, Operacje informacyjne państwa w działaniach sił powietrznych, rozprawa habilitacyjna. AON, Warszawa 2002; R.Kwećka, Informacja w walce zbrojnej. AON, Warszawa 2001; Siły specjalne w kontekście współczesnych zagrożeń./współautor M.Gryga, AON, Warszawa 2002; J.Kręcikij, Działania sieciocentryczne. Wybrane problemy. AON, Warszawa 2008; J.Posobiec, Organizacja dowodzenia w środowisku sieciocentrycznym. AON, 2008; J.Jańczak, A.Wisz, Sieci teleinformatyczne w działaniach sieciocentrycznych. Materiały konferencyjne, AON, Warszawa 2007; Z.Mierczyk (red.), Nowoczesne technologie systemów uzbrojenia, WAT, 2008; A.Campen, The First Information War, NY, 1991; M.Libicki, P.Chale, M.Sisson, Exploring Terrorist Targeting Preeferences, RAND, 2007; John J.Garstka, Network Centric Warfare: An Overview of Emerging Theory.

[59] D.E.Denning, Wojna informacyjna i bezpieczeństwo informacji. WNT, Warszawa 2002; E.Yourdon, Wojna na bity. WNT, 2004; L.Pipkin, Bezpieczeństwo informacji. WNT, Warszawa 2002; R.Anderson, Inżynieria zabezpieczenia. 2005.

[60] I.Arguilla, D.Ronfeldt, "*Cyberwar is Coming*" , Comparative Strategy, 12, 1993; end *In Athena's Camp: Preparing for Conflict in the Information Age*, Santa Monica 1997.

[61] Film Piracy, Organized Crime, and Terrorism, RAND. Org.

Rozdział 2

WSPÓŁCZESNE ZAGROŻENIA INFORMACYJNE DLA BEZPIECZEŃSTWA PAŃSTWA

2.1. Wprowadzenie

W nowych warunkach rozwojowych spowodowanych postępem technologicznym, a ukształtowanych na przełomie XX i XXI wieku, bezpieczeństwo informacyjne stało się istotną dziedziną bezpieczeństwa narodowego. Pojawiło się wraz z pełną integracją systemów informatycznych i komunikacyjnych (ICT), a także ich globalizacją (rysunek 2-1). Pogłębiło to charakter procesów globalizacyjnych, przenosząc procesy gospodarcze, społeczno-polityczne i kulturowe w przestrzeń cybernetyczną[62], którą można rozpatrywać jako interaktywny i multimedialny system globalnej komunikacji społecznej.[63] Cyberprzestrzeń ukształtowały następujące procesy:[64]

- integracji podstawowych form przekazu i prezentacji informacji (*data+texts+pictures+voices+movies*), który przyniósł multimedialność, „ucyfrowienie" infosfery i ikonosfery;
- konwergencji ICT: systemów informatycznych, systemów telekomunikacyjnych i mediów elektronicznych;
- integracji technosfery, który ukształtował globalną zintegrowaną platformę teleinformatyczną.

Pozwoliło to na wirtualizację wielu procesów gospodarczych i biznesowych przynosząc zjawisko „nowej gospodarki", lecz przyniosło również nowe zagrożenia, których wystąpienie mogłoby wpłynąć na destabilizację państwa, w szczególności zagrażając jego bezpieczeństwu ekonomicznemu, energetycznemu itp. Medium, które wywarło największy wpływ na strukturę społeczną, a także wywołało zmiany w pracy i nauce, oraz wpłynęło na zmianę zachowań społecznych jest Internet.

---

[62] P.Sienkiewicz, *Terroryzm w cybernetycznej przestrzeni.* [w:] T.Jemioło, J.Kisielnicki, K.Rajchel (red.), *Cyberterroryzm nowe wyzwania XXI wieku.* Warszawa 2009. W tekście znajduje się skonkretyzowana charakterystyka terminu „cyberprzestrzeń", nazwy wprowadzonej przez William Gibsona w powieści „Neuromancer", określając ją jako „graficzny obraz danych", co nie oddaje charakteru zjawiska, którego dotyczy.

[63] P.Sienkiewicz, H.Świeboda, *Bezpieczeństwo europejskiej przestrzeni cybernetycznej.* Konferencja nt. Europa, integracja, polityka i bezpieczeństwo. Gdynia 2009.

[64] P.Sienkiewicz, *Terroryzm,...,2009,* op.cit., s.195.

Procesowi modernizacji społeczeństw równolegle towarzyszył proces zmian w środowisku bezpieczeństwa międzynarodowego. Pojawiły się nowe desygnaty bezpieczeństwa w wyniku gwałtownego rozwoju technologii ICT i ich konwergencji, co miało wpływ na wyłanianie się nowego paradygmatu bezpieczeństwa. Znalazło to wyraz w społeczno-politycznym obszarze bezpieczeństwa międzynarodowego. Nadal jednak zwiększa się przepaść technologiczna, mająca niekiedy cechy luki cywilizacyjnej, między państwami Zachodu a państwami tzw. Trzeciego Świata, poszerza się obszar wykluczenia i biedy, co przynosi między innymi zwiększoną migrację w poszukiwaniu lepszego życia (tabela 2-1).[65]

Tabela 2-1. Zagrożenia dla bezpieczeństwa

ZAGROŻENIA DLA BEZPIECZEŃSTWA SPOŁECZEŃSTWA INFORMACYJNEGO	NOWE ŚRODOWISKO BEZPIECZEŃSTWA
– Zorganizowany terroryzm międzynarodowy (*) – Proliferacja BMR – CYBERTERORYZM (***) – Wymuszone masowe migracje – Przestępczość transgraniczna – Niekontrolowane operacje finansowe (**) – Wrażliwość krytycznej infrastruktury (***) – Degradacja ekosfery – Nowe choroby zakaźne – Degradacja infosfery (***) – Wrażliwość globalnego systemu gospodarczego (*) – Bezrobocie (*)	– Globalizacja i integracja („oddanie części suwerenności") (*) – Kryzys państwowości – „Płn–Płd" (przepaść ekonomiczna, technologiczna, społeczna) (*) – Słabość struktur bezpieczeństwa (ONZ, NATO, UE, OBWE, UA) – Niedostatki prawa międzynarodowego – Jednobiegunowość w sferze militarnej – Rewolucja technologiczna w siłach zbrojnych (***) – Zróżnicowanie koncepcji bezpieczeństwa, nowa rola Sił Zbrojnych (prewencja + "soft power") • Trudności w adaptacji do nowych warunków (ONZ, OBWE) • Asymetryczność w czasie i przestrzeni (*) • Ograniczona przewidywalność • Nieokreśloność doktryn i struktur • Myślenie w kategoriach kryzysu

* oznacza wpływ IT na zagrożenia wywoływane technologiami lub wzmocnienie zagrożeń klasycznych (ilość gwiazdek oznacza wielkość wpływu).

Źródło: P. Sienkiewicz, *Modelowanie zarządzania bezpieczeństwem systemów w społeczeństwie informacyjnym*. BOS'06, Szczecin 2006.

[65] Zmiany środowiska bezpieczeństwa akcentowano w kolejnych raportach *Global Trends, 2010, 2015,2020,2025* przez Nationale Intelligence Council (NIC) (Narodowa Rada Wywiadu USA), także raporty Unii Europejskiej, NATO. W Polsce do roku 2000 prognozy długoterminowe (strategiczne) publikował Komitet Prognoz „Polska 2000 plus" PAN. Obecnie obserwuje się dobrą praktykę powrotu do myślenia strategicznego. Coraz więcej placówek nie tylko naukowych poświęca problematyce globalizacji i technicyzacji więcej uwagi.

Cyberprzestrzeń, którą tworzy globalna infosfera i globalna infrastruktura teleinformatyczna, nie jest ograniczona czasem i odległością, a granice jej wyznacza w istocie aktualny poziom rozwoju ICT. Wraz z postępem technologicznym i w zasadzie niekontrolowanym rozwojem Internetu, pojawiły się nowe zagrożenia, co wraz z kumulacją i transformacją zagrożeń już istniejących stworzyło nową przestrzeń bezpieczeństwa. Pojawiły się nowe obszary bezpieczeństwa informacyjnego, które w przeszłości kojarzone było z ochroną informacji stanowiących tajemnicę państwową i służbową. Wówczas w sferze zagrożeń dominowały takie zjawiska, jak: szpiegostwo, działalność dywersyjna, przekazywanie informacji nieuprawnionym podmiotom.

Wraz z rozwojem technologicznym wystąpiła konieczność zapewnienia bezpieczeństwa systemów i sieci informacyjnych, ich poufności, integralności i nienaruszalności. Pojawiły się zagrożenia związane z subiektywnym odbiorem stosowania nowych technik komunikowania, przede wszystkim mediów elektronicznych.

W tej sytuacji szczególnego znaczenia nabiera typologia zagrożeń, bowiem od poprawności ich identyfikacji zależy właściwy wybór efektywnych środków przeciwdziałania. Poprawnie wykonana analiza zagrożeń i ocena ryzyka ich wystąpienia (kluczowy element w sferze zarządzania bezpieczeństwem) jest dla danego systemu gwarancją bezpieczeństwa.

2.2. Ewolucja technologii informacyjnych

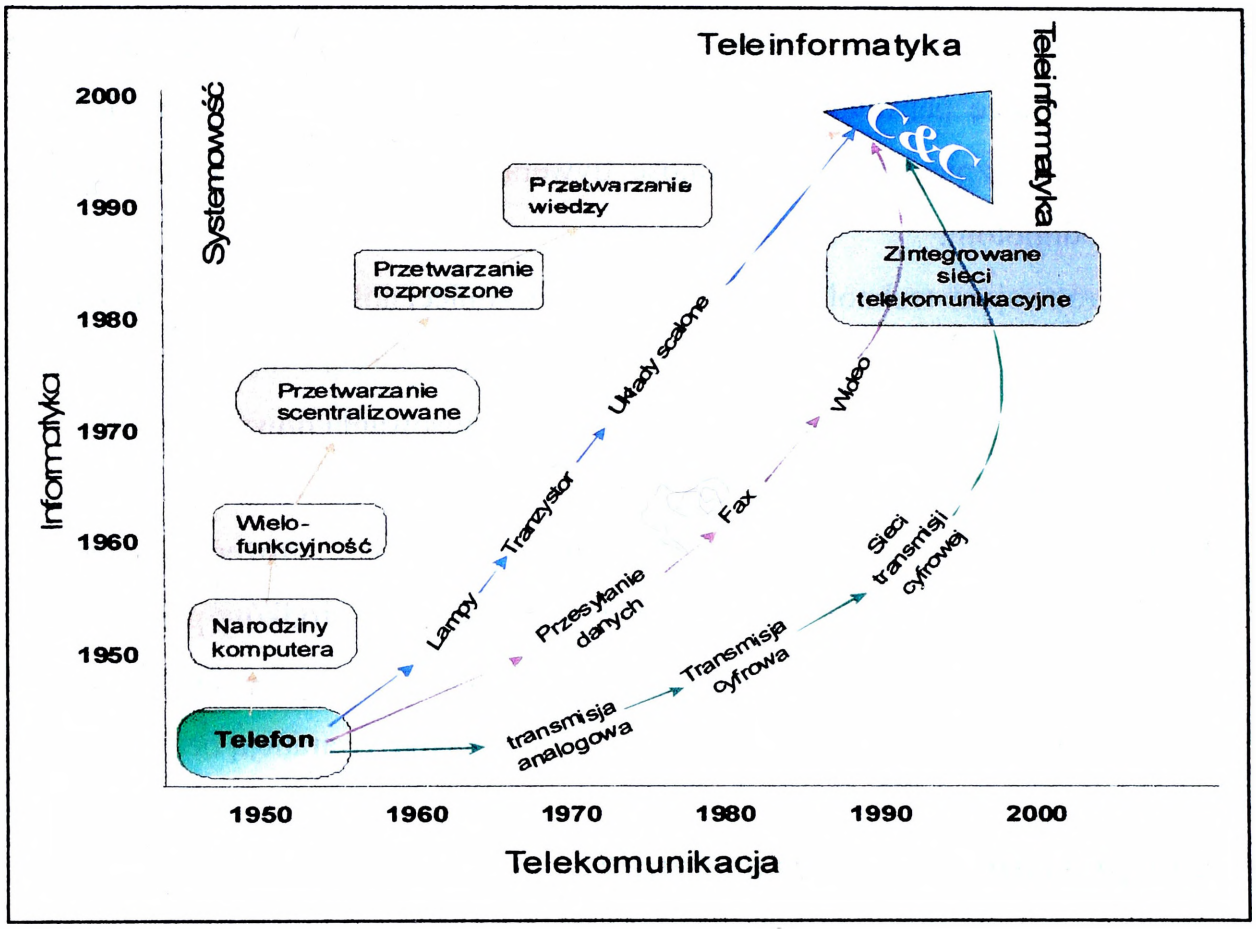
Podwalin technologicznych rozwoju społeczeństwa informacyjnego należy szukać w latach 40-tych ubiegłego wieku. Stworzono wtedy podstawy techniki cyfrowej i uruchomiono pierwsze komputery (Z-3 w 1943 roku i ENIAC w roku 1946). Claude E. Shannon stworzył podstawy teorii informacji i narodziła się cybernetyka Norberta Wienera. Źródłem rozwoju technologii informatycznych był postęp, jaki dokonał się w dziedzinie fizyki ciała stałego, bez czego *„... nie było by - w obecnym kształcie - informatyki i telekomunikacji, automatyki i robotyki"*, zaś postęp w tej dziedzinie wyznaczają wynalazki: tranzystora w 1948 roku, układu scalonego w 1958 roku i mikroprocesora w 1971 roku. [66]

Do innowacji i wynalazków, które w połowie XIX stulecia, rozpoczęły erę telekomunikacji należy wynalezienie telegrafu (1837-1840), fotografii (1839), telefonu (1876), płyty gramofonowej i filmu. W pierwszej połowie dwudziestego wieku pojawiło się radio i telewizja. Od czasu II wojny światowej dokonywał się nieustanny rozwój i doskonalenie wszelkich

---

[66] P.Sienkiewicz, *„Zatrudnienie i praca w społeczeństwie informacyjnym"*, Informator „Telepraca, rynek pracy bez barier", Warszawa 2001; P.Sienkiewicz, *Od Eniaca do Internetu i społeczeństwa wiedzy.* Zeszyty Naukowe WWSI, nr 1, 2006.

metod zbierania, przetwarzania i przesyłania informacji w dowolnej formie i na dowolne odległości. Podstawą stała się elektronika, głównym narzędziem komputer, a zasadniczą jego częścią – procesor. Nastąpiła integracja technologii komputerowych z technikami przekazu (telefonem, monitorem telewizyjnym, kompaktową płytą muzyczną) w nowe formy komunikowania i mediów (rysunek 2-1).



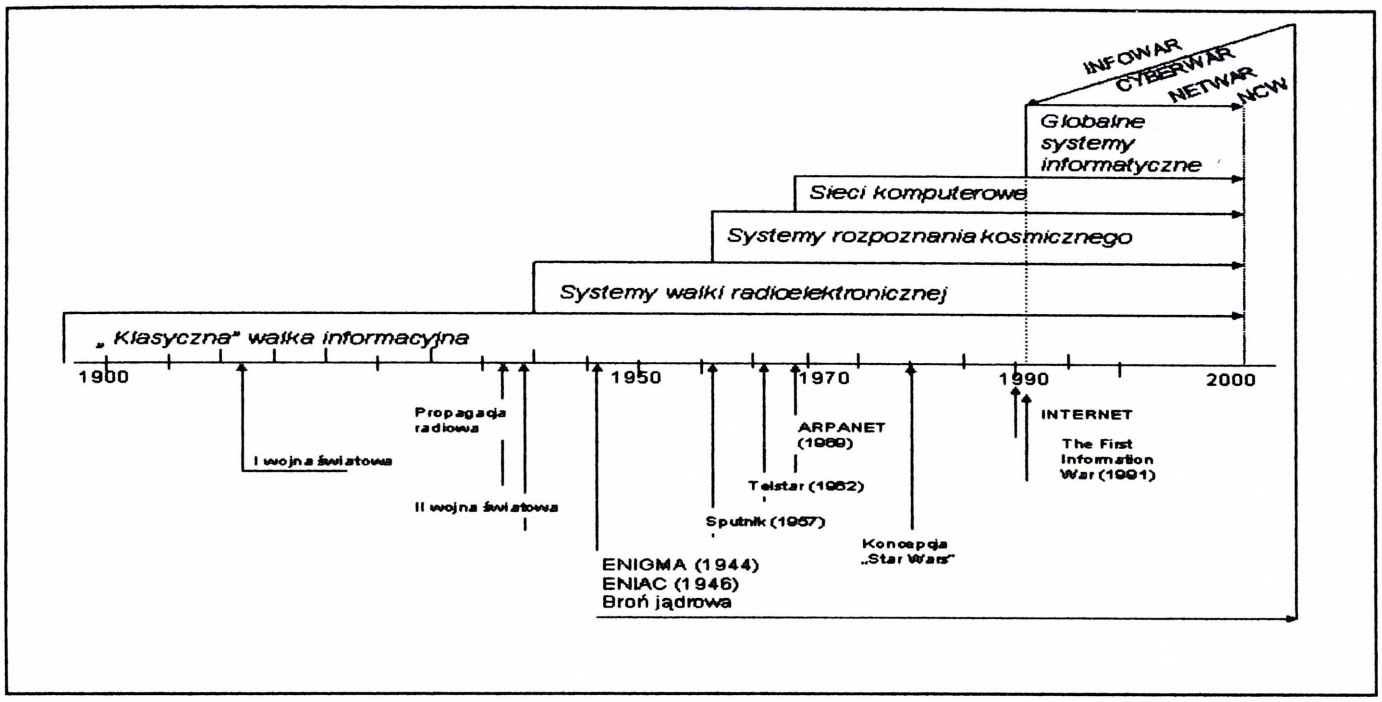
Rysunek 2-1. Rozwój technologii informacyjnych (informatycznych)

Źródło: opracowanie na podstawie: H.Kobayashi, *The evolution of computer and communication technologies*. Hokkaido, 1985; [w:] P.Sienkiewicz, *Globalizacja, informacja, bezpieczeństwo*. Transformacje, 1-4 (27-30), Warszawa 2002.

Ważną, bo przełomową datą był rok 1990, który przyniósł jedną z najważniejszych innowacji XX wieku, którą było powstanie globalnej „sieci sieć", czyli Internetu – obecnie siły napędowej „nowej gospodarki". Oczywiste są konsekwencje rozwoju Internetu dla bezpieczeństwa narodowego (międzynarodowego), gdyż jego zalążkiem była pierwsza sieć komputerowa Arpanet (1969), powstała w ramach programu realizowanego na zlecenie Departamentu Obrony USA.[67] Technologie informacyjne wpłynęły również na powstanie nowych koncepcji wojny i zmianę paradygmatu bezpieczeństwa narodowego. Rozwój narzędzi walki informacyjnej spowodował, że analizowanych jest wiele nowych koncepcji polityczno-militarnych (*Joint Vision 2010, 2020*) (rysunek 2-2). Kluczowymi czynnikami operacji wo-

[67] Koncepcję sieci komputerowej odpornej na uderzenia przeciwnika opracował zespół z RAND pod kierownictwem P.Barana.

jennych lub operacji innych niż wojna, stała się platforma teleinformatyczna umożliwiająca przetwarzanie i przesyłanie informacji w czasie rzeczywistym, dysponowanie szerszym zakresem informacji o polu walki („świadomość sytuacyjna") oraz wykorzystanie informacji umożliwiających optymalizacje decyzji (wielowariantowa analiza wariantów działania).



Rysunek 2-2. Technologie informacyjne i ich wpływ na koncepcje walki informacyjnej w XX wieku
Źródło: P.Sienkiewicz, [w:] *Modelowanie procesów walki informacyjnej. Model „cyberwar"*. AON, Warszawa 2006, s.10.

Nowoczesne operacje oparte będą na przepływie informacji w czasie rzeczywistym, atakach dokonywanych w cyberprzestrzeni, zaś przewaga (dominacja) informacyjna, stała się obecnie kluczową kategorią.[68] Potrzeba bezpieczeństwa informacyjnego wynika z faktu, że narzędzi tych można użyć także w czasie pokoju. Chociaż obecnie prawo międzynarodowe nie jest przygotowane do rozstrzygania problemów występujących w przypadku wykorzystania sieci teleinformatycznej jako środka prowadzania działań uznanych za działania wrogie, to wkrótce uregulowania takie staną się koniecznością.[69] Zmiana charakteru współczesnych zagrożeń wymusza coraz większy, aktywny udział wszystkich obywateli, instytucji, firm i grup społecznych w systemie bezpieczeństwa i ochrony. Rozwój technologii informacyjnych

[68] R.Szpyra, Militarne operacje informacyjne, AON, Warszawa 2003; Militarne operacje informacyjne instrumentem bezpieczeństwa państwa, ZN1(58)A, AON, Warszawa 2005.

[69] Warto wspomnieć wydarzenia, które miały miejsce pod koniec kwietnia i na początku maja 2007r. w Estonii a dotyczyły ataków na serwery w estońskim sektorze Internetu. Wynikiem blokady stron internetowych całkowicie zinformatyzowanej Estonii był paraliż służb państwowych i gospodarczych, jest podjęcie tematu cyberwojny przez polityków, przedstawicieli sił zbrojnych i ekspertów komputerowych z całego świata. Po raz pierwszy oficjalnie użyto określenia w dyplomacji „cyberwojna". Według Gadi Evrona z izraelskiej firmy Beyond Security, sprawcami owych ataków były niepowiązane ze sobą grupy internautów, zaś scenariusz i efekt ataków bardzo przypominają działania rozjuszonego tłumu - z tym, że w wersji internetowej - doskonały przykład e-zamieszek. Źródło: http://securitystandard.pl/katalog/katalog.asp?c=313

i ich zastosowanie w gospodarce sprawił, że zasoby informacyjne różnych podmiotów narażone są na zagrożenia podobne, jak w koncepcji walki informacyjnej (NCW).

Niejako równolegle do nowych koncepcji walki zbrojnej postępował proces coraz silniejszego uzależniania się od technologii teleinformatycznych wszystkich niemal sfer życia społecznego. Rezultatem tego zjawiska był wzrost efektywności ekonomicznej gospodarki, co jednak nie uchroniło wielu firm, w tym tzw. Internetowych, od upadku. Technologie teleinformatyczne decydują o rozszerzeniu możliwości poznawczych człowieka, przyczyniając się do eksploracji naukowej, a także odkrywania nowych obszarów politycznej i gospodarczej ekspansji. Powstały warunki „walki o przewagę" i poszukiwania skutecznej strategii konkurencji. Wybór strategii konkurencji wiąże się z uzyskaniem przewagi konkurencyjnej, która ma wymiar zarówno przewagi czasowej (np. redukcja czasu realizacji projektów i wdrożeń, czasu dostaw, zbytu itp.), jak i przewagi informacyjnej (np. dysponowanie pełniejszymi i bardziej aktualnymi, niż konkurencja, informacjami o potrzebach i preferencjach klientów). Przewaga informacyjna (wiedzy) stała się warunkiem przewagi strategicznej „w walce i biznesie".[70]

2.3. Istota zagrożeń informacyjnych

Pojęcie zagrożenia semantycznie kojarzy się z niebezpieczeństwem, na przykład z utratą jakiejś wartości czegoś lub ze stanem zagrożenia dla kogoś lub czegoś.[71] Antonimem zagrożenia jest bezpieczeństwo, a więc zagrożenie pojawia się w relacji do jakiegoś obiektu (człowiek, artefakt) lub systemu (społeczeństwo, państwo), dla którego istnieje jako źródło ryzyka. Zagrożenie występuje w wyniku pojedynczych zdarzeń lub ich koincydencji odniesionych do podatności określonego obiektu, czego skutkiem jest powstawanie szkód (strat). Mogą one stanowić przyczynę np.: ograniczenia warunków niezakłóconego rozwoju, utraty zdolności rozwojowych, politycznych, ekonomicznych, bojowych, itp., utraty suwerenności, strat finansowych, a w szczególności start ludzkich (utrata zdrowia lub życia).

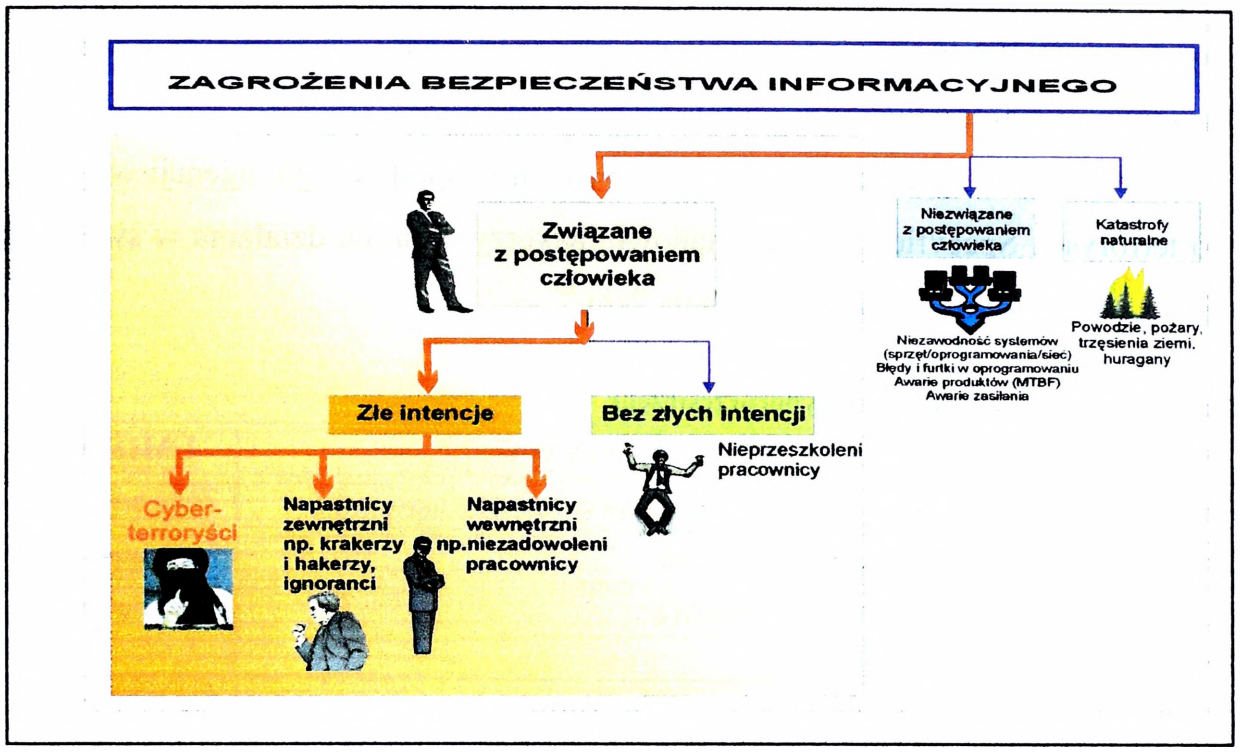
Zagrożeniem dla bezpieczeństwa systemu, określać będziemy każde zjawisko (proces, zdarzenie) niepożądane z punktu widzenia, niezakłóconego działania systemu. Takie zjawiska lub ich kumulacja w określonym miejscu i czasie, oddziaływujące destrukcyjnie na system, tworzy sytuacje niebezpieczne dla egzystencji (rozwoju) systemu. Należy także zwrócić uwa-

---

[70] P.Sienkiewicz, *Przewaga informacyjna w walce i biznesie*. [w:] *10 wykładów*. AON, Warszawa 2005; BOS'04, IBS PAN, Warszawa 2004.

[71] Słownik języka polskiego, PWE, Warszawa 1981, s.907.

gę na możliwość powstawania sytuacji niebezpiecznych dla systemu, będących skutkiem zagrożeń wewnętrznych wynikających np. z zawodności systemu (rysunek 2-3).[72]



Rysunek 2-3. Ogólna typologia zagrożeń bezpieczeństwa systemów informacyjnych
Źródło: P.Sienkiewicz, H.Świeboda, *Cyberterrorism as a threat to the security of mass events.* Konferencja nt.*„Terrorism and security of mass events”.* Waplewo 2008.

Oprócz poznanych zagrożeń „naturalnych” (np.: pożary, awarie budynków itp.) oraz zagrożeń wynikających z zawodności środków technicznych i programowych, szczególne znaczenie mają te, które są rezultatem działalności ludzi. Mniej groźne wydają się być zagrożenia niezamierzone, będące konsekwencjami niewłaściwego doboru personelu lub ich ograniczeń zawodowych (niedostateczne kwalifikacje, brak opanowania określonych procedur itp.). Nie można ich jednak lekceważyć, gdyż ignorancja i arogancja była niemal zawsze przyczyną poważnych katastrof technicznych i technologicznych. Nie można także wykluczyć działań zamierzonych, prowadzonych przez pracowników firmy lub kontrahentów, czy karierowiczów łamiących prawo. Zwykle dysponują pewnymi prawami dostępu i posiadają umiejętności w wystarczającym stopniu mogące szkodzić.[73]

---

[72] P.Sienkiewicz, (red.), *Teoria bezpieczeństwa systemów. Synteza doświadczeń.* Cz. I, AON, Warszawa 2004, s.8.

[73] Np. z raportu Computer Crime and Security Survey for 2007 opracowanego przez Computer Security Institute wynika, że właśnie pracownicy stanowią główny powód występowania incydentów związanych z bezpieczeństwem informatycznym. Spośród 500 specjalistów z zakresu bezpieczeństwa (59%) stwierdziło, iż w ostatnim roku pracownicy przyczynili się do powstania incydentu zagrażającego bezpieczeństwu informatycznemu w ich organizacji. W badaniu tym uwzględniano m.in. świadome lub nieświadomie udostępnienie danych, wykorzystywanie nielegalnego oprogramowania czy też przeglądanie podejrzanych stron w Internecie. W badaniu zwrócono również uwagę na wzrost liczby kradzieży urządzeń przenośnych, na których znajdowały się dane organizacji.

Zagrożenia świadome są efektem zorganizowanego działania, którego celem jest destrukcja, tzn. zniszczenie lub zmniejszenie efektywności systemów informacyjnych (lub ich elementów), albo określonych obiektów tworzących tzw. infrastrukturę krytyczną. Stanowią one nowe wyzwanie dla odpowiedzialnych za bezpieczeństwo państwa, gotowość systemów informacyjnych, zarządzanie zasobami informacyjnymi itp.[74]

Napastnicy mogą rekrutować się z wywiadu gospodarczego, agencji wywiadu, mogą być to terroryści. Specyficzna grupę stanowią hakerzy, których działania w sytuacji konfliktowej są szczególnie niebezpieczne (tabela 2-2).[75]

Tabela 2-2. Profile napastników w cyberprzestrzeni

NAPASTNICY	MOTYWY	UMIEJĘTNOŚCI
Wywiad gospodarczy	Konkurencja, finansowe, interesy narodowe	Zaawansowane
Agencje wywiadu	Interesy narodowe	Zaawansowane
Napastnicy wewnętrzni (personel kontrahenci)	Zemsta, finansowe	Średnie - wysokie
Karierowicze	Zdobycie władzy, finansowe	Średnio-wysokie
Terroryści	Fanatyzm religijny i polityczny	Zaawansowane
Hakerzy:		
Nowicjusze	Ciekawość chęć wyróżnienia się	Słaba
Black Hat	Ciekawość chęć wyróżnienia się, rzekome zwiększanie bezpieczeństwa	Średnio-wysokie
Grey Hat	Do wynajęcia	Zaawansowane
White Hat	Zwiększanie bezpieczeństwa	Średnio-wysokie
Hacktivist	Polityczni aktywiści, chcą coś zademonstrować	Zaawansowane

Źródło: NetWorld Akademia, www.symantec.pl

Dobór kryteriów klasyfikacji zagrożeń uzależniony jest przede wszystkim od zamierzonego celu analizy i dobranej metody badawczej (tabela 2-3). Incydenty, ataki naruszające bezpieczeństwo w sieci, możemy klasyfikować zarówno od strony technicznej, sprzętowej

---

[74] P.Sienkiewicz, H.Świeboda, E.Lichocki, *Analiza systemowa zjawiska cyberterroryzm*. ZN AON Nr2(63), 2006.

[75] Nie jest to wprawdzie istotą dociekań naukowych, ale warto zaznaczyć, że wśród zidentyfikowanych zagrożeń niezwykle ważne są zagrożenia fizyczne, na które narażona jest infrastruktura organizacji czy systemu. Zagrożenia fizyczne mogą realizować się poprzez fizyczne zdobycie dostępu do pomieszczeń oraz poprzez atak w formie kradzieży laptopa, dysków, przeszukiwanie kosza na śmieci w celu znalezienia dokumentacji papierowej. W formie zaawansowanej zagrożenia fizyczne mogą realizować się według scenariuszy, jak np.:

- pokonanie systemu alarmowego, wrażliwego na ruch, z pasywnym detektorem IR (zmiany temperatury), mikrofalami (odbicia);
- złamanie czytnika kart lub zduplikowanie;
- wykorzystanie błędnej weryfikacji przez system biometryczny (wady projektowe), złamanie czytnika odcisków palców, użycie powtórzeń.

Zaawansowane ataki polegają np. na podsłuchiwaniu łączy przewodowych oraz na nagrywaniu wideo i audio, przechwytywaniu obrazu monitora, zdobyciu prywatnych kluczy szyfrujących, mogą to być ataki z wykorzystaniem koni trojańskich.

bądź też programowej, a także ze względu na zamiar i cel dokonywania działań przestępczych czy wrogich. Zagrożenia możemy różnicować ze względu na skutki i straty poniesione w wyniku ataków. Zagrożenia informacyjne tym bardziej są niebezpieczne dla stabilności kraju, ponieważ mogą kumulować się lub działać synergetycznie potęgując skutki i straty, stąd często podkreśla się ekonomiczny wymiar bezpieczeństwa informacyjnego. Głównymi celami, dla których dokonuje się klasyfikacji, (w zależności przyjętego kryterium), może być np. obserwacja trendów, koordynacja incydentów czy też sporządzanie, gromadzenie i łączenie statystyk.

Tabela 2-3. Kryteria klasyfikacji zagrożeń

LP	KRYTERIUM WYRÓŻNIENIA	ZAGROŻENIA	ASPEKT
1	własności fizykalne	Materialne	Drogowe, powietrzne
		Energetyczne	Cieplne, radioaktywne
		Informacyjne	Sieciowe, ekonomiczne, społeczne
		Niematerialne`	Psychospołeczne, polityczne
2	czas trwania	zagrożenia krótkotrwałe, sporadyczne;	informacyjny
		zagrożenia długotrwałe, narastające, ewoluujące	informacyjny
		zagrożenia cykliczne, powracające	informacyjny
3	zasięg	zagrożenia lokalne zagrożenia rozległe	budynek, dzielnica, miasto regionalne, globalne
4	stałość zasięgu terenowego	zagrożenia rozprzestrzeniające się	informacyjny

Źródło: opracowanie własne.

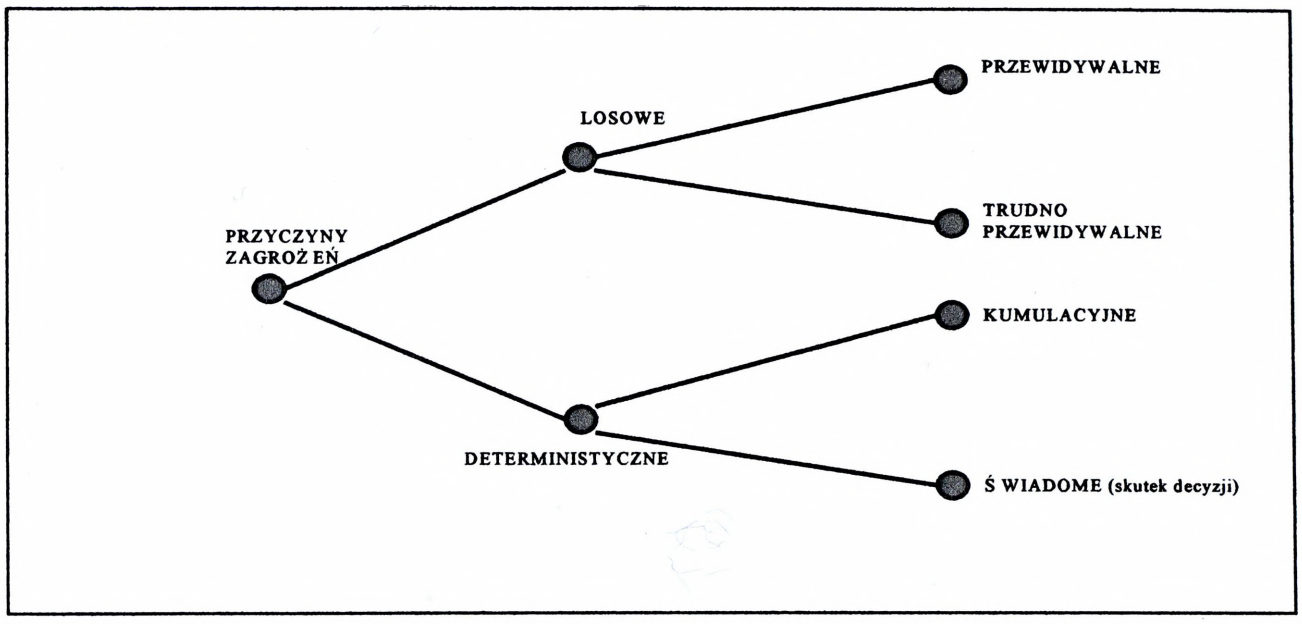
Zagrożeniem informacyjnym określa się takie zagrożenia, którego skutkiem może być:

- obniżenie (degradacja) wartości zasobów informacyjnych określonego obiektu;
- obniżenie (degradacja) niezawodności (potencjału) obiektu;
- obniżenie efektywności działania (skuteczności, ekonomiczności);
- obniżenie potencjału obronnego, społeczno-gospodarczego państw;
- degradacja krytycznej infrastruktury państwa KIP;
- degradacja zdolności systemu obronnego.

Podziału możemy dokonać ze względu na przyczyny wystąpienia zagrożeń (rysunek 2-4):

- Zagrożenia losowe, będące rezultatem zmian środowiskowych (np. zmiana warunków propagacji fal radiowych), mogą wpływać na obniżenie jakości przesyłania informacji. Współczesna telekomunikacja stworzyła jednak efektywne systemy zabezpieczenia zapewniające wysoką jakość transmisji.

– Zagrożenia deterministyczne mogą być rezultatem kumulacji wielu procesów, z których każdy z osobna nie stanowi istotnego zagrożenia, lecz ich kumulacja w określonym miejscu i czasie takim zagrożeniem (np. dla bezpieczeństwa systemów informacyjnych) się staje.[76]



Rysunek 2-4. Klasyfikacja ze względu na przyczyny zagrożeń

Źródło: P.Sienkiewicz, P.Górny: *Analiza systemowa sytuacji kryzysowych*, Zeszyty Naukowe AON Nr 4, Warszawa 2001.

Tabela 2-4. Klasyczna klasyfikacja zagrożeń

KRYTERIUM	KLASYFIKACJA	CHARAKTERYSTYKA
Pochodzenia: skąd przeprowadzany jest atak	Zewnętrzny	Atak przeprowadzany jest z systemu znajdującego się poza atakowaną siecią
	Wewnętrzny	Atak przeprowadzany jest z systemu w atakowanej sieci, np. atak przeprowadza pracownik w celu sprawdzenia swoich umiejętności
Zamiar przeprowadzanego ataku	Zamierzony (celowy)	Celowe działania własnych pracowników, szpiegostwo
	Niezamierzony (losowy)	Niezamierzone błędy użytkowników, pomyłki
Ze względu na rodzaj motywów i celów ataku	**Cyberterroryzm**	Umotywowane politycznie, ideologicznie działanie w cyberprzestrzeni obliczone na wywołanie strat, paniki
	Cyberprzestępstwo	Przestępstwo dokonywane w cyberprzestrzeni dla korzyści osobistych lub z powodów autotelicznych
Efekt ataku	Aktywny	Aktywne oddziaływanie na system – bezpośrednie lub pośrednie np. Świadome działania w celu uzyskania konkretnych informacji;

[76] P.Sienkiewicz, H.Świeboda, *Niebezpieczna,...*, 2006, op.cit.

KRYTERIUM	KLASYFIKACJA	CHARAKTERYSTYKA
	Pasywny	Brak aktywnej reakcji oddziaływania na system (atakujący przypadkowo dokonuje ataku, pracownik przypadkowo obchodzi system autoryzacji). podsłuch lub podgląd w celu zdobycia informacji niejawnych; analiza ruchu w sieci w celu zlokalizowania najważniejszych jej elementów (np. stanowisk kierowania).

Źródło: opracowanie własne.

Wyżej wymienione kryteria (tabela 2-4), w szczególności dotyczące pochodzenia i losowości są całkowicie niezależne, stąd poniżej przedstawiono ich możliwe kombinacje ilustrując to przykładami z praktyki (tabela 2-5).

Tabela 2-5. Podział zagrożeń wg kryterium pochodzenia i losowości

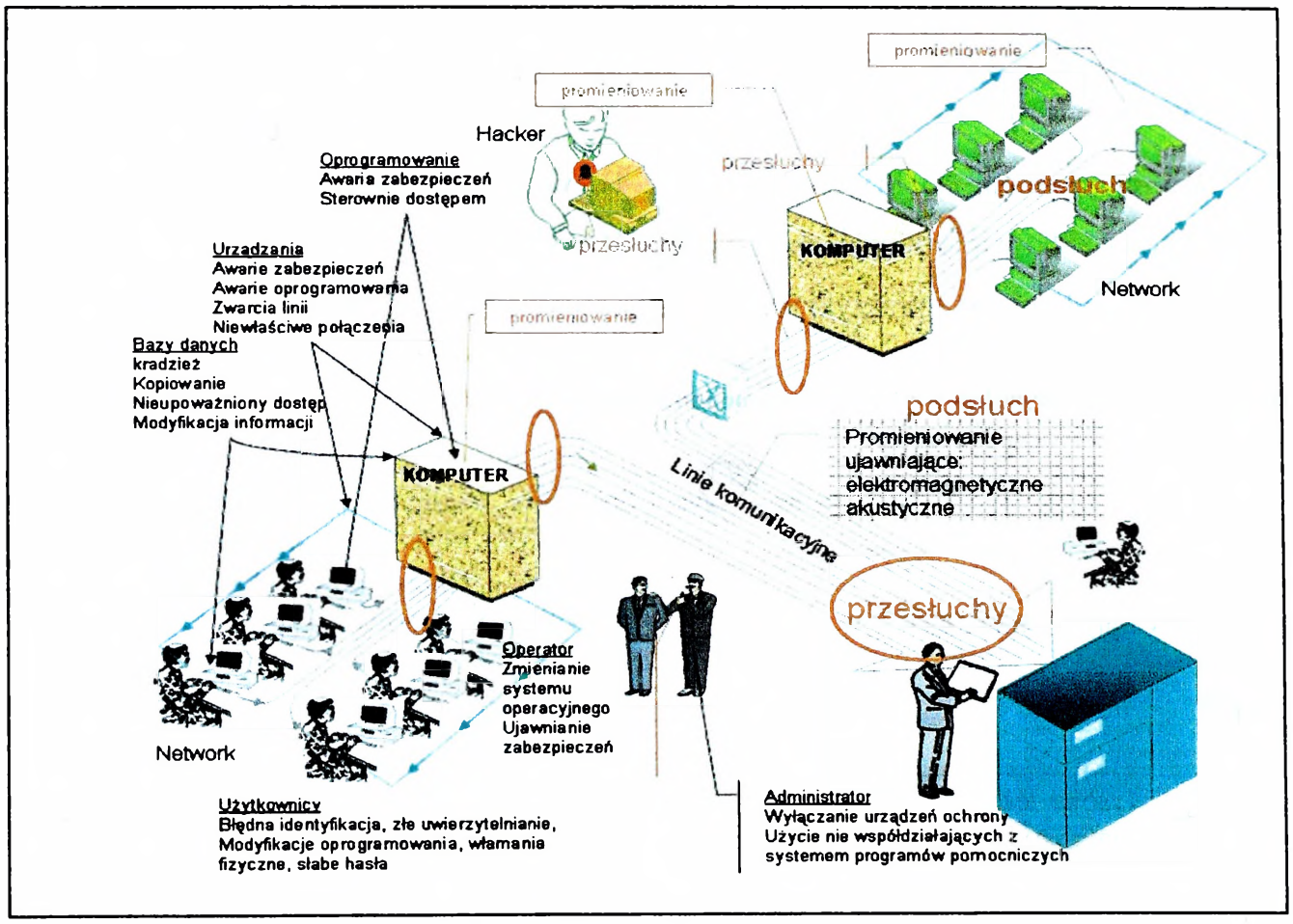
	LOSOWE	CELOWE
WEWNĘTRZNE	Niezamierzone błędy operatorów i użytkowników Wady sprzętu Wady oprogramowania	Działania własnych pracowników wynikające z chciwości, chęci rewanżu, itp. Działania użytkowników wykraczające poza ich obowiązki, nadgorliwość itp. Szpiegostwo Wandalizm, chuligaństwo terroryzm
ZEWNĘTRZNE	Zbyt wysoka temperatura lub wilgotność (pożar, zalanie) Zanieczyszczenie powietrza, kurz, pył Zakłócenia w zasilaniu Zakłócenia w procesach komunikacji Wyładowania atmosferyczne, klęski żywiołowe, itp.	Działanie przestępców komputerowych podejmowane z chęci zysku Działania przedstawicieli prasy i innych mediów, szukających dostępu do informacji Szpiegostwo Wandalizm, chuligaństwo terroryzm

Źródło: A.Barczak, T.Sydoruk, *Bezpieczeństwo systemów informatycznych*. Wyd. Akademii Podlaskiej, Siedlce 2002, s. 84.

Zagrożenia informacyjne mogą realizować się w obszarze bezpieczeństwa informacji, bezpieczeństwa sieci systemów informatycznych oraz bezpieczeństwa systemów teleinformatycznych. W odniesieniu do bezpieczeństwa informacji, zagrożenia mogą szkodzić poufności, integralności i ochronie informacji strategicznych (rysunek 2-5).

Nieodzowna i interesująca, ze względu na cel pracy, jest klasyfikacja złośliwych programów, które są przedmiotem eksploracji, a mianowicie: wirus, robak komputerowy i koń trojański. Wirus właściwy, to złośliwy program, który dokleja część lub cały kod do innego pliku. Zarażone pliki to zwykle pliki wykonywalne lub pliki danych z częścią wykonywalną. Robaki (*worm*) to wirusy rozmnażające się przez sieć w postaci złośliwego programu, których

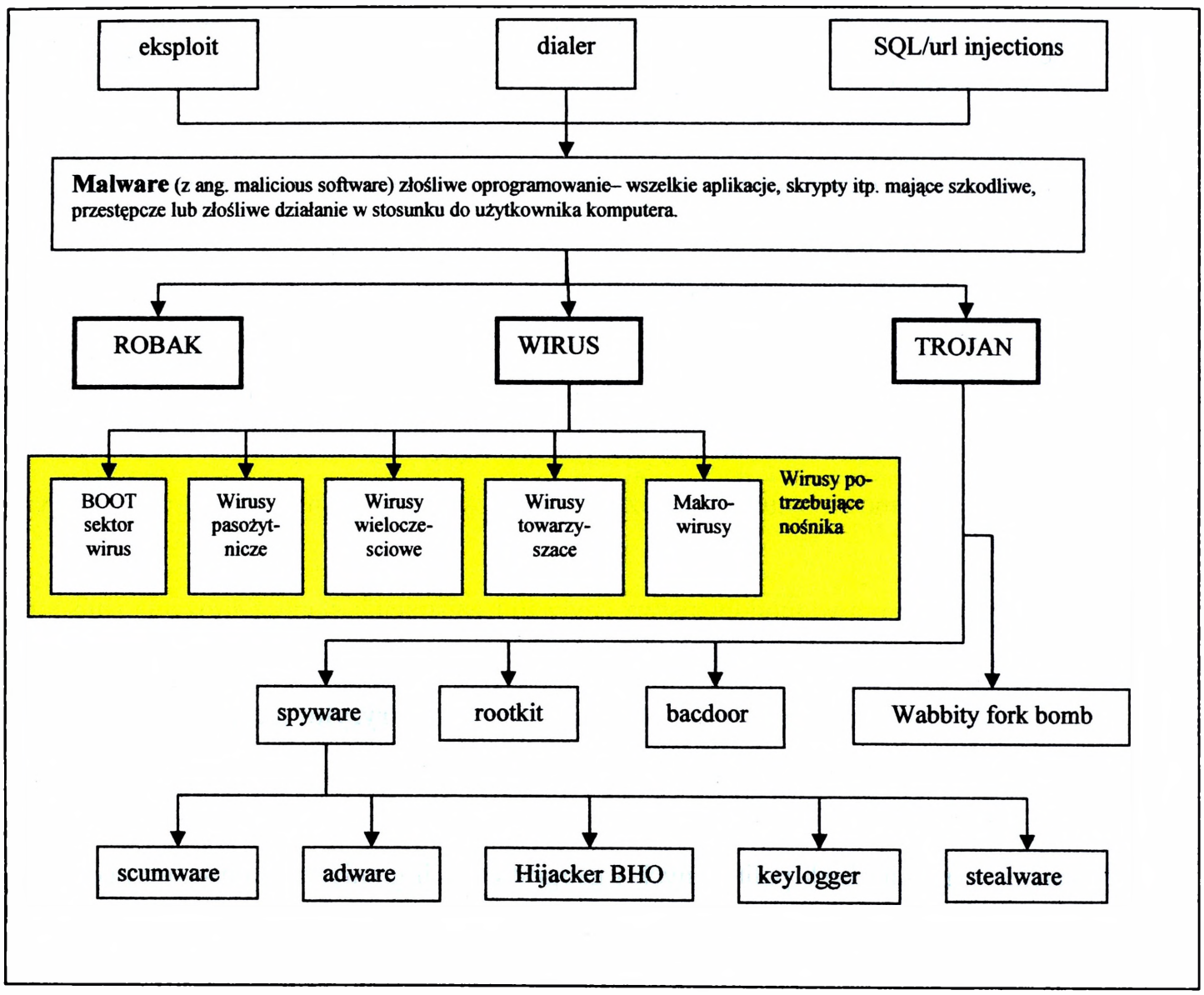
najczęściej spotykaną formą dystrybucji jest e-mail. Trojan to złośliwy program, który kamufluje się jako oprogramowanie użyteczne lub służące do rozrywki, ale w rzeczywistości przeprowadza szkodliwe działania. Zdarzają się wirusy w postaci szkodliwych programów, które rozprzestrzeniają się za pośrednictwem poczty, dyskietek i wszelkich elektronicznych nośników.



Rysunek 2-5. Zagrożenia systemów informacyjnych
Źródło: H.Świeboda, *Zagrożenia informacyjne*. BOS'08.

Pierwszy wirus pojawił się pod koniec roku 1988 i jest znany jako „robak Morrisa".[77] Natomiast pierwszy wirus na peceta pojawił się w 1996. Od tego czasu, tego typu zagrożenia wielokrotnie ewoluowały nie tylko stając się coraz bardziej wyrafinowane w działaniu, ale pojawiły się ich nowe odmiany. Obecnie są najbardziej niebezpiecznymi i uciążliwymi zagrożeniami informacyjnymi. Mnogość odmian ilustruje rysunek 2-6 z krótkim opisem działania, natomiast obszerniejszą informację na temat zagrożeń zawiera załącznik V i VII.

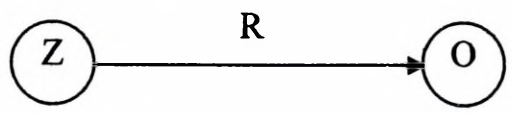
[77] Robert Tappan Morris jako doktorant informatyki badał błędy systemowe, wykorzystując lukę BSD Unix napisał szkodliwy program. Wskutek błędów programisty robak wymknął się spod kontroli i praktycznie sparaliżował działanie całego Internetu. Źródło: R.Ścisłowski, *Pierwszy wirus w historii* [dostęp on line] http://www.pcworld.pl/news/84726/Pierwszy.wirus.w.historii.html



Rysunek 2-6. Taksonomia zagrożeń: podstawowe grupy złośliwego oprogramowania oraz ich wzajemne powiązania

Źródło: opracowane własne na podstawie: www. wikipedia.org.

W analizie systemowej istotę zagrożenia odnosimy do elementarnej relacji między zagrożeniem, a obiektem zagrożenia, które poglądowo możemy wyrazić:



Zagrożenie Obiekt zagrożenia

gdzie:

O – system będący **obiektem** zagrożeń;

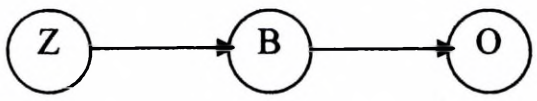
R – relacje;

Z – otoczenie, które tworzą zbiór obiektów będących **źródłem** zagrożeń;

$R \subset Z \times O$ – zbiór relacji, czyli przedmiotem analizy systemowej jest wystąpienie zagrożeń bezpieczeństwa.

Relację zagrożenia można scharakteryzować za pomocą następujących charakterystyk: czasu trwania zagrożenia, podatności obiektu na zagrożenia, intensywności zagrożeń, średniej wartości szkody (straty) itp.

System zabezpieczenia wyrazić można za pomocą relacji między zagrożeniem, system zabezpieczania i obiektem zagrożenia:



B – system zabezpieczenia (środki zewnętrzne stosowane do zabezpieczania i ochrony wartości obiektów przed zagrożeniami Z.

$R_B \subseteq Z \times B \times O$ wtedy przedmiotem analizy jest system $<Z,B,O,R_B>$.

Analiza systemowa sytuacji zagrożenia może być „skalowana" według dwóch **kryteriów oceny:**

1) kryterium prawdopodobieństwa (*security*) zaistnienia stanu zagrożenia (lub innej miary charakteryzującej możliwość wystąpienia zagrożenia, np. miary rozmytej);
2) kryterium powagi (*severity*) stanu zagrożenia (np. **ryzyko** oraz **wartość** zabezpieczanego systemu lub wartość dysponowanych przez niego zasobów).[78]

Wśród cech konstytutywnych, wyróżniających zagrożenia informacyjne spośród innych, należy wyróżnić: brak politycznych i geograficznych granic, anonimowość przeciwników, niejasne prawo lub brak uregulowań prawnych, niejasna odpowiedzialność. Trudności w rozróżnieniu aktów dokonywanych w cyberprzestrzeni mogą dotyczyć odróżnienia aktu kryminalnego od cyberterroryzmu lub aktu wojny. Do tego typu niebezpiecznej działalności zachęcają sprawców uproszczenia funkcjonalności technologii, czemu towarzyszy spadek cen urządzeń, a także coraz bardziej rozwinięty rynek usług cyberprzestępstw „zdobywania informacji". [79]

Aktualna, rzetelna i dokładna informacja jest istotną wartością w każdej dziedzinie bezpieczeństwa narodowego. W warunkach konkurencji, rywalizacji i konfliktu celem każdej ze stron sytuacji jest uzyskanie przewagi informacyjnej (biznesowej, strategicznej, politycznej). Jednym z wymogów skutecznego zwalczania terroryzmu jest terminowe wykrywanie

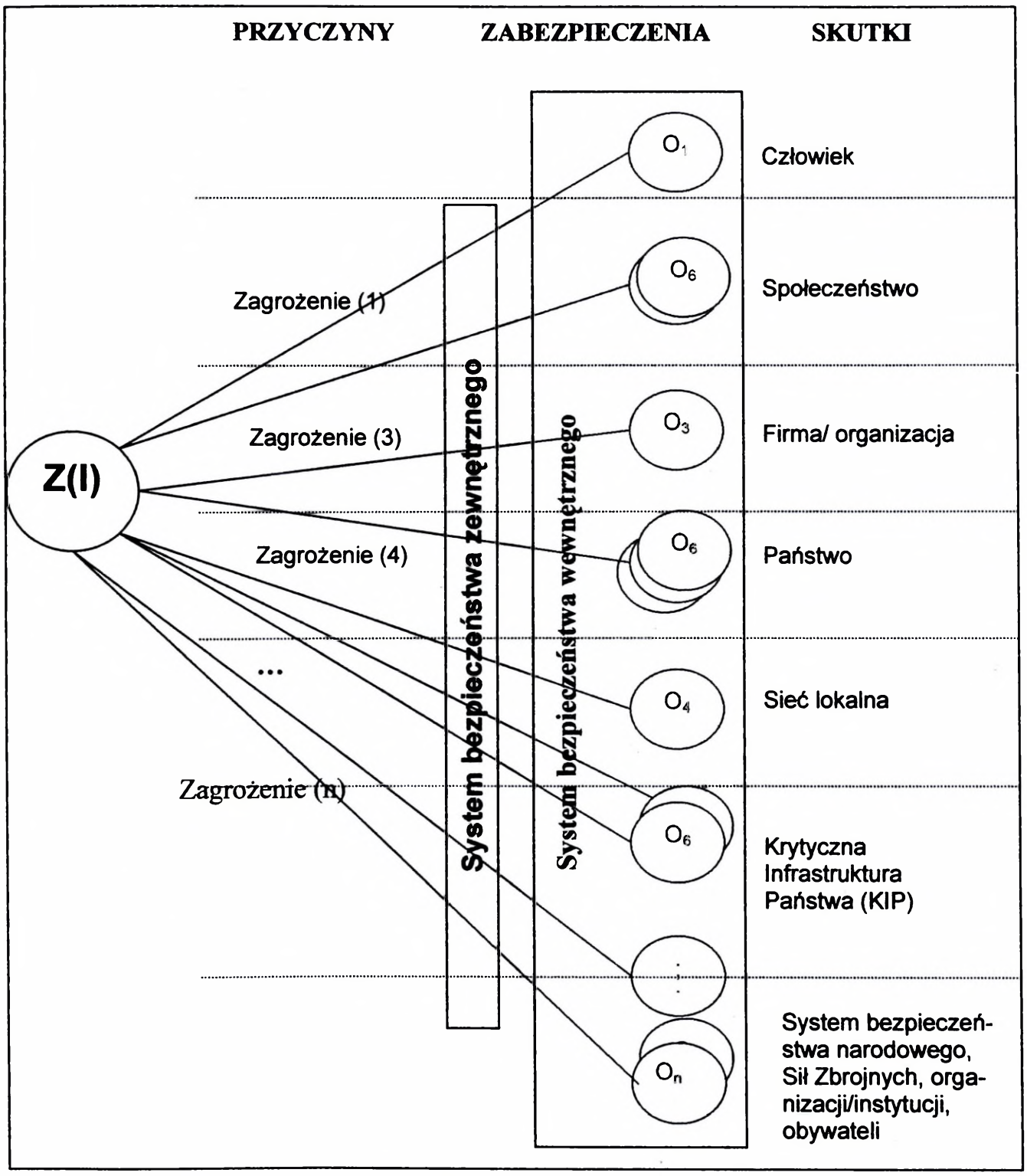
---

[78] P. Sienkiewicz (red.), *Teoria ,..., op.cit.,* s.10.

[79] Karty kredytowe, 22%, 0,30-5 USD; Konta bankowe, 21%, 30-400 USD; Hasła do kont e-mail, 8%, 1-350 USD; Programy do wysyłki poczty: 8%, 8-10 USD; Adresy e-mail: 6%, 2-4 USD/MB; Serwery Proxy: 6%, 0,5-3 USD; Pełne dane osobowe: 6%, 10-150 USD; informacje o oszustwach: 6%, 10 USD/na tydzień; Numery SSN (*social security numbers*): 3%, 5-7 USD; Serwery Unix ze złamanymi zabezpieczeniami: 2%, 2-10 USD. Źródło: Raport o zagrożeniach pochodzących z Internetu. Tom XII, październik 2007

symptomów zagrożenia przez system wczesnego ostrzegania (monitoringu) i informowanie ośrodków decyzyjnych.[80]

Istotę zagrożeń informacyjnych, wskazując na przyczynę, zabezpieczenia i skutki przedstawia rysunek 2-7.

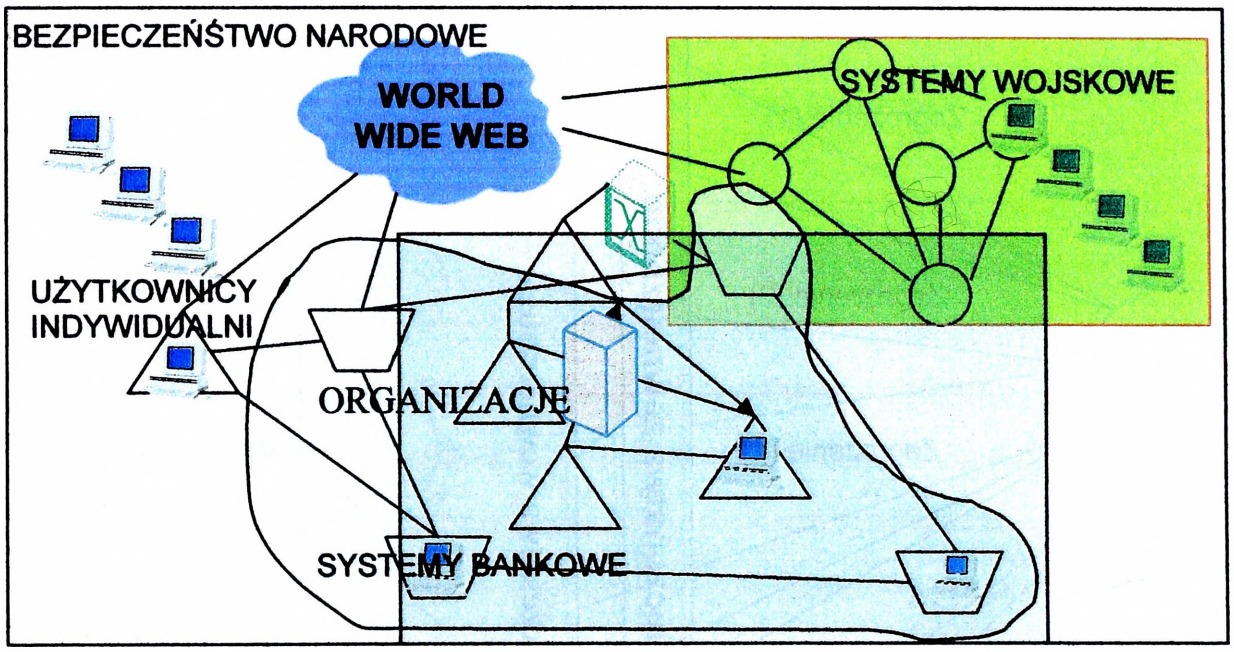


Rysunek 2-7. Istota zagrożeń informacyjnych
Źródło: opracowanie własne.

[80] K.Lidel, Zarządzanie informacjami w sytuacji zagrożeń terrorystycznych dla bezpieczeństwa państwa. Rozprawa doktorska, AON, Warszawa 2009.

2.4. Sytuacje zagrożeń dla bezpieczeństwa informacyjnego

Możliwe i prawdopodobne sytuacje zagrożeń dla bezpieczeństwa informacyjnego należy rozpatrywać w różnych płaszczyznach bezpieczeństwa, bowiem zagrożenia mogą występować na różnych poziomach organizacyjnych: państwowym, organizacji i indywidualnego człowieka. Zagrożenia związane zwłaszcza z infrastrukturą krytyczną, mogą przenosić się poza granice państwa. Wpłynęło to na propozycję prowadzania wspólnej polityki bezpieczeństwa w ramach Unii Europejskiej i NATO. Obecnie każdy system informacyjny jest narażony na możliwość ataku, którego ofiarami stają się indywidualni odbiorcy różnych usług internetowych (rysunek 2-8).



Rysunek 2-8. Obszary informacyjnie wrażliwe, newralgiczne w systemie bezpieczeństwa państwa
Źródło: H. Świeboda, *Zagrożenia informacyjne*. BOS'08, op.cit.

Sytuacje zagrożeń dla bezpieczeństwa informacyjnego, mogą się pojawiać w przypadku „napięć" w stosunkach między państwami, prowadząc do sytuacji kryzysowych.[81]

Bezpieczeństwo informacyjne może być zagrożone w sytuacji działania grup przestępczych stricte kryminalnych, dokonujących ataków na system bankowy. Grozi to destabilizacją finansów państw i wzrostem „społecznego wzburzenia". Niebezpieczeństwo stwarzają organizacje typu korporacje, manipulujące informacją przekazywaną do mediów, dążące np. do

[81] W przypadku Polski takie sytuacje występują w stosunkach z Rosją szczególnie napięte po zaangażowaniu się Polski w „pomarańczową rewolucję" na Ukrainie. Dodatkowo rozbieżności obciąża kwestia budowy elementów amerykańskiej tarczy antyrakietowej. Latem 2008 roku pojawiła się informacja w formie groźby o możliwym ataku w polskiej cyberprzestrzeni. Jedna z najtrudniejszych kwestii obciążających stosunki polsko-rosyjskie jest niewyjaśniona sprawa zbrodni katyńskiej. Udział Polski w wojnie w Iraku, a obecnie w Afganistanie również skutkuje podwyższonym ryzykiem ataków w cyberprzestrzeni.

zachwiania wartości złotego.[82] Oczywiste jest też, że bezpieczeństwo może być także zagrożone przez różnego rodzaju szaleńców, którzy chcą popisać się swoimi umiejętnościami.

Z punktu widzenia bezpieczeństwa państwa, najistotniejszym obszarem jest Krytyczna Infrastruktura Państwa (KIP), na którą składają się obiekty szczególnie ważne dla bezpieczeństwa państwa i obronności, ale również systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie inne obiekty. Dotyczy to takich obiektów, jak: obiekty budowlane, urządzenia, instalacje, usługi istotne z punktu widzenia bezpieczeństwa obywateli, ale także służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, instytucji i przedsiębiorców.[83] Istotnymi składnikami infrastruktury krytycznej są m.in. systemy: zaopatrzenia w energię i paliwa, łączności i sieci teleinformatycznych, finansowe, zaopatrzenia w żywność i wodę, ochrony zdrowia, transportowe i komunikacyjne, ratownicze, zapewniające ciągłość działania administracji publicznej.[84] Należy podkreślić, że najsłabszym punktem infrastruktury jest styk sektorów prywatnego i publicznego oraz brak zadawalających rozwiązań instytucjonalnych zapewniających bezpieczeństwo informacyjne.

Wiele działań w przestrzeni cybernetycznej definiowana jest jako cyberprzestępczość, która coraz częściej przejmuje wymiar terroryzmu[85]. Powodem są dane na temat krytycznej infrastruktury dostępne w Internecie a przejęcie kontroli nad energią, wodą, transportem, telekomunikacją, bankowością, finansami, służbami medycznymi, czy w końcu instytucjami rządowymi są coraz częściej celem terrorystów. Cyberprzestępczość jest faktem, a cyberterroryzm pozostaje nadal fikcją. Coraz częściej mamy do czynienia z terroryzmem informacyjnym inaczej nazywanym „piractwo informacyjne" są odmianami wojny informacyjnej pozwalającej osiągnąć założone cele.[86]

W nowoczesnych państwach krytyczna infrastruktura w znacznym stopniu odpowiada za procesy homeostazy, czyli dynamicznej równowagi funkcjonalnej (w rozumieniu systemowym), warunkując prawidłowe działanie mechanizmów adaptacyjnych społeczeństw, w tym reakcji na coraz bardziej dynamicznie pojawiające się nowe zagrożenia np. przestępstw

---

[82] Znamiona działania destabilizującego gospodarkę (2008), dla osiągnięcia własnych korzyści z osłabienia złotego, miała informacja o spadku jego wartości przekazana przez bank JP Morgana. A także spekulacje kursem złotego na początku roku 2009 przez banki inwestycyjne, wykorzystujące światowy kryzys by poprawić swoje wyniki finansowe.

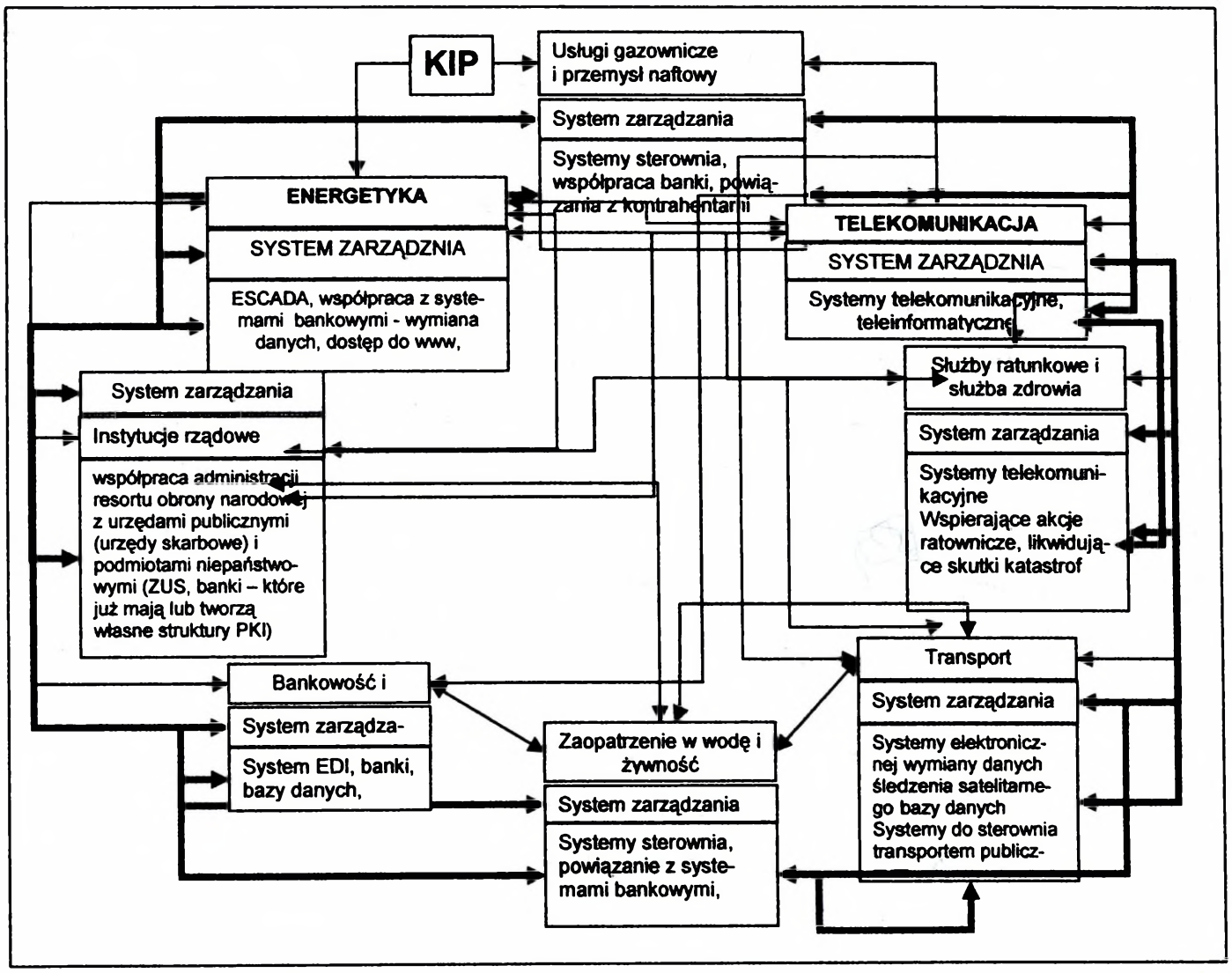
[83] Ustawa z dnia 26 kwietnia 2007r. o zarządzaniu kryzysowym, Dziennik Ustaw Nr 89/2007r., poz. 590.

[84] P.Sienkiewicz, H.Świeboda, M.Pelc, *Aspekty logistyczne bezpieczeństwa krytycznej infrastruktury państwa.* Wyd. Specjalne ZN AON nr 2(67)B Warszawa 2007.

[85] Pogląd taki wyraża np. S.Ghernaouti-Heli z Lozanny specjalistka od cyberprzestępczości [za:] M.M.Szewczyk, *Cyberterroryzm jako zagrożenie współczesnego świata.* Warszawa 2009, s.43. [w:] *Cyberterroryzm nowe wyzwania XXI wieku.* pod red. T.Jemioły, J.Kiselnickiego, K.Rajchela, Wyd. WSP w Szczytnie, Warszawa 2009.

[86] T.Jemioło, Wyzwania i zagrożenia dla globalnego bezpieczeństwa informacyjnego w pierwszych dekadach XXI wieku. Wyd. WSP w Szczytnie, Warszawa 2009, s.75.

komputerowych. Wynika to z wielopoziomowych interakcji pomiędzy sektorami gospodarki powiązanej sieciami telekomunikacyjnymi, bowiem elementy tej infrastruktury są współzależne (rysunek 2-9).[87]



Rysunek 2-9. Strefy współzależności systemów informatycznych i teleinformatycznych
Źródło: P.Sienkiewicz, *Methods of analysis of the risk of terrorist threats*. Międzynarodowa konferencja „Terrorism and security of mass events", Waplewo 2008.

Według danych zawartych w raporcie o globalnym bezpieczeństwie, rządy niektórych państw coraz częściej używają Internetu do celów wywiadowczych i ataków obejmujących systemy energetyczne, finansowe, kontroli ruchu powietrznego czy sytemu agencji rządowych.[88] Główne wnioski z raportu wskazują, że rządy oraz organizacje z nimi współdziałające wykorzystują Internet do przeprowadzania cyberataków oraz do szpiegostwa internetowego. Ataki wymierzane są w strategiczne elementy infrastruktury państw, takie jak elektryczność, kontrola ruchu powietrznego, rynki finansowe czy komputerowe sieci rządowe.

---

[87] P.Sienkiewicz, H.Świeboda, *Bezpieczeństwo europejskiej przestrzeni cybernetycznej*. AMW, Gdynia 2009 (w druku).

[88] Virtual Criminology Raport MCAfee, 2007, dostęp online: www.mcafee.com.

W celach szpiegowskich Internet jest obecnie wykorzystywany przez 120 krajów. Stwierdzono również, że wiele cyberataków pochodzi z Chin i mogą być sponsorowane przez chiński rząd, przy czym przeprowadzane są tak, aby pozostały niezauważone przez systemy obronne atakowanego kraju. Problem bezpieczeństwa teleinformatycznego stanowi jedno z głównych przedsięwzięć w zakresie uregulowań prawnych i wdrażanych programów naukowych w Unii Europejskiej.[89]

Składowe systemu Krytycznej Infrastruktury Państwa są ze sobą powiązane. Siła powiązań zależy między innymi od: niezależności energetycznej państwa; technicznego i technologiczny rozwoju, poziomu gospodarczego. Zdefiniowania macierz współzależności[90] wskazuje na ważność energetyki i telekomunikacji (tabela 2-6).

Tabela 2-6. Macierz współzależności sektorów infrastruktury krytycznej państwa

	usługi informacyjne i łączność	finanse i bankowość	wodociągi i dystrybucja żywności	energetyka	surowce energetyczne	transport	służba zdrowia i system ratowniczy	władza centralna
usługi informacyjne i łączność	–	M	L	H	M	L	M	M
finanse i bankowość	H	–	L	H	M	M	L	M
wodociągi i dystrybucja żywności	M	M	–	H	M	H	M	L
energetyka	H	M	M	–	H	M	M	M
surowce energetyczne	H	M	M	H	–	H	M	M
transport	H	M	L	H	H	–	L	M
służba zdrowia i system ratowniczy	H	M	M	H	H	H	–	M
władza centralna	H	M	L	H	H	M	M	–

Źródło: T.Jemioło, (kier.) ***Modelownie zagrożeń dla bezpieczeństwa informacyjnego państwa. Teoria walki informacyjnej.*** **AON ,Warszawa 2004, s. 116.**

---

[89] W 2003 roku Komisja Europejska zaproponowała powołanie ponadnarodowej, europejskiej agencji zajmującej się zapewnieniem bezpieczeństwa w Internecie. Europejska Agencja Bezpieczeństwa Sieci i Informacji (*The European Network and Information Security Agency*) rozpoczęła działalność w styczniu 2004 roku i będzie działać przez okres siedmiu lat. Wówczas kompetencje ENISA, przejmie ustanowiony w grudniu 2007 roku, Europejski Urząd ds. Rynku i Łączności Elektronicznej. Na bazie rezultatów badań, przeprowadzonych w latach 2006-2007 w ENISA, a dotyczących możliwości utworzenia systemu typu EISAS (*European Information Sharing and Alerting System*), czyli ogólnoeuropejskiego systemu wymiany i dostępu do informacji dotyczących bezpieczeństwa komputerowego oraz ostrzegania przed zagrożeniami w sieci Internet przystąpiono do jego realizacji w ramach projektu FISHA (*A Framework for Information Sharing and Alerting*). W pracach tych uczestniczy CERT Polska.

[90] R.Gogela, L.Novàk, A.Šefčik: *Critical Infrastructure Modelling*, [w:] Security and Protection of Information, 2003.

2.5. Cyberterroryzm jako zagrożenie dla bezpieczeństwa narodowego

Ryzyko zagrożeń informacyjnych dla bezpieczeństwa państwa związane jest również ze zjawiskiem określanym mianem cyberterroryzmu. Jakkolwiek różne są definicje tego zjawiska, realizuje się ono w postaci działań blokujących, niszczących lub zniekształcających informację przetwarzaną, przechowywaną i przekazywaną w systemach teleinformatycznych, powodując również ich destrukcję. Jest to bardzo szeroki zakres działań w przestrzeni cybernetycznej, prowadzący do niszczenie zasobów (i baz danych) strony atakowanej, ale również służy działaniom propagandowym, skierowanym na oddziaływania psychologiczne, których celem jest destrukcja w sferze psychicznej i moralnej ludności cywilnej i walczących wojsk. Dowolność manipulacji informacją, jak i wykorzystywanie jej do doraźnych celów politycznych przynosi z gruntu negatywne skutki w postaci chociażby braku zaufania, apatii i wycofania społecznego, może być przyczyną niepokojów społecznych.[91] Na stopień zagrożenia wpływa również ranga instytucji, organizacji, regionu itp., jako obiektu działań destrukcyjnych. Nawet, jeżeli zagrożenia informacyjne, a w szczególności zagrożenie cyberterroryzmem jest wyolbrzymiane, to realnym zagrożeniem pozostają tzw. cyberprzestępstwa, które zdarzają się codziennie. Trudno przewidzieć konsekwencje np. wielokrotnego ataku na system bankowy, którego jednym z następstw może być bankructwo banku i wzrost „społecznego wzburzenia".

Cyberterroryzm (traktowany niekiedy jako *soft terrorism*) rozumiany jest najczęściej, jako działania mające na celu niszczenie bądź zniekształcanie informacji przesłanej, przetwarzanej i przechowywanej w systemach teleinformatycznych. Można także najkrócej ująć to jako działania terrorystyczne w przestrzeni cybernetycznej. Mogą być one dziełem wielu zróżnicowanych podmiotów, tak jak różne, o różnej skali i intensywności, mogą być ich następstwa (rysunek 2-10).

Przyjmując cyberterroryzm, jako *politycznie motywowany atak lub groźbę ataku na komputery, sieci, lub systemy informacyjne w celu zniszczenia infrastruktury oraz zastraszenia lub wymuszenia na rządzie i ludziach daleko idących politycznych i społecznych celów,* możemy wyróżnić dwa rodzaje akcji cyberterrorystycznych:

- destrukcyjne działania informacyjne w cyberprzestrzeni;
- ataki fizyczne na systemy informacyjne.

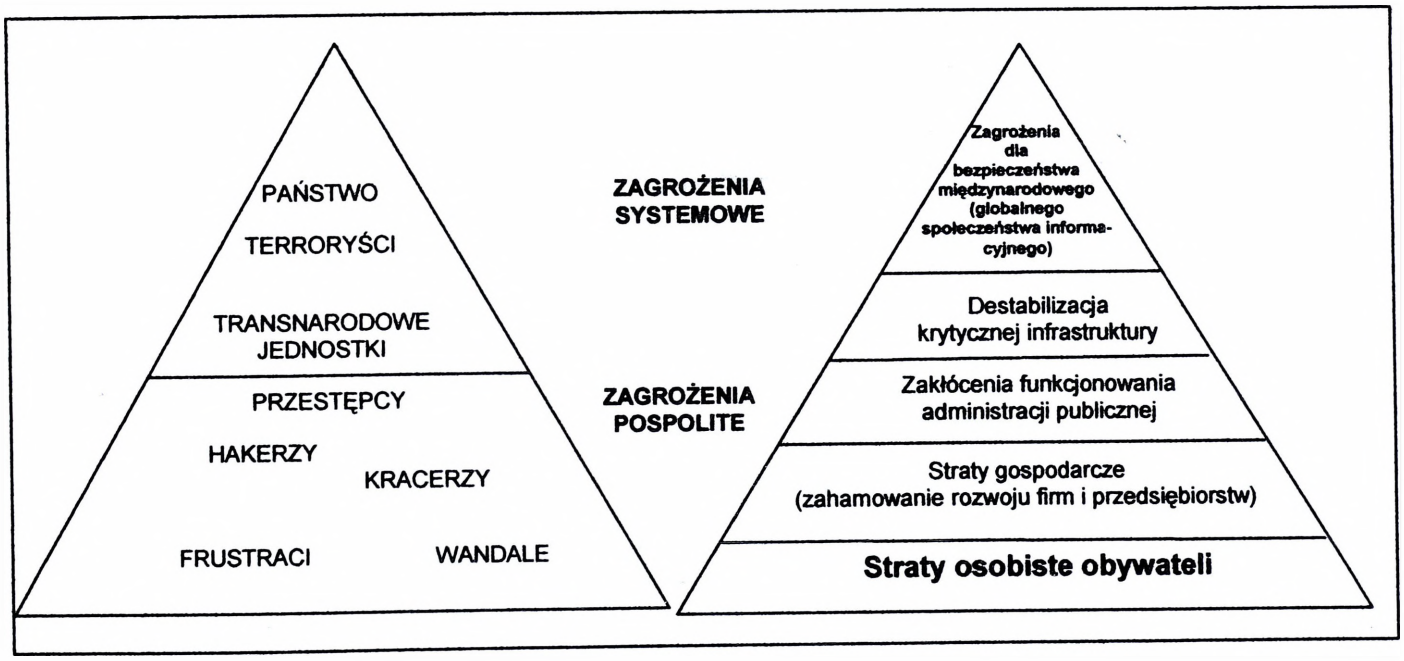
---

[91] Dobrym przykładem jest wymuszenie, przez społeczeństwo, przyjęcia warunków pokojowego rozwiązania konfliktu w Kossowie,. Przyczyną nie był atak cyberterrorystyczny a zrzucenie bomb grafitowych, które spowodowały brak energii na ¾ obszaru kraju. Łatwo wyobrazić sobie podobny atak ale przeprowadzony w cyberprzestrzeni na system sterujący SCADA elektrowni. Zdecydowanie ekonomiczniejszy, niegrożący śmiercią cywilom.

Bez trudu można przyjąć za możliwe i prawdopodobne sytuacje, w których występują różne kombinacje powyższych zagrożeń. Zapewne w niedalekiej przyszłości możemy być świadkami zsynchronizowanego ataku, polegającego na cybernetycznym sparaliżowaniu sieci telefonicznej lub elektrycznej z jednoczesnym użyciem np. materiałów wybuchowych. Organizacje terrorystyczne doceniają znaczenie zasobów informacyjnych we współczesnym świecie, zakładając, że atak paraliżujący infrastrukturę informacyjną może przynieść większy efekt, niż „zwykły" akt terrorystyczny.[92]

Sprawców zagrożeń informacyjnych dla bezpieczeństwa państwa, (organizacji i instytucji), można podzielić na dwie główne kategorie (rysunek 2-10):

1) sprawcy zagrożeń „systemowych" (*structured threat*), do których należy zaliczyć organizacje państwowe (agendy, specjalistyczne jednostki), organizacje terrorystyczne i różnego rodzaju transnarodowe grupy przestępcze;
2) sprawcy zagrożeń „pospolitych"(*instructured threat*) (np.: przestępcy, frustraci, wandale, hakerzy, krakerzy itp.).[93]



Rysunek 2-10. Hierarchia zagrożeń informacyjnych i ich skutków
Źródło: P.Sienkiewicz, H.Świeboda, *„Analiza systemowa zjawiska cyberterroryzmu".* ZN AON nr 2(63) 2006, s.10.

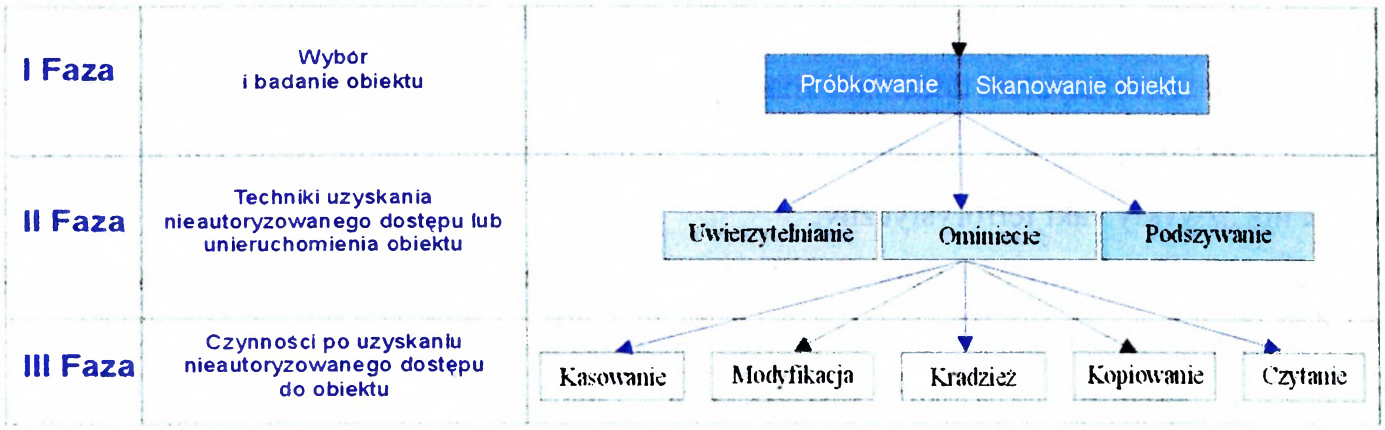
Działania podmiotów pozapaństwowych (sprawców „pospolitych"), które w pewnych warunkach mogą być inspirowane przez państwo, można określić, jako „cyberataki". W typowym procesie cyberataku można wyróżnia się trzy podstawowe fazy, z których pierwsza obejmuje „próbkowanie" (skanowanie), będące formą rozpoznania słabych stron obiektu

---

[92] H.Świeboda, P.Sienkiewicz, E.Lichocki, *Analiza systemowa zjawiska cyberterroryzmu.* ZN AON, Nr 2(63), Warszawa 2006.

[93] K.Kennedy, B.Lawlor, A.Nilson, *Grand Strategy for Information Age National Security.* Air University Press, Maxwell Air Force Base, Alabama August 1997, s.8.

lub systemu, druga wiąże się z uzyskaniem dostępu do zasobów systemu, trzecia zaś stanowi realizację właściwego celu działania (np.: kradzież, kopiowanie, kasowanie, czytanie, modyfikacja) (rysunek 2-11).



Rysunek 2-11. Model „cyberataku" na obiekty teleinformatyczne
Źródło: P.Sienkiewicz, H.Świeboda, E.Lichocki, *Analiza systemowa zjawiska cyberterroryzmu*. Zeszyty Naukowe Nr 2 (63), AON, Warszawa 2006.

Z punktu widzenia bezpieczeństwa informacja ma następujące cechy: (1) tajność (*confidentiality*), (2) integralność (*integrity*), (3) dostępność (*availability*). Każdy atak stanowi zagrożenie dla poszczególnych atrybutów lub ich kombinacji. Złożoność samego zjawiska przestępstw komputerowych, popełnianych przez podmioty nieustrukturalizowane oraz świadomość braku doskonałych systemów zabezpieczeń powoduje, że zagrożenia teleinformatyczne, w szczególności zaś cyberterrorystyczne, stały się nowym wyzwaniem dla bezpieczeństwa narodowego.

Po raz pierwszy termin „cyberterroryzm" pojawił się w raporcie o zagrożeniach komputerowych w Szwecji, w 1979 roku. Obejmował on wszelką działalność z użyciem komputerów, mającą na celu niszczenie systemów teleinformatycznych, systemów nadzoru i kontroli, programów, danych itp., a w konsekwencji zastraszanie rządów i społeczeństw, wywieranie presji psychologicznej, doprowadzenie do zagrożenia życia lub powstania znacznych strat materialnych.

W latach 80. terminem „cyberterroryzm" posługiwano się w amerykańskich służbach specjalnych, wskazując na możliwości przeprowadzenia ataków elektronicznych przez wrogów Stanów Zjednoczonych. W 1998 r., w Centrali FBI utworzono Centrum Ochrony Infrastruktury Narodowej (NIPC), którego zadaniem jest koordynowanie działań w zakresie gromadzenia informacji o zagrożeniach, reagowanie na zagrożenia informacyjne lub zamachy na elementy krytycznej infrastruktury państwa.

W Internecie znajduje się bardzo wiele programów, które umożliwią odszyfrowanie kodu dostępu do komputera lub bazy danych oraz włamanie się do systemu. Wraz ze zmniej-

szaniem się potrzebnych umiejętności do przeprowadzenia cyberataku, zwiększa się skuteczność i jakość programów mających to ułatwić. W konsekwencji uważa się, że każdy może zostać „cyberterrorystą".[94]

Po wydarzeniach z 11 września 2001 r. zwrócono uwagę na możliwość podobnych ataków terrorystycznych na całym świecie, w tym na możliwe i prawdopodobne zmasowane „cyberataki" na systemy teleinformatyczne USA i sprzymierzeńców, wykorzystywane w walce ze światowym terroryzmem. Wówczas w amerykańskiej ustawie antyterrorystycznej rozszerzono definicję terroru o cyberterroryzm (np. hakerska penetracja systemów informacyjnych o dużym znaczeniu dla bezpieczeństwa narodowego zagrożona jest w USA nawet karą dożywotniego więzienia).

W raporcie pt.: *"Cyberataki podczas wojny z terroryzmem"*, opracowanym przez Institute for Security Technology Studiem, wyróżniono cztery podstawowe potencjalne kategorie źródeł cyberterroryzmu, a mianowicie: (1) typowe grupy terrorystyczne; (2) „państwa zbójeckie", do których mogą dołączyć inne kraje; (3) sympatycy terrorystów oraz antyamerykańscy hakerzy; (4) poszukiwacze silnych wrażeń, niekierujący się przesłankami politycznymi lub ideologicznymi.

Jednocześnie, ze względu na specyfikę cyberprzestrzeni, należy zjawisko cyberterroryzmu rozpatrywać w aspekcie:

- skutków destrukcyjnych (tak jak w klasycznych zamachach terrorystycznych);
- środka propagandowego i informacyjnego (dezinformacyjnego).

Można stwierdzić, że w wąskim znaczeniu cyberterroryzm to działalność terrorystyczna w systemach teleinformatycznych ukierunkowana na zniszczenie lub modyfikację danych w tych systemach, których następstwem mogą być ofiary śmiertelne lub zniszczenie mienia w znacznych rozmiarach (zazwyczaj celem jest jedno i drugie). W szerszym znaczeniu jest to wszelka działalność terrorystyczna związana z cyberprzestrzenią (systemami teleinformatycznymi), włączając w to fizyczne ataki na systemy oraz aktywność propagandową. Działalność taka może przyczynić się do pozyskiwania informacji przydatnych do realizacji bardziej złożonych celów klasycznych akcji terrorystycznych, na przykład zamachów bombowych. Typologię destrukcyjnych działań na obiekty informacyjne oraz kwalifikację sprawców i ich działań przedstawiają tabele 2-7 i 2-8.

---

[94] A.Bógdał-Brzezińska, M.F.Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa.* Oficyna Wydawnicza ASPRA-JRS, Warszawa 2003, s.90.

Tabela 2-7. Typologia destrukcyjnych działań na obiekty informacyjne

NAZWA DZIAŁANIA	CEL DZIAŁANIA
Próbkowanie (*probe*)	Dostęp do obiektu poprzez analizę jego charakterystyk
Przepełnienie (*flood*)	Dostęp poprzez „przepełnienie" możliwości systemu przetwarzania
Uwierzytelnianie (*authenticate*)	Dostęp osoby nieuprawnionej podającej się za uprawnioną oraz w razie konieczności przekazanie informacji potrzebnej do poprawnego uwierzytelniania
Ominięcie (*bypass*)	Ominięcie zabezpieczeń, poprzez wykorzystanie alternatywnej drogi osiągnięcia obiektu
Podszywanie (*spoof*)	Przedstawienie się lub modyfikowanie pakietów w trakcie połączenia, aby osiągnąć prawo dostępu do zasobów
Czytanie (*read*)	Dostęp do informacji, do której brak jest uprawnienia
Kopiowanie (*copy*)	Możliwość tworzenia kopii informacji przez osoby nieuprawnione
Kradzież (*steal*)	Przejęcie zasobów przez osobę nieuprawnioną, bez pozostawienia kopii w obiekcie
Modyfikacja (*modify*)	Zmiana zawartości lub charakterystyk obiektu
Usunięcie (*detale*)	Zniszczenie obiektu ataku

Źródło: A.Barczak, T.Sydoruk, *Bezpieczeństwo systemów informatycznych*. Wyd. Akademii Podlaskiej, Siedlce 2002, s.35.

Tabela 2-8. Klasyfikacja sprawców i ich działań

SPRAWCY	DZIAŁANIA
Hakerzy	Czytanie i/lub modyfikacja zasobów obiektu
Szpiedzy	Kradzież i kopiowanie danych w celu przekazania ich do określonego adresata
Terroryści	Modyfikacja zasobów w celu destrukcji lub wywołania efektu propagandowego.
Nieuczciwi pracownicy	Kradzież i/lub kopiowanie danych w celu udostępnienia ich konkurencji lub kompromitacji firmy z powodów osobistych
Profesjonalni przestępcy	Kradzieże i kopiowanie zasobów systemu, ich kasowanie i modyfikowanie w celu uzyskania korzyści majątkowej
Wandale	Bezmyślne kasowanie danych i/lub ich modyfikacja
Voyeur	Czytanie cudzych danych, lub kopiowanie z powodów emocjonalnych

Źródło: A.Barczak, (2002), *Bezpieczeństwo*, ..., op.cit., s.34

Złożoność zjawiska przestępstw komputerowych i świadomość braku doskonałych systemów zabezpieczeń powoduje, że zagrożenia teleinformatyczne, w szczególności zaś cyberterrorystyczne stały się nowym wyzwaniem dla bezpieczeństwa narodowego.[95]

[95] Wizja Sił Zbrojnych RP 2030, MON, Departament Transformacji, Warszawa 2008, s.10: systematycznie rosnący poziom uzależnienia społeczeństwa od systemów teleinformatycznych spowoduje, że realnym zagrożeniem dla bezpieczeństwa państwa stanie się cyberterroryzm. Jego istotą będzie atak i zniszczenie zasobów informacyjnych, systemu obronnego państwa oraz zasadniczych elementów systemu informatycznego (infosfe-

Liczne przykłady funkcjonowania stron WWW poświęconych terroryzmowi (szacuje się, że stron poświęconych tylko dżihadowi jest w sieci 150–200), potwierdzają znaczenie technologii internetowych jako efektownego narzędzia propagandy terrorystów. W sieci znajdują się dane o organizacjach terrorystycznych i ich celach, a ponadto oferowana jest sprzedaż „gadżetów", takich jak koszulki, plakaty, kasety video itp. Inne strony werbują za pomocą Internetu ochotników do walki ze swoimi przeciwnikami. Oferowane są informacje o metodach przeprowadzania zamachów terrorystycznych, technologii konstrukcji bomb, ponadto dostępne są informacje o źródłach dofinansowania przedsięwzięcia o charakterze przestępczym.[96]

Aktywność w sieciach teleinformatycznych umożliwia organizacjom terrorystycznym:

- bezpieczne, wzajemne komunikowanie się ze sobą, w tym przesyłanie danych;
- prowadzenie działalności informacyjno-propagandowej;
- pozyskiwanie informacji z różnych działań, w tym uzyskanych z penetracji stron www;
- działalność sensu stricte terrorystyczną, na przykład podejmowanie próby spowodowania katastrofy lotniczej na skutek zniekształcenia danych w wyniku włamania do systemów kontroli lotu.

Internet stał się pozbawionym granic swoistym „obozem szkoleniowym" trudnym do zlokalizowania dzięki sprawności i szybkości zacierania śladów działań w sieci. Specjaliści prognozują szczególne nasilenie tego typu działalności ze strony islamskich terrorystów. Od kilku lat w sieci toczy się „cyberwojna", wywołana przedrukiem karykatur Mahometa, której efektem są nasilone ataki hakerów islamskich na strony internetowe państw zachodnich.[97]

Przykłady ataków uznanych za cyberterrorystyczne przedstawia tabela 2-9.

---

ry) zarządzającego m.in. energetyką, gospodarką oraz finansami państwa. Wzrośnie również poziom zagrożeń dla bezpieczeństwa energetycznego Polski.

[96] Interesującym przykładem cyberterroryzmu może być działalność Usamy Ibn Ladina w sieci, bowiem podczas wojny w Iraku i Afganistanie przechwycono komputery a także wyrafinowane oprogramowanie pozwalające modelować (kształtować) katastrofy zapór i diagnozować sposób efektywnego ich uszkodzenia. Znaleziono również instrukcje obsługi Internetu oraz przykłady łącznia się z Pakistanem i innymi miejscami. Rozpoznanie zasobów Al Quaidy pozwala na przypuszczenie, że terroryści nie tylko doskonalą umiejętności telekomunikacyjne, ale również opanowują narzędzia do hakingu i taktyki przeprowadzania ataków komputerowych w sieci. Stwierdzono korzystanie ze stron oficjalnych, z których można było uzyskać specyficzne informacje o elektrowniach i wodociągach, a także innych systemach krytycznych infrastruktur.

[97] P.Sienkiewicz, H.Świeboda, E.Lichocki, *Analiza systemowa cyberterroryzmu* ZN AON, Nr 2(63), Warszawa 2006.

Tabela 2-9. Przykłady ataków uznanych za cyberterrorystyczne[98]

ROK	ATAK CYBERTERRORYSTYCZNY	OPIS
1979	Raport o zagrożeniach komputerowych (Szwecja)	
1992	Koncepcja „autostrad informacyjnych"	
1995	Widmo „elektronicznego Pearl Harbor"	
1986	Próba kradzieży wyników badań z laboratorium Berkeley Labs przez hakera z Hanoweru	Laboratorium pracowało dla Pentagonu Haker działał na zlecenie Rosji
1998	Groźba sabotażu wobec indonezyjskiego systemu bankowego w przypadku odmowy uznania wyborów w Timorze Wschodnim	
1999	Ataki typu DoS na komputery NATO w Kosowie	
	Od marca 1999 do 2000 dokonano 89 cyberataków na 60 agencji rządowych w Malezji	Celem były wrażliwe resorty opieka społeczna, imigracja, skarb państwa
2000	Blokada Yahoo, Amazon, CNN, eBay Grupa pakistańskich hakerów zniszczyła ok.600 indyjskich stron internetowych, oraz przejściowo przejęła kontrolę nad niektórymi indyjskimi sieciami komputerowymi	Atak DDoS
	Wirus I Love You	Wielomilionowe straty
2001	USA i CHRL w stanie „wojny elektronicznej"	164 ataki na strony internetowe. Obie strony użyły systemów komputerowych Korei dla wejścia do systemu przeciwnika unikając odkrycia
	Blokada witryny Białego Domu i New York Times. Atak z Chin	
	Chińscy hakerzy dokonali kilkuset cyberataków na największe japońskie firmy Chin działające w CHRL	W odwecie za zaostrzenie przez Japonię polityki wobec Chin
2002	Zaatakowano 13 podstawowych serwerów DNS, które kierują ruchem w całej amerykańskiej sieci	Atak typu Dos
2007	Atak na Estonię – atak na strony rządowe, serwisy bankowe.	Eskalacja konfliktu miedzy Rosją a Estonią, którego powodem było przeniesienie pomnika żołnierzy radzieckich z centrum Talina.
	Penetracja sieci wojskowej Pentagonu Atak na Departament Obrony Stanów Zjednoczonych	Atakujący Ludowa Armia Wyzwolenia
	Penetracja sieci rządowej Niemiec przez Chiny Ostry protest Angeli Merkel	Zainstalowali na niemieckich systemach rządowych, programy typu „koń trojański" do przejęcia kontroli nad systemem

[98] Dane zebrane z raportów i stron firm profesjonalnie zajmujących się bezpieczeństwem sieciowym.

	Blokada angielskich stron rządowych, również należących do korporacji finansowych i banków	Rząd W. Brytanii oskarżył Chiny Szpiegostwo przemysłowe
	USA: Powtórzenie ataku podobnego, jaki miał miejsce w 2002.	Atak Dos na 13 komputerów DNS
2008	Dopełnienie konfliktu zbrojnego między Gruzją a Rosją	Ataki DDoS Ataki przypisywane są cyberprzestępczej organizacji Russian Business Network
	Szereg ataków na serwery Estonii, Łotwy, Litwy, Ukrainy. Przyczyną prawdopodobnie ustawy zakazujące wykorzystywania symboli ZSRR	Atak na strony WWW i umieszczenie czerwonych flag z sierpem i młotem
	Groźba Kremla cyberatakiem na Polskę jako odpowiedź na budowę tarczy antyrakietowej	
2009	Włamanie do sieci energetycznej w USA, byli również zainteresowani wodociągami i systemami kanalizacyjnymi.[99]	Chińscy i rosyjscy cyberprzestępcy pozostawili oprogramowanie, które mogło posłużyć do zakłócenia pracy całego systemu
	Departament Obrony USA posądził o kradzież supertajnych planów myśliwca F-35 Chiny	Chińscy szpiedzy

Źródło: opracowanie własne.

Efektem wzrastającej liczby „cyberataków" jest pojawienie się tendencji do stworzenia kontrofensywnej osłony. Obecnie taki system posiadają: USA, Chiny, Korea Północna, Wielka Brytania, Kuba, Irak, Libia, Francja i Tajwan.[100]

2.6. Współczesna walka informacyjna

Uważa się, że nie istnieje powszechnie uzgodniona definicja walki informacyjnej (załącznik III). Wyróżnić jednak można wspólną treść większości definicji wyrażającą pogląd, że walka informacyjna jest formą konfliktu, w którym informacja jest jednocześnie zasobem, środkiem walki, obiektem ataku i bronią.[101] Walka informacyjna obejmuje także fizyczną destrukcję infrastruktury, która wykorzystywana jest przez przeciwnika do działań operacyjnych. Warto odnotować spór, co do rozumienia pojęcia *Information Warfare*. Termin ten można przetłumaczyć na język polski zarówno jako „walka informacyjna", jak i „wojna informacyjna".[102]

---

[99] *Cyberatak na sieci energetyczne.* Za: Gazeta Wyborcza z 9 kwietnia 2009.

[100] A.Pietrzak, *Cyberterroryzm*. Niezależne Inicjatywa Naukowa Paradygmat. http://www.paneuropa.1.pl/index.php3?id=1063721220 .

[101] R.Stark, Future Warfare: Information Superiority through Info War. AUM AFB, 1995.

[102] J.Bloch przetłumaczyła tytuł książki D.E.Denning „*Information Warfare end Security*" jako „*Wojna informacyjna i bezpieczeństwo informacji*". W niektórych polskich publikacjach można także znaleźć

Podsumowaniem dyskusji może być stwierdzenie, że *cyberwar, infowar*, walka informacyjna, cyberterroryzm, *netwar, cyberpunks*, informacyjni wojownicy, informacyjna dominacja, obrona w cyberprzestrzeni (*cyberspace defense*), czy informacyjny chaos to tylko neologizmy dotyczące tego samego, ale bardzo szerokiego pojęcia - wojny ery informacyjnej (*infornation age warfare*).[103]

W dostępnej literaturze przedmiotu[104] brak jest wyczerpujących opracowań monograficznych na temat walki informacyjnej. Zgodnie z doktryną USA - funkcjonują trzy terminy dotyczące walki informacyjnej, a mianowicie:

- walka z systemami dowodzenia i kontroli (*Command end Control Warfare - C2W*);
- walka informacyjna (*Information Warfare - IW*);
- operacje (działania) informacyjne (*Information Operations - IO*).

Walką informacyjną są działania (operacje) informacyjne prowadzone w czasie kryzysów lub konfliktów, aby wspierać określone zadania lub osiągnąć określone cele w obszarze kontroli przeciwnika. Według niektórych specjalistów wojskowych, walka informacyjna dotyczy zmagania się we wszystkich dziedzinach aktywności społecznej (militarnej, politycznej, dyplomatycznej, ekonomicznej, etnicznej, socjalnej, infrastrukturze, kryminalnej, ideologicznej, religijnej i możliwie jeszcze innych) o uzyskanie kontroli nad określonym obszarem (dziedziną) i przewagi informacyjnej (dominacji). Walka informacyjna może być prowadzona bez formalnego wypowiedzenia (deklaracji) wojny i może być stosowana na szerokim froncie lub na wybranym polu walki - otwarcie lub skrycie. Ataki informacyjne na systemy dowodzenia, kierowania, rozpoznania i telekomunikacji, a także na elementy infrastruktury krytycznej państwa (KIP) traktowane są jako szczególnie efektywny sposób niszczenia siły przeciwnika.

Obiektem walki informacyjnej są zasoby informacyjne, systemy transmisji, zbierania, przetwarzania informacji oraz w konsekwencji procesy decyzyjne. Walka informacyjna jest prowadzona we wszystkich fazach działań wojennych, począwszy od mobilizacji do rozmieszczenia, przydziału zadań, utrzymania, zachowania i przegrupowania sił i środków na wszystkich poziomach konfliktu. Może przyjmować postać walki defensywnej i ofensywnej. Defensywna walka informacyjna jest stale stosowana zarówno w czasie pokoju i kryzysu, jak

---

termin „wojna informacyjna". Jednak R.Szpyra argumentuje, że wojna jest kategorią obejmującą wszystkie formy walki. Jest kategorią integrującą różne rodzaje walki: zbrojną, informacyjną, ekonomiczną itd.

[103] Timothy L. Sanz, "Information-Age Warfare: A Working Bibliography." Military Review. Volume LXXVIII, Number 2, March-April, 1998.

[104] Obszerne opracowanie literatury przedmiotu zawiera rozprawa habilitacyjna R.Szpyry pt. *Operacje informacyjne państwa w działaniach sił powietrznych.* AON, 2002.

i stanowi element zabezpieczenia i obrony. Ofensywna walka informacyjna może być prowadzona w różnych sytuacjach we wszystkich operacjach militarnych, a także innych niż wojna. W pełni rozwinięta i zintegrowana, ofensywna walka informacyjna stanowi potencjał efektywnie wspierający działania na polu walki.

Przyjmuje się, że walka informacyjna obejmuje trzy komponenty:

1) zdobywanie informacji z rozpoznania i wywiadu;
2) wykorzystanie systemów informacyjnych zarówno w działaniach ofensywnych jak i defensywnych;
3) kombinację różnych form działań (np. w postaci C2W).

Zdobywanie informacji z rozpoznania i wywiadu polega na pozyskiwaniu pożądanych informacji o:

- własnych siłach zbrojnych (ich dyslokacji, skuteczności prowadzenia walki oraz aktualnej działalności);
- siłach zbrojnych przeciwnika (ich dyslokacji, możliwościach bojowych, skuteczności walki, zamiarach), niezbędnych do podejmowania decyzji.

Wykorzystanie systemów informacyjnych daje dowódcom i sztabom możliwość kontrolowania aktualnej sytuacji na polu walki, synchronizacji działań oraz integracji z systemami walki (*Battlefield Operation Systems*), zapewniając: interoperacyjność i harmonizację działań dzięki:

- koordynacji działań z siłami powietrznymi i marynarką wojenną;
- pozyskaniu niezbędnych danych do efektywnego użycia nowoczesnych systemów broni;
- prowadzeniu kontroli działań oraz ich skuteczności;
- synchronizacji różnego typu operacji zarówno na tyłach, jak i wysuniętych rubieżach w działaniach połączonych.

Oczekiwane skutki walki informacyjnej przedstawia tabela 2-10.

Operacje (działania) informacyjne, są określane jako ciągłe działania sił zbrojnych w ramach wojskowego środowiska informacyjnego, które przyczyniają się do wzmocnienia możliwości sił własnych oraz ich obrony w zakresie zdobywania, przetwarzania i przekazywania informacji, w celu uzyskania przewagi, w całym spektrum walki zbrojnej, prowadzonej wewnątrz globalnego środowiska informacyjnego, przy jednoczesnym pozba-

wieniu takiej możliwości strony przeciwnej.[105] Są to działania wpływające na informacje przeciwnika i jego systemy informacyjne, z zapewnieniem ochrony własnych informacji i systemów informacyjnych.

Tabela 2-10. Oczekiwane skutki walki informacyjnej

SIŁY WŁASNE	SIŁY PRZECIWNIKA
Ochrona systemów dowodzenia, łączności i rozpoznania	Zakłócanie procesów informacyjno-decyzyjnych w systemach dowodzenia
Minimalizacja wpływu walki elektronicznej	Minimalizacja efektywności systemów dowodzenia, kierowania środkami walki, teleinformatyki, rozpoznania i walki elektronicznej
Minimalizacja zagrożeń informacyjnych bezpieczeństwa systemów dowodzenia i kierowania	Uniemożliwianie wykorzystania pełnej siły rażenia oraz obniżanie tempa działań (operacji)
Minimalizacja wpływu działań psychologicznych	Zwiększenie podatności na działania psychologiczne

Źródło: P.Sienkiewicz, H.Świeboda, *Sieci teleinformatyczne jako instrument państwa – walka informacyjna i szpiegostwo elektroniczne.* PISM, Warszawa 2008.

W operacje informacyjne mogą być angażowane wszystkie instytucje administracji rządowej, publiczne (media) i militarne (stosownie do skali operacji, szczebla wykonawczego i okoliczności), których funkcje są związane z oddziaływaniem na potencjał informacyjny własny, przeciwnika i potencjalnych przeciwników, sojuszników i potencjalnych sojuszników.

Model walki informacyjnej zakłada, że walka informacyjna występuje w trzech dziedzinach, a mianowicie: w umyśle ludzkim, w cyberprzestrzeni i w przestrzeni fizycznej. Atakujący i obiekty (cele) ataku występują, zatem na trzech poziomach (warstwach): percepcyjnym (wiedza ludzka), informacyjnym (infrastruktura informacyjna) i fizycznym (dane).[106]

Poziom najwyższy stanowi warstwa ludzkiej percepcji, postanowień decydentów, polityków, dowódców wojskowych i całego społeczeństwa. Na tym poziomie określane są działania typu wyboru obiektów ataków oraz przewidywanie najbardziej prawdopodobnych i możliwych następstw tych działań. Na średnim poziomie jest warstwa informacyjna, która obejmuje infrastrukturę wykorzystywaną do akceptowania, przetwarzania, zarządzania i przechowywania informacji. W tej warstwie wykorzystuje się fałszywe oprogramowanie oraz podstępne ataki na systemy informacyjne realizowane przez hackerów. Efekty tych działań są odczuwalne zarówno w warstwie fizycznej (danych), jak i w warstwie percepcyjnej (wiedzy).

[105] Globalne środowisko informacyjne (*Global Information Environment*) – to wszystkie systemy informacyjne (zarówno indywidualne, połączone, i wojskowe) oraz media i organizacje, które zbierają opracowują i przekazują informacje dla rządów, wojsk i przedstawicielstw.

[106] P.Sienkiewicz, D.Mąka, *Sieciocentryczna infrastruktura procesów decyzyjnych.* ZN nr 4 (73) AON, Warszawa 2008.

Na najniższym poziomie znajduje się warstwa fizyczna, która zawiera fizyczne elementy systemu informacyjnego, a mianowicie: komputery, sieci telekomunikacyjne i informatyczne oraz urządzenia pomocnicze (zasilanie, zdalne sterowanie, zarządzanie, itp.). W tej warstwie znajdują się również osoby administrujące systemy, mające ciągły wpływ na ich funkcjonowanie.

Definicja operacji informacyjnych została określona w dokumencie MC-422 „NATO *Information Operations Policy*", który został zaaprobowany przez Komitet Wojskowy NATO 15 grudnia 1998 roku oraz Radę NATO w dniu 22 stycznia 1999 roku. Zgodnie z tym dokumentem operacje informacyjne są działaniami wpływającymi na proces podejmowania decyzji w sferze politycznej i militarnej poprzez ochronę własnych systemów informacyjnych i destrukcyjne oddziaływanie na systemy informacyjne przeciwnika.

Współczesne konflikty, nawet lokalne, rozwiązywane są przez siły koalicyjne. Tendencja ta wymusza nowe zasady interoperacyjności, kooperacji i synchronizacji działań na polu walki. Zasady, które przyjęto dla tego typu działań, zostały sformułowane w postaci koncepcji zwanej ogólnie „sieciocentrycznymi działaniami wojennymi"[107] (*Network Centric Warfare*)[108]. W kontekście dowodzenia mówi się coraz częściej o „operacjach sieciocentrycznych"[109] (NCO - *Network Centric Operations*). Operacjami NCO nazwano działania operacyjne z wykorzystaniem informacji przekazywanej bezpiecznymi środkami telekomunikacyjnymi zarówno dla planowania, jak i szybkiego, w ściśle zadanym czasie i zdecydowanego wykonania operacji przeciwko siłom zbrojnym przeciwnika, biorącego udział w konflikcie. Sieciocentryczne działania wojenne (NCW), jako rozwinięcie dotychczasowych działań nazwanych „platformo-centrycznymi"[110], zdefiniowano jako koncepcję działań w celu osiągnięcia przewagi informacyjnej poprzez uzyskanie (przez zaangażowane siły) specyficznej zdolności nazywanej zdolnością sieciocentryczną (ang. *Network Enabled Capability* – NEC), zwiększając w ten sposób efektywność mocy uderzeniowej sił zbrojnych. Pożądanym tutaj efektem jest skrócenie cyklu operacyjnego i tworzenie wspólnej świadomości sytuacyjnej, jako warunku maksymalizacji efektywności takich działań. Sieć w ujęciu sieciocentrycznym

---

[107] Dayid S.Alberts, John J.Garstka, Frederick P.Stein, *Network Centric Warfare - Deyeloping and Leyeraging Inforrnation Superiority*, 2-nd Edition of CCRP, ISBN I 57906-01 9-6, August 1999.

[108] Network Centric Warfare — przetłumaczono jako sieciocentryczna architektura Zautomatyzowanych Systemów Dowodzenia [za:] A.Stokalski, *Sieciocentryczna architektura zautomatyzowanych systemów dowodzenia - Bazowa Infrastruktura Informacyjna*, część 1, Warszawa 1991, s. 5-17.

[109] Hans E.Keus, *Network Centric Operations. implications for Allied and Coalition Operations*, Konferencja SMi Conferences on Network Centric Warfare, London 4-5 October 2000.

[110] Odnoszącym się do sieci komputerowej i środków walki.

oznacza stworzenie relacji społecznych pomiędzy wszystkimi podmiotami biorącymi udział w operacji, umożliwiającej im współdzielenie informacji oraz bezpośrednią współpracę.[111]

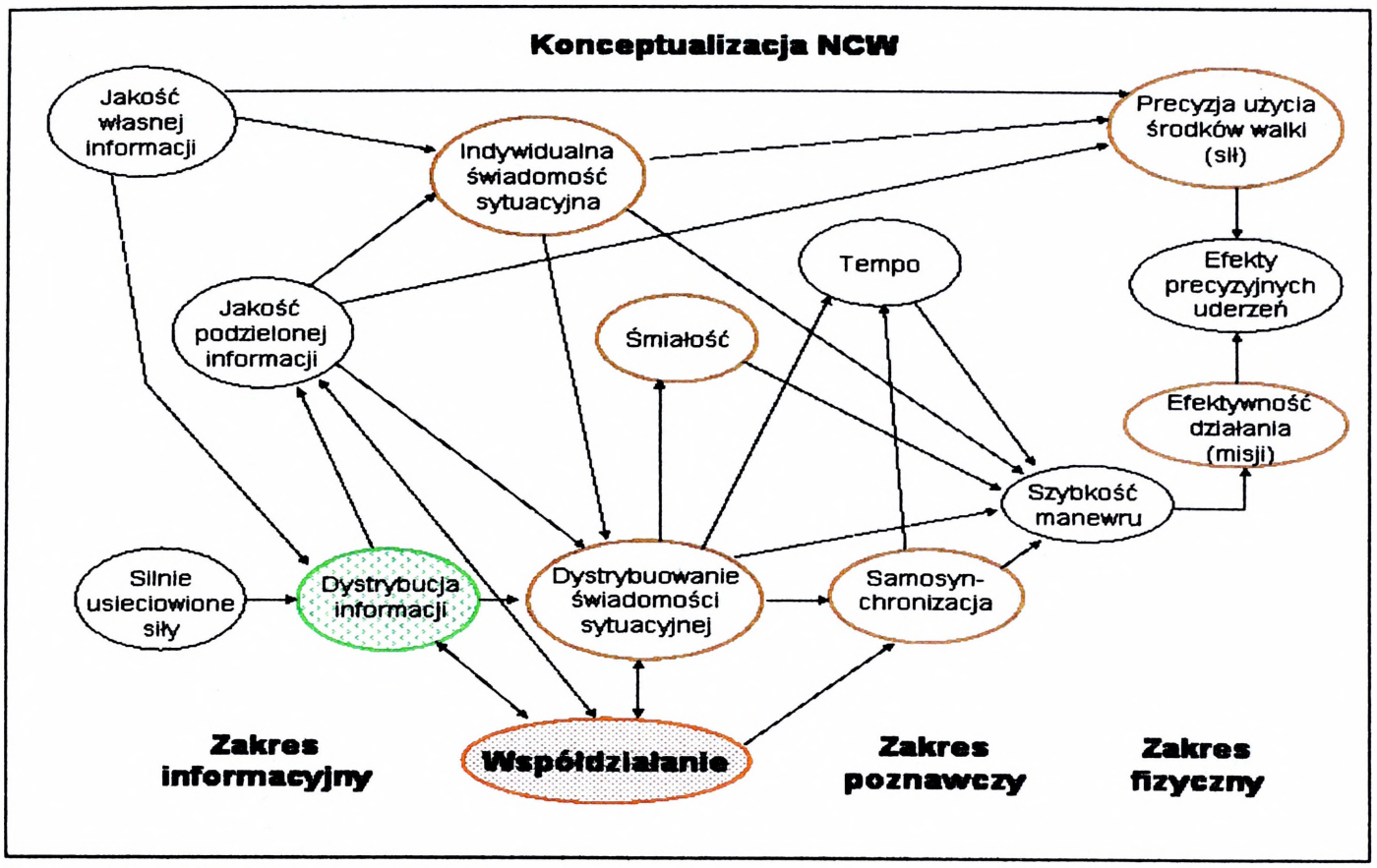
Realizacja tej zasady wymaga zaawansowanej wymiany informacji oraz łączenia w kompleksy informacyjne danych otrzymywanych z rozproszonych terytorialnie sensorów, w celu dokonania analizy współzależności tych danych oraz planowania wspólnych z innymi siłami działań, w rozproszonym wielozadaniowym środowisku. Podstawowymi elementami sieciocentrycznej architektury są:[112]

- **siatka informacyjna** (*information grid*), zwana infostrukturą, jest zabezpieczeniem zadań sieciocentrycznych: obliczeń dla przetworzenia i analizy aktualnych danych i komunikacji; wśród operacji dominują przyjmowanie, przetwarzanie, przesyłanie, zapamiętywanie i zabezpieczenie informacji niezbędnych dla działania połączonych sił;
- **siatki sensorów** (*sensor grids*), obejmują czujniki zbierające informacje; czujniki stanowią wyposażenie środków walki: w powietrzu, na morzu, na ziemi, w przestrzeni kosmicznej oraz w cyberprzestrzeni; są elementem, sieci: środków walki informacyjnej, w postaci: dedykowanych sensorów, (radarów, sonarów na okrętach i samolotach rozpoznania, pojazdach specjalnych itp.) oraz sensorów będących indywidualnym wyposażeniem pojedynczych żołnierzy, oraz stanowiących wyposażenie logistyczne wojsk; siatki te zabezpieczają działalność połączonych sił w wysokiej jakości dane o sytuacji sił własnych, sił przeciwnika oraz środowisku w jakim trwają działania bojowe;
- **siatki środków walki** (*engagement grids*), to system skoordynowanych środków walki, umieszczonych na różnorakich platformach (okręty, samoloty, czołgi), umożliwiający jak najszybsze, we właściwym czasie i przestrzeni, przeciwstawienie się zagrożeniom lub osiągnięcia precyzyjnie określonego celu zarówno w czasie jak i przestrzeni.

---

[111] M.Amanowicz (red.): *Podstawy programu osiągania zdolności sieciocentrycznych w polskich siłach zbrojnych*. Opracowanie wewnętrzne, Zegrze kwiecień 2006; T.Buckman (ed.): NNEC Feasibility Study version 2.0, NC3A, October 2005.

[112] Por. G.R.Maddison, *The Naval C41 WayAhead* - A Blueprint for 2010. Materiały NGI5 NATO, s. 44, [za:] P.Sienkiewicz, D.Mąka, op.cit.



Rysunek 2-12. Konceptualizacja NCW

Źródło: M.Kinasiewicz (red.), *Modelowanie procesów walki informacyjnej. Model „Cyberwar"*. AON, Warszawa 2006, s.5.

NCW jest sieciowym połączeniem sensorów i środków walki rozpiętych na siatce informacyjnej z użyciem architektury zapewniającej przewagę informacyjną oraz zwiększającej efektywność użycia sił. Konceptualizację NCW przedstawia rysunek 2-12.

Uważa się, że główni architekci NCW oraz FCS (*Future Combat System*), admirał A. Cebrowski i J. Garstka[113], stworzyli koncepcje militarne na podstawie wnikliwej analizy sieci Wal-Mart, największej sieci handlowej na świecie, która dzięki nowej logistyce i strukturze organizacyjnej opartej na Internecie, radykalnie zwiększyła swoją efektywność. Należy także odnotować opinie krytyczne, chociażby z powodu nader wysokich kosztów realizacji projektów FCS i NCW.[114]

---

[113] A.Cebrowski, J.Garstka, Network Centric Warfare: Its Origin and Future. US Navy, 1998.

[114] O tych problemach interesująco pisze E.Bendyk, *Miłość, wojna, rewolucja*. WAB. Warszawa 2009, s.314.

Gdy w 2005 roku Arthur Cebrowski odchodził z przyczyn zdrowotnych na emerytur, chwilę po rezygnacji poddał ocenie koncepcję NCW. Podczas konferencji poświęconej bezpieczeństwu narodowemu bronił swego stanowiska, twierdząc, że od transformacji sił zbrojnych nie ma odwrotu. Ostrą krytyką odpowiedział na to Ralph Peters, autor opracowania *Beyond Bagdad: Postmodern War and Peace* (*Po Bagdadzie: ponowoczesna wojna i pokój*). Stwierdził, że doktryna Cebrowskiego nie nadaje się do prowadzenia wojny z terrorem, bo terroryści do perfekcji opanowali sztukę działania w sieciach. Robią to lepiej od amerykańskich wojskowych, ponieważ łączą wykorzystanie nowoczesnych technologii sieciowych z doskonałą znajomością sieci społecznych, w których przyszło im działać. To właśnie te społeczne sieci są nieprzeniknione dla amerykańskich technologii, a tym samym niemożliwe staje się uzyskanie „przewagi informacyjnej" nad przeciwnikiem. Odwrotnie, to przeciwnik ma przewagę.

2.7. Bezpieczeństwo informacyjne jako kategoria poznawcza

Dla współczesnych nauk społecznych, których częścią pozostają nauki o bezpieczeństwie, użyteczny wydaje się być sposób ujęcia Immanuela Wallersteina (rysunek 2-13). Jeżeli uzupełnimy schemat Wallersteina o „pozaspołeczne" obszary badań, to można przyjąć jako racjonalne wyróżnienie problematyki obejmującej: bezpieczeństwo narodowe (polityczne), bezpieczeństwo informacyjne, bezpieczeństwo społeczne (socjalne), bezpieczeństwo ekonomiczne, bezpieczeństwo biznesowe, bezpieczeństwo techniczne, bezpieczeństwo medyczne i bezpieczeństwo ekologiczne.

Trudno przyjąć, iż są to obszary spełniające warunki zupełności i rozłączności. Jednakże zapewne język każdej z wyróżnionych dziedzin zawiera pojęcia: BEZPIECZEŃSTWO i RYZYKO.

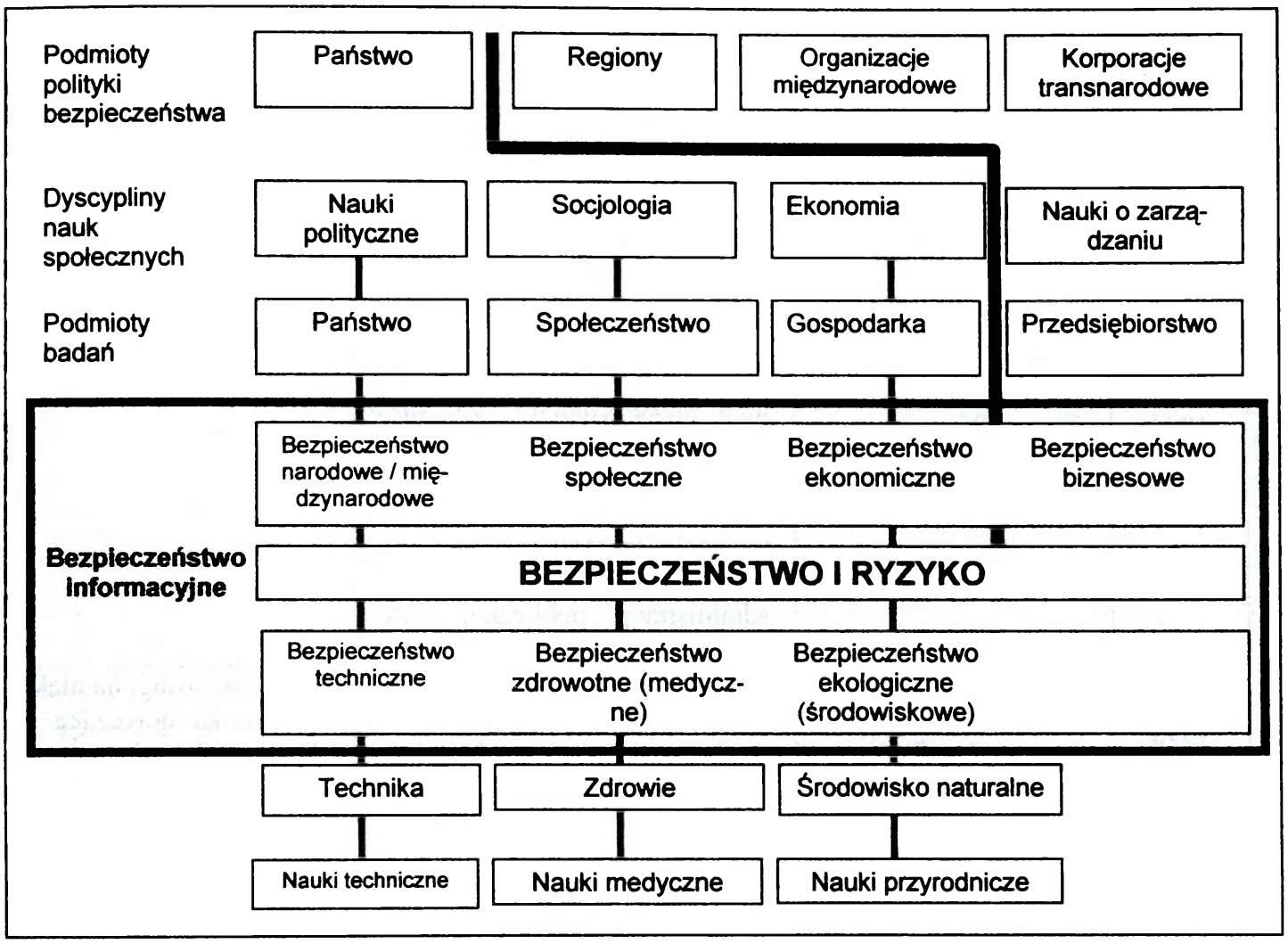
Wspólne dla wielu dziedzin badań społecznych (np. politologii, socjologii, nauk wojskowych), są stosowane procedury badania naukowego, zasady poprawnego formułowania problemów naukowych, stawiania hipotez oraz racjonalnego rozumowania, a także dyskusji naukowej (często polemiki lub krytyki), co stanowi w istocie metodologię badań naukowych. Obecnie w naukach społecznych coraz częściej sięga się do kognitywistyki i metod badań systemowych.

Badania w naukach społecznych koncentrują się wokół struktury, dziejów, kultury, prawidłowości i praw rozwoju społeczeństw. Wykształciły metodologię szczegółową, a każda z dyscyplin dostosowuje narzędzia badań do swoich potrzeb, korzystając np. ze statystki, modeli ekonometrycznych, modeli matematycznych, symulacji komputerowych itp.

Do opisu pewnej rzeczywistości używa się pryncypiów takich, jak: zagrożenie, ryzyko, niebezpieczeństwo. Jednolitą platformę metodologiczną na gruncie paradygmatu holistyczno-systemowego dla nauk wojskowych, społecznych, technicznych, itd., proponuje się analizę systemową, jako jedną z dziedzin współczesnych badań systemowych.[115]

---

[115] P.Sienkiewicz, cz.II – Teoria...op.cit., *Transformacje* (w druku).



Rysunek 2-13. Multidyscyplinarny aspekt badań nad bezpieczeństwem

Źródło: opracowanie własne na podstawie P.Sienkiewicz (red.), *Teoria bezpieczeństwa systemów. Metodologia badań nad bezpieczeństwem systemów*. Cz.II, AON, Warszawa 2006, s.10-11.

2.8. Bezpieczeństwo informacyjne jako czynnik bezpieczeństwa narodowego

Bezpieczeństwo narodowe jest tą dziedziną, której nie można zredukować do bezpieczeństwa wewnętrznego. Dychotomia podziału na bezpieczeństwo wewnętrzne i zewnętrzne być może wygodniejsza w analizie, w rzeczywistości jest umowna. Zmiany technologiczne i globalizacja, czynią ten podział nieostry.[116] Zagrożeń informacyjnych nie można zredukować do zjawisk ograniczonych w przestrzeni i czasie.

Obecnie nie istnieje polska strategia bezpieczeństwa informacyjnego. Podwaliny pod strategię tworzone są w oparciu o dokumenty Unii Europejskiej, obligujące Polskę do dostosowania gospodarki, do wymagań gospodarki społeczeństwa informacyjnego, w tym wymaganego poziomu rozwoju naukowo-technicznego. Równolegle z inicjatywami promocyjnymi budowy społeczeństwa informacyjnego (załącznik I) postępowały prace wspierające działania w dziedzinie polityki bezpieczeństwa informacyjnego (tabela 2-11 i załącznik II).

---

[116] S.Sulowski, M.Brzeziński, *Bezpieczeństwo wewnętrzne państwa. Wybrane zagadnienia*. Dom Wyd. ELIPSA, Warszawa, 2009.

Tabela 2-11. Inicjatywy UE w zakresie bezpieczeństwa informacyjnego

ROK	INICJATYWY	PRIORYTETY	ZALECENIA W SPRAWIE BEZPIECZEŃSTWA INFORMACYJNEGO
1994	Raport Bangemmana	10 inicjatyw w celu rozwoju nowoczesnych technik teleinformacyjnych: telepraca, szkolenia na odległość, sieci łączące uczelnie i jednostki badawcze, usługi teleinformatyczne dla małych i średnich przedsiębiorstw, zarządzanie ruchem drogowym, kontrolę ruchu powietrznego, sieci na użytek sektora zdrowia, komputeryzację sektora zamówień publicznych, transeuropejską sieć administracji publicznej, infostradę dla obszarów miejskich	Brak zaleceń
1996	Zielona Księga: *Living and Working in the Information Society - People First*	Mówi on o konsekwencjach wynikających z transformacji oraz o wpływie nowoczesnych technologii (ICT) na życie	Zwrócenie uwagi na niektóre zjawiska dotyczące np. jakości usług informacyjnych oraz jakości życia
1999	Program eEurope - *An Information Society for All*	Wskazano priorytetowe obszary jego rozwoju, takie jak: edukacja, transport, sektor zdrowia i aktywizacja zawodowa osób niepełnosprawnych	Brak zaleceń
23-24 marca 2000 r.	Strategia Lizbońska	Zakładała ona osiągnięcie przez UE do 2010 r. dominującej w świecie pozycji gospodarczej, przy jednoczesnym zapewnieniu obywatelom Wspólnoty zatrudnienia i standardów socjalnych.	Bezpieczna infrastruktura informacyjna: Powołanie Agencji ds. Sieci Europejskiej i Bezpieczeństwa Informacji – ENISA (2004), Centrum ekspertyzy nt. bezpieczeństwa informacji, Kultura bezpieczeństwa' (koniec 2005), Bezpieczeństwo komunikacji pomiędzy organami administracji publicznej
2000	Plan dzialania *eEurope 2002 - An Information Society for All*	Rozwinięto priorytety Strategii Lizbońskiej	Ataki na systemy informacyjne uznano za zagrożenie dla społeczeństwa informacyjnego i zalecono wspólną prewencję na poziomie struktur unii.
2002	eEurope 2005 - *An Information Society for All - Action Plan*	Dzielenie się wiedzą podczas realizacji projektów, tzw. dobra praktyka Technologia szerokopasmowa, e-Bezpieczeństwo, e-Rząd, e-Zdrowie, e-Nauka, e-Biznes	Opublikowano komunikat o tworzeniu bezpiecznego społeczeństwa informacyjnego poprzez wspólną walkę z przestępstwami cybernetycznymi. Zbudowanie systemu bez-

			pieczeństwa dla infrastruktury informacyjnej
2005	Inicjatywa strategiczna i2010, związana z głównymi osiami zaktualizowanej strategii lizbońskiej	Realizacja idei Europejskiej Przestrzeni Informacyjnej wzrost inwestycji w sektorze badań nad technologią ICT Stworzenie integracyjnego Europejskiego Społeczeństwa Informacyjnego Podniesienie jakości życia w oparciu o technologie informacyjne	Wspieranie bezpieczniejszego korzystania z Internetu i nowych technologii online. Zwiększenie bezpieczeństwa w sieci, w tym: Strategia na rzecz Bezpiecznego Społeczeństwa Informacyjnego, walka ze spamem, Program Bezpieczny Internet plus, podpis elektroniczny, ocena funkcjonowania Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA), wykorzystanie darmowych numerów telefonicznych dla usług o znaczeniu społecznym;

Źródło: opracowanie własne.

Z tej perspektywy należy ocenić *Rządowy Program Ochrony Cyberprzestrzeni RP na lata 2009-2011*, jako tworzący klimat do ujednolicenia pojęć, postaw i praktyk w zakresie bezpieczeństwa narodowego - nie tylko sprowadzonego do fizycznych ataków na infrastrukturę materialną (budynki, drogi), bezpieczeństwa energetycznego, albo walki z żywiołami, ale także inwazji internetowych robaków, czy ataków typu DoS. Ma to istotne znaczenie, bowiem według raportu Pentagonu:[117] *Ludowa Armia Wyzwolenia (LAW) postrzega operacje sieciami komputerowymi (CNO computer network operations) jako kluczowe dla osiągnięcia „dominacji elektromagnetycznej" we wczesnej fazie konfliktu. LAW ustanowiła jednostki wojny informatycznej, które badają wirusy przeznaczone do ataku na sieci i systemy komputerowe wroga, a także rozwijają taktykę i metody obrony własnych systemów. W 2005 roku LAW zaczęła wprowadzać ofensywne CNO do swych ćwiczeń wojskowych.*[118]

2.9. Bezpieczeństwo informacyjne jako czynnik jakości życia

Poziom życia określa wiele zmiennych w postaci wskaźników syntetycznych oraz potencjalnych mierników. Zmienne te reprezentują różne grupy potrzeb ludzkich, w tym potrzeb wynikających z rozwoju sektora informacyjnego. Stopień ich zaspokojenia jest wynikiem analizy, a także wskazówką prognostyczną dla polityki społeczno-ekonomicznej.

---

[117] Potęga militarna Chińskiej Republiki Ludowej 2007. US Department of Defense.
[118] H.Świeboda, P.Sienkiewicz, BOS'08, op.cit.

Poziom jakości życia (QofL ang. *Quality of Live*) odnosi się również: do bezpieczeństwa, w tym także bezpieczeństwa informacyjnego, stanu samorealizacji i stanu środowiska. Dla jego oceny, poddaje się analizie czynniki związane z ochroną zdrowia, bezpieczeństwem socjalnym, dostępnością kultury, a także do różnego rodzaju usług, w tym do poszczególnych elementów infrastruktury.

Czynników wpływających na jakość życia obywateli związanych z rozwojem sektora informacyjnego należy poszukiwać w trzech obszarach:

1) technicznym (awarie technicznych środków infrastruktury, brak dostępu do zasobów);
2) społecznym (dezinformacja mediów masowych, „smog informacyjny", inwigilacja przez służby państwowe, inwigilacja w pracy i w domu);
3) psychicznym (poczucie niemożności pełnego wykorzystania zasobów, ucieczka od wyboru – paraliż decyzyjny, lęki z powodu poczucia utraty, ograniczenia wolności).

Istotą nowego ujęcia jakości życia społecznego, indukowanej przez rozwijający się sektor informacyjny, jest kompresja czasoprzestrzeni wyrażana poprzez: „odterytorialnienie" (Internet, sieci), cyberprzestrzeń, wizję świata jako jednego miejsca oraz wzajemne uwarunkowania tego co lokalne i tego, co globalne. Jedną z cech konstytutywnych społeczeństwa informacyjnego jest dominacja sektora usług informacyjnych związanych z realizacją procesów zbierania (zdobywania), przesyłania, przetwarzania, przechowywania i udostępniania (rozpowszechniania) informacji. Rozwój usług informacyjnych uzależniony jest od efektywności informacyjnej infrastruktury państwa, czyli sprawności jego systemów teleinformatycznych i systemów masowego komunikowania. Z kolei rozwój informacyjnej infrastruktury ma niewątpliwy wpływ na stopień zaspokojenia poszczególnych potrzeb: społecznych (wyższa jakość w dziedzinie zdrowia, edukacji, bezpieczeństwa, uczestnictwa w życiu politycznym i życiu kulturalnym), gospodarczych (telepraca, gospodarka oparta na wiedzy) i ekologicznych (bezpieczeństwo ekologiczne, wypoczynek, turystyka). Stanowi to obszar „pośrednich" wpływów infrastruktury informacyjnej na podstawowe czynniki jakości życia.

Obszar wpływu „bezpośredniego" należy wiązać z rozwojem takich potrzeb informacyjnych jak:[119]

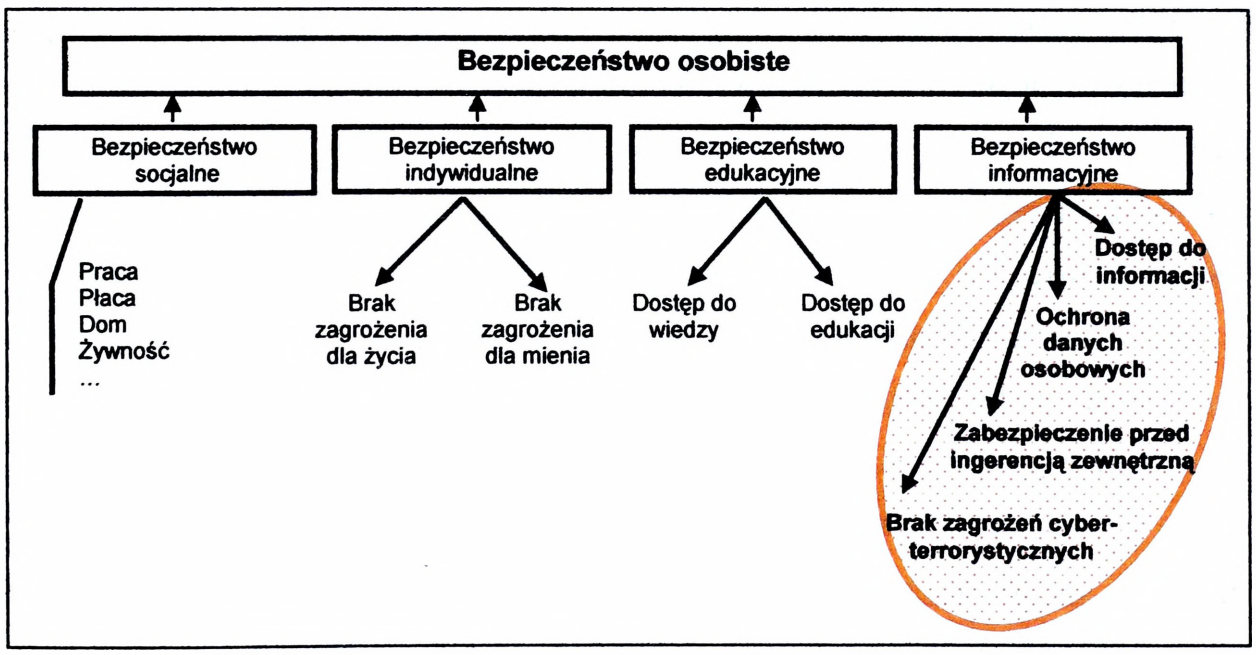
- potrzeba szybkiego dostępu do baz danych i informacji aktualnej;
- potrzeba dostępu do wiedzy ogólnej i specjalistycznych baz wiedzy;

[119] P.Sienkiewicz, H.Świeboda, Analiza systemowa jakości życia w społeczeństwie informacyjnym. BOS'06, Warszawa 2006.

- potrzeba komunikowania „bez granic";
- potrzeba aktywnego uczestnictwa w globalnej społeczności Internetu;
- potrzeba aktywności zawodowej (e-praca);
- potrzeby ludyczne – korzystanie z gier komputerowych, wirtualnej rzeczywistości itp.

Jakość życia w społeczeństwie informacyjnym warunkuje realizacja potrzeb związanych z sektorem informacyjnym oraz potrzeba zapewnienia bezpieczeństwa przed zagrożeniami związanymi z rozwojem tego sektora. Istotne dla jakości życia ma bezpieczeństwo osobiste (rysunek 2-14).

Bezpieczeństwo, antycypacja oraz percepcja zagrożeń, stanowią składnik syntetycznych wskaźników jakości życia. Współczesny człowiek odczuwa potrzebę bezpieczeństwa w obliczu narastającej ilości informacji, nierzadko nieprawdziwej, manipulowanej, szybko ewoluującej techniki komunikowania oraz innych zagrożeń płynących z systemów teleinformatycznych.



Rysunek 2-14. Obszary personalnego bezpieczeństwa informacyjnego
Źródło: opracowanie własne.

W dyskursie o kształcie przemian modernizacyjnych pojawiają się sądy dotyczące skutków tychże zmian, od ocen pozytywnych po sądy krytyczne. Coraz więcej jest obszarów społecznej aktywności, gdzie osobista satysfakcja z jakości usług jest wyraźnie uzależniona od zastosowanych rozwiązań teleinformatycznych.[120] Pozytywnym przykładem jest telemedycyna, bowiem telemedyczne sieci zwiększają dostęp do specjalistów najwyższej klasy, nieosiągalnych dla wielu pacjentów mieszkających poza dużymi aglomeracjami. Zmiany w tech-

[120] A.Szewczyk, Oblicza ubóstwa w społeczeństwie informacyjnym. PWN, Warszawa 2006, s.22.

nologiach informatycznych spowodowały rozwój systemów obserwacji, kontroli i monitoringu (na drogach, w mieście, w powietrzu) oraz systemów o charakterze obronnym, które mają wpływ na wzmocnienie bezpieczeństwa. Wymierne korzyści w postaci skrócenia czasu załatwiania spraw, uzyskania informacji, pozbycia się syndromu „kafkowskiego" wynikającego z kontaktu z urzędem, może odnieść obywatel korzystający z sieci usług publicznych i rozwoju elektronicznych urzędów (e-goverment). Rozwój zastosowań ICT daje się także odczuć w sztuce, zarówno w tworzeniu nowych środków wyrazu artystycznego, jak i w upowszechnianiu jej osiągnięć. Rozwój Internetu umożliwił korzystanie z bibliotek na całym świecie, oraz rozwój e-handlu, e-biznesu itp. Ma to niewątpliwy związek z poprawą poziomu jakości życia.

Jednym z megatrendów współczesnego świata jest budowa gospodarki opartej na wiedzy, której filarami oprócz rozbudowanej infrastruktury ICT i zarządzania wiedzą na poziomie organizacji, są inwestycje w kapitał ludzki i społeczny. Zmiany technologiczne stymulują: (1) powstawanie nowych zawodów, (2) redukcję lub eliminację niektórych zawodów już istniejących, (3) zwiększają lub zmniejszają wymagania dotyczące kwalifikacji, (4) zmieniają charakter wymaganych kwalifikacji. Większość dodatkowo wykreowanych miejsc pracy powstaje w rozwijającym się sektorze usług. Szczególnie koncentruje się w usługach rynkowych (informatyka, turystyka, transport lotniczy, usługi biznesowe), usługach publicznych, jak edukacja i zdrowie oraz usługach osobistych (np. kultura, rekreacja i wypoczynek).[121]

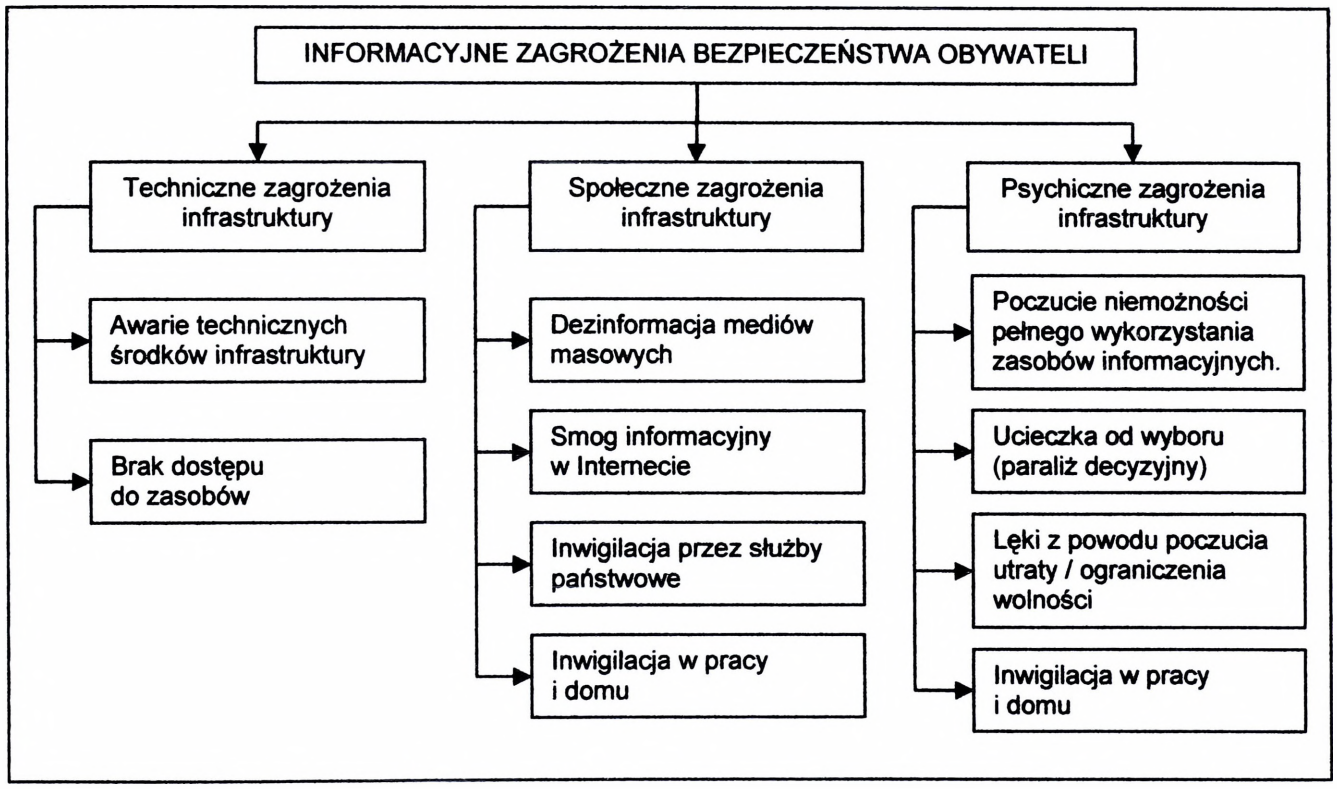
Przyjmuje się, że paradygmat technologiczno-gospodarczy XXI wieku opierał się będzie na rozwoju biotechnologii i jej zastosowaniach w medycynie, w tym w rozwoju biomedycyny, rolnictwie oraz produkcji żywności wysokiej jakości. Tendencje te z jednej strony powodują wzrost poczucia bezpieczeństwa, z drugiej zaś narasta poczucie braku stabilizacji wynikające z często fałszywej świadomości istoty nowych zagrożeń. Nie pozostaje to bez wpływu na jakość życia.[122]

---

[121] H.Świeboda, *Bezpieczeństwo informacyjne* ..., BOS,06, op.cit.

[122] H.Świeboda, *Bezpieczeństwo informacyjne dla bezpieczeństwa narodowego*, Zeszyty Naukowe nr 2, AON, Warszawa 2007. Dynamiczny rozwój sieci komputerowych, a szczególnie Internetu sprawił, iż nastąpił lawinowy przyrost dostępnych informacji (np. bazy wiedzy, biblioteki). W marcu 2007r. firma EMC Corporation ogłosiła wyniki pionierskich badań IDC. W dokumencie "*The Expanding Digital Universe: A Forecast of Worldwide Information Growth Through 2010*" ("*Rozszerzający się cyfrowy wszechświat: prognoza wzrostu ilości informacji na świecie do 2010 r.*") zaprezentowano ilości informacji, które będą tworzone i kopiowane na całym świecie w 2010r. W badaniach tych po raz pierwszy zmierzono i przedstawiono prognozy dotyczące ilości i rodzaju informacji cyfrowych tworzonych i kopiowanych na całym świecie, zarówno pochodzących od osób fizycznych, jak i przedsiębiorstw. Ten ogromny wzrost zmieni jeszcze radykalniej sposób wykonywania zadań w przedsiębiorstwach, zmieni także sposób korzystania z informacji przez konsumentów.

Coraz częściej wskazuje się na nieznane wcześniej zagrożenia, obejmujące zarówno infosferę jak i technosferę, stanowiącą rolę filtru informacji[123], a których skutki lokalizują się w obszarze społecznym, ekonomii i psychologii (rysunek 2-15). Zagrożenia mają wymiar zarówno personalny jak i regionalny, ale również globalny. W wielu pracach akcentuje się podejście aksjologiczne do zachodzących zmian, zwraca się uwagę na wykształcenie się nowej formacji cywilizacyjnej, z nowym postrzeganiem świata i zmienionym systemem wartości społecznych.[124] Komunikacja i informacja wkracza we wszystkie wymiary ludzkiego życia, często staje się wartością samą w sobie i jednym z istotnych wyznaczników kultury naszych czasów. Czasem wręcz tworzy rzeczywistość wirtualną.



Rysunek 2-15. Obszary zagrożeń bezpieczeństwa obywateli
Źródło: opracowanie własne.

W „katalogu zagrożeń" pojawiły się niebezpieczeństwa związane z subiektywnym odbiorem stosowania nowych technik komunikowania, przede wszystkim mediów elektronicznych.

W wielu pracach akcentuje się podejście aksjologiczne do zachodzących zmian, zwraca uwagę na wykształcenie się nowej formacji cywilizacyjnej z nowym postrzeganiem świata i zmienionym systemem wartości społecznych. Konsekwencją rozwoju społeczeństwa informacyjnego jest pojawienie się kulturowego AIDS, czyli *Anti-Information Deficiency Syndro-*

---

[123] P.Sienkiewicz. *10 wykładów.* AON, Warszawa 2005, s.74,75.
[124] T.Goban-Klas, P.Sienkiewicz, *Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania.* Wyd. Postępu Telekomunikacji, Kraków 1999.

me, a więc syndromu braku odporności na informację.[125] Zakłócone zostały wartości aksjologiczne stanowiące do tej pory pewne standardy, pomagające ludziom antycypować uwarunkowania działania i oszacowywać możliwości. Niewątpliwie zmiany te wywierają wpływ na postrzeganie zagrożeń i ryzyka, zaburzając poczucie bezpieczeństwa i wzmagając lęk i strach. Stan niepewności, intensywnego poczucia zagrożenia, podsycany przekazami mediów, często nie zainteresowanych rzetelnym informowaniem - wpływa na jakość życia (tabela 2-12).[126]

Tabela 2-12. Zagrożenia społeczeństwa w różnych obszarach działalności

W obszarze polityki
– pokusa „totalitaryzmu informacyjnego" (państwowego monopolu); – możliwość wzrostu zagrożeń bezpieczeństwa informacyjnego społeczeństwa; – podatność na zakłócenia informacyjne; – poczucie ograniczonej wolności i prywatności;
W obszarze życia społecznego
– dehumanizacja i alienacja; – zalew niewiarygodnymi informacjami; – zmniejszenie prywatności przez zwiększoną i łatwiejszą kontrolę; – możliwość powstania nowych form terroryzmu (infoterroryzm);
W obszarze gospodarki
– możliwość wystąpienia konfliktów społecznych na tle automatyzacji i robotyzacji; – redukcja zatrudnienia (zwłaszcza wśród „niebieskich kołnierzyków"); – wzrost wymagań dotyczących obsługi systemów zautomatyzowanych; – nadmierna standaryzacja wyrobów i usług; – możliwość nowych przestępstw;
W obszarze edukacji i wiedzy
– zróżnicowanie dostępu do wiedzy; – konieczność kształcenia ustawicznego; – kopiowanie prac; – załamanie kontroli prac autorskich; – koncentrowanie się na kształceniu analitycznym i funkcjonalnych umiejętnościach, kosztem twórczego myślenia; – niedobór odpowiednio przygotowanych kadr;
W obszarze pracy
– zwiększenie bezrobocia poprzez automatyzacje pewnych stanowisk pracy; – zmniejszenie zatrudnienie w przemyśle i rolnictwie; – powiększenie luki pokoleniowej; – konieczność częstych przekwalifikowań;

[125] J.Morbitzer, Świat wartości w Internecie. [w:] http://www.wsp.krakow.pl/konspekt/18/wartosci.html.

[126] H.Świeboda, Informacyjne determinanty jakości życia [w:] P.Sienkiewicz (red.), Bezpieczeństwo obywateli RP jako czynnik jakości życia. AON, Warszawa 2009.

w obszarze ochrony zdrowia
– dehumanizacja służby zdrowia; – wykorzystanie danych o stanie zdrowia do celów poza medycznych; – nowe choroby cywilizacyjne; – zróżnicowanie dostępu do pomocy medycznej.

Źródło: T.Goban-Klas, P.Sienkiewicz, (1999) *Społecz*..., op.cit. s.139,157.

Wśród zidentyfikowanych powyżej zagrożeń, których podstawę podziału stanowiło kryterium obszaru występowania, dostrzega się proces ich ewolucji. Wcześniej antycypowano możliwość ich wystąpienia, zaś obecnie objawiły się w znacznie groźniejszej formie i z większą intensywnością. Ogół zagrożeń informacyjnych i określenie ryzyka ich występowania często wykracza poza czysto inżynierskie ujęcie.[127] Zagrożenie jest wyrazem bliskoznacznym ryzyka i często z nim utożsamianym, stąd pojawia się trudność w ewaluacji jako następstwa ich percepcji przez człowieka. Strukturalizując zagrożenia informacyjne w odniesieniu do bezpieczeństwa obywateli obejmującej warstwę infosfery wewnętrznej i zewnętrznej wyróżniono zagrożenia dla:

- wartości własnych zasobów (infosfera zewnętrzna i wewnętrzna);
- jakości informacji bieżących związanych z atrybutami informacji: aktualność / terminowość, pełność / kompletność, wiarygodność / niezawodność, relewantność, swobody komunikowania.[128]

Człowiek współczesny ma szansę aktywnego uczestnictwa w wielu sprawach świata, jednocześnie nadmiar informacji powoduje trudności w rozumieniu treści, analizie i syntezie informacji. Równowaga informacyjna jest cechą indywidualną każdego odbiorcy informacji, zależną od wewnętrznego stanu organizmu, doświadczeń, wykształcenia i reakcji obronnych. Naruszenie homeostazy informacyjnej człowieka, objawia się chorobą informacyjną, której przyczyny tkwią w nadmiarze informacji, bądź w jej patogennych cechach takich jak: fałszywość, niekompletność i nieaktualność.

Naturalne jest dążenie do uzyskania pełnego bezpieczeństwa informacyjnego: poczucia bezpieczeństwa i uzyskanie pewności, że odbierane są przez nas informacje faktycznie ważne, prawdziwe i wiarygodne. Zagrożenie stanowi zarówno chaos informacyjny w Internecie, niedobór informacji (luka informacyjna), jak i jej nadmiar (zalew informacji, smog informacyjny[129]). Z powodu źle zorganizowanego systemu komunikacji społecznej, pojawiło się zjawisko, zidentyfikowane na Zachodzie na początku lat 80. ubiegłego wieku, jako *dise-*

---

[127] P.Sienkiewicz, Teoria i inżynieria bezpieczeństwa systemów. AGH, Kraków 2003.
[128] H.Świeboda, BOS'08, op.cit.
[129] R.Tadeusiewicz, *Społeczność Internetu*. Wyd.Exit, 2002.

ases of information, czyli niedomagania spowodowane dopływem informacji z zewnętrznej infosfery (tabela 2-13).

Tabela 2-13.. Choroby informacyjne

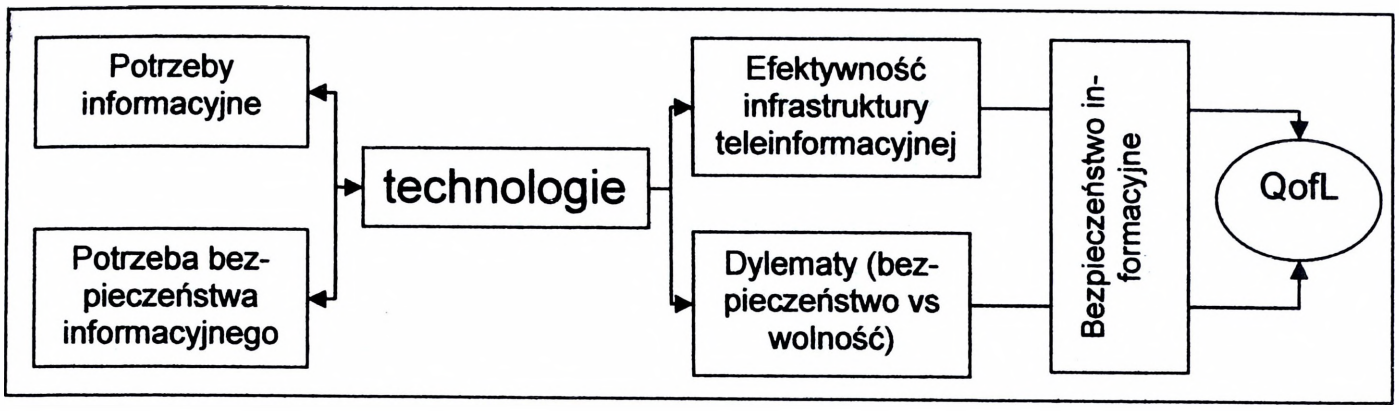
Nadawca informacji	– brak poczucia odpowiedzialności za nadawany komunikat; – brak troski o prawdziwość komunikatu; – nieprzekazywanie komunikatu w całości wraz ze wszystkimi towarzyszącymi mu informacjami, które mogą być potrzebne odbiorcy do pełnego i poprawnego odbioru komunikatu; – urojenia informacyjne: generowanie informacji w oparciu o własne domysły nie poparte faktami (na przykład plotki);
Poszukujący informacji	– frustracja informacyjna; – stres informacyjny; – przeciążenie informacyjne;
Odbiorca informacji	– bezkrytyczny odbiór i przekazywanie informacji, często bez jej zrozumienia i internalizacji; – tendencyjny (życzeniowy) odbiór informacji; – selektywny odbiór tylko tych informacji, których spodziewa się odbiorca, czyli intencjonalne nastawienie na odbiór informacji; – ignorowanie tych informacji, które są w konflikcie z doświadczeniami odbiorcy; – kompletny brak zaufania do nadawcy komunikatu; – niewłaściwe rozumienie komunikatów; – przeciążenie informacyjne.

Źródło: W. Babik, Uniwersytet Jagielloński, Kraków 2006 [w:] www.ap.krakow.pl/ptn/ref2006/Babik.pdf.

Należy podkreślić dualny charakter niektórych zagrożeń. Niektóre z nich, związane z obszarem bezpieczeństwa obywateli np. monitoring wizyjny, mogą stanowić szansę rozwoju, jak choćby w przypadku telemedycyny czy teleedukacji. Obserwacja, kontrola i monitoring zagrożonych obiektów i obszarów, z jednej strony wzmacnia bezpieczeństwo, a z drugiej prowadzi do inwigilacji i ograniczenia swobód obywatelskich.

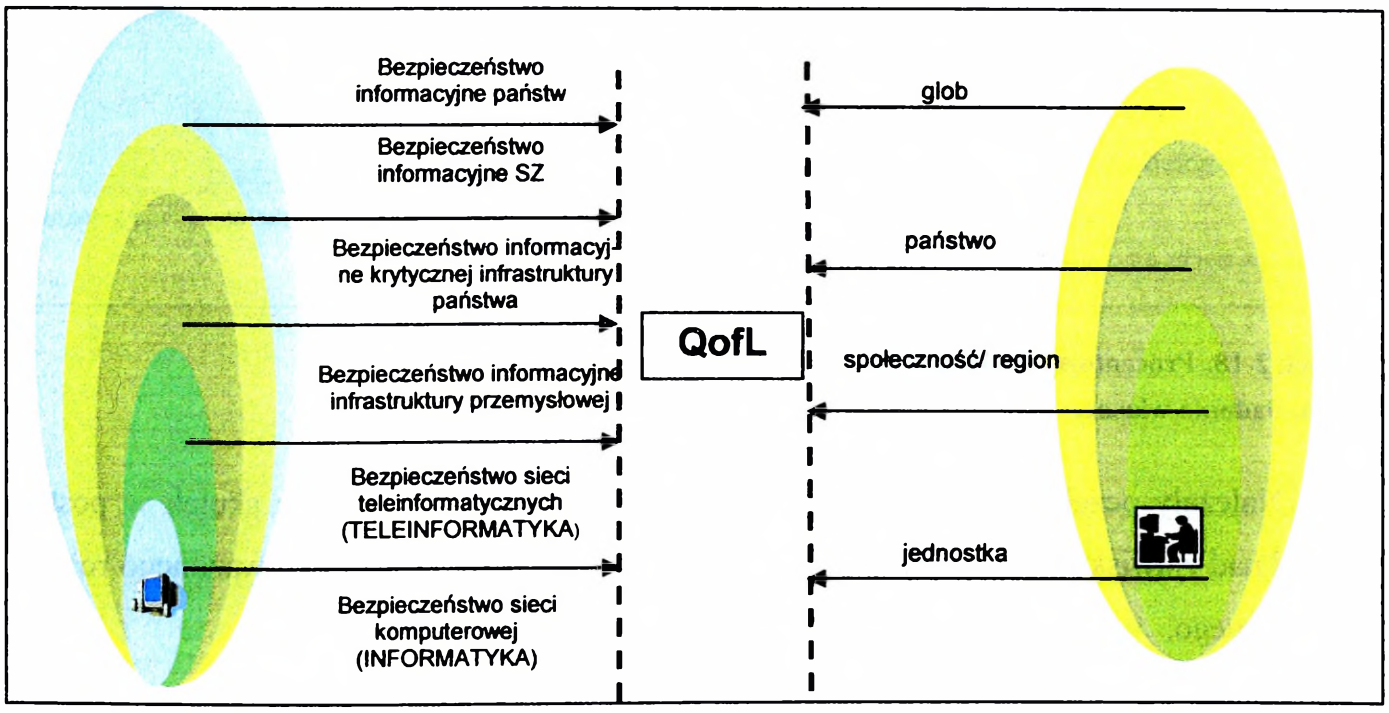
Najbardziej spektakularnym zagrożeniem ostatnich lat jest groźba cyberterroryzmu, oraz narastający rozwój przestępstw pospolitych w cyberprzestrzeni.

Jakość życia w społeczeństwie informacyjnym uwarunkowana jest, zatem stopniem zaspokojenia potrzeb informacyjnych oraz zapewnieniem pożądanego poziomu bezpieczeństwa informacyjnego (rysunek 2-16).



Rysunek 2-16. Interakcje między potrzebami społecznymi a techniką
Źródło: opracowanie własne.

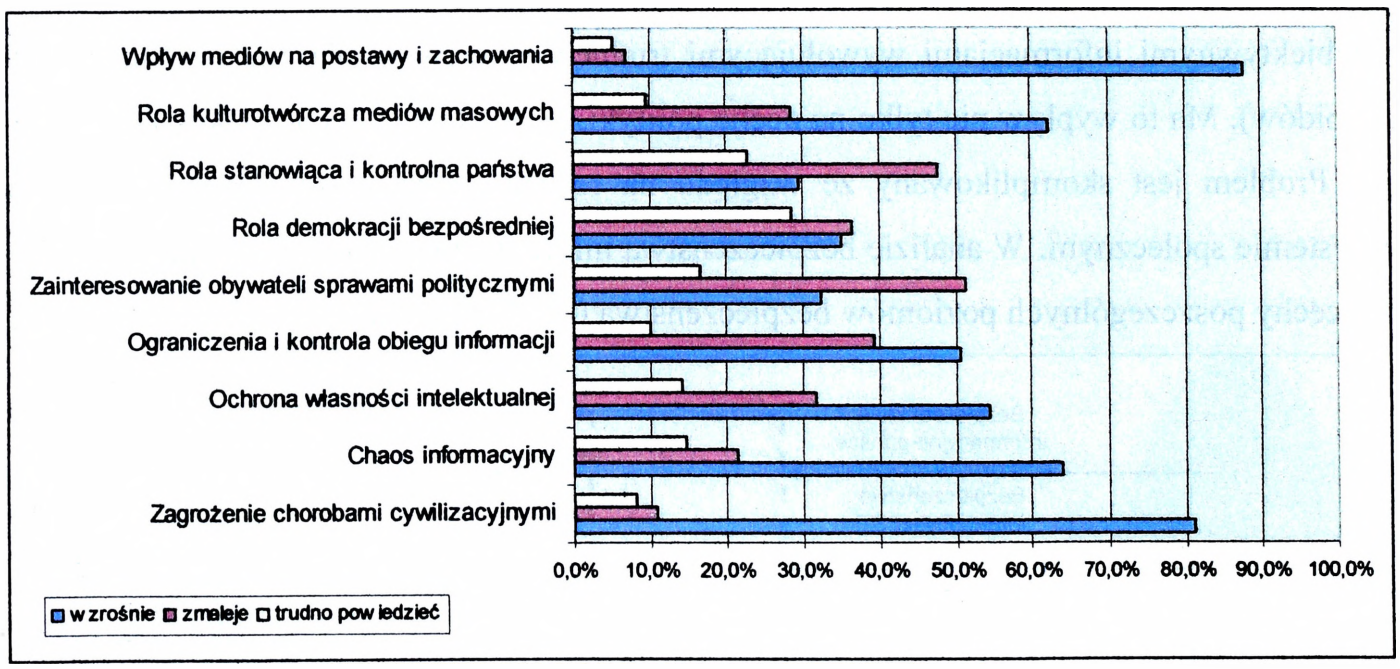
Bezpieczeństwo informacyjne w kontekście wpływu na jakość życia, należy rozpatrywać w wielu płaszczyznach, uwzględniając swoistą hierarchię zagrożeń. Poziom życia określa wiele zmiennych, pozwalających na przyjęcie mierzalnych wskaźników syntetycznych. Zmienne te reprezentują różne grupy potrzeb ludzkich, co skłania do zmian tradycyjnej hierarchii potrzeb (np. w ujęciu Maslowa). Stopień ich zaspokojenia jest wynikiem analizy, która może być podstawą prognoz niezbędnych dla kreowania polityki społeczno-ekonomicznej. Percepcja zagrożeń, a także obaw i lęku, jaki wywołują technologie, często kształtowana jest nieobiektywnymi informacjami wywołującymi trudne do przewidzenia emocje (np. wpływ tabloidów). Ma to wypływ nie tylko na ocenę polityki, lecz także na ocenę zadowolenia z życia. Problem jest skomplikowany ze względu na rosnącą liczbę różnorodnych interakcji w systemie społecznym. W analizie bezpieczeństwa informacyjnego należy rozpatrywać swoiste cechy poszczególnych poziomów bezpieczeństwa (rysunek 2-17).



Rysunek 2-17. Poziomy bezpieczeństwa wpływające na jakość życia
Źródło: H.Świeboda, *Bezpieczeństwo informacyjne dla bezpieczeństwa narodowego*. ZN AON NR 3(68) Warszawa 2007.

Dostrzeganie zmian i tendencji jako konsekwencji modernizacji społecznej wywołanej pojawieniem się nowych mediów, a także ich konwergencją, potwierdzają badania prowadzone w 2003 i 2004 roku na populacji studentów Akademii Obrony Narodowej (285 osób). W ankiecie[130] zawierającej 50 pytań, które najczęściej pojawiają się w dyskusjach dotyczących konsekwencji społecznych, ekonomicznych itp. w kontekście dynamicznego rozwoju ICT, pytanie brzmiało: czy przewidywany skutek wzrośnie, czy zmaleje w wyniku rozwoju społeczeństwa informacyjnego?

W obszarze informacyjnym blisko 90% badanych podkreśliło znaczący wzrost wpływu mediów na postawy i zachowania, 62% wskazało na rosnącą rolę kulturotwórczą mediów masowych, a ponad 80% uważa, że wzrośnie zagrożenie chorobami cywilizacyjnymi. Ponad 60% ankietowanych wyraża opinię, że wzrośnie chaos informacyjny przy wzroście ochrony własności intelektualnej (55%), wzrosną również ograniczenia i kontrola obiegu informacji (51%). Nie może dziwić spadek (52%) zainteresowania obywateli sprawami politycznymi, zaś około 50% badanych uważa, że zmaleje rola stanowiąca i kontrolna państwa, a 37% sądzi, że zmaleje także rola demokracji bezpośredniej (rysunek 2-18).



Rysunek 2-18. Procentowy rozkład odpowiedzi
Źródło: badania własne.

Należały oczekiwać, że postrzeganie i percepcja zmian przyniesie skutek w postaci refleksji nad zjawiskami nie zawsze korzystnymi z punktu widzenia zrównoważonego rozwoju społecznego.

[130] W badaniu posłużono się ankietą socjologa A. Sicińskiego i inżyniera J. Lubacza.

2.10. Teoria bezpieczeństwa informacyjnego

Teoretyczne podstawy bezpieczeństwa informacyjnego należy wywieść z podstaw teoretycznych bezpieczeństwa,[131] uwzględniając związki z bezpieczeństwem narodowym, internami narodowymi itp.[132] Istotne jest umiejscowienie pojęcia bezpieczeństwa informacyjnego w szerokim kontekście pojęć i kategorii stosownych w opisie zjawiska.

Można zatem rozpatrywać bezpieczeństwo informacyjne jako (tabela 2-14):

- sytuacje braku zagrożeń informacyjnych dla określonych obiektów;
- zdolność środków zabezpieczenia: technologii i /lub organizacji (instytucji odpowiedzialnych za zabezpieczenie określonych obiektów przed zagrożeniami informacyjnymi;
- wartość, wynikająca z braku realnych zagrożeń informacyjnych lub poczucia tego braku.

Zmiana podejścia do problematyki bezpieczeństwa narodowego i międzynarodowego dokonała się wraz z przemianami systemowymi końca XX minionego stulecia. Pojawiły się zagrożenia o charakterze globalnym za sprawą postępującego procesu globalizacji i internacjonalizacji, który wzmacniany jest rozwojem technologii informacyjno-komunikacyjnych. Nie zmieniają się natomiast wartości egzystencjalne najczęściej łączone z bezpieczeństwem narodowym.

Z informatyki i kryptologii, telekomunikacji i teleinformatyki wyłania się dziedzina, którą można określić mianem „teorii bezpieczeństwa informacyjnego". Aczkolwiek podejmowane próby trudno uznać za w pełni satysfakcjonujące, to należy oczekiwać w przyszłości ich integracji na jednolitej płaszczyźnie metodologicznej.

Jeszcze kilka lat temu bezpieczeństwo informacyjne łączono bądź z ochroną informacji, przede wszystkim, niejawnych, bądź z bardzo rozwiniętymi metodami matematycznymi stosownymi w kryptologii (kryptografii) i dotyczącymi konstrukcji kodów, technik szyfrowania i deszyfrowania.[133] Inną dziedziną zainteresowaną problemami bezpieczeństwa informa-

---

[131] Najczęściej rozpatruje się trzy ujęcia pojęcia bezpieczeństwa, a mianowicie: a) bezpieczeństwo jako brak zagrożeń, b) bezpieczeństwo jako wartość (w sensie hierarchii Maslowa), c) jako system instytucjonalnych i pozainstytucjonalnych gwarancji likwidacji lub minimalizacji zagrożeń. [w:] P.Sienkiewicz, *Teoria i inżynieria bezpieczeństwa systemów*. ZN nr 1(70) AON, Warszawa 2008.

[132] Do podstawowych wartości, które składają się na bezpieczeństwo zalicza się: przetrwanie państwowe, etniczne i biologiczne; integralność terytorialną; niezależność polityczną; jakość życia (w sensie poziomu życia, szczebla rozwoju społeczno - gospodarczego i systemu kulturalnego). [w:] J.Stańczyk, *Współczesne pojmowanie bezpieczeństwa.* Instytut Studiów Politycznych PAN, Warszawa 1996, s.26.

[133] Jako przykład może posłużyć znakomite osiągnięcie polskich matematyków: M.Rejewskiego, J.Różyckiego i H.Zygalskiego, którzy w 1937r. dokonali złamania kodu niemieckiej maszyny szyfrującej – Enigmy, używanej podczas II Wojny Światowej. S.Singh twierdzi, że: pierwsza wojna była wojna che-

cyjnego jest organizacja i działanie wywiadu i kontrwywiadu, w szczególności wywiadu gospodarczego.[134] Trudno jednak wskazać prace o ambicjach teoretycznych, w sensie teorii naukowej.

Tabela 2-14. Istota bezpieczeństwa narodowego i informacyjnego

BEZPIECZEŃSTWO NARODOWE	BEZPIECZEŃSTWO INFORMACYJNE
Brak zagrożenia	Brak zagrożeń informacyjnych dla określonych obiektów
System instytucjonalnych i poza instytucjonalnych gwarancji likwidacji lub minimalizacji zagrożeń	System instytucjonalnych (służby) likwidacji źródeł zagrożeń lub minimalizacja zagrożeń informacyjnych albo zapewniających minimalizację podatności obiektów na zagrożenie
Jedna z wartości egzystencjalnych wiążąca się z poczuciem stabilności, trwałości korzystnego stanu rzeczy, wrażeniem pewności itp.	Stan poczucia stabilnego, niezawodnego i efektywnego działania obiektów w warunkach potencjalnych zagrożeń
Bezpieczeństwo narodowe (państwa) jako stan uzyskany w rezultacie odpowiednio zorganizowanej obrony i ochrony przed wszelkimi zagrożeniami militarnymi i niemilitarnymi, tak zewnętrznymi, jak i wewnętrznymi, przy użyciu sił i środków pochodzących z różnych dziedzin Wg. Słownik terminów z zakresu bezpieczeństwa narodowego. Suplement do wybranych haseł. AON, Warszawa 2002, s.169,	Zarządzie bezpieczeństwem systemów teleinformatycznych obejmuje zespół procesów zmierzających do osiągnięcia i utrzymywania w systemach teleinformatycznych ustalonego poziomu bezpieczeństwa, to jest poziomu poufności, integralności, dostępności, rozliczalności, autentyczności i niezawodności Wg. A. Białas, Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie. WNT, Warszawa 2006, s. 43.

Źródło: Opracowanie własne.

Aspekt informacyjny mający wpływ na wszystkie aspekty bezpieczeństwa, wynikający z rosnącej współzależności państw, powodowanych rozwojem konwergentnych technologii informacyjno-komunikacyjnych, a w szczególności pojawieniem się Internetu, stał się jedną z dominujących determinant bezpieczeństwa narodowego.

Bezpieczeństwo informacyjne potraktowane jako podsystem systemu bezpieczeństwa narodowego nie doczekało się tylu opracowań, co np. problematyka rozwoju społeczeństwa informacyjnego czy Internetu. Aby zdefiniować bezpieczeństwo informacyjne należy w sposób wielopłaszczyznowy i wieloaspektowy odnieść się do bezpieczeństwa narodowego, a po części do bezpieczeństwa ekonomicznego.

Układ istotnych relacji systemowych obejmuje stosunki nie tylko pomiędzy podmiotami bezpieczeństwa, lecz również między innymi uczestnikami środowiska bezpieczeństwa,

---

mików (po raz pierwszy zastosowano chlor i gaz musztardowy w charakterze gazów bojowych). Druga wojna była wojna fizyków (skonstruowano bombą atomową). Trzecia wojna światowa będzie wojna matematyków (kontrolują najważniejsza broń – informację).

[134] L.Korzeniowski, A.Pepłoński, *Wywiad gospodarczy. Historia i współczesność*. EAS, Kraków 2005.

zarówno tymi, którzy są podmiotami prawa, jak i tymi, którzy tej podmiotowości nie mają. System bezpieczeństwa nie jest systemem statycznym, bowiem ewoluuje, podlegając modernizacji i adaptacji do zmian środowiska (otoczenia).

O przesuwaniu się środka ciężkości w pojmowaniu zakresu bezpieczeństwa mówią kolejne Strategie Bezpieczeństwa Narodowego RP. Już w strategii Bezpieczeństwa Narodowego z 2003 roku znajdujemy odniesienie do zagrożeń związanych „z operacjami penetracji, dezorganizacji i dezinformacji kluczowych systemów informacyjnych państwa i baz danych przez obce służby specjalne, terrorystów ekstremistów i zorganizowane grupy przestępcze".[135] Potwierdza to tezę o zacieraniu się różnic pomiędzy zewnętrznymi i wewnętrznymi aspektami bezpieczeństwa, i konieczności podejścia holistyczno-systemowego do nowej przestrzeni bezpieczeństwa. Podobną, choć zwięźlej sformułowaną opinię zawiera Europejska Strategia Bezpieczeństwa (ESS)[136]. Słynne hasło Klubu Rzymskiego o konieczności myślenia globalnego i działania lokalnego weszło do powszechnego słownictwa w dziedzinie bezpieczeństwa międzynarodowego. Problem bezpieczeństwa informacyjnego jest również obecny w wielu dokumentach strategicznych dotyczących rozwoju społeczeństwa informacyjnego.[137]

Poddając analizie bezpieczeństwo informacyjne należy dokonać ewaluacji (analizy i ceny): środowiska, technologii, zasobów informacyjnych, polityki bezpieczeństwa, stosowanej na różnych szczeblach społecznego zorganizowania, poczynając od pojedynczego człowieka poprzez organizację, państwo, region a kończąc na aspektach globalnego bezpieczeństwa. Systemowe podejście do problemu bezpieczeństwa, znajomość zagrożeń, poszukiwanie alternatywnych rozwiązań w świetle ich konsekwencji, pozwala opracować optymalną strategię postępowania w złożonych sytuacjach problemowych.

Rozwój sieci, a przede wszystkim Internetu spowodował, że współczesne państwa i społeczeństwa funkcjonują w globalnym środowisku informacyjnym, a informacja stała się strategicznym zasobem, podobnie jak: ziemia, kapitał i praca w okresie industrialnym. Wraz z rozwojem technologii komunikacyjno-informacyjnych, pojawiła się przestępczość komputerowa, w tym cyberterroryzm. Pojawiło się również pojęcie Krytycznej Infrastruktury Państwa szczególnie wrażliwej na wszelkiego rodzaju zagrożenia, której zakłócenie może powodować straty ekonomiczne osłabić bezpieczeństwo państwa. Potrzeba bezpieczeństwa infor-

---

[135] Strategia Bezpieczeństwa Narodowego 2003, s.3.

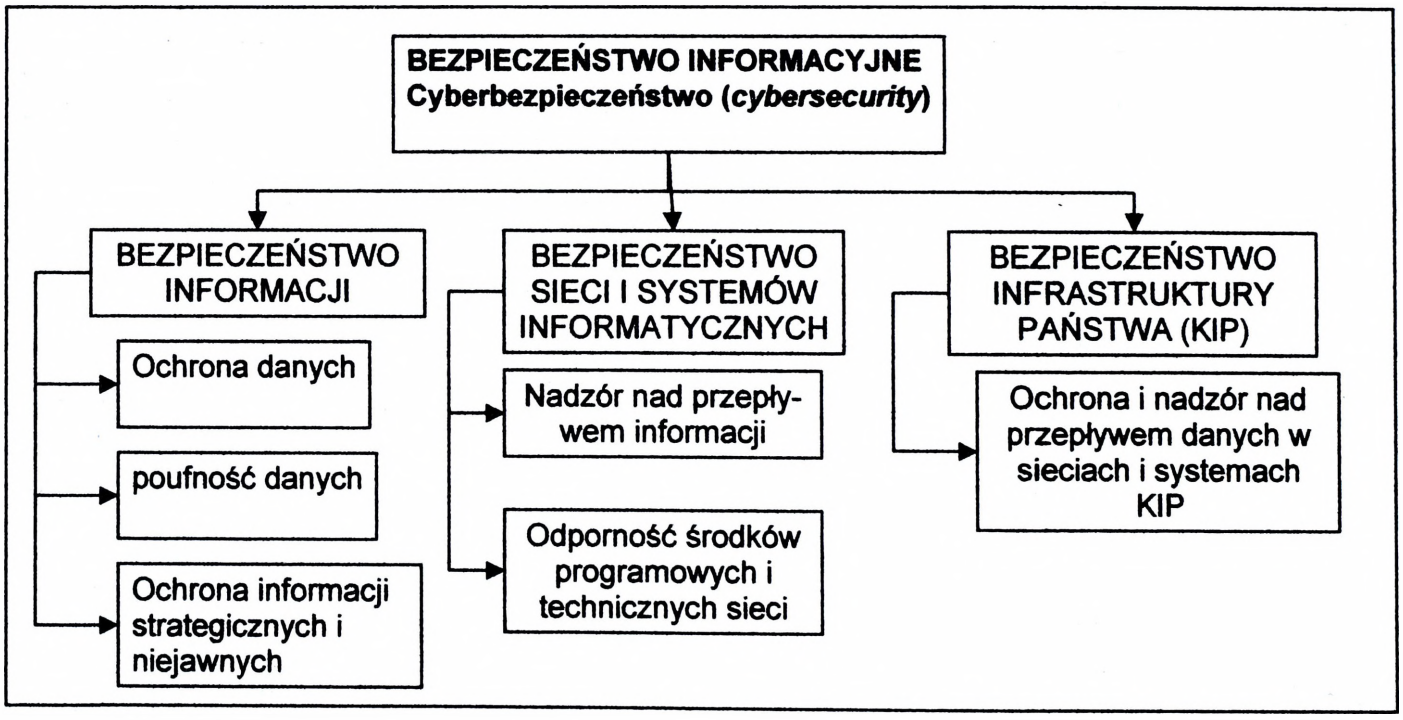
[136] "We live in a world that holds brighter prospects but also greater threats than we have known. The future will depend partly on our actions. We need both to think globally and to act locally." Europejska Strategia Bezpieczeństwa (ESS - *European Security Strategy*), została zatwierdzona 13 grudnia 2003 przez Radę Europejską; s.4; http://ue.eu.int/cms3_fo/showPage.ASP?id=266&lang=EN&mode=g s.4.

[137] Raport KBN dla Rady Ministrów: Cele i kierunki rozwoju społeczeństwa informacyjnego w Polsce.. Warszawa 2000.

macyjnego była odpowiedzią na coraz częściej pojawiające się zagrożenia zarówno natury losowej, przypadkowej, jak i zagrożenia umyślne, stosowane w celu osiągnięcia korzyści finansowych, i/lub politycznych (ideologicznych).

Brak jest uniwersalnej definicji bezpieczeństwa informacyjnego. Współcześnie obserwuje się odnoszenie bezpieczeństwa informacyjnego do trzech obszarów a mianowicie (rysunek 2-19):[138]

1) bezpieczeństwa informacji odnoszące się do ochrony danych, poufności danych, informacji niejawnych i informacji strategicznych;
2) cyberbezpieczeństwa rozumianego jako bezpieczeństwo sieci i systemów informacyjnych, kontrola przepływów danych;
3) bezpieczeństwa teleinformacyjnego jako pojęcia, określającego ochronę dziedzin strategicznych (KIP), zinformatyzowanych, do których można dotrzeć przy pomocy połączeń sieciowych.



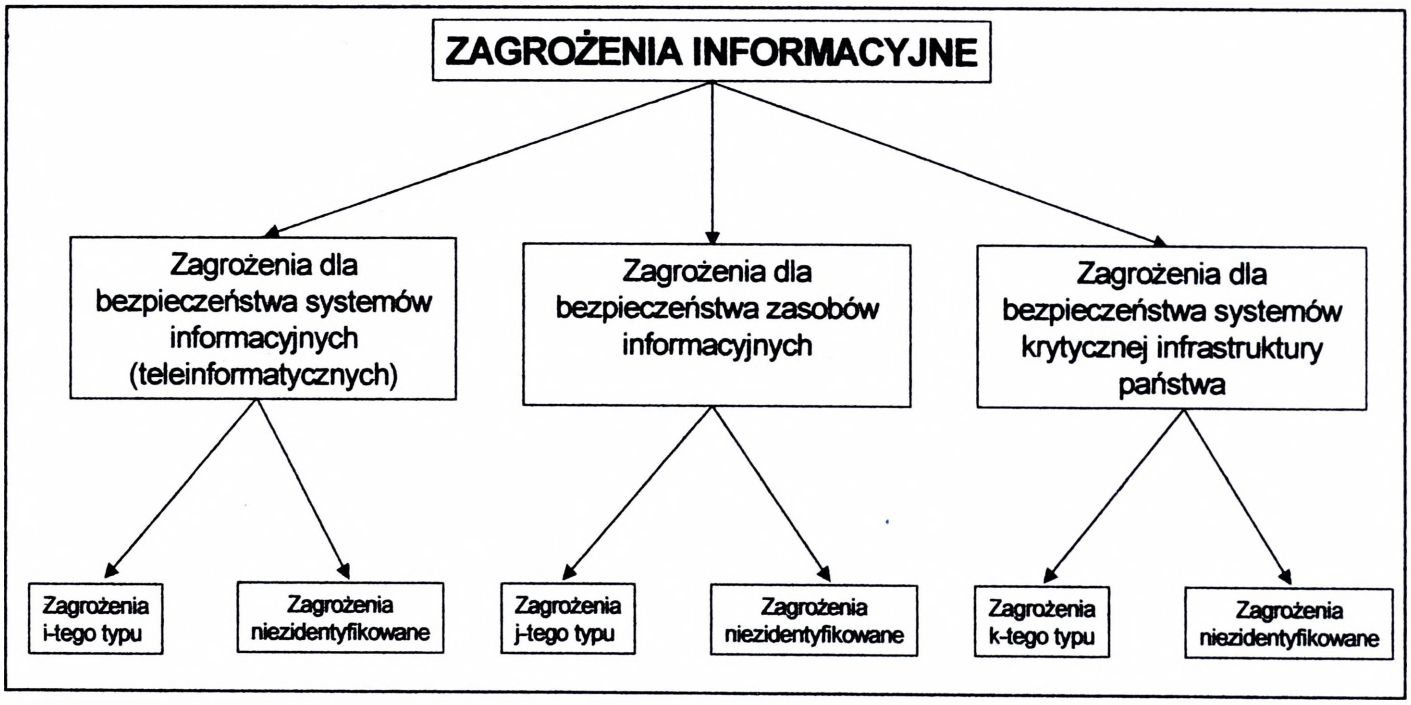
Rysunek 2-19. Obszary bezpieczeństwa informacyjnego
Źródło: opracowanie własne.

Istotą bezpieczeństwa informacyjnego jest przekonanie o konieczności ochrony wszelkich „informacji treściowych" i parametrów technicznych: kodów dostępu, konfiguracji komputerów itp., które mają zastosowanie w coraz większej liczbie działów gospodarek narodowych i administracji państwowych. Podstawą tej koncepcji jest sposób postrzegania kom-

[138] Takie sformułowania definicyjne znajdujemy w publikacji Bógdał-Brzezińskiej i Gawryckiego: *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie.* Warszawa 2003, s.307-309.

putera w teoriach walki informacyjnej: jako „magazynu informacji" (bazy danych i bazy wiedzy), jako środki kontroli i sterowania.[139]

Dynamika zjawisk związanych z pozyskiwaniem, przetwarzaniem, przesyłaniem, przechowywaniem, informacji wymusza monitoring oraz adaptację systemów bezpieczeństwa do zmieniającego się otoczenia. Bezpieczeństwo informacyjne można rozpatrywać w aspekcie organizacyjnym, technicznym oraz prawnym. Na bezpieczeństwo informacyjne można również spojrzeć od strony własności systemów informacyjnych, wyróżniając systemy państwowe (publiczne) i prywatne. Bezpieczeństwo informacyjne dotyczy bezpieczeństwa informacji oraz bezpieczeństwa systemów przetwarzania i przesyłania informacji, czyli zasobów teleinformatycznych (sieci, komputery), jak i ich wzajemnych relacji (stosunków i sprzężeń) zachodzących w środowisku (otoczenia) (rysunek 2-20).



Rysunek 2-20. Zagrożenia informacyjne w kontekście KIP

Źródło: T.Jemioło, *Modelownie zagrożeń dla bezpieczeństwa informacyjnego państwa. Teoria walki informacyjnej,* AON, Warszawa 2004.

W związku z powyższym można przyjąć następujące podstawowe grupy obiektów zagrożeń informacyjnych:

- systemy informacyjne (państwowe i pozapaństwowe): systemy informatyczne, telekomunikacyjne, sieci teleinformatyczne (rozpoznania, WRE, systemy wspomagające decyzje),
- zasoby informacyjne (państwowe i pozapaństwowe): bazy danych, bazy wiedzy oraz inne zbiory informacyjne istotne dla efektywnego działania określonych organów (instytucji),

[139] Ibidem, s.308.

- indywidualne urządzenia techniczne i systemy informatyczne (osobiste obywateli lub osób odpowiedzialnych za efektywne spełnianie funkcji
- elementy (podsystemy) KIP.

Podejście systemowe w badaniach nad bezpieczeństwem stanowi zasadniczą alternatywę dla podejścia klasycznego, rozpatrującego przede wszystkim zachowanie pojedynczych aktorów, czyli podejścia redukcjonistycznego.

Analiza systemowa zastosowana w badaniach bezpieczeństwa informacyjnego charakteryzuje się:

1) ujmowaniem zjawiska, zabezpieczeń i obiektów zagrożeń jako systemu, czyli całości złożonej z elementów w określony sposób zależnych od siebie oraz od właściwości tej całości;
2) uwzględnianiem ogółu warunków, czyli bliższego i dalszego otoczenia systemu;
3) szukaniem przyczyn, przekształceń wewnętrznych systemu, jego zdolności samosterowania, koordynacji i adaptacji do zmian w otoczeniu;
4) badaniem, nie tylko własności relacji wewnątrzsystemowych, lecz przede wszystkim ich efektywności (zależności między efektami a nakładami);
5) dążeniem do ujęcia funkcjonowania systemu w kategoriach optymalizacji.

Przyjmuje się następujące kategorie podstawowe:

Z – zbiór realnych i potencjalnych źródeł zagrożeń informacyjnych;

O - zbiór obiektów, na które skierowane są zagrożenia **Z**;

B – zbiór środków (metod, technik) zabezpieczenia obiektów **O** przed zagrożeniami **Z**.

Rozpatruje się trzy sytuacje systemowe:

I. System pasywnego bezpieczeństwa informacyjnego

$<Z,O,R_p>$ lub $<Z,O,F_p>$,

gdzie: $R_p \subset Z \times O$, $Fp: Z \rightarrow O$

R_p – relacja zagrożenia informacyjnego

F_p – funkcja zagrożenia informacyjnego

(np. $F_p: Z \times T \rightarrow O$, $F_p(z,t)=o \in O$ – obiekt **o** zagrożony jest w chwili $t \in T$ przez zagrożenie typu $z \in Z$).

Ponadto dana jest funkcja strat obiektu spowodowanych przez zagrożenie:

$G_p: Z \times T \times O \rightarrow V$ taka, że $G_p(z,t,o)=v \in V$

Jeżeli obiekt $o \in O$ posiada wartość V_o, to $v \leq V_o$. Nie oznacz to, że obiekt jest „bezbronny" wobec zagrożeń, lecz dysponuje np. autonomicznym zabezpieczeniem.

II. System aktywnego bezpieczeństwa informacyjnego

$<Z,B,O,R_a>$ **lub** $<Z,B,O,F_a>$

Gdzie: $R_a \subset B \times O$ **lub** $Fa: Z \times O \rightarrow B$, np. $Fa(z,O)=b$ – obiekt **o** jest zabezpieczany przez **b** przed zagrożeniem **z**.

Funkcja strat obiektu

$G_a: Z \times B \times T \times O \rightarrow V$ taka, że $G_a(z,b,t,o)=v \leq V_o$

Efektywny system bezpieczeństwa aktywnego posiada takie zabezpieczenie $b^* \in B$, że spełniona jest relacja:

$$G_a(z,b^*,t,o) \leq G_a(z,b,t,o) \text{ dla } b \in B.$$

III. System reaktywnego bezpieczeństwa informacyjnego

$<Z,B,C,O,R_r>$ lub $<Z,B,C,O,F_r>$

gdzie: $R_r \subset Z \times B \times C \times O$

$$Fr: Z \times B \times O \rightarrow C$$

C- zbiór działań podejmowanych jako reakcji obiektu **o** zabezpieczanego przez **b** przed zagrożeniami **z**.

$F_r(z,b,o)=c \in C$ – obiekt **o** zabezpieczany przez **b** przez z podejmuje działania reaktywne **c** (np. w celu likwidacji źródła zagrożeń).

Funkcja strat obiektu

$G_r: Z \times B \times T \times O \times C \rightarrow V$ taka, że $G_r(z,b,t,o,c)=v=V_o$

Efektywny system bezpieczeństwa reaktywnego posiada takie zabezpieczenie $b^* \in B$ i podejmuje taka reakcję $c^* \in C$ na zagrożenie $z \in Z$ w czasie $t \in T$, że spełniony jest warunek:

$$Gr(z,b^*,t,o,c^*) \leq Gr(z,b,t,o,c) \text{ dla } b \in B,\ c \in C.$$

Rozpatruje się aspekt kosztowy bezpieczeństwa: zakłada się, że każdy obiekt charakteryzuje użyteczność **U** będąca funkcją poniesionych na jej uzyskanie nakładów **N**, tj. $U(N)=u(N)$.

Bezpieczny obiekt $(Z=0)$ jest efektywny gdy $U(N)>N$.

Obiekt w sytuacji zagrożeń dokonuje racjonalnego wyboru zabezpieczeń **B**, których koszt wynosi K_B oraz może podejmować reakcje **C**, wymagające poniesienia kosztów K_C. Wtedy obiekt jest efektywny, w sensie bezpieczeństwa, gdy spełniony jest warunek: $(N)>N+K_B+K_C$.

Zakłada się , że powinien być spełniony warunek: $Gp(z,o)>Ga(z,b,o) \geq Gr(z,b,c,o)$

Przedstawione uwagi można potraktować jako próbę uogólnienia istotnych zagadnień bezpieczeństwa informacyjnego i, jako przykład sformułowania problemu analizy systemowej

zagrożeń (bezpieczeństwa) informacyjnego. Egzemplifikacją **Z** mogą być zidentyfikowane typy i rodzaje zagrożeń informacyjnych (rozdział 2 i załącznik V), natomiast **B** charakteryzuje „podatność" obiektu na zagrożenia (im skuteczniejsze **B**, tym mniejsza podatność **O** na **Z**).

Z przedstawionego modelu mogą również wynikać wnioski, pozwalające sformułować ogólną analityczną postać wartości ryzyka, a mianowicie:[140]

$$R_o(z)=\gamma_o \times \beta_o \times \eta_o \ , \ o \in O$$

gdzie $\gamma_o \equiv P_r(z), z \in Z$ prawdopodobieństw wystąpienia zagrożenia $z \in Z$;

$\beta_o \equiv P_r\{b/z\}, \ b \in B, \ z \in Z$, prawdopodobieństwo zastosowania środka **b** przez obiekt **o** pod warunkiem wystawienia zagrożenia **z**;

$\eta_o \equiv E[v,b,z]$ – wartość oczekiwana strat jakie mógłby ponieść obiekt **o** stosujący zabezpieczenie η w warunkach wystąpienia zagrożenia **z.**

W sytuacji zagrożenia dla bezpieczeństwa systemu, problem zarządzania bezpieczeństwem systemu można sprowadzić do wyboru takiej strategii bezpieczeństwa (zbioru strategii dopuszczalnych), dla której np. wartość oczekiwana skutków (strat) zagrożeń przyjmuje wartość minimalną, pod warunkiem, że koszty wdrożenia środków zabezpieczenia nie przekroczą wartości granicznej (dopuszczalnej).

2.11. Wnioski

Od ponad półwiecza, technologie, a ICT w szczególności są przyczyną przeobrażeń społecznych o dynamice, jakiej wcześniej nie doświadczano. Dzięki rozwojowi systemów informatycznych i telekomunikacyjnych oraz ich konwergencji z systemami mediów, wykreowano informację jako czwarty czynnik produkcji. Technologie informacyjne przyniosły syndrom „kurczenia się czasu i przestrzeni", zmieniły (na dobre i na złe) oblicze kultury masowej, uczyniły pracę lżejszą, (choć niekoniecznie przyjemniejszą), lecz przyczyniły się także do wzrostu bezrobocia strukturalnego ale jednocześnie stworzyły nowe zawody, jak również przyczyniły się do wzrostu skuteczności działań przestępczych.

Nowoczesne technologie mimo, że są nośnikiem postępu i wzrostu jakości życia społecznego wywołały kumulację różnorodnych zagrożeń i ekspansję ryzyka dla bezpiecznego rozwoju. Zmienił się zakres polityki bezpieczeństwa, pojawiły obszary zagrożeń niemilitarnych, wymagających udziału sił zbrojnych. Zacierają się, bowiem coraz bardziej granice między tym, co cywilne a tym, co wojskowe. Problem bezpieczeństwa posiada wymiar lokalny

[140] W analizach RAND stosuje się oznaczenia T (*threats*), V (*vulnerabilty*), C (*consequence*), R (*risk*).

i globalny, co skłania do przytoczenia myśli założyciela Klubu Rzymskiego A. Peccei: „*myśleć globalnie, działać lokalnie*".

Oprócz skumulowanych zagrożeń charakteryzujących społeczeństwo industrialne, występują nowe zagrożenia o charakterze informacyjnym, będące efektem przyspieszonego rozwoju infosfery. Następstwem jest wzrost interakcji społecznych, lecz także nadprodukcja informacji o pomijalnej wartości („smog informacyjny", parainformowanie, dezinformowanie, wirtualizacja faktów i zdarzeń). Wśród wielu interesujących konkluzji wynikających z analizy monograficznej, jako przesłanki dla badań podjętych w rozdziale trzecim wyróżnić można następujące wnioski:

1. Zmieniło się środowisko bezpieczeństwa międzynarodowego. Skutecznym środkiem prowadzącym do osiągania celów politycznych, militarnych, a także ekonomicznych stają się strategie walki informacyjnej (cybernetycznej, sieciowej).
2. Zasoby informacyjne (wiedzy) stały się zasobami strategicznymi, wymagającymi złożonych (i wielce kosztownych) systemów zabezpieczeń przed „obcą ingerencją".
3. Zastosowanie ICT w gospodarce spowodowało, że zasoby informacyjne różnych podmiotów są narażone na zagrożenia podobnie, jak w koncepcji walki informacyjnej (NCW).
4. W opiniach specjalistów przeważa stwierdzenie, że głównym celem cyberataków terrorystycznych będą systemy sterowania głównymi elementami krytycznej infrastruktury państwa (np. system energetyczny, bankowy).
5. Wśród zagrożeń katastrofalnych wyróżnia się:
   - niszczenie systemów telefonów alarmowych takich jak 911 czy 112 (istnieją potwierdzone przypadki takich działań),
   - sterowanie nadajnikami stacji radiowych i telewizyjnych i nadawanie komunikatów mających powodować panikę wśród ludności,
   - zmiany tras pociągów prowadzące do katastrof o trudnych do przewidzenia skutkach,
   - zniszczenie archiwów bankowych, stanów kont, systemu kredytowego,
   - powodowanie awarii w elektrowniach i fabrykach chemicznych, rafineriach,
   - uszkadzanie sieci rurociągów paliwowych i tym samym wywołanie oprócz zniszczeń materialnych, także kryzysu paliwowego.

6. Wśród zagrożeń informacyjnych od lat szczególnie szkodliwe pozostają zagrożenia typu: spam, wirusy i trojany. Zagrożenia te ewolują wraz z rozwojem zabezpieczeń[141] zwiększając stopień zaawansowania złośliwego oprogramowania (*malvare*). Nastąpił rozwój „czarnego rynku" produktów złośliwego oprogramowania.
7. Potrzeba bezpieczeństwa informacyjnego wynika faktu, iż narzędzi (broni) można użyć także w czasie pokoju i do ataku na cele „cywilne", których skutkiem byłoby osłabienie lub „paraliż" państwa. Wynika to z faktu, że obecnie systemy finansowe, energetyczne, komunikacyjne, użyteczności publicznej i transportu są dużo bardziej zintegrowane niż w przeszłości. Może to w znaczący sposób zwiększyć efektywność ataku asymetrycznego (terrorystycznego) wykorzystującego wrażliwości (podatności) ważnych obszarów infrastruktury państwa (KIP).
8. Wzrost ataków na banki i instytucje finansowe negatywnie wpływa na postrzeganie „gospodarki opartej na wiedzy"
9. Cyberprzestępczość rozwija się tak dynamicznie, że obecnie nie jest już zagrożeniem dla poszczególnych obywateli, czy też przemysłu, ale coraz bardziej zagraża bezpieczeństwu narodowemu (destabilizacja rynków finansowych, giełdy).
10. Ponadto badania wykazują słaby stan zabezpieczeń sieci komputerowych, co czyni je wrażliwymi na ataki nawet niezbyt sprawnych hackerów.
11. Wzrasta społeczna obawa przed cyberprzestepczością i cyberterroryzmem przy czym zagrożenia te coraz częściej trudno jest odróżnić.
12. Problematyka zagrożeń informacyjnych i bezpieczeństwa informacyjnego stanowi wyzwanie dla edukacji społecznej dla bezpieczeństwa.
13. Zasadniczym dylematem cywilizacyjnym staje się pytanie: „bezpieczeństwo czy wolność", albowiem pogodzenie w pożądanym stopniu obu tych szczególnie pożądanych wartości jest niemożliwe. [142]

---

[141] Wystąpiły nowe typy zagrożeń, np: vishing: metoda kradzieży danych, wywodząca się z phisingu. Polega na wykorzystywaniu telefonii internetowej. Napastnicy, najczęściej oszuści podszywają się przede wszystkim pod instytucje finansowe. Jedną z praktykowanych przez nich metod jest rozesłanie spamu, w którym podawany jest numer 0-800, pod którym odbiorcy e-maila zaleca się zaktualizowanie swoich danych przy koncie bankowym. Stosowane są również sposoby pozwalające na ominięcie pośrednictwa e-maila. Używa się programów, samoczynnie telefonujących przez VoIP pod zadaną im listę numerów telefonicznych. W momencie odbioru takiego telefonu przez ofiarę, automatycznie puszczana jest informacja o próbie wykorzystania karty kredytowej danej osoby oraz prośba o przejście procedury weryfikacyjnej, w której należy podać numer karty oraz dane jej właściciela. Nowym sposobem kradzieży tożsamości jest wykorzystanie portali społecznościowych jako cele ataku.

[142] Wybierając, zatem bezpieczeństwo oddajemy niejako znaczną część swej wolności (suwerenności), godząc się na liczne ograniczenia. W gruncie rzeczy oznacza to, że urzeczywistnia się w globalnym społeczeństwie informacyjnym antyutopia G. Orwella („*Big Brother is watching you*!") [za:] P.Sienkiewicz, *Bezpieczeństwo i wolność w globalnym społeczeństwie informacyjnym*. USz, Szczecin 2008.

14. W świadomości społecznej funkcjonuje przekonanie, że nie istnieją „absolutnie pewne" systemy bezpieczeństwa odporne na ataki informacyjne (cyberterrorystyczne).
15. W coraz szerszym zakresie poddawane są standaryzacji i regulacji kolejne obszary bezpieczeństwa informacyjnego.[143] Stosowane rozwiązania bezpieczeństwa przyniosły nowe problemy zarówno technologiczne, jak i organizacyjne zwiększając podatności systemów ujednolicaniem rozwiązań.
16. Istnieje ogromna potrzeba[144] badań nad zagrożeniami informacyjnymi, bezpieczeństwem informacyjnym i jego wpływem na stan bezpieczeństwa państwa, jako zjawiskami nowymi, ciągle ewoluującymi wraz z dynamicznie zmieniającą się technologią i środowiskiem bezpieczeństwa międzynarodowego.
17. Otwartą sprawą pozostaje problem prognozowania zagrożeń informacyjnych dla bezpieczeństwa narodowego.

---

[143] Praktyka wykazała (np. wspólne działania antykryzysowe „Concordia" - operacja NATO-UE na terenie byłej Jugosławii), konieczność standaryzacji w zakresie ochrony informacji niejawnych, ze względu na wymagania stawiane przez UE i NATO.

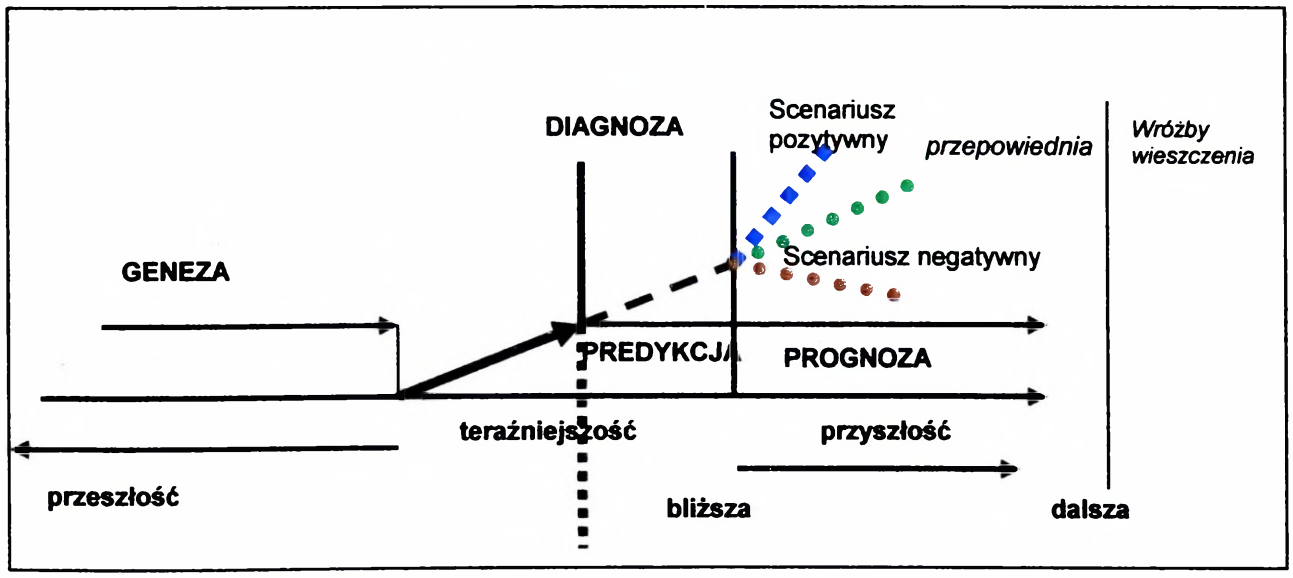
[144] Przypominają o tym programy dotyczące poprawy bezpieczeństwa przywoływane w poszczególnych rozdziałach.

Rozdział 3

PROGNOZOWANIE ZAGROŻEŃ INFORMACYJNYCH

3.1. Wprowadzenie

Dążenie do skutecznego zarządzania organizacjami i sterowania procesami wymaga efektywnego prognozowania zjawisk społecznych, ekonomicznych, technologicznych itp. Zagrożenia dla bezpieczeństwa informacyjnego, których obiektem są systemy krytycznej infrastruktury państwa grożą destabilizacją jego struktur i gospodarki. Stają się problemem i wymagają analiz prognostycznych, w wyniku, których można podejmować przedsięwzięcia planistyczne w systemie zarządzania bezpieczeństwem państwa. Celem prognozowania jest określenie ogólnego kierunku tendencji i dynamiki zmian badanych wielkości w przyszłości określonej przy tym horyzontem analizy. Prognozy zagrożeń informacyjnych, stanowią czynnik wspomagający procesy podejmowania racjonalnych decyzji (rysunek 3-1). W przypadku zjawisk o charakterze stochastycznym, a w szczególności wykazujących się niestacjonarnością i nieregularnością, a dotyczy to przede wszystkim zjawisk incydentalnych, większość metod formalnych (matematycznych) zawodzi (zwłaszcza w przypadku dłuższego horyzontu prognozowania). Pozostaje wtedy podejście typu foresight, scenariusze alternatywnych wizji przyszłości, opinie ekspertów itp.



Rysunek 3-1. Predykcja, prognozy i scenariusze

Źródło: H.Świeboda, *Metody scenariuszowe.* [w:] P.Sienkiewicz (red.), *Wybrane metody naukowych badań nad bezpieczeństwem i obronnością.* AON, Warszawa 2008, s.219.

Wiele typów zagrożeń informacyjnych ma charakter masowy (np. spam, wirusy), a to skłania przyjęcie do weryfikacji takich metod jak: analiza szeregów czasowych, sztuczne sieci neuronowe itp.

W przypadku wystąpienia niektórych zagrożeń, szczególnie tych o charakterze incydentalnym, możemy tylko przeciwdziałać ich skutkom. Istotne jest jednak poznanie tendencji w zachodzących zjawiskach. Rozważanie różnych procesów w postaci scenariuszy przyszłych zdarzeń, których realizacja zależy od tego czy zajdą pewne okoliczności (podatność systemu, brak zabezpieczeń), przyczynia się do tworzenia strategii postępowania, a tym samym do zwiększenia bezpieczeństwa systemu. W sytuacji jednak, gdy jest to możliwe warto próbować zastosować prognozowanie, szczególnie wtedy, gdy przypadki zagrożeń tworzą szeregi czasowe.

Niezwykle istotną sprawą staje się prognozowanie ataków w cyberprzestrzeni, z wykorzystaniem m.in. trojanów, wirusów i spamu. Są to zagrożenia wybrane z dużego „repertuaru" możliwości szkodliwego działania w sieci, o szczególnym znaczeniu dla bezpieczeństwa informacyjnego. Istnieje pilna potrzeba rejestrowania, a więc ewidencjonowania informacji o występowaniu zdarzeń zagrażających bezpieczeństwu informacji i danych (monitoring). Stanowi to warunek efektywnych analiz statystycznych w celu rozpoznania tendencji zmian. Z kolei, prognozowanie niektórych negatywnych zjawisk jest warunkiem podjęcia działań zapobiegawczych. Konsekwencją takiej analizy byłoby również śledzenie dynamiki tych zjawisk i kontrolowanie skuteczności podjętych działań.[145]

W założonej analizie prognostycznej niezbędna jest miara liczbowa obserwowanych zmiennych, które mogą stanowić szeregi czasowe uwzględniające zarejestrowane ataki. Do wyznaczania prognoz zagrożeń można wykorzystać prosty model wygładzania wykładniczego Holta, czy Holta-Wintersa. Statystyka ilościowa poszczególnych rodzajów zdarzeń stanowi podstawę prognozowania zjawiska i oceny prawdopodobieństwa ich wystąpienia w przyszłości. Podobne badania przeprowadzone w USA (na danych udostępnionych przez Departament Obrony) pozwoliły określić wielkość strat finansowych w zależności od prawdopodobieństwa wystąpienia ataków.[146]

Przedstawiony model analizy i prognozowania zachowania się zagrożeń w postaci szeregów czasowych, oparty jest na założeniu o probabilistycznym charakterze rozpatrywanych zjawisk, czyli zakłada się występowanie czynników losowych (o znanym lub nie rozkładzie

---

[145] P.Sienkiewicz, H.Świeboda, M.Pelc, *Aspekty logistyczne bezpieczeństwa krytycznej infrastruktury państwa.* Nr Specjalny ZN AON nr 2B, 2007.

[146] A.Korzyk, B.Violino, *A Forecasting model for internet security attacks*; The Security Facade, Information Week, October 21 1996.

prawdopodobieństwa). Skomplikowanie, działających często różnokierunkowo i nieznanych czynników warunkuje występowanie elementu przypadkowości. Ma to odzwierciedlenie w odchyleniach obserwowanych wielkości od poziomu wyznaczonego przez główną tendencję rozwojową. Składnik losowy jest związany z prawdopodobieństwem określającym szansę występowania wartości rozpatrywanej zmiennej.

Do przeprowadzenia prognozowania wykorzystano dane z raportów CERT (*Computer Emergency Response Team*)[147] zarejestrowane dla wielkości spamu, trojanów i robaków sieciowych w latach 1996-2006-2009. Do wyznaczenia prognozy posłużono się modelami formalnymi stosownymi w prognozowaniu szeregów czasowych, używając metodologii prognozowania z obszaru ekonomicznego.

3.2. Prognozowanie na podstawie szeregów czasowych

Fundamentalną cechą metod prognozowania zagrożeń na podstawie szeregów czasowych jest budowanie obrazu przebiegu zjawiska w przyszłości na podstawie zaobserwowanych wartości. Modele szeregów czasowych, szczególnie przy złożonych zjawiskach, pozwalają na wyznaczenie prognozy bez odwoływania się do przyczyn występowania zaburzeń kształtowania się zjawiska prognozowanego.[148]

W szeregach czasowych wyróżnia się dwie składowe:

- systematyczną, związaną z działaniem przyczyn głównych na zmienną prognozowaną, która może występować w postaci: stałego (przeciętnego) poziomu zmiennej prognozowanej, trendu[149], składowej okresowej inaczej nazywanej periodyczną, która dzieli się na składową cykliczną[150] i sezonową[151];
- przypadkową zwaną składnikiem losowym.

W przypadku prognozowania na podstawie szeregów czasowych, przetworzenie informacji o przeszłości odbywa się dzięki odpowiedniemu modelowi formalnemu, natomiast przejście od informacji przetworzonej do prognozy przez wybór reguły prognozowania, która może być regułą podstawową[152] lub regułą z poprawką[153]. Modelem szeregu czasowego słu-

---

[147] http://www.cert.pl/raporty.

[148] A.Zeliaś, B.Pawełek, S.Wanat, Prognozowanie ekonomiczne. Teoria, przykłady, zadania. PWN, Warszawa 2004.

[149] Trend - długookresowa skłonność do jedno-kierunkowych zmian (wzrostu lub spadku) wartości badanej zmiennej.

[150] Długookresowe rytmiczne wahania wartości zmiennej wokół tendencji rozwojowej (jej trendu) lub stałego (przeciętnego) poziomu tej zmiennej. Wiąże się z cyklem koniunkturalnym.

[151] Okresowe rytmiczne wahania wartości zmiennej wokół tendencji rozwojowej (trendu) lub stałego poziomu tej zmiennej w krótszym okresie (np. 1 roku).

[152] Przyjmujemy założenie, że model będzie aktualny w chwili, na którą określa się prognozę.

żącym do określenia przyszłej wartości zmiennej prognozowanej *Y w* momencie lub okresie prognozowanym *t*, tj. y^*_t, jest model formalny, którego zmiennymi objaśniającymi mogą być tylko: zmienna czasowa oraz przeszłe wartości lub prognozy zmiennej Y.

Prognoza zmiennej *Y* jest wartością funkcji *f* zależnej od czasu, przeszłych wartości i prognoz tej zmiennej

$$y_t^* = f\left(t, y_{t-1}, \ldots, y_{t-p}\ y_{t-1}^*, \ldots, y_{t-p}^* \xi_t\right) \qquad (3\text{-}1)$$

gdzie:

$y^*_t, y^*_{t-1}, \ldots, y_{t-p}$ - prognozy zmiennej *Y* wyznaczone na moment lub okres *t,t-1,...,t-p;*

$y_{t-1}, \ldots, y_{t-p}$ - zaobserwowane wartości zmiennej *Y w* momencie lub okresie *t-1,...,t-p;*

t - zmienna czasowa;

p - wielkość opóźnienia; składnik losowy.

Szereg czasowy może przyjmować postać modelu addytywnego lub multiplikatywnego. W modelu addytywnym zakłada się, że obserwowane wartości zmiennej prognozowanej są sumą (wszystkich lub niektórych) składowych szeregu czasowego. Przyjmuje się, że nie występują interakcje pomiędzy poszczególnymi składowymi szeregu, składowe są niezależne. Każda ze składowych jest wyrażona w tych samych jednostkach miary, co zmienna prognozowana. W procesie dekompozycji wahania okresowe oraz przypadkowe są wyrażone jako odchylenia od tendencji rozwojowej lub od stałego poziomu zmiennej prognozowanej. Natomiast w modelu multiplikatywnym przyjmuje się, że obserwowane wartości zmiennej prognozowanej są iloczynem składowych szeregu czasowego. W modelu tylko jedna ze składowych - na ogół tendencja rozwojowa lub stała - poziom średniej prognozowanej, jest wyrażona w jednostkach zmiennej prognozowanej. Pozostałe składowe szeregu są w procesie dekompozycji wyrażane jako względne odchylenia, bądź od tendencji rozwojowej, bądź od stałego poziomu zmiennej.[154]

W badaniu sformułowano następujące zadanie prognostyczne:

Wyznaczyć prognozy zagrożeń informacyjnych, pojawiających się w sieciach teleinformatycznych w postaci szkodliwych kodów, które reprezentowane są przez spam, wirusy i konie trojańskie.

---

[153] Wykorzystujemy wtedy, gdy występują uzasadnione przypuszczenia, co do tego, że ostatnio zaobserwowane odchylenia danych empirycznych od modelu utrzymają się w przyszłości.
Reguła przybiera następującą postać: $y_t^* = E(Y_t) + p. \quad t > n,$

[154] M.Cieślak (red.), *Prognozowanie gospodarcze*. PWN, Warszawa 2000.

Sformułowane zadnie jest wyrazem szerzej ujętego problemu:

Czy zaproponowane modele mogą być przydatne w prognozowaniu zagrożeń informacyjnych? Jakie czynniki wpływają na zwiększenie dokładności prognozowania?

Pojawiające się zagrożenia w sieci są wyrażone w postaci danych i reprezentują ciąg wartości liczbowych uporządkowanych według czasu, tworząc szereg czasowy (jednowymiarowy) jako ciąg zaobserwowanych stanów zmiennej Y uporządkowanych według wartości zmiennej czasowej t.

$$y = [y_1, y_2, ..., y_t, ..., y_n], \qquad (t = 1, 2, ..., n), \qquad (3\text{-}2)$$

gdzie y_t to stan zmiennej w momencie t.

Zebrane dane dotyczącą: ogólnej liczby incydentów, spamu, wirusów i zagrożeń w postaci trojanów, zarejestrowanych przez CERT (*Computer Emergency Response Team*)[155] i udostępnionych w raportach, zamieszczanych na stronach www. Do prognozowania wybrano metodę ilościową opartą na formalnym modelu prognostycznym zbudowanym na podstawie danych o kształtowaniu się wartości zmiennej prognozowanej w przeszłości.

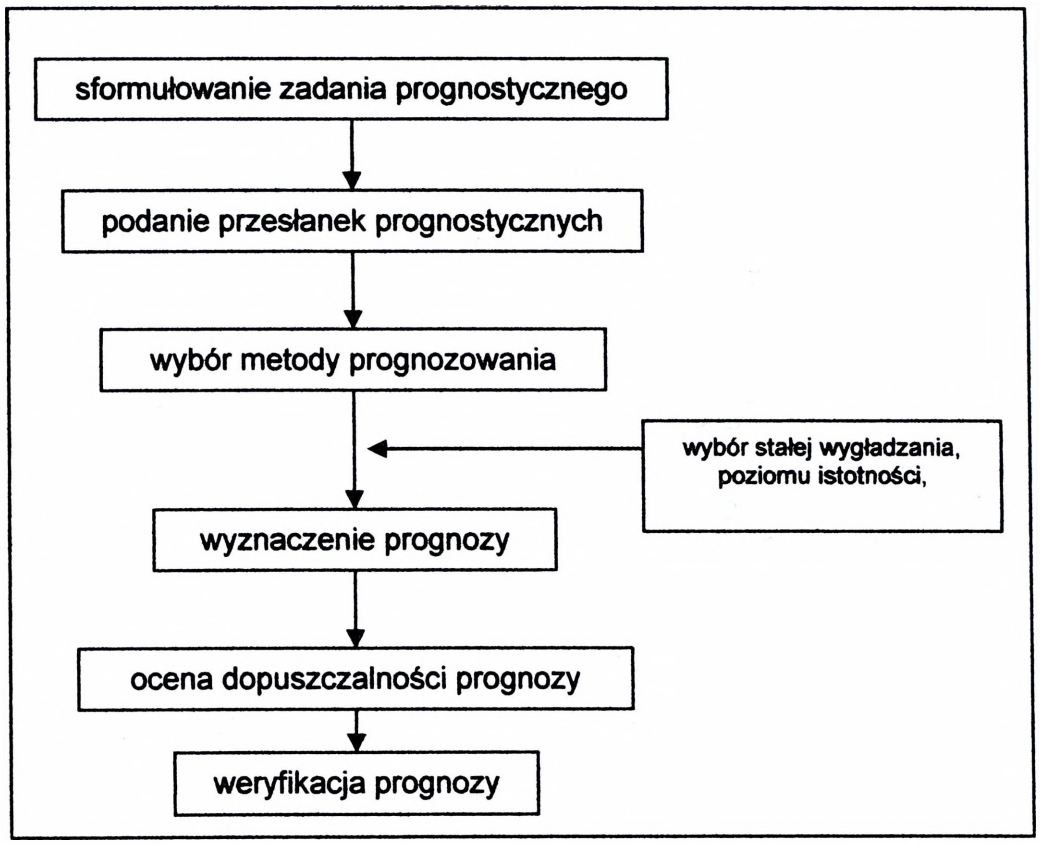
Cel wyznaczania prognozy ma charakter badawczy, wobec tego prognoza nie jest obłożona wysokimi wymaganiami, co do dopuszczalności, bowiem celem oprócz wyznaczenia prognozy, jest badanie kształtowania się zjawiska czy trendu zagrożeń. **Horyzont prognozy** jest determinowany wyborem modelu, a także przyjęciem postawy aktywnej dopuszczającej, że przyszłość mniej lub bardziej jest niezależna od przeszłości. W związku z tym dopuszcza się zmianę dotychczasowych związków występujących między prognozowanym zjawiskiem (zagrożeniami), a oddziaływaniami nań innych zjawisk. Celem prowadzonych badań jest poznanie przydatności modelu formalnego do prognozowania zagrożeń.

Przesłanki prognostyczne: prognozowanie zjawisk społecznych jest niezwykle trudne ze względu na wielość czynników wpływających na dane zjawisko. W przypadku zagrożeń typu wirusy, spam czy konie trojańskie czynniki, które kształtują te zjawiska, lokalizują się w kilku obszarach i są trudne do zidentyfikowania, bowiem wiążą się z psychologicznymi pobudkami podejmowania tego typu działalności. Wśród nich można wymienić: umyślne działanie powodowane pobudkami ideologicznymi lub motywowane politycznie, etnicznie albo też działaniami typu terroryzm państwowy lub działalnością szpiegowską. Może być powodowana również chęcią zysku oraz zmierzenia się z zabezpieczeniami dla rozgłosu. W obszarze technicznym tego typu ataki ułatwiają coraz prostsze, tańsze i dostępne narzędzia penetracji sieci.

---

[155] http://www.cert.pl/raporty.

Prognozowanie przeprowadzono według planu zaprezentowanym na schemacie.



Rysunek 3-2. Proces wyznaczania prognozy
Źródło: opracowanie własne.

Wyboru metod modeli formalnych dokonano w oparciu o analizę graficzną danych, a brakujące dane uzupełniono wykorzystując średnią z kilku wyrazów szeregu, czasem stosując dominantę lub medianę (w zależności od charakterystyki rozkładu analizowanych danych). Wykorzystano także możliwość budowania szeregów w oparciu o generator liczb pseudolosowych z wykorzystaniem pakietu analizy danych w arkuszu Excel.

Weryfikacji prognoz dokonano w oparciu o liczenie błędów dla każdego momentu należącego do przedziału czasu [n+1,...,T] zwanego przedziałem empirycznej weryfikacji prognoz. Zastosowano podstawową postać błędu prognozy *ex post* w postaci bezwzględnego błędu prognozy *ex post* w czasie t:

$$q_1 = y_t - y_t^*, \quad t > n \tag{3-3}$$

gdzie:

y_t - realizacja zmiennej Y w czasie $t > n$ (wartość rzeczywista zaobserwowana);

y_t^* - prognoza zmiennej Y na czas $t > n$ otrzymana z danej metody.

Wartość błędu informuje, jak wielkie było w chwili $t > n$ odchylenie prognozy od wartości rzeczywistej zmiennej Y. Znak błędu wskazuje, czy rzeczywista wartość była wyż-

sza od prognozy (+), czy niższa (-). Ponadto policzono względne błędy prognozy *ex post* w czasie *t*:

$$\Psi_t = \frac{y_t - y_t^*}{y_t} \cdot 100, \quad t = n+1,\ldots,T \tag{3-4}$$

Oznaczenia jak we wzorze powyżej.

Wartość błędu informuje, jak wielkie było w chwili $t > n$ odchylenie prognozy od wartości rzeczywistej zmiennej Y, liczone w procentach wartości rzeczywistej. Dowiadujemy się, więc o rozmiarach odchylenia względnego i kierunku odchylenia. Dokonano również obliczeń średnich względnych błędów prognoz *ex post* w przedziale weryfikacji wg wzoru:

$$\Psi = \frac{1}{T-n} \sum_{t=n+1}^{T} \frac{\left[y_t - y_t^*\right]}{y_t} \cdot 100 \tag{3-5}$$

Oznaczenia jak wyżej.

Z obliczeń (według tego wzoru) otrzymujemy informację, jaki procent rzeczywistej wartości zmiennej Y stanowiło przeciętnie, w przedziale weryfikacji, bezwzględne odchylenie prognoz od danych rzeczywistych. W obliczeniach posłużono się również średnim kwadratowym błędem prognoz *ex post* w przedziale weryfikacji.

$$S^* = \left[\frac{1}{T-n} \sum_{t=n+1}^{T} \left(y_t - y_t^*\right)^2\right]^{0,5} \tag{3-6}$$

Oznaczenia jak wyżej.

Wartość S^* informuje o przeciętnych odchyleniach prognoz od wartości rzeczywistych w przedziale empirycznej weryfikacji prognoz. Wartość S^* jest porównywalna z *s*, tj. odchyleniem standardowym reszt. Wektor prognoz można uznać za zadowalający, gdy jest spełniona relacja:

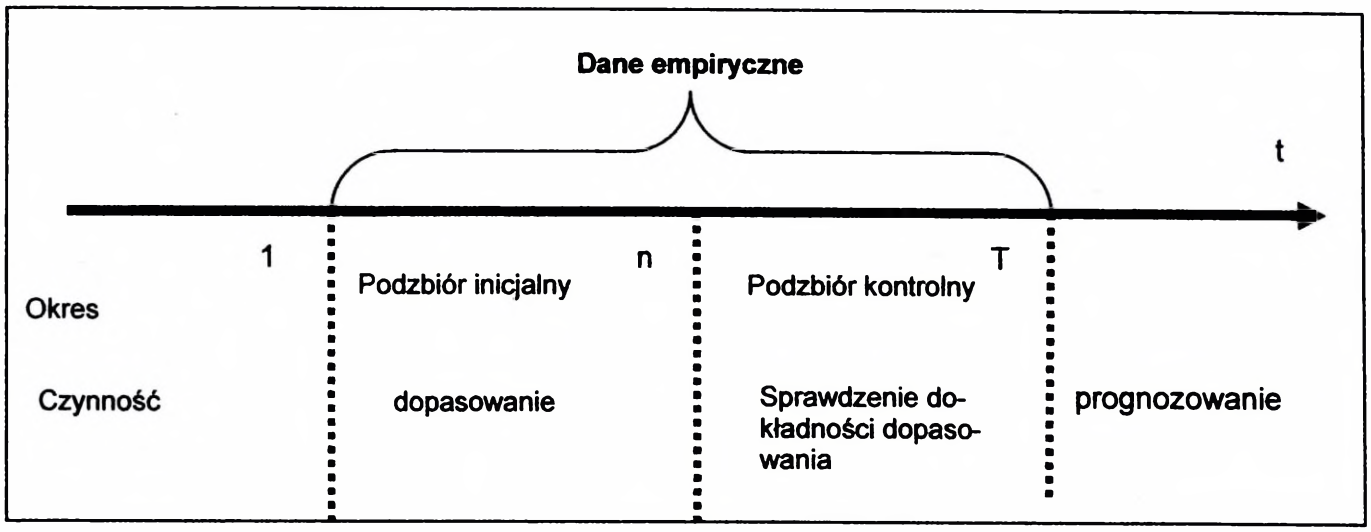
$$s^* \leq s \tag{3-7}$$

Dla określania dopasowania prognoz do danych rzeczywistych zastosowano współczynnik Theila:

$$I^2 = \frac{\sum_{t=n+1}^{T} \left(y_t - y_t^*\right)^2}{\sum_{t=n+1}^{n} y_t^2} \tag{3-8}$$

Miernik ten przyjmuje wartość równą zeru, gdy prognozy są idealnie trafne. Im większe są różnice między prognostycznymi i rzeczywistymi wartościami badanej zmiennej, tym większa jest jego wartość.

W każdym zbiorze danych wydzielono podzbiór inicjalny sprawdzając dopasowanie modelu do danych. Wartości parametrów wygładzania wyznaczono korzystając z modułu Solver arkusza Microsoft Office Excel, za pomocą optymalizacji polegającej na minimalizacji średniego błędu kwadratowego w podzbiorze kontrolnym. W następnym kroku dokonywano prognozowania (rysunek 3-3).



Rysunek 3-3. Proces prognozowania
Źródło: opracowanie własne.

W badaniu odwołano się do średniej ruchomej, metody, która polega na uśrednianiu kolejnych sekwencji wyrazów szeregu czasowego przez obliczanie tzw. średnich ruchomych i zastępowanie nimi pierwotnych wyrazów szeregu czasowego. Do wygładzania stosuje się *k* o parzystej lub nieparzystej liczbie wyrazów w szeregu. Obliczoną wartość przypisuje się środkowej z pośród obserwacji, na podstawie, których obliczana jest wartość średniej ruchomej:

$$y_T^P = \frac{1}{k} \sum_{t=n-k+1}^{n} y_t \qquad (3\text{-}9)$$

Stałą wygładzania *k* dobiera się na podstawie kryterium najmniejszego błędu ex *post* prognoz wygasłych. Może to być średni względny błąd prognoz ex *post* lub średniego kwadratowego błędu prognoz *ex post (s).*

W badaniach odwołano się również do modeli wygładzania wykładniczego, które polegają na tym, że szereg czasowy wygładza się z pomocą średniej ruchomej ważonej, przy czym wagi określa się według prawa wykładniczego.[156]

[156] A.Manikowski, Z.Tarapata, *Prognozowanie i symulacja rozwoju przedsiębiorstw.* WSE, Warszawa 2002, s.134.

W prostym modelu wygładzania wykładniczego prognoza zmiennej na moment lub okres t równa jest prognozie tej zmiennej na moment lub okres *t*-1 skorygowanej o iloczyn parametru wygładzania α i wartości jej bezwzględnego błędu ex post:[157]

$$y_t^* = \alpha y_{t-1} + (1-\alpha) y_{t-1}^* \tag{3-10}$$

Parametr wygładzania dobierano na podstawie kryterium najmniejszego błędu *ex post* prognoz wygasłych, posługując się dodatkiem Solver w arkuszu kalkulacyjnym Excel.

W badaniach zastosowano dwurównaniowy model Holta, który służy do wygładzania szeregu czasowego, w którym występuje zarówno tendencja rozwojowa jak i wahania przypadkowe:

$$F_t = \alpha y_t + (1-\alpha)(F_{t-1} + S_{t-1}) \tag{3-11}$$

$$S_t = \beta(F_t - F_{t-1}) + (1-\beta) S_{t-1} \tag{3-12}$$

Równanie I - służy do wyznaczania wygładzonych wartości szeregu czasowego w momencie/okresie *t*-1.

Równanie II - służy do wyznaczania wygładzonych wartości przyrostu trendu na moment/okres *t*-1.

gdzie:

F_t wartość wygładzona zmiennej prognozowanej;

y_t wartość rzeczywista (empiryczna) zmiennej prognozowanej w okresie *t*;

S_t wartość wygładzona przyrostu trendu na moment lub okres czasu *t*;

α stała wygładzania wartości zmiennej prognozowanej;

β stała wygładzania wartości przyrostu zmiennej prognozowanej, spowodowanego tendencją rozwojową.

Rekomendacje literaturowe w przypadku znacznych i nieregularnych zmian trendu w czasie, zalecają nadawać większą wagę najnowszej wartości zmiennej (parametr α powinien być zbliżony do jedności), a mniejszą ocenie trendu w poprzednim okresie, (1-α) powinno być bliskie zera.

W praktyce dobiera się je stosując postępowanie symulacyjne za pomocą metody kolejnych przybliżeń empirycznych tak, aby otrzymać najmniejszy kwadratowy błąd ex post prognoz wygasłych. Poszukujemy, więc takich stałych wygładzania, przy których otrzymane prognozy najlepiej aproksymują rzeczywiste realizacje zmiennej prognozowanej.

---

[157] B.Radzikowska, *Metody prognozowania. Zbiór zadań.* WAE, Wrocław 2004, s.33.

Prognozę zmiennej Y na moment/okres T (T>n), gdzie n jest liczbą obserwacji zmiennej prognozowanej), otrzymuje się przez dodanie do wartości wygładzonej z momentu/okresu t=n (F_n), wielokrotności (T-n) wygładzonej wartości przyrostu trendu na moment/okres t=n(S_n):

$$y_t^* = F + (t-n)S_n \ , t > n \tag{3-13}$$

Do wygładzenia szeregu tą metodą, konieczna jest znajomość wartości początkowych wygładzonych wartości zmiennej prognozowanej oraz wygładzonego przyrostu tej zmiennej, wynikającego z tendencji rozwojowej. W literaturze przedmiotu można znaleźć, co najmniej kilka propozycji rozwiązania tego problemu. Dla potrzeb tej analizy przyjęto standardowo:

1. Za wartość początkową wygładzenia zmiennej prognozowanej pierwszej rzeczywistej (empirycznej) wartości tej zmiennej tj. $F_1 = y_1$
2. Za początkową wartość wygładzenia przyrostu trendu przyjęto różnicę między drugą a pierwszą rzeczywistą wartością zmiennej prognozowanej tj.

$$S_1 = y_2 - y_1 \tag{3-14}$$

Kolejnym modelem zastosowanym do badania jest model Wintersa występujący w dwóch postaciach: multiplikatywnej i addytywnej. Model może być stosowny w przypadku występowania wahań sezonowych. Z powodu braku danych do prognozowania zastosowano dane generowane losowo.

W modelu multiplikatywnym wygładzona wartość zmiennej w szeregu czasowym po eliminacji wahań sezonowych na moment/okres t-1 dana jest wzorem:

$$F_{t-1} = \alpha \frac{y_{t-1}}{C_{t-1-r}} + (1-\alpha)(F_{t-2} + S_{t-2}) \tag{3-15}$$

Jest odpowiednikiem wygładzonej wartości otrzymanej z prostego modelu wygładzania wykładniczego dla momentu lub okresu *i*;

Wygładzona wartość przyrostu trendu na moment/okres t-1 dana jest wzorem:

$$S_{t-1} = \beta(F_{t-1} - F_{t-2}) + (1-\beta)S_{t-2} \tag{3-16}$$

Ocena wskaźników sezonowości na moment /okres t-1 obliczamy ze wzoru:

$$C_{t-1} = \gamma \frac{y_{t-1}}{F_{t-1-r}} + (1-\gamma)C_{t-1-r} \tag{3-17}$$

gdzie:

r- długość cyklu sezonowego (liczba faz w cyklu),

α, β, γ - parametry wygładzania przyjmujące wartości z przedziału (0,1).

Równanie prognozy na moment/okres t>n obliczane jest za pomocą wzoru:

$$y_t^{\bullet} = (F + (t-n)S_n)C_{t-r} \tag{3-18}$$

Postać militplikatywna zakłada, że każda wartość szeregu czasowego jest iloczynem wartości z wykluczoną sezonowością oraz indeksem sezonowości dla danego okresu. Prognozę wyznacza się w sposób sekwencyjny, korzystając z trzech równań zawierających parametry wygładzania:

- dla komponenty F przyjąć wartość rzeczywistą zmiennej z szeregu czasowego odpowiadającą pierwszej fazie drugiego cyklu lub średnią wartość z pierwszego cyklu; $F_r = \frac{1}{r}\sum_{t=1}^{r} y_t$ (3-19)
- dla komponenty S przyjąć różnicę średnich wartości z drugiego i pierwszego cyklu bądź przyjąć 0 $S_r = \frac{1}{r}(y_r - y_1)$ (3-20)
- dla komponenty C (w poszczególnych fazach pierwszego cyklu) przyjąć ilorazy wartości rzeczywistej zmiennej z pierwszego cyklu w odniesieniu do średniej wartości w pierwszym cyklu bądź przyjąć 1.

$$C_t = 1, \quad dla\ t \in \overline{1,r}$$

gdzie:

r- długość cyklu sezonowego (liczba faz w cyklu);

α, δ, γ - parametry wygładzania przyjmujące wartości z przedziału (0,1).

Wartości parametrów dobiera się na podstawie kryterium najmniejszego średniego błędu ex post (względnego, kwadratowego) prognoz wygasłych.

Postać addytywna

Zasada określania wartości początkowych jest identyczna jak w przypadku modelu multiplikatywnego. Obliczenia poszczególnych komponent realizuje się w oparciu o prezentowane wzory.

$$F_{t-1} = \alpha(y_{t-1} - C_{t-1-r}) + (1-\alpha)(F_{t-2} - S_{t-2}) \tag{3-21}$$

$$S_{t-1} = \beta(F_{t-1} - F_{t-2}) + (1-\beta)S_{t-2} \tag{3-22}$$

$$C_{t-1} = \gamma(y_{t-1} - F_{t-1-r}) + (1-\gamma)C_{t-1-r} \tag{3-33}$$

gdzie:

F_t - odpowiednik wygładzonej wartości otrzymanej z prostego modelu wygładzania wykładniczego dla momentu lub okresu *i*;

S_t - wygładzona wartość przyrostu trendu szeregu na moment lub okres *j*;

C_r - ocena wskaźnika sezonowości na okres *r*;

n - liczba wyrazów szeregu czasowego zmiennej prognozowanej;

α, δ, γ - parametry modelu – przy szybkiej zmienności składowych szeregu są bliskie 1.

Wartości parametrów dobiera się na podstawie kryterium najmniejszego średniego błędu ex post (względnego, kwadratowego) prognoz wygasłych.

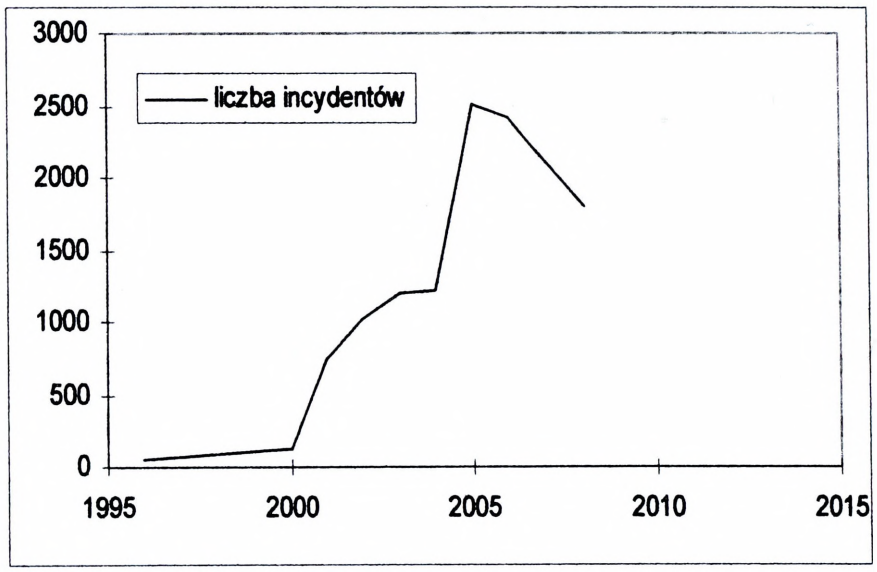
W obu modelach przy wyborze parametrów wygładzania zastosowano kryterium minimalizacji średniego kwadratowego błędu prognoz ex post. W tym celu wykorzystano dodatek Solver w arkuszu kalkulacyjnym.

Wyniki analiz

W pierwszym etapie badaniu poddano ogólną liczbę zarejestrowanych incydentów. Dane obejmowały lata 1996-2008 (tabela 3-1, rysunek 3-4.)

Tabela 3-1. Ogólna liczba incydentów w latach 1966-2008

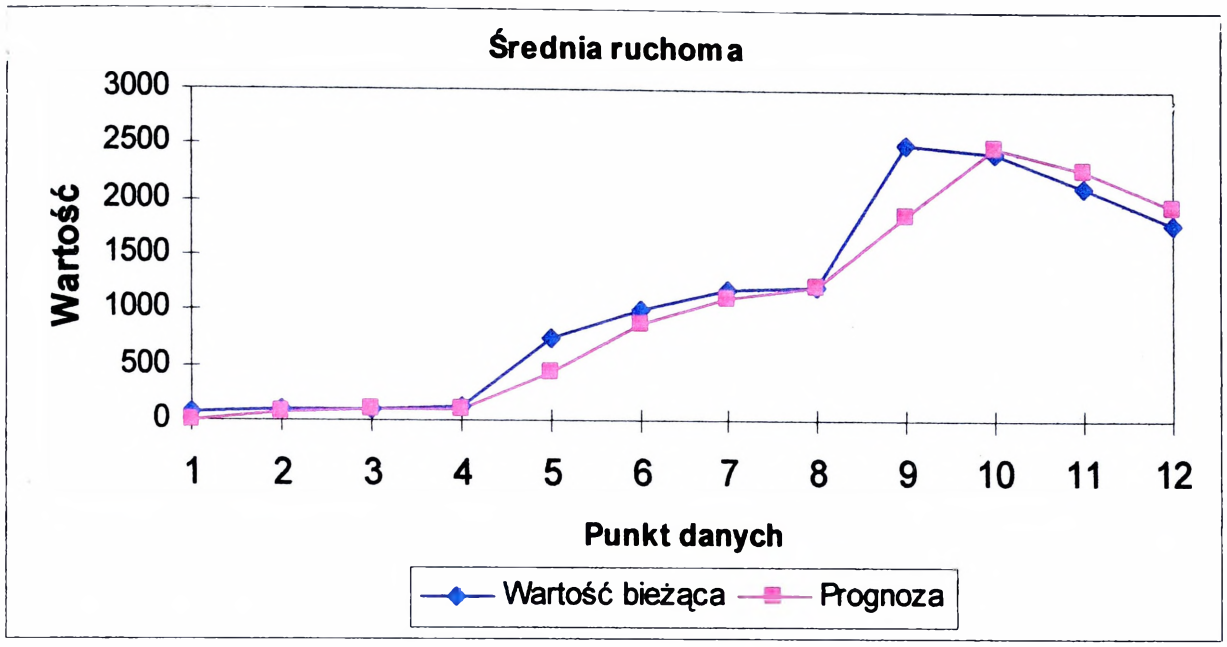
lata	Ogólna liczba incydentów
1996	50
1997	75
1998	100
1999	105
2000	126
2001	741
2002	1013
2003	1196
2004	1222
2005	2516
2006	2427
2007	2108
2008	1796



Rysunek 3-4. Liczba incydentów w latach 1996-2008
Źródło: CERT 2008.

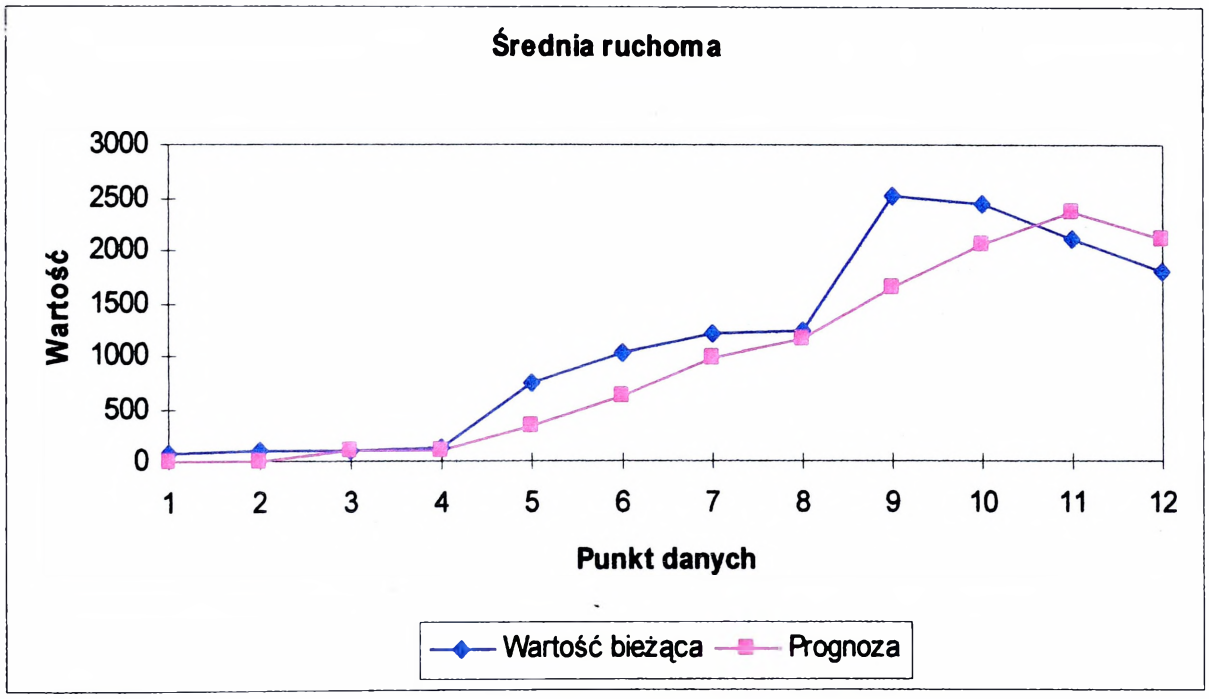
Ocena wzrokowa wskazuje, że w badanym szeregu nie występuje składowa systematyczna, potwierdza to wysoka wartość współczynnika zmienności, który wynosi 0,865, obliczonego według wzoru: $(V = \frac{s}{\bar{y}} * 100\%)$. Występują wahania przypadkowe, do roku 2007 utrzymywała się silna tendencja wzrostowa, poczym nastąpiło zmniejszenie ilości zaobserwowanych incydentów.

W modelu średniej ruchomej zastosowano wygładzanie przy k=2 (rysunek 3-5) i k=3 (rysunek 3-6).



Rysunek 3-5. Dane rzeczywiste teoretyczne i prognoza przy k=2 dla zagrożenia „ogólna liczba incydentów"

Źródło: opracowanie własne.



Rysunek 3-6. Dane rzeczywiste, teoretyczne i prognoza przy k=3 dla zagrożenia „ogólna liczba incydentów"

Źródło: opracowanie własne.

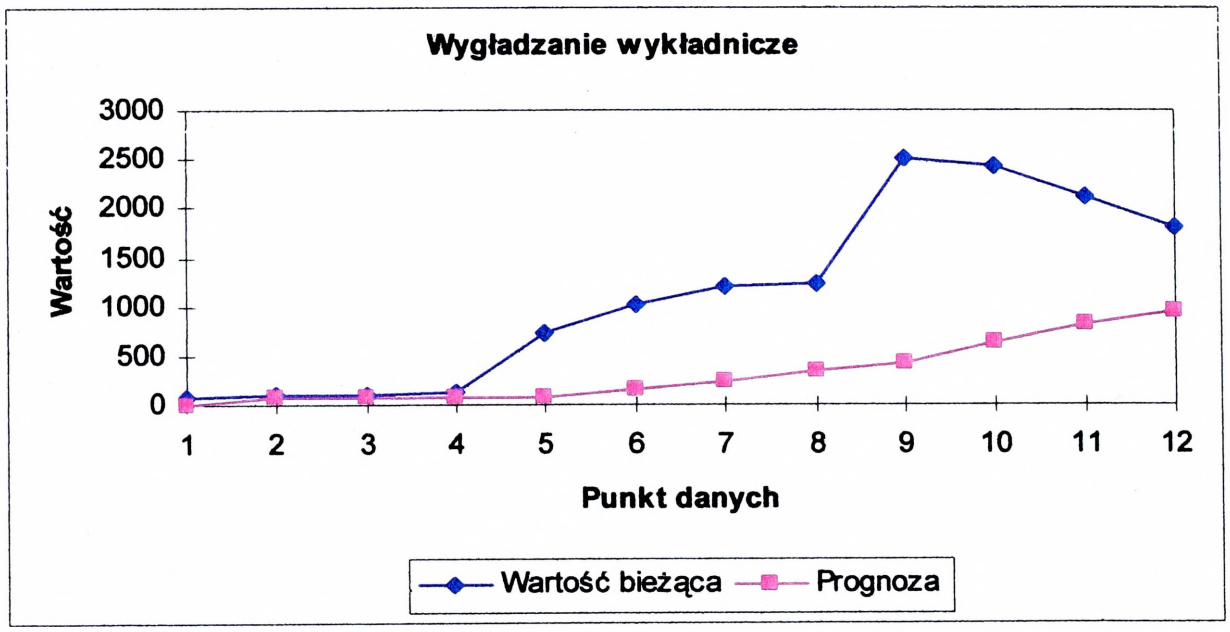
Wygładzony szereg o k=2 stałej wygładzania wyraźniej podąża za szeregiem empirycznym, zachowując część z jego nieregularności. Szereg o k=3 i większych stałych wygładzania jest bardziej regularny, ale nie osiąga poziomu, do którego docierają wartości zmiennej Y.

Pierwiastek średniego kwadratowego błędu ex post prognoz wygasłych przy k=2 wyniósł 708,3. Prognozowania „liczby incydentów" na rok dokonano również z wykorzystaniem narzędzia - średnia ruchoma - znajdującego się w dodatku Analiza Danych. Błąd odniesiono

do wartości wyznaczonej prognozy i stanowił on 11,8%. Przy stałej wygładzania k=3 pierwiastek średniego kwadratowego błędu *ex post* prognoz wygasłych wyniósł 15,5 incydentów na rok. Błąd prognozy wyniósł 103%. Ponieważ istnieją różnice w obliczeniach stosowanych z wykorzystaniem narzędzia znajdującego się w dodatku Analiza Danych, a liczeniem z samodzielnie wpisywanymi formułami - dokonano prognozowania z zastosowaniem formuł. Błędy oparte o wartości pierwiastków średniego kwadratowego błędu *ex post* prognoz wygasłych przy k=2 wyniosły 503,09 a przy k=3, s=673.

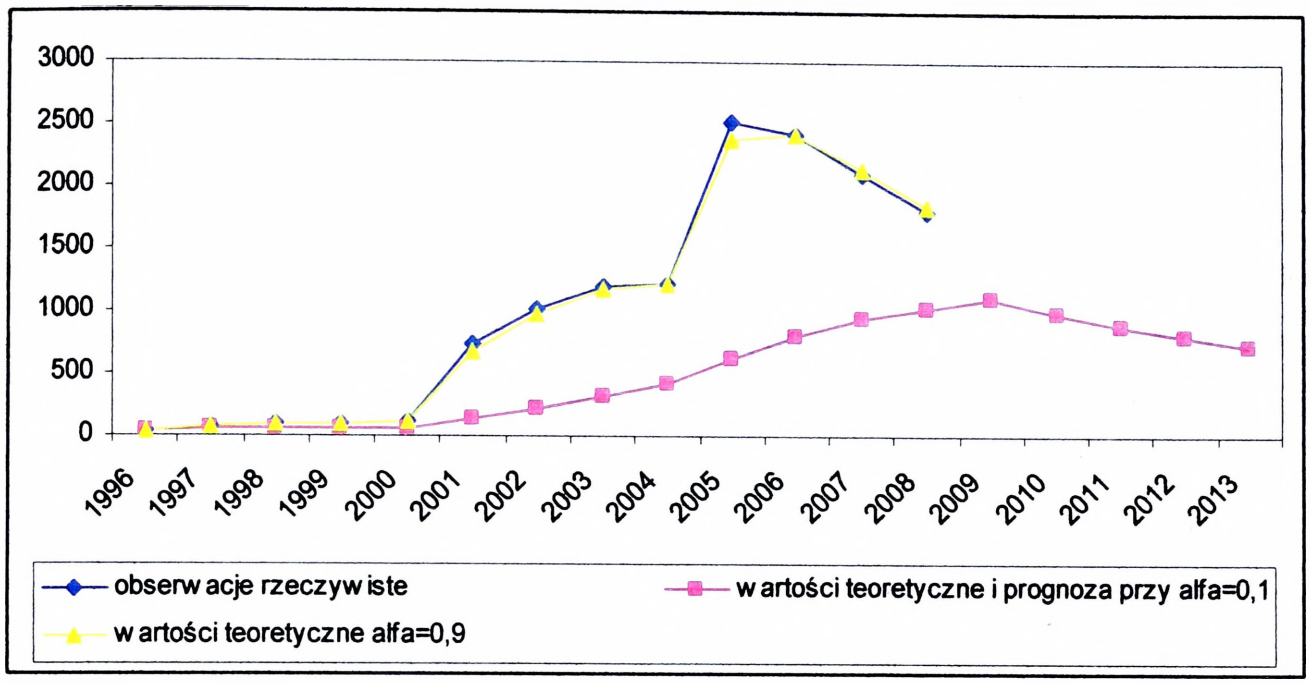
Manipulując stałą wygładzania przez zwiększanie liczby wyrazów *k* powodujemy większe wygładzenie szeregu kosztem zwiększenia błędów. Prognozy uzyskane metodą średniej, odzwierciedlają średnią tendencję występującą w danych. Prognozy obarczone są dużym błędem, zaletą jest wskazywanie ogólnej tendencji analizowanej zmiennej.

Szereg czasowy zawierający ogólną liczbę incydentów na przestrzeni 1996-2008 poddano prognozowaniu przy wykorzystaniu modelu prostego wygładzania wykładniczego.



Rysunek 3-7. Prognoza z zastosowaniem modelu prostego wygładzania wykładniczego przy α=0,1 dla zagrożenia „ogólna liczba incydentów"

Źródło: opracowanie własne.



Rysunek 3-8. Rzeczywiste realizacje oraz wartości teoretyczne i prognozy przy różnych stałych wygładzania dla zagrożenia „ogólna liczba incydentów"

Źródło: opracowanie własne.

Wartość parametru alfa wyznaczono eksperymentalnie, ponadto posiłkowano się rozwiązując zadanie optymalizacyjne, w którym minimalizowano błąd średni kwadratowy dla okresu kontrolnego. Im większą wagę nadawano dla parametru alfa, wtedy prognozy były empirycznymi wartościami szeregu z poprzedniego okresu, parametr bliski zeru powodował, że duża liczba obserwacji ma wagi o zbliżonych wartościach. Model może być stosowany przy założeniu, że wartości stałej wygładzania danego szeregu czasowego, dobiera się każdorazowo dla danego szeregu czasowego.

Tabela 3-2. Wartości błędów dla okresu kontrolnego przy α=0,1

Dla okresu kontrolnego	
ME - błąd średni (ang. *Mean Error*)	1368,108
MPE - średni błąd procentowy (ang. *Mean Percentage Error*)	0,603248
MSE - średni błąd kwadratowy (ang. *Mean Square Error*)	2054133
MAE - średni błąd bezwzględny (ang. *Mean Absolute Error*)	1368,108
MAPE - średni bezwzględny błąd procentowy (ang. *Mean Absolute Percentage Error*)	0,603248
Thiel	0,413101

Źródło: opracowanie własne.

Ponieważ wartości bezwzględne z miar ME (błąd średni) i MEA (średni błąd bezwzględny) są sobie równe, to wartości teoretyczne systematycznie są niższe lub wyższe od wartości rzeczywistych (tabela 3-2).

Szereg poddano również prognozowaniu, w którym do wykonania prognozy posłużono się metodą modelu Holta, stosowaną do wygładzania szeregów czasowych, w których występuje trend liniowy oraz wahania przypadkowe. Metoda ta należy do grupy metod wygładzania wykładniczego[158], w której wyznacza się wartości średniej trendu oraz wahań sezonowych występujących w szeregu czasowym. W analizie przyjęto 2 parametry wygładzania: α i β zgodnie z założeniami modelu. Parametry wygładzania należą do przedziału (0;1). Im większa jest wartość parametru α tym większą uwagę przykłada się do bliskich obserwacji, a mniejszą do odległych w czasie. Wartości parametru wyznaczano eksperymentalnie. Odwołano się również do zadnia optymalizacyjnego, w którym rozwiązanie otrzymuje się w wyniku minimalizowania średniego błędu kwadratowego prognoz wygasłych, jako funkcję parametru α i β. Przyjęto wartości początkowe dla α=0,8 i β=0,5. Minimalizując średni błąd kwadratowy, wyznaczono α=0,9923 i β= 0. Gdy β przyjmuje wartość bliska zeru, mamy do czynienia z silnym wpływem poprzedniego przyrostu (w przeciwnym przypadku β jest bliskie jedności). Prognozę zmiennej Y na moment lub okres T (T>n), gdzie n jest liczbą wyrazów szeregu czasowego zmiennej prognozowanej, otrzymuje się przez dodanie do wartości wygładzonej z momentu/okresu t=n (F_n) wielokrotności (T-n), wygładzonej wartości przyrostu trendu na moment/okres t=n(S_n). Jako wartości wygładzone szeregu czasowego w momencie/okresie t-1 przyjęto $F_1=y_1$ i dla wyznaczenia wygładzonych wartości przyrostu trendu na moment/okres t-1 przyjęto $S_1=y_2-y_1$.

W literaturze przedmiotu można spotkać propozycję, aby za początkowe wartości przyjmować odpowiednio wyraz wolny i współczynnik kierunkowy liniowej funkcji trendu.[159] Funkcja trendu wyrażona jest równaniem y=137,23 x-17,206. Prognoza punktowa na t=14 wyniosła 1904,16 incydentów na rok 2009. Wartość ocen ex ante średniego błędu obliczono ze wzoru:

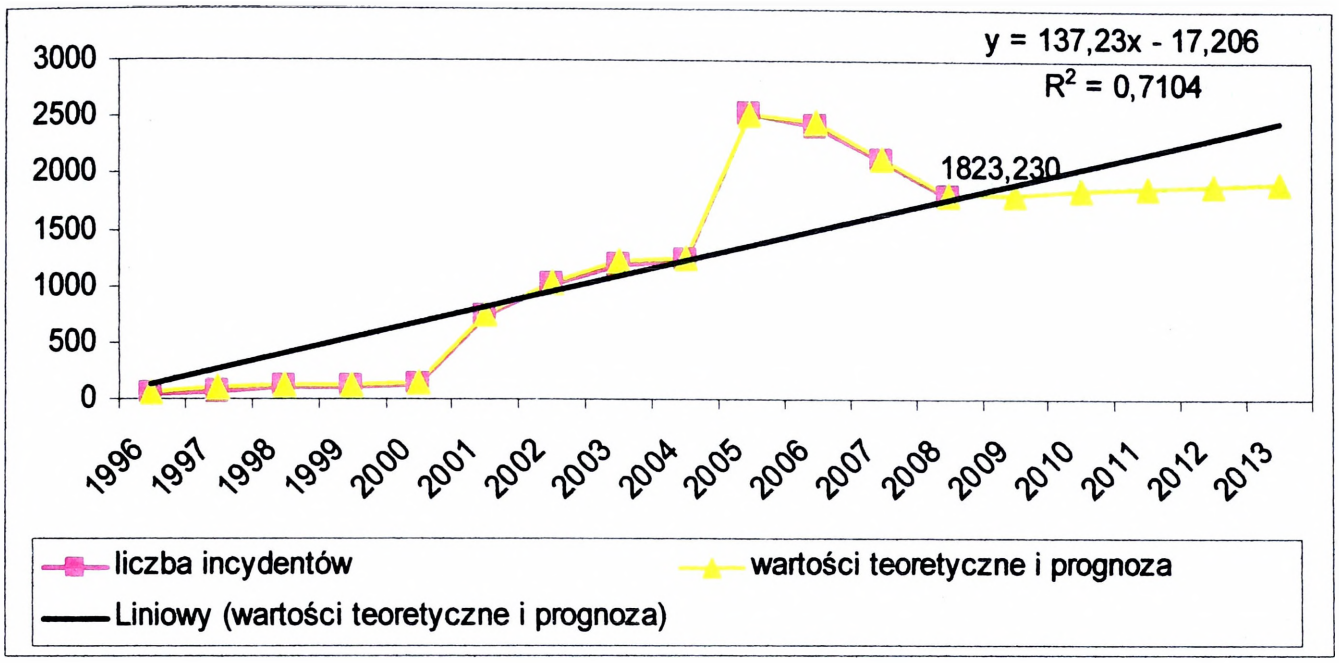
$$s_{D_T} = \sqrt{s_e^2 \left[1 + \frac{1}{n} + \frac{(T-\bar{t})^2}{\sum_{t=1}^{n} (t-\bar{t})^2} \right]} \qquad (3\text{-}34)$$

---

[158] Nazwa wykładnicze pochodzi stąd, że w miarę zwiększania się odległości w czasie między wartościami bieżącymi a wartościami historycznymi, waga tych ostatnich zmniejsza się wykładniczo.

[159] A.Zeliaś, *Prognozowanie ekonomiczne*, PWN, Warszawa 2004, s.149.

S_{DT}=0,546. Względny błąd predykcji policzono ze wzoru: $V_{D_T} = \frac{s_{D_T}}{y_T^P}$ i wyniósł 0,03%.



Rysunek 3-9. Wartości empiryczne, wartości teoretyczne oraz prognoza przyrostu liczby incydentów
Źródło: opracowanie własne.

Tabela 3-3. Zestawienie błędów dla okresu kontrolnego i wyznaczone prognozy

Błędy dla okresu kontrolnego

Dla okresu kontrolnego	
ME	-0,0131502
MPE	24,3669661
MSE	609,3876343
MAE	0,0131502
MAPE	0,0000000
Theil	0,0000000

Wyznaczone prognozy na lata 2009-2011

Prognozy	2009	1823,230
	2010	1848,230
	2011	1873,230

Źródło: opracowanie własne.

Tak skonstruowane prognozy obarczone są pewnym błędem. Metoda wygładzania wykładniczego Holta nie pozwala jednak określić błędu prognozy *ex ante*. Tym większej wagi w tym przypadku nabiera określenie błędu prognozy *ex post*, szczególnie w świetle przyjętego założenia, że należy dobrać takie stałe wygładzania, aby średni kwadratowy błąd ex post prognoz wygasłych był minimalny. Badamy zatem dopuszczalność prognozy. Dla potrzeb badawczych przyjmiemy, iż średni względny błąd prognozy nie może przekraczać 5%. Jeśli warunek ten będzie spełniony, prognozę uznamy za dopuszczalną. Błąd względny średni procentowy liczono ze wzoru: $\frac{s^*}{x_{16}} * 100\%$, wyniósł 1%. Ponieważ błąd średni i średni błąd bezwzględny są sobie równe to wartości teoretyczne są systematycznie niższe od wartości rze-

czywistych. Tabela 3-4 zawiera zestawienie wyników predykcji dla zagrożenia „zarejestrowane incydenty w latach 1996-2008" osiągniętych w procesie prognozowania z zastosowaniem wybranych modeli formalnych. Ponadto zestawiono wyniki oceny jakości prognoz wyrażone wielkością błędów: średni błąd kwadratowy MSE i względny błąd prognozy.

Tabela 3-4. Zestawienie wyników prognoz oraz ich błędów *ex post* dla zagrożenia „ogólna liczba incydentów"

OGÓLNA LICZBA INCYDENTÓW	PROGNOZA	MSE	WZGLĘDNY BŁĄD PROGNOZY[160]:
Model średniej ruchomej			16,4
K=2	1406	504,4	35,8
K=3	2110	212,84	10,3
Model Browna α=0,1	1096	955,1	87
α= 0,9	1830,35	45,17	2,463
Metoda Holta	1823	1,97	1

Źródło: opracowanie własne.

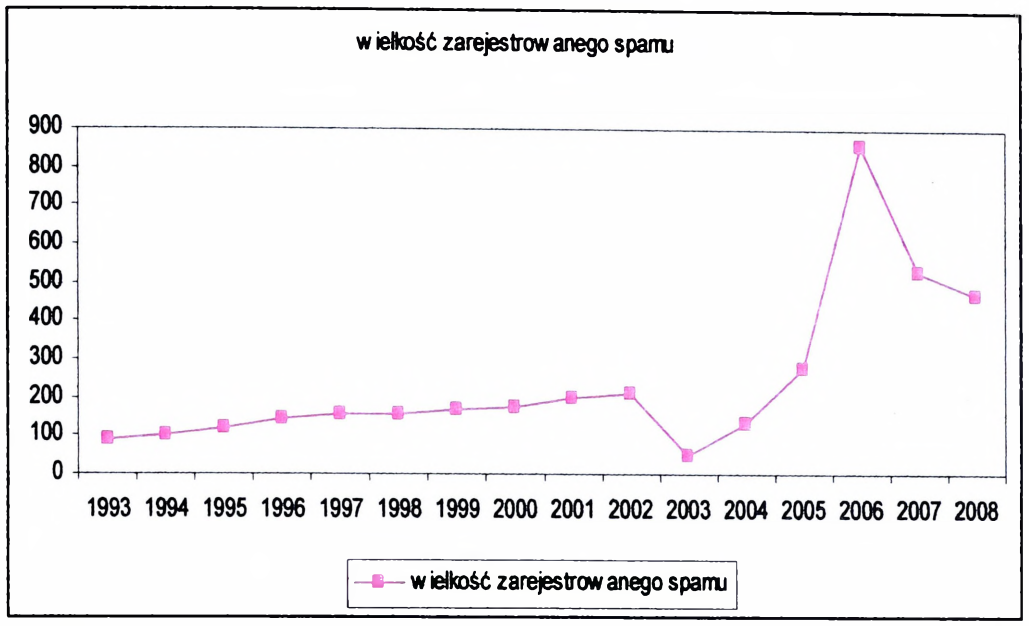
Szereg czasowy przedstawiający zarejestrowane zagrożenia „spam" w latach 1993-2008 zawarte są w tabeli 3-5. Ocena wzrokowa wykresu (rysunek 3-10) wskazuje, że do roku 2002 ilość spamu wzrastała regularnie, w 2003 roku nastąpiło załamanie trendu, ilość spamu wyraźnie uległa zmniejszeniu, poczym od 2004 do 2006 obserwujemy gwałtowny wzrost, a w 2007 ponownie zmniejszyła się ilość spamu i ta tendencja się utrzymuje. Analiza graficzna pozwala na zidentyfikowane następujących składowych: trendu wznoszącego (1993-2002), trendu potęgowego wznoszącego (2003-2007), trendu potęgowego opadającego (2006-2008). Trend najlepiej opisuje wielomian kwadratowy (rysunek 3-11).

Wartości wygładzane α i β wyznaczono empirycznie oraz na podstawie minimalizowania średniego błędu kwadratowego prognoz wygasłych przy wykorzystaniu Solvera, jako narzędzia optymalizacji. Zestawienie błędów dla okresu kontrolnego na podstawie, którego wyznaczane były α i β zawiera tabela 3-6.

[160] Pierwiastek średniego błędu kwadratowego błędu *ex post* prognoz wygasłych / wartość prognozy w %.

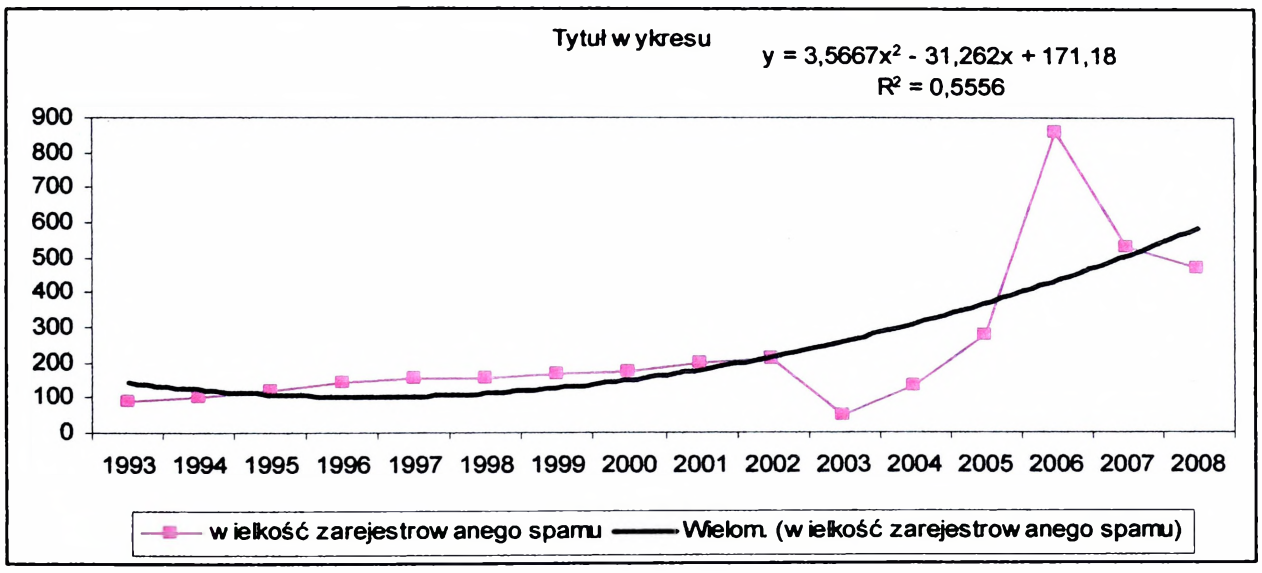
Tabela 3-5. Dane zarejestrowane CERT Spam

lata	spam
1993	89
1994	100
1995	120
1996	143
1997	155
1998	157
1999	169
2000	176
2001	199
2002	208
2003	48
2004	130
2005	275
2006	857
2007	531
2008	466



Rysunek 3-10. Wielkość zarejestrowanego spamu w latach 1993-2008

Źródło: opracowanie własne.



Rysunek 3-11. Opis trendu za pomocą wielomianu kwadratowego zagrożenia „wielkość zarejestrowanego spamu"

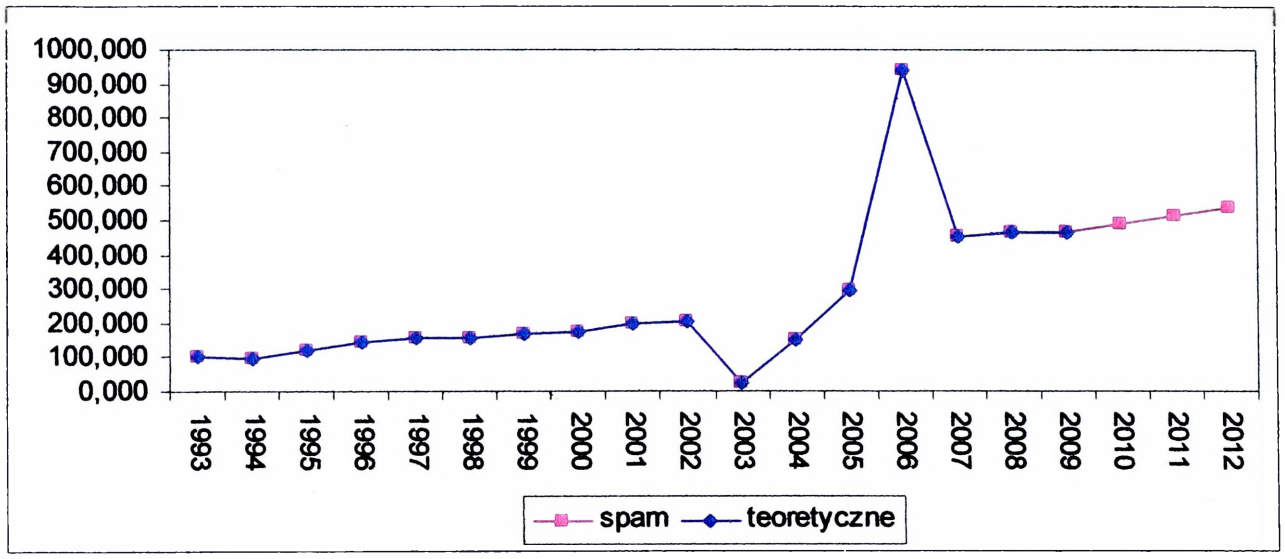
Źródło: opracowanie własne.

Tabela 3-6. Zestawienie zbiorcze wyników błędów dla podzbioru kontrolnego, prognoz i ich błędów dla zagrożenia „wielkość zarejestrowanego spamu"

Wartości błędów dla podzbioru kontrolnego		Wyznaczone prognozy przy alfa=0,88 i beta= 0,15		Wartości względnych błędów prognoz	
ME	0,681104	2009	463,671	2009	1,09%
MPE	0,118026	2010	488,515	2010	1,04%
MSE	664,0315	2011	513,359	2011	0,99%
MAE	17,63237	2012	538,203	2012	0,94%
MAPE	0,261236				
Theil	0,018685				

Źródło: opracowanie własne.

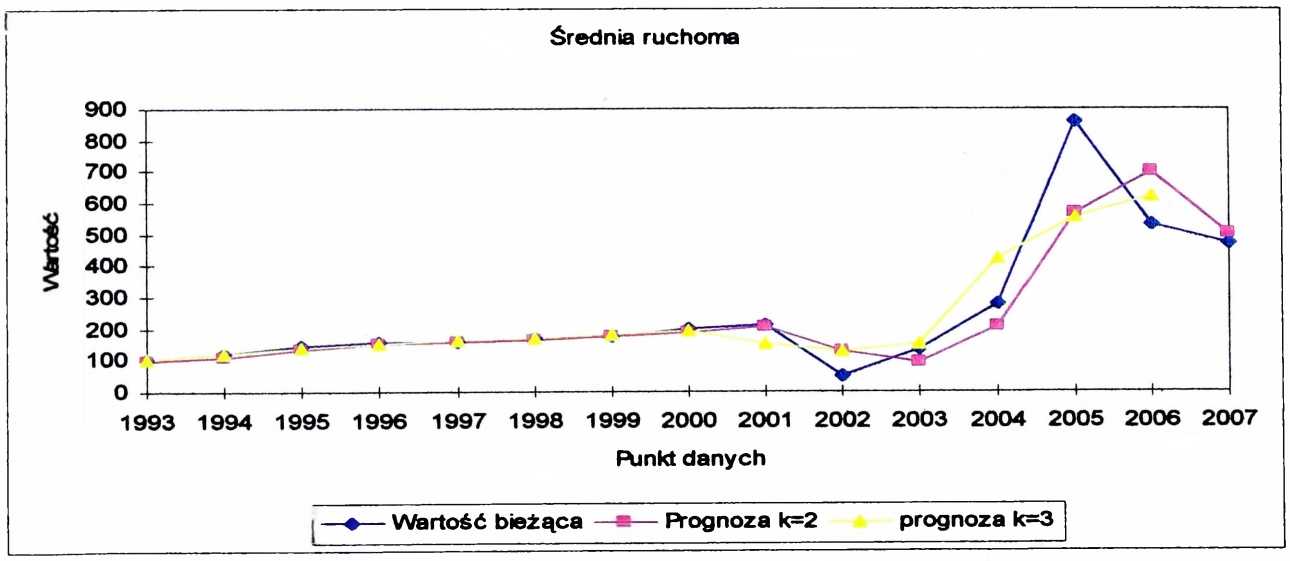
Przy empirycznie wyznaczonych wartościach stałych wygładzania: $\alpha = 0,88$ i $\beta=0,15$, widać wyraźnie trend wznoszący w następnych latach dla wyznaczonych prognoz. Pierwiastek średniego błędu kwadratowego, błędu ex post dla prognoz wygasłych wyniósł: 5,07, co stanowi około 1% wartości względnych błędów prognoz w porównaniu z wartością prognoz na kolejne lata (rysunek 3-12).



Rysunek 3-12. Prognoza przy empirycznie wyznaczonych alfa i beta dla zagrożenia „wielkość zarejestrowanego spamu"

Źródło: opracowanie własne.

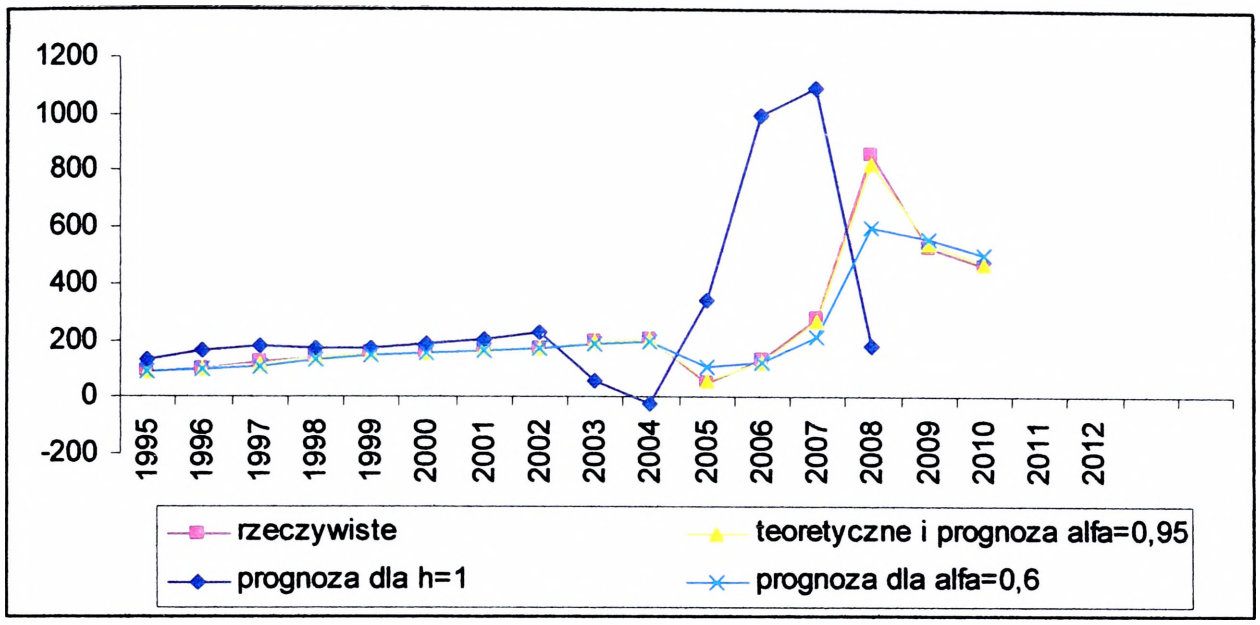
Prognozy otrzymane w wyniku zastosowania modelu wygładzania za pomocą średniej ruchomej dla k=2 i k=3 (rysunek 3-13) przedstawiały się następująco: rok 2009 k=2 prognoza=498,5, pierwiastek średniego błędu kwadratowego 97,1, natomiast błąd względny prognozy wyniósł 18,4%; dla k=3 prognoza=618, pierwiastek średniego błędu kwadratowego wyniósł 152,3, a błąd względy prognozy wyniósł 24,6%.



Rysunek 3-13. Wartości bieżące dla zagrożenia „wielkość zarejestrowanego spamu" oraz prognoza dla k=2 i k=3

Źródło: opracowanie własne.

W modelu Browna za wartość początkową przyjęto pierwszą wartość rzeczywistą zmiennej prognozowanej. Wyznaczanie wartości alfa dokonano obserwując zachowanie krzywych na wykresie podczas manipulacji wielkością stałej wygładzania (rysunek 3-14).



Rysunek 3-14. Wartości rzeczywiste oraz prognozowane dla zagrożenia „wielkość zarejestrowanego spamu" przy różnych wielkościach alfa

Źródło: opracowanie własne.

Tabela 3-7. Porównanie metod prognozowania dla zarejestrowanych wielkości spamu

ZAREJESTROWANE WIELKOŚCI SPAMU	PROGNOZA	MSE	WZGLĘDNY BŁĄD PROGNOZY[161]:
Model średniej ruchomej			
K=2	498,5	91	18,4
K=3	618	152,3	24,6
Model Browna α=0,6	503	71,4	14,2
α= 0,95	479,99	8,81	1,8
Prognoza z wyprzedzeniem 1 okresu h=1	184	177,8	96,4
Metoda Holta	463,671	5,07	Ok. 1

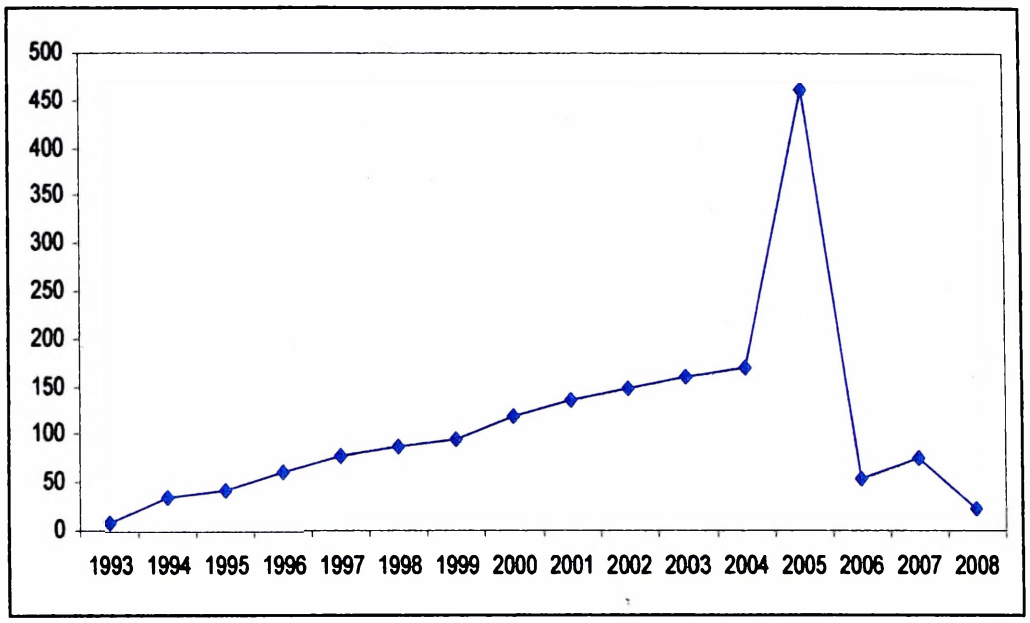
Źródło: opracowanie własne.

Prognoza zagrożenia określana mianem Robak sieciowy (*worm*) to prognoza dla złośliwych programów, które mają zdolność do rozprzestrzeniania się do komputerów innych użytkowników. Podstawę stanowią dane pozyskane z raportu CERT. Obejmują dane zarejestrowane od 1993 roku do 2008 (tabela 3-8 i rysunek 3-15).

[161] Pierwiastek średniego błędu kwadratowego błędu ex post prognoz wygasłych / wartość prognozy w %.

Tabela 3-8. Wartości zarejestrowane zagrożenia „robak sieciowy" przez CERT na przestrzeni lat 1993-2008

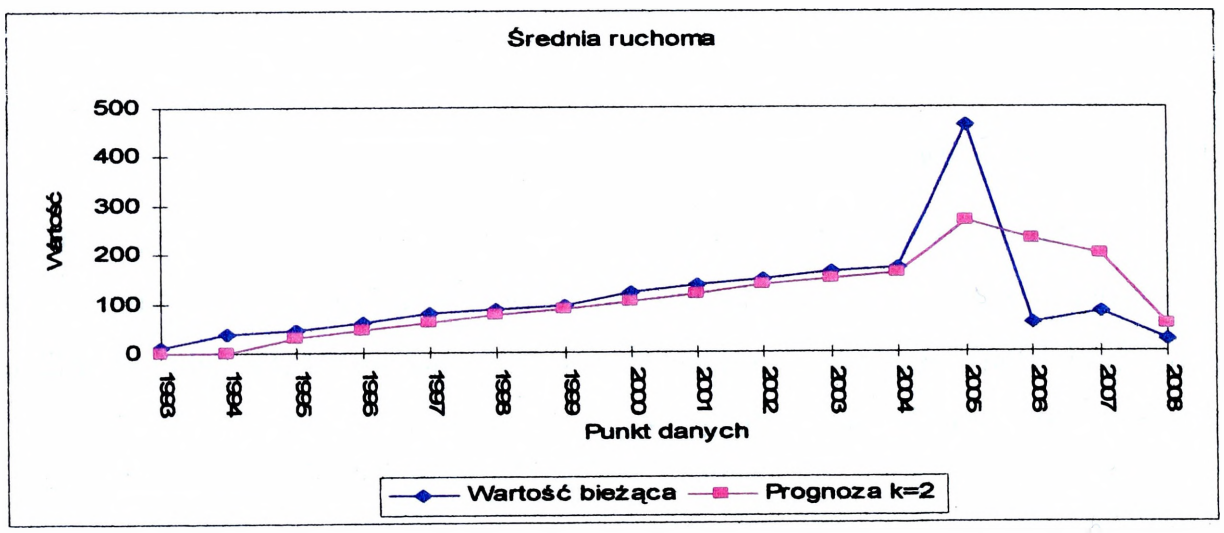
1993	10
1994	36
1995	44
1996	62
1997	79
1998	88
1999	95
2000	120
2001	138
2002	149
2003	161
2004	170
2005	462
2006	55
2007	78
2008	24



Rysunek 3-15. Zarejestrowane incydenty „robak sieciowy"
Źródło: opracowanie własne.

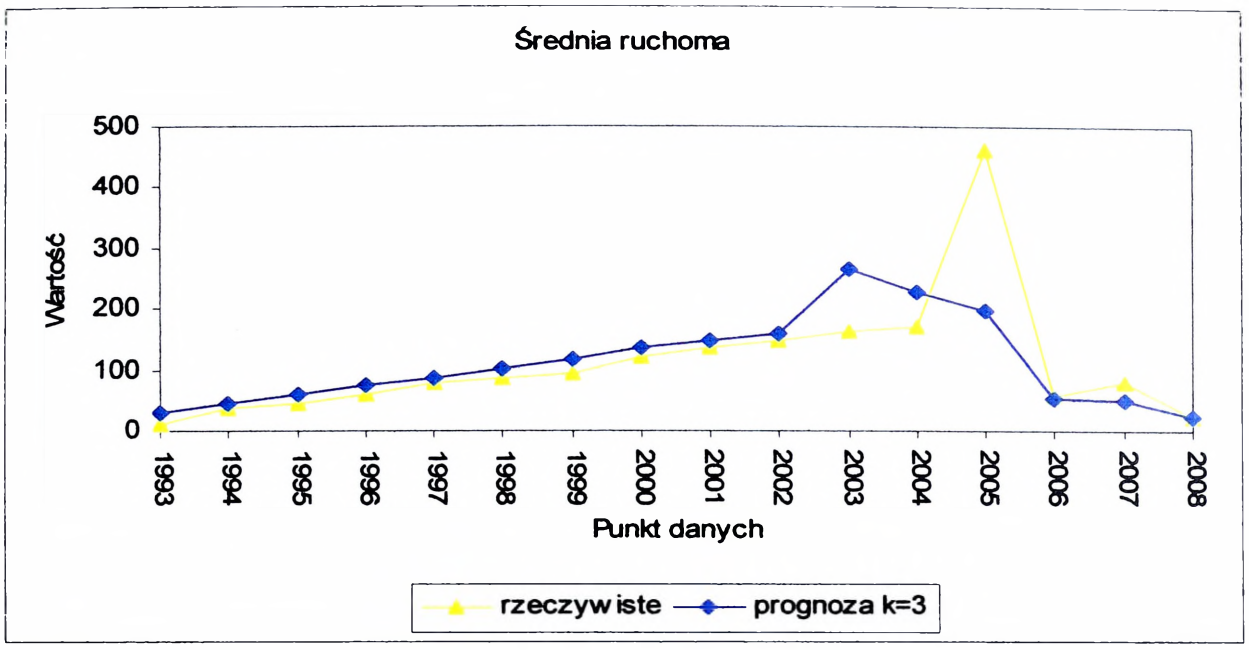
Analiza graficzna ujawnia trend liniowy dodatni do roku 2004, w którym nastąpił gwałtowny przyrost tego typu zagrożeń, od 2005 gwałtownie obniżyła się ilość zarejestrowanych zagrożeń, po czym w 2007 wzrósł niewiele, aby w 2008 ponownie się obniżyć.

Kolejność postępowania zachowano jak w predykcji z poprzednich przykładów, odwołując się kolejno do wyznaczenia prognoz przy wykorzystaniu metody średnich ruchomych i wygładzania wykładniczego. Dla stałej wygładzania k=2 (rysunek 3-16) prognoza wyniosła 24 przypadki dla roku 2009, pierwiastek średniego błędu kwadratowego =65,46, a względny błąd prognozy 1,3%.

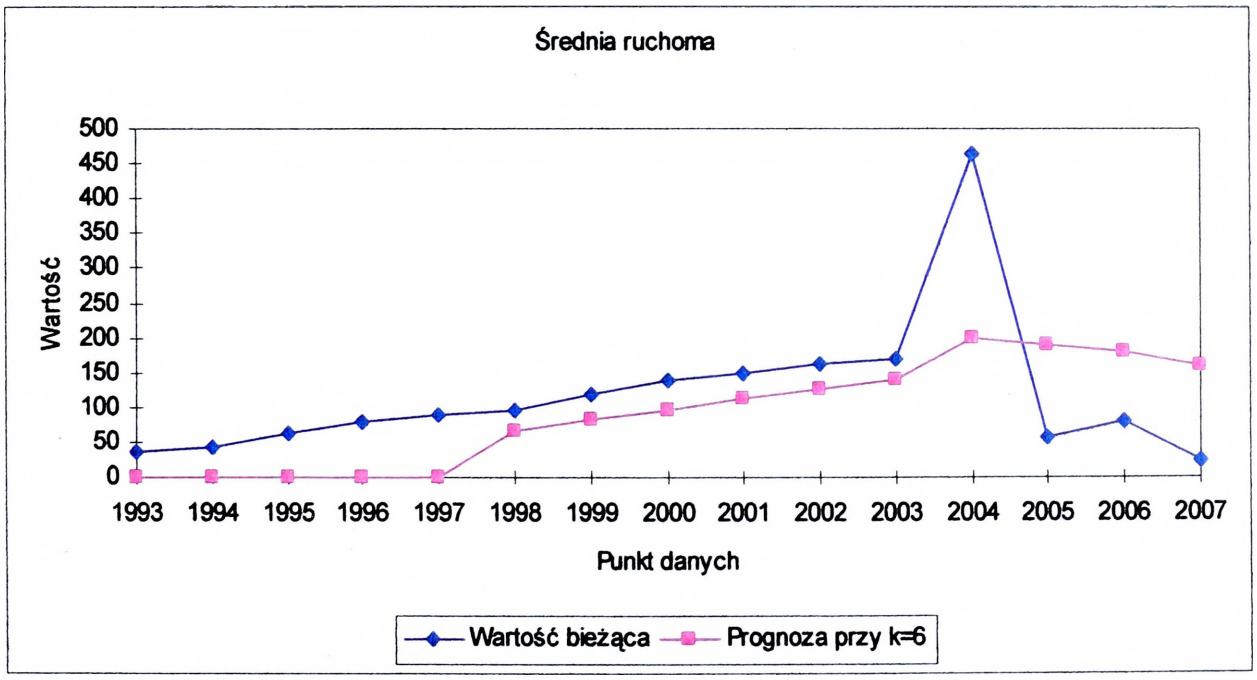


Rysunek 3-16. Wartość bieżąca i prognozowana dla zagrożenia „robak sieciowy", przy k=2
Źródło: opracowanie własne.

Przy zastosowaniu stałej wygładzania k=3, prognoza na 2009 wyniosła również 24 incydenty, pierwiastek średniego błędu kwadratowego równa się 173,4, a względny błąd prognozy wyniósł 7,24 (rysunek 3-17).



Rysunek 3-17. Wartość prognozy dla zagrożenia „robak sieciowy" przy k=3
Źródło: opracowanie własne.

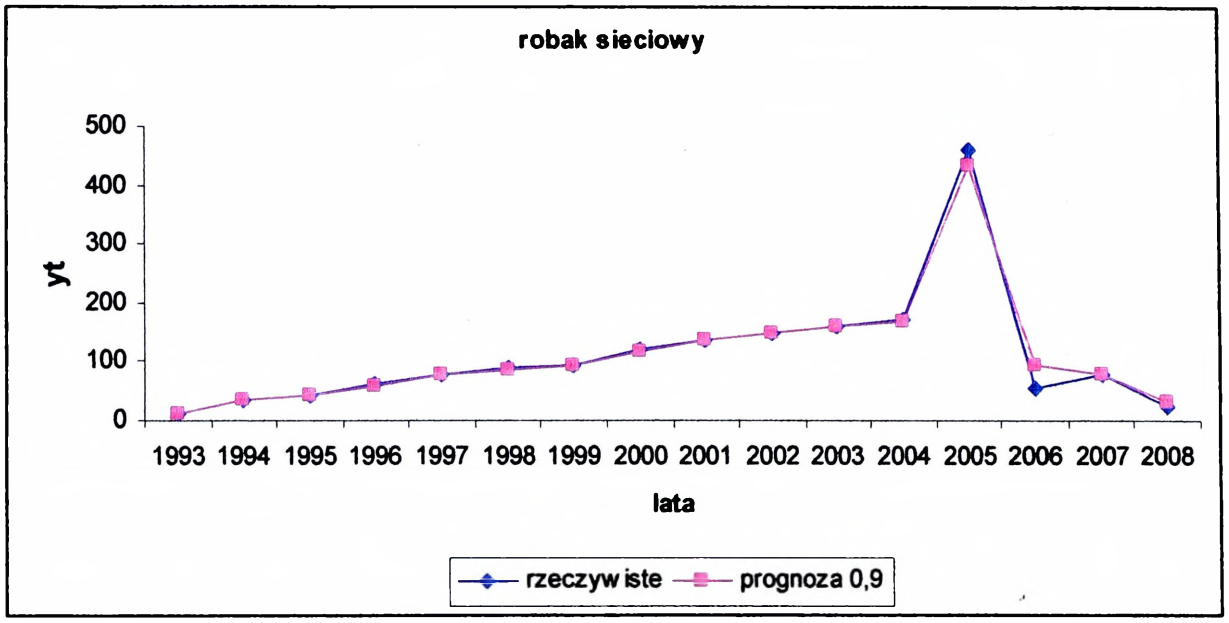


Rysunek 3-18. Wartość prognozy dla zagrożenia „robak sieciowy" przy k=6
Źródło: opracowanie własne.

Gdy stała wygładzania wzrasta do k=6 (rysunek 3-18) szereg jest bardziej regularny i wygładzony. Prognoza jest obarczona dużym błędem. Pierwiastek średniego błędu kwadratowego wynosi 144,5, a względny błąd prognozy wynosi 79,3%.

W modelu prostego wygładzania wykładniczego Brona, stałą wygładzania α wyznaczono doświadczalnie, wykonując symulacje z różnym poziomem stałej mieszczącej się

w granicach (0,1). Wykorzystano również narzędzie optymalizacji - dodatek Solver, minimalizując średni kwadratowy błąd w okresie kontrolnym predykcji (tabela 3-9).



Rysunek 3-19. Szereg prognozowany przy alfa=0,9 dla zagrożenia „robak sieciowy"
Źródło: opracowanie własne.

Przy α=0,9 otrzymujemy najlepiej dopasowany szereg teoretyczny, który jest jednocześnie prognozą (rysunek 3-19).

Tabela 3-9. Błędy dla okresu kontrolnego i dla prognoz wygasłych dla zagrożenia „robak sieciowy"

Błędy dla okresu kontrolnego „robak sieciowy"	
ME	7,006169
MPE	0,020289
MSE	173,4925
MAE	7,006169
MAPE	7,006169
Theil	0,002803

Błędy dla prognoz wygasłych „robak sieciowy"	
ME	0,135748
MPE	5,73504
MSE	146,91
MAE	5,73504
MAPE	112,4223
Theil	0,006461

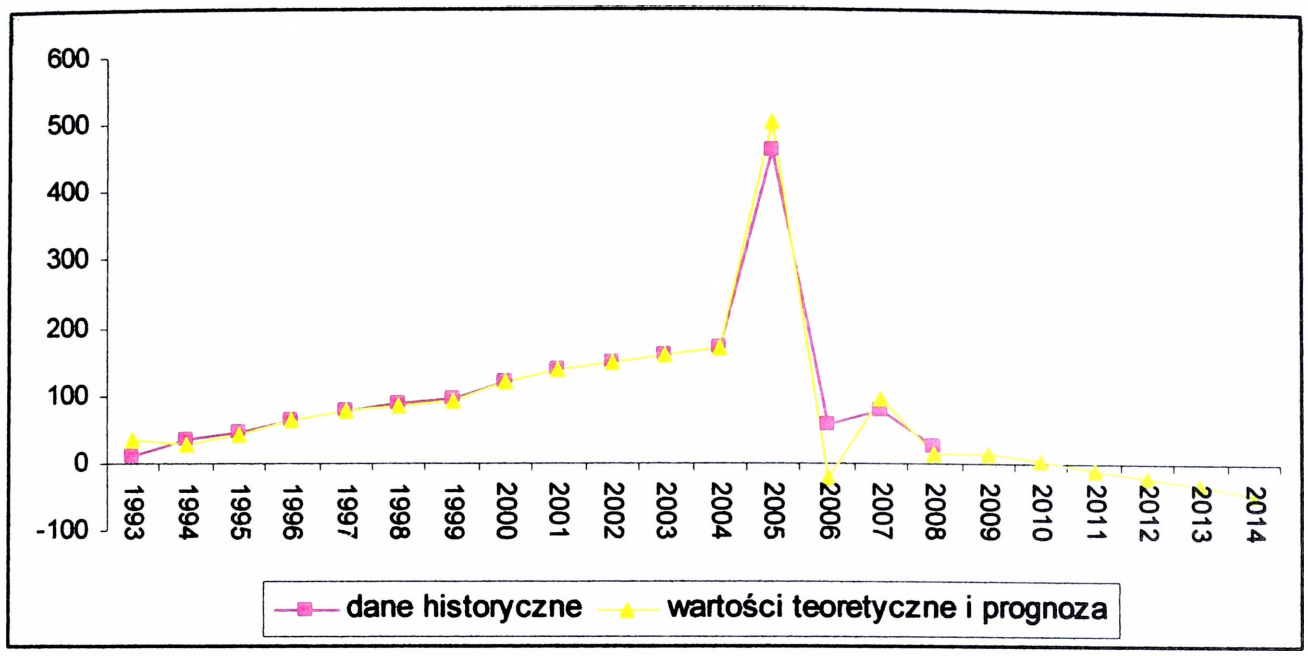
Źródło: opracowanie własne.

W prognozowaniu z zastosowaniem modelu Holta stałe wygładzania przyjęto na poziomie α=0,9 i β=0,15. Uzyskano prognozy w trendzie ujemnym (tabela 3-10 i rysunek 3-20).

Tabela 3-10. Wartości błędów dla okresu kontrolnego dla zagrożenia „robak sieciowy" przy α=0,9 i β=0,15 (Holt)

ME	-7,7436
MPE	-0,01431
MSE	347,2877
MAE	8,912451
MAPE	24,08365
Theil	0,00561

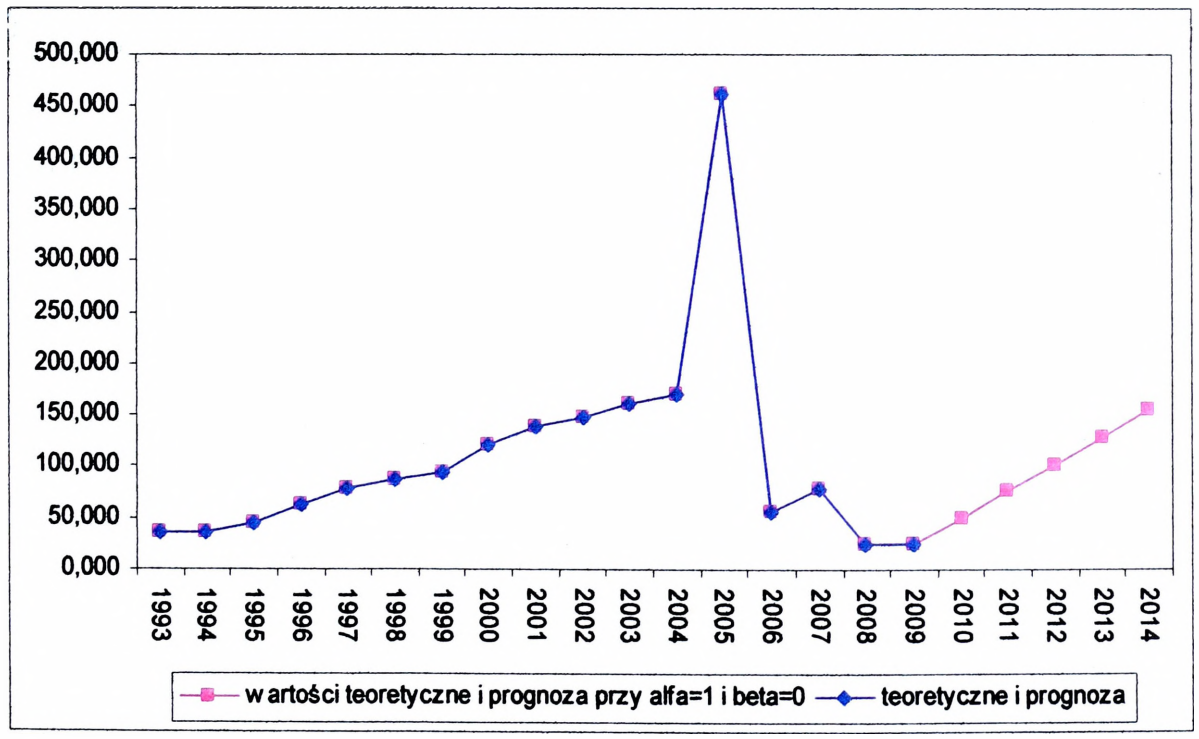
Błędy wygładzania są różnokierunkowe.



Rysunek 3-20. Wartości historyczne, teoretyczne i prognoza dla zagrożenia „robak sieciowy"
Źródło: opracowanie własne.

Pierwiastek średniego błędu kwadratowego prognoz wygasłych wyniósł 23,25. Względny błąd prognozy na 2009 rok, która wyniosła 13,424 równa się 1,7%.

Minimalizacja średniego błędu kwadratowego spowodowała, że alfa przyjęło wartość 1, beta natomiast zero, MSE wyniosło 42,05, otrzymane prognozy są w wyraźnym trendzie wzrostowym (rysunek 3-21).



Rysunek 3-21. Prognozy „robaka sieciowego" przy alfa=1 i beta=0
Źródło: opracowanie własne.

Tabela 3-11. Porównanie metod prognozowania dla „robaka sieciowego"

ZAREJESTROWANE WIELKOŚCI SPAMU	PROGNOZA	MSE	WZGLĘDNY BŁĄD PROGNOZY[162]:
Model średniej ruchomej			
K=2	24	4285,6	1,3
K=3	24	30234,9	72,4
K=6	158,3	200011,5	89
Model Browna α=0,9	29,55	146,9	41
Metoda Holta α=0,9 β=0,15	13,424	540,3	173
α=0,89993 β=0	24	42,05	27,2

Źródło: opracowanie własne.

Prognozy wykonano również dla danych pozyskanych z systemu ARAKIS.[163] Dane obrazują ilość prób ataków w ciągu doby (tabela 3-12).[164]

Stałe wyznaczono za pomocą Solvera minimalizując średni błąd kwadratowy, dla okresu kontrolnego predykcji przyjęły wartości: α=0,608 i β=0,664

Prognozy dla kolejnych czterech godzin zawiera tabela 3-13.

Ten model danych najlepiej opisuje równanie trendu potęgowego. Na wykresie umieszczono wyliczone równanie z wyznaczonym R-kwadrat dopasowania wynoszącym 0,9703 (rysunek 3-22).

Pierwiastek średniego błędu kwadratowego, błędu ex post prognoz wygasłych wyniósł: 1,08.

---

[162] Pierwiastek średniego błędu kwadratowego błędu ex post prognoz wygasłych / wartość prognozy w %.

[163] Agregacja, Analiza i Klasyfikacja Incydentów Sieciowych systemem wczesnego ostrzegania o zagrożeniach w sieci. Jego głównym zadaniem jest wykrywanie i opisywanie zautomatyzowanych zagrożeń występujących w sieci na podstawie agregacji i korelacji danych z różnych źródeł, w tym rozproszonej sieci honeypotów, sieci darknet, firewalli oraz systemów antywirusowych.

[164] Statystyki związane z alarmami snortowymi wytwarzanymi na bazie przepływów do sieci honeypotowych w ciągu ostatnich 24 godzin. W tabeli przedstawiane są znane ataki, nowości są uzupełniane w miarę aktualizacji reguł snort. Statystyki te można traktować jako uzupełnienie innych danych przedstawianych w systemie mających na celu wykrycie nowych ataków.

Tabela 3-12. Zestawiane danych, stałych wygładzania, prognoz i ich błędów dla zagrożenia „zarejestrowane ataki dobowe"

DANE PRÓB ATAKÓW DOBOWYCH

t	próby ataków w ciągu 24 h
1	5150
2	5148
3	2128
4	2128
5	1240
6	1239
7	952
8	893
9	873
10	767
11	687
12	648
13	559
14	535
15	516
16	463
17	447
18	445
19	364
20	312

BŁĘDY DOPASOWANIA MODELU DLA OKRESU KONTROLNEGO

Dla okresu kontrolnego	
ME	0,0290148
MPE	260,7138944
MSE	0,0036705
MAE	0,0553979
MAPE	0,0000000
Theil	0,0000000

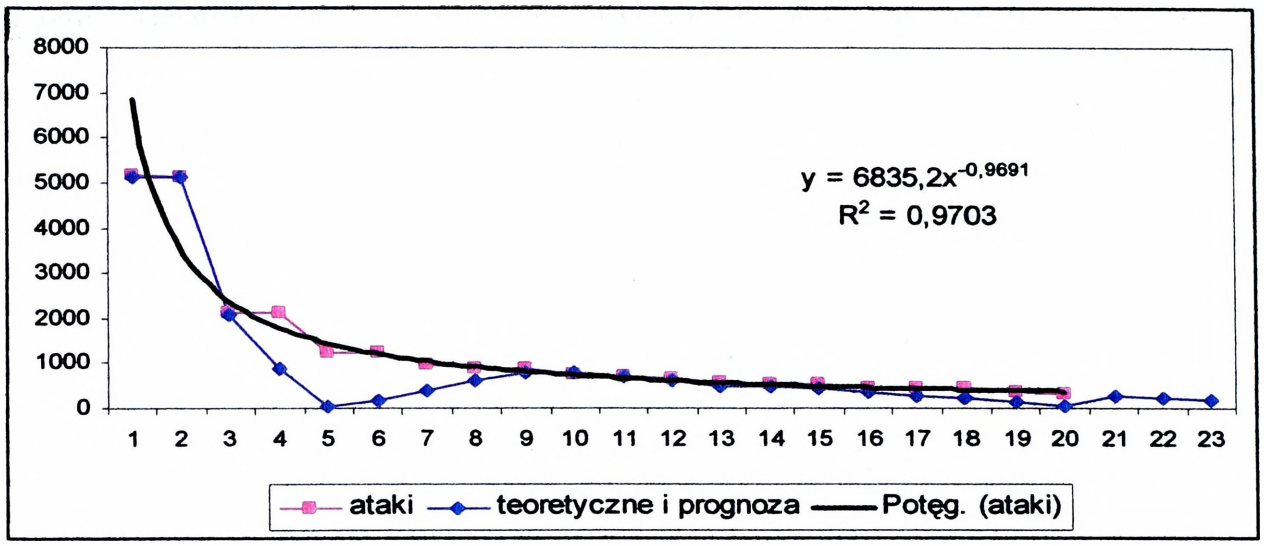
WYZNACZONE STAŁE WYGŁADZANIA

α	β
0,6089159	0,66454

PROGNOZY PRÓB ATAKÓW

21	276,517
22	226,042
23	175,568
24	125,093

Źródło: opracowanie własne.



Rysunek 3-22. Wartości teoretyczne oraz prognozy dla zagrożenia „zarejestrowane ataki dobowe"
Źródło: opracowanie własne

Kolejnym badaniem było sprawdzenie modelu na danych dobowych dotyczących unikalnych ataków. Wartości stałych wygładzania wyznaczono za pomocą Solvera, minimalizując średni błąd kwadratowy dla okresu kontrolnego predykacji i uzyskano dla α=0,9 i β=0,1 (tabela 3-13 i rysunek 3-23).

Tabela 3-13. Zestawienie danych dla zagrożenia „unikalne skanowania", analiz oraz prognoz

DANE „UNIKALNE SKANOWANIA

Godziny	Unikalne skanowanie
1	205
2	205
3	106
4	106
5	516
6	293
7	76
8	81
9	74
10	12
11	488
12	465
13	312
14	65
15	294

BŁĘDY DLA OKRESU KONTROLNEGO

ME	-7,6057
MPE	0,058953
MSE	525,6558
MAE	13,8812
MAPE	17,18442
Theil	0,004716

WYZNACZONE STAŁE WYGŁADZANIA

α	β
0,9	0,1

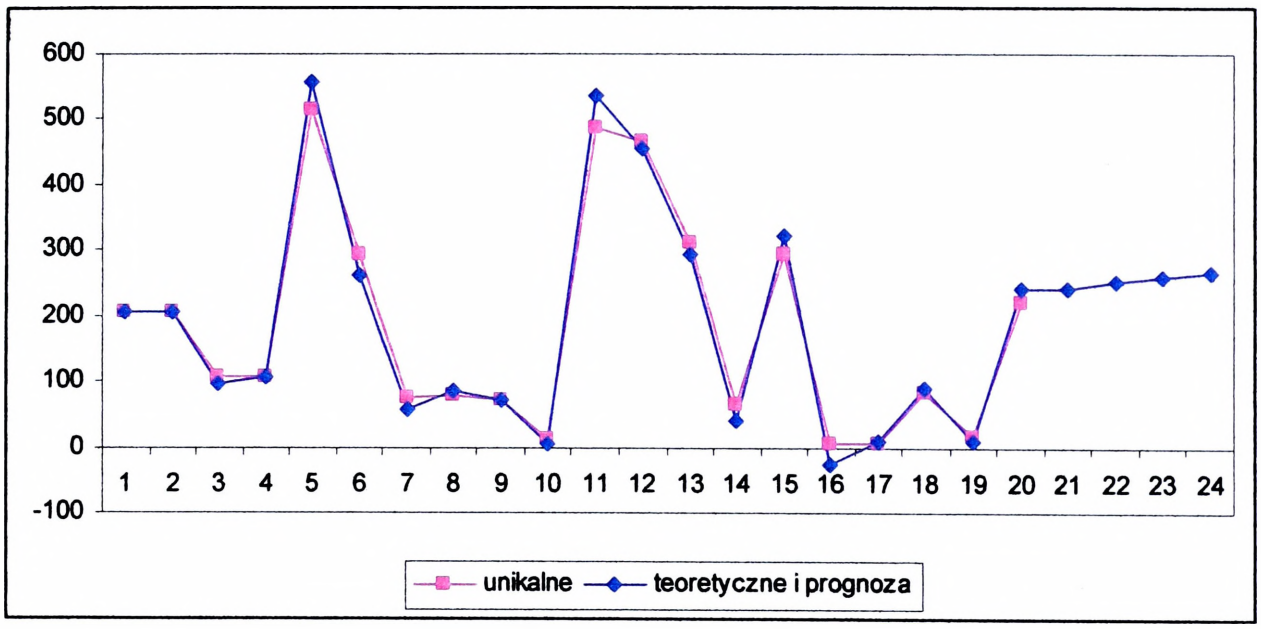
wyznaczone prognozy

21	242,7015
22	250,1251
23	257,5486
24	264,9721

Źródło: opracowanie własne.

Do oceny dopuszczalności prognozy, podobnie jak w poprzedniej analizie, posłużono się błędami prognoz wygasłych. Obliczono pierwiastek średniego błędu kwadratowego, błędu ex post prognoz wygasłych. Wartości względną błędu otrzymano przez porównanie otrzyma-

nego błędu z wartością prognozy. Ze względu na przyjęte założenie, że prognozę przyjmujemy za dopuszczalną, jeżeli będzie obarczona błędem nie większym niż 5% - prognoza jest prognozą niedopuszczalną. Błąd względny wyniósł: 8-9%

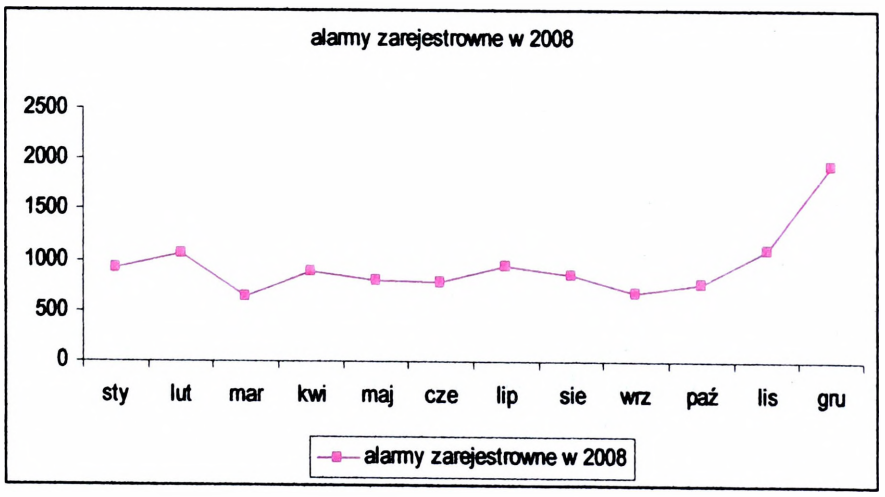


Rysunek 3-23. Wartości rzeczywiste, teoretyczne oraz prognoza dla zagrożenia „unikalne skanowania"
Źródło: opracowanie własne.

Wybranymi modelami formalnymi posłużono się również w prognozowaniu dla danych miesięcznych (tabela 3-14).

Tabela 3-14. Szereg czasowy zagrożenia „zarejestrowane alarmy w 2008 roku"

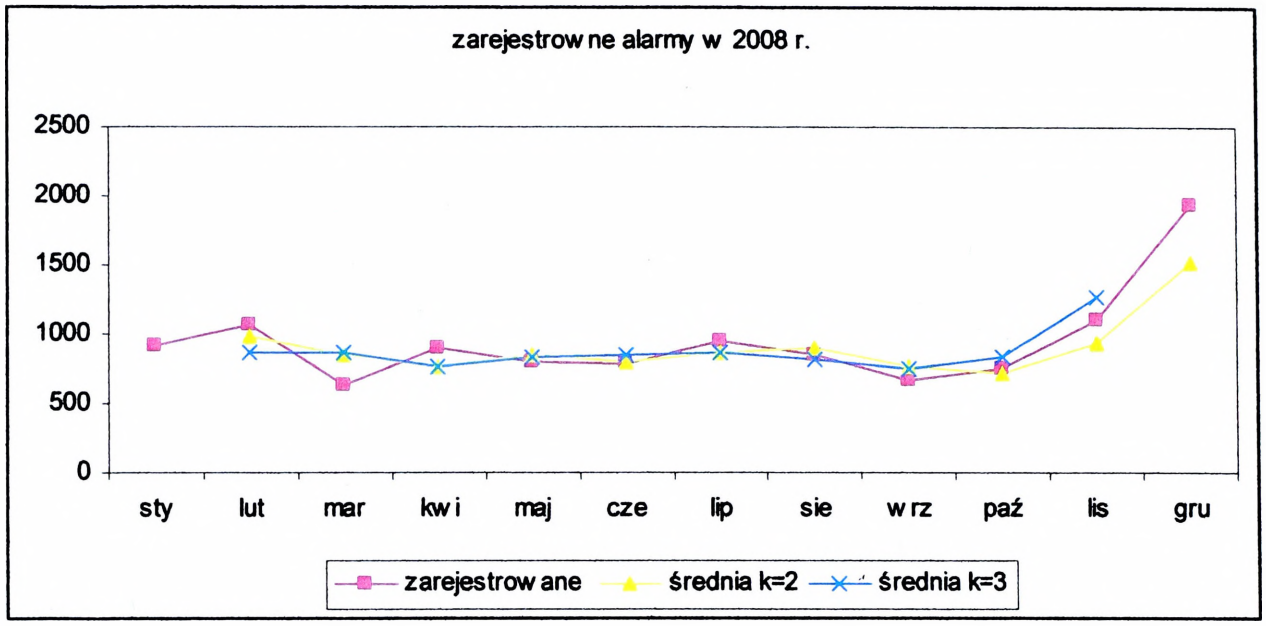
lp	Czas	yt
1	styczeń	916
2	luty	1061
3	Marzec	633
4	Kwiecień	893
5	Maj	798
6	czerwiec	786
7	Lipiec	947
8	Sierpień	846
9	Wrzesień	671
10	Październik	755
11	Listopad	1098
12	grudzień	1931



Rysunek 3-24. Wykres zagrożenia „zarejestrowane alarmy w 2008 roku"
Źródło: opracowanie własne.

Prognozy wykonano stosując średnie ruchome wygładzania dla k=2, k=3. Prognozą są wartości wygładzonego szeregu czasowego ekstrapolowane na miesiące roku następnego.

Wygładzony szereg o małej stałej podąża za szeregiem empirycznym, zwiększając stałą wygładzania staje się bardziej regularny, ale zwiększają się również błędy prognozowanych wielkości (rysunek 3-25).



Rysunek 3-25. Zarejestrowane dane z 2008 roku oraz wygładzone stałą wygładzania k=2 i k=3
Źródło: opracowanie własne.

W tabeli 3-15 zaprezentowano prognozy oraz błędy liczone dla różnych k.

Tabela 3-15. Prognozy oraz błędy wyznaczone z wykorzystaniem modeli średniej ruchomej

STAŁA WYGŁADZANIA	PROGNOZA	MSE	WZGLĘDNY BŁĄD PROGNOZY %
K=2	1514,5	24298,31	10,2
K=3	1261,3	323812,5	45

Źródło: opracowanie własne.

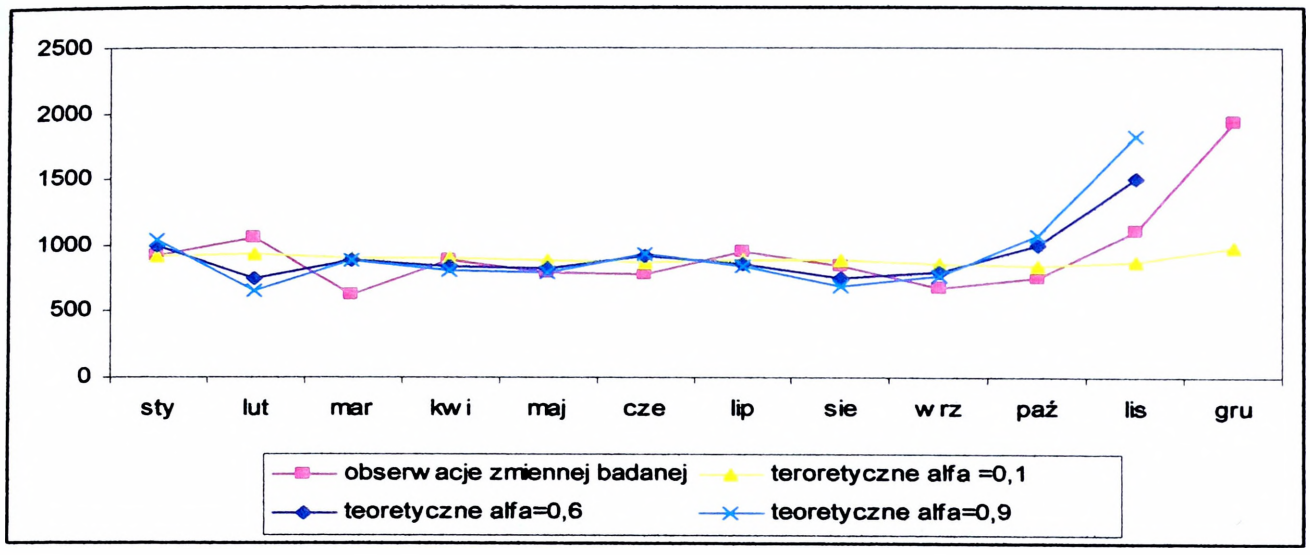
Stosując model Browna otrzymano prognozy oraz średnie błędy kwadratowe i średni bląd prognozy (tabela 3-16).

Tabela 3-16. Wyznaczone prognozy według modelu Browna przy różnych stałych wygładzania dla zagrożenia „zarejestrowane alarmy w 2008 roku"

PROGNOZA	MSE PROGNOZ WYGASŁYCH			ŚREDNI BŁĄD PROGNOZY %
980,77	α= 0,1	100793,96	317,4806	32,37
1508,67	α= 0,6	18315,86	135,3361	8,97
1825,41	α=0,9	1244,37	35,27563	68,17

Źródło: opracowanie własne.

Prognozą są wartości teoretyczne wygładzonego szeregu dla poszczególnych miesięcy, w tabeli zestawiono wielkości prognoz oraz błędy dla grudnia 2009 (rysunek 3-26).



Rysunek 3-26. Prognozowanie z wykorzystaniem modelu Browna przy różnych wielkościach alfa dla zagrożenia dla zagrożenia „zarejestrowane alarmy w 2008 roku"
Źródło: opracowanie własne.

Badając możliwość wykorzystania w prognozowaniu zagrożeń, odwołano się do modelu Wintersa. W modelu zastosowano symulowane dane. Oznaczono je jako dane miesięczne, uzyskując na przestrzeni kilku lat szereg 300 wyrazowy.

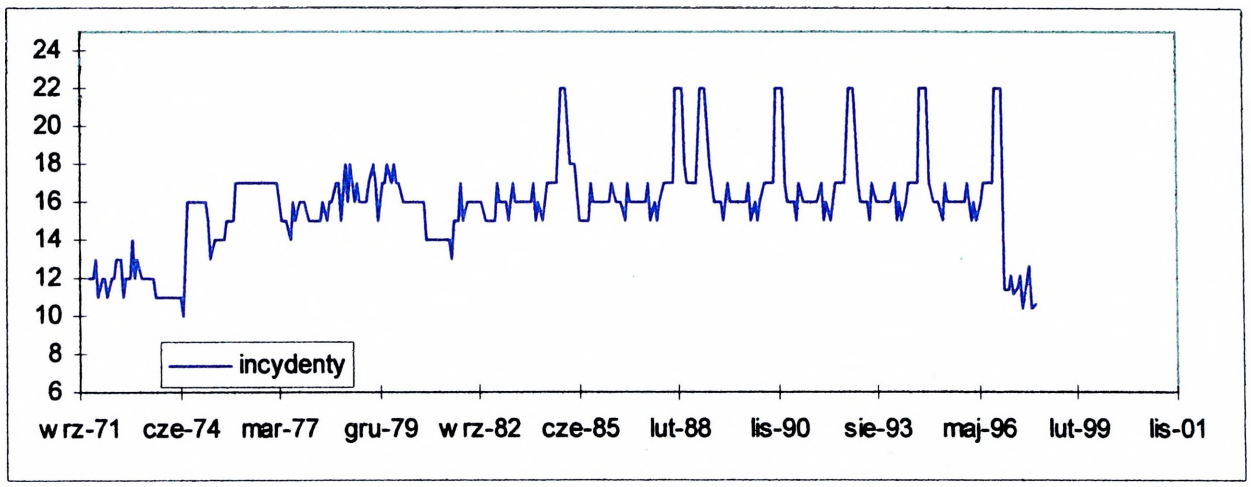
Postać multiplikatywna

Wielkości stałych wygładzania dobrano za pomocą dodatku Solver arkusza kalkulacyjnego, minimalizując średni błąd kwadratowy dla okresu kontrolnego (tabela 3-17 i rysunek 3-27).

Tabela 3-17. Zestawienie dla zagrożenia „symulowane dane"

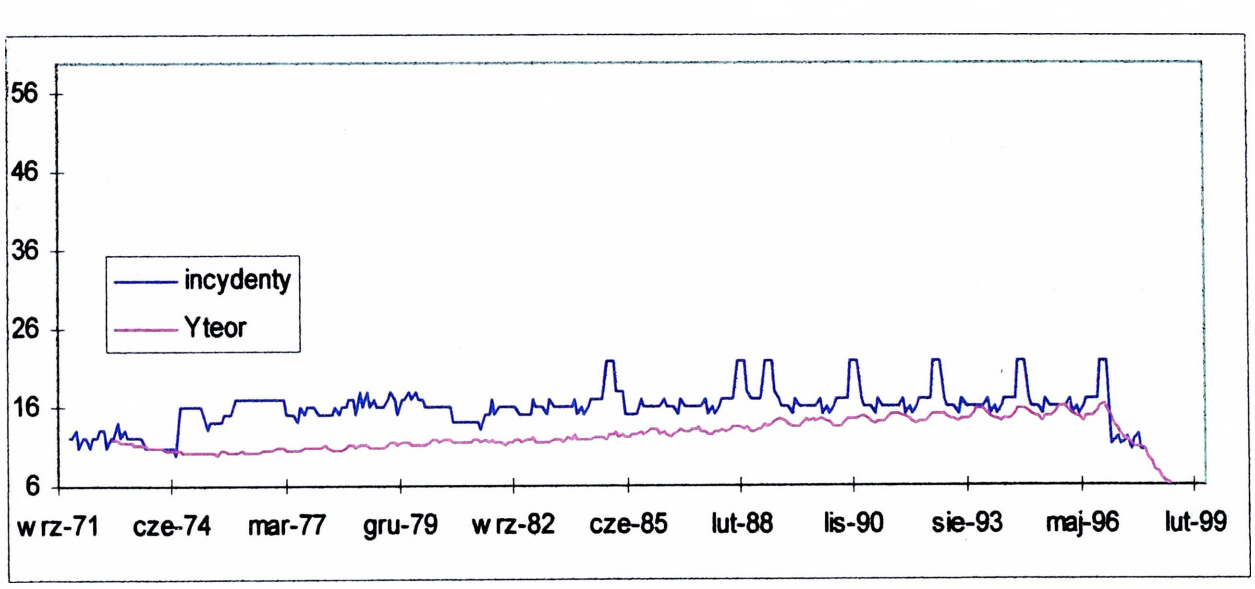
WIELKOŚCI STAŁYCH WYGŁADZANIA			BŁĘDY DLA OKRESU KONTROLNEGO		WYZNACZONE PROGNOZY	
α	β	γ	Dla okresu kontrolnego		I kw roku X	1,780
0,010775	0,008607	0,076067	ME	-0,009	II kw	1,722
			MPE	-0,026	III kw	1,653
			MSE	5,423	IV kw	1,647
			MAE	1,611		
			MAPE	0,119		
			Theil	0,034		

Źródło: opracowanie własne.



Rysunek 3-27. Zagrożenia „symulowane dane" jako rzeczywiste dane o występowaniu incydentów
Źródło: opracowanie własne.

Prognozy wyznaczono na pierwsze miesiące pierwszego kwartału następnego roku. Dla okresu kontrolnego średni błąd prognozy wyniósł 5,4. Pierwiastek średniego błędu kwadratowego *ex post* prognoz wygasłych wyniósł 2,3 incydentów na miesiąc. Również błąd liczony dla wyznaczonych prognoz, odnoszony do wartości wyznaczonych prognoz stanowi około 13%, co w świetle założeń o dopuszczalności prognozy przy progu błędu 5% sprawia, że prognozy mogą być uznane za niedopuszczalne (rysunek 3-28).



Rysunek 3-28. Wyznaczone wartości teoretyczne i prognoza dla zagrożenia „symulowane dane"
Źródło: opracowanie własne.

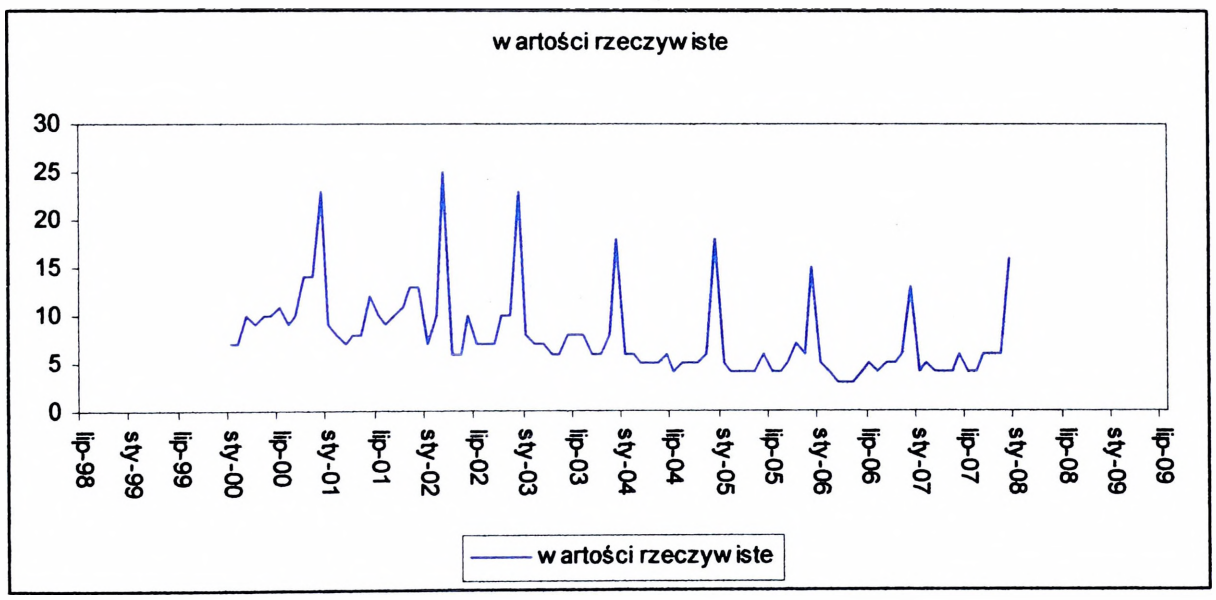
Postać addytywna

Wielkości stałych wyznaczono przy pomocy Solvera, według reguły minimalizacji średniego błędu kwadratowego dla okresu kontrolnego (tabela 3-18 i rysunek 3-29).

Tabela 3-18. Zbiorcze zestawienie wyników analiz dla zagrożenia „symulowane dane"

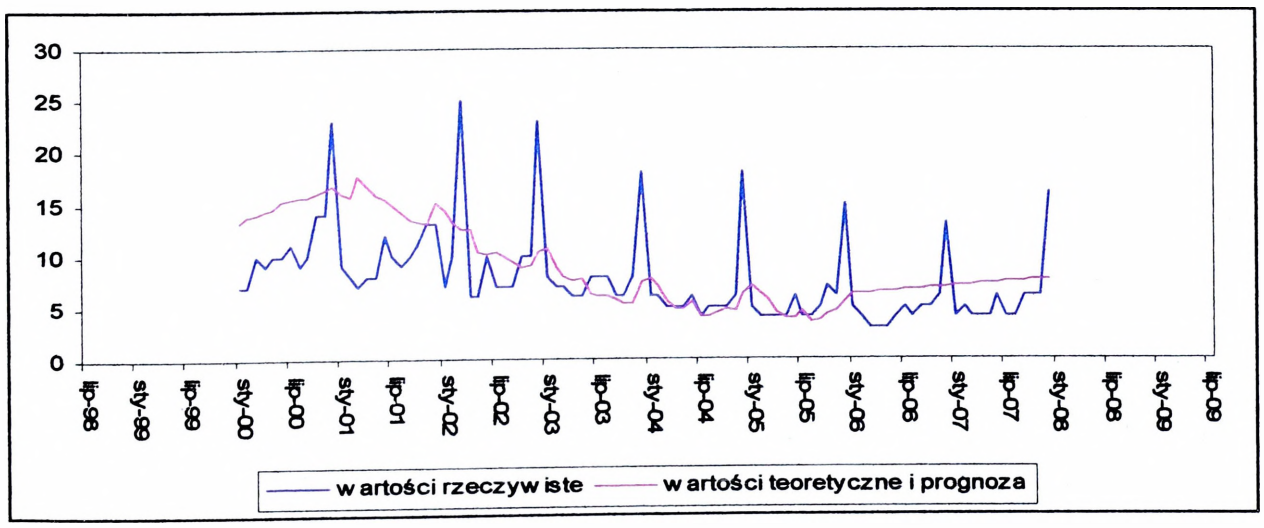
WIELKOŚCI STAŁYCH WYGŁADZANIA DLA POSTACI ADDYTYWNEJ MODELU WINTERSA			WARTOŚCI BŁĘDÓW DLA OKRESU KONTROLNEGO	
α	β	γ	Dla okresu kontrolnego	
0,14284	0,058761	0,0811	ME	0,000
			MPE	-0,086
			MSE	6,467
			MAE	1,848
			MAPE	0,303
			Theil	0,149

Źródło: opracowanie własne.



Rysunek 3-29. Wartości szeregu czasowego zagrożenia „symulowane dane 2"

Źródło: opracowanie własne.



Rysunek 3-30. Wartości rzeczywiste jako zarejestrowane dla zagrożenia „symulowane dane 2" i teoretyczne oraz prognoza

Źródło: opracowanie własne.

Prognozowanie zagrożeń nastręcza wielu trudności. Pierwszym ograniczeniem jest dostępność danych do prowadzania tego typu badań. Przeprowadzone badania pozwalają na wysunięcie następujących wniosków:

- prognozowanie powinno być prowadzone dla krótkiego horyzontu czasowego;
- modele średniej ruchomej wskazują tendencję rozwojową analizowanej zmiennej;
- dokładniejsze wyniki prognoz otrzymujemy prognozując szeregi zawierające więcej danych.

Modele Wintersa (addytywny jak i multiplikatywny) mogą być stosowane do szeregów, w których występuje sezonowość i posiadamy, co najmniej 5 danych na sezon. Zestawienie analiz dla zagrożenia „symulowane dane 2" zawarto w tabeli 3-19

Tabela 3-19. Zestawienie analiz dla zagrożenia „symulowane dane 2"

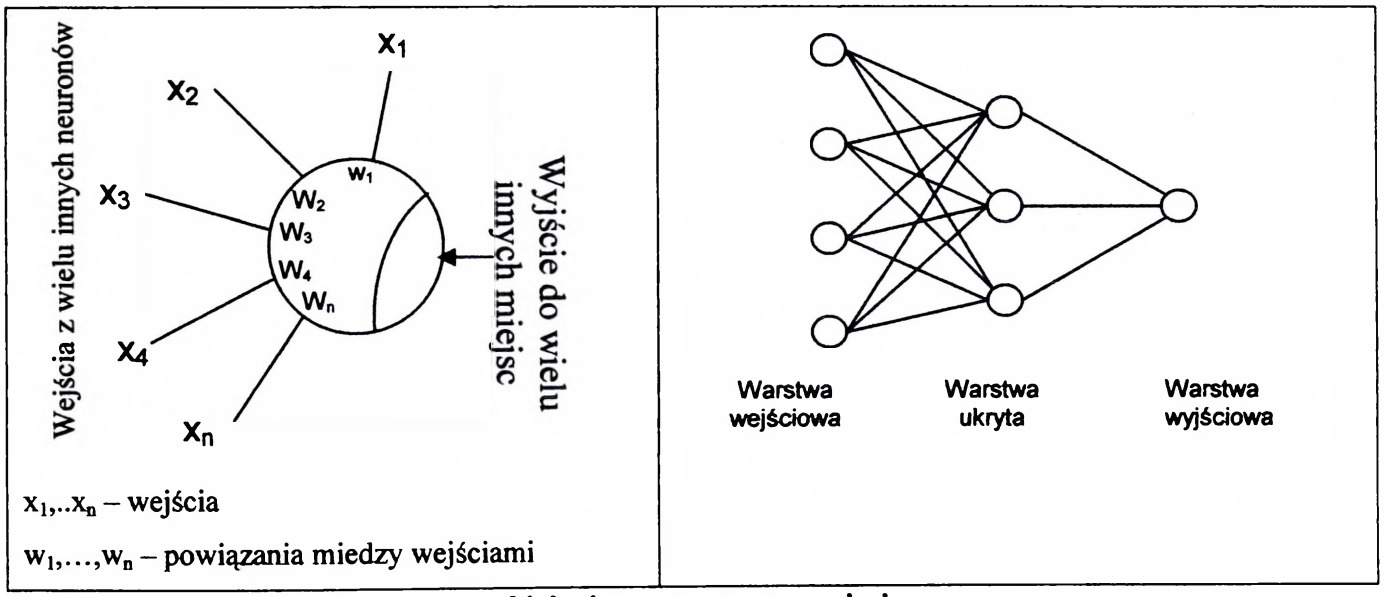
MODEL		PROGNOZA	MSE	BŁĄD PROGNOZY W %
Brown	α= 0,1 α=0,6 α=0,9	980,77 1508,67 1825,41	100793,96 18315,86 1244,37	33 9,0 68,2
Holt				
Winters miltplikatywny		15,680	5,423	34,0
Addytywny 0,052624 0,111462 8,64E-10		2,623	6,467	29,0

Źródło: opracowanie własne.

3.3. Sztuczne sieci neuronowe

Zdolność przyswajania wiedzy na podstawie zgromadzonych danych, jest unikatową cechą sztucznych sieci neuronowych, wykorzystywaną między innymi w rozwiązywaniu różnorodnych problemów ekonomicznych, naukowych i przemysłowych. W praktyce sieci neuronowe znajdują zastosowanie w diagnostyce lekarskiej, kontroli lotów, rozpoznawania terenu, prognozowaniu stanów alarmowych na rzekach, a w szczególności w prognozowaniu finansowym i szacowaniu ryzyka papierów wartościowych, a także np. w prognozowaniu obciążenia obrabiarek.

Najprostsze określenie istoty sztucznych sieci neuronowych odnosi się do uproszczonego modelu ludzkiego mózgu, w którym podstawowym elementem przetwarzającym informacje jest neuron powiązany za pomocą połączeń synaptycznych. W sieciach neuronowych odpowiednikiem szczeliny synaptycznej jest waga (miara znaczenia) powiązań pomiędzy sztucznymi neuronami (rysunek 3-31).[165]



Rysunek 3-31. Porównanie schematu biologicznego neuronu z siecią neuronową

Źródło: na podstawie: E.Gately, *Sieci neuronowe. Prognozowanie finansowe i projektowanie systemów transakcyjnych*. Wig Press, Warszawa 1999, s. 6-7.

---

[165] Każdy z neuronów przetwarza skończoną liczbę sygnałów wejściowych x_i, i=1,...n, na jedno wejście y. Na podstawie danych, wprowadzonych na wejście sieci, obliczane jest całkowite pobudzenie neuronu e, najczęściej w postaci kombinacji liniowej wejść: $e = w_0 + \sum_{i-1}^{n} w_i x_i = w_0 + w_x^T$, gdzie x=[x1,x2,...xn]T –wektor sygnałów wejściowych, w_0 – wyraz wolny, $w=[w_1,w_2,...,w_n]^T$ – wektor wag. Wagi wyrażają stopień ważności informacji przekazywanej i-tym wejściem, jednocześnie stanowią pamięć neuronu, czyli zapamiętane relacje zachodzące miedzy sygnałami wejściowym i wyjściowym.

Nazwą „sztuczna sieć neuronowa" określa się model symulacyjny w postaci programów komputerowych lub sprzętowych, które naśladują zdolność przetwarzania informacji w sposób podobny do funkcjonowania ludzkiego mózgu. Podstawą są modele matematyczne realizujące pseudo-równoległe przetwarzanie informacji, korzystając z wielu wzajemnie połączonych neuronów, wzorujących się na neuronie biologicznym.

Najważniejszą cechą sieci neuronowych jest zdolność generalizacji, czyli uogólniania wiedzy dla nowych danych wcześniej nieznanych. Osiąga się to w procesie uczenia sieci. Sieć uczy się prawidłowo działać na podstawie prezentowanych jej przykładów. Bazując na przedstawionych rzeczywistych przypadkach, sieć stara się odkryć i zapamiętać ogólne prawidłowości charakteryzujące te obiekty. Rozpoznane reguły sztuczna sieć neuronowa przechowuje w postaci rozproszonej, w wartościach współczynników wagowych neuronów. Proces uczenia polega na prawidłowym określeniu wartości współczynników wagowych neuronów na podstawie informacji wydobytych w trakcie procesu uczenia ze zbioru uczącego.[166] Uczenie sieci rozpoczyna się od nadania wagom neuronów wartości losowych. W każdym kroku iterakcyjnego procesu uczenia, wartości wag jednego lub kilku neuronów ulegają zmianie, przy czym reguły tych zmian są tak pomyślane, by każdy neuron sam potrafił określić, które ze swoich wag ma zmienić, w którą stronę, a także o ile. Możliwe są dwa warianty procesu uczenia: z nauczycielem[167], bez nauczyciela[168]. Od stopnia nauczenia się sieci w dużej mierze zależy jakość prognoz. Możliwe jest również stworzenie sieci wykorzystującej jej zdolności adaptacyjne. Wtedy stworzona sieć neuronowa, będzie nie tylko uwzględniała wiedzę o prognozowanym zjawisku, nabytą w trakcie treningu, ale także pozytywne lub negatywne doświadczenia zdobywane podczas realnego prognozowania. W takim wypadku mamy do czynienia z douczaniem sieci. Uczenie i stosowanie sztucznych sieci neuronowych wymaga postępowa-

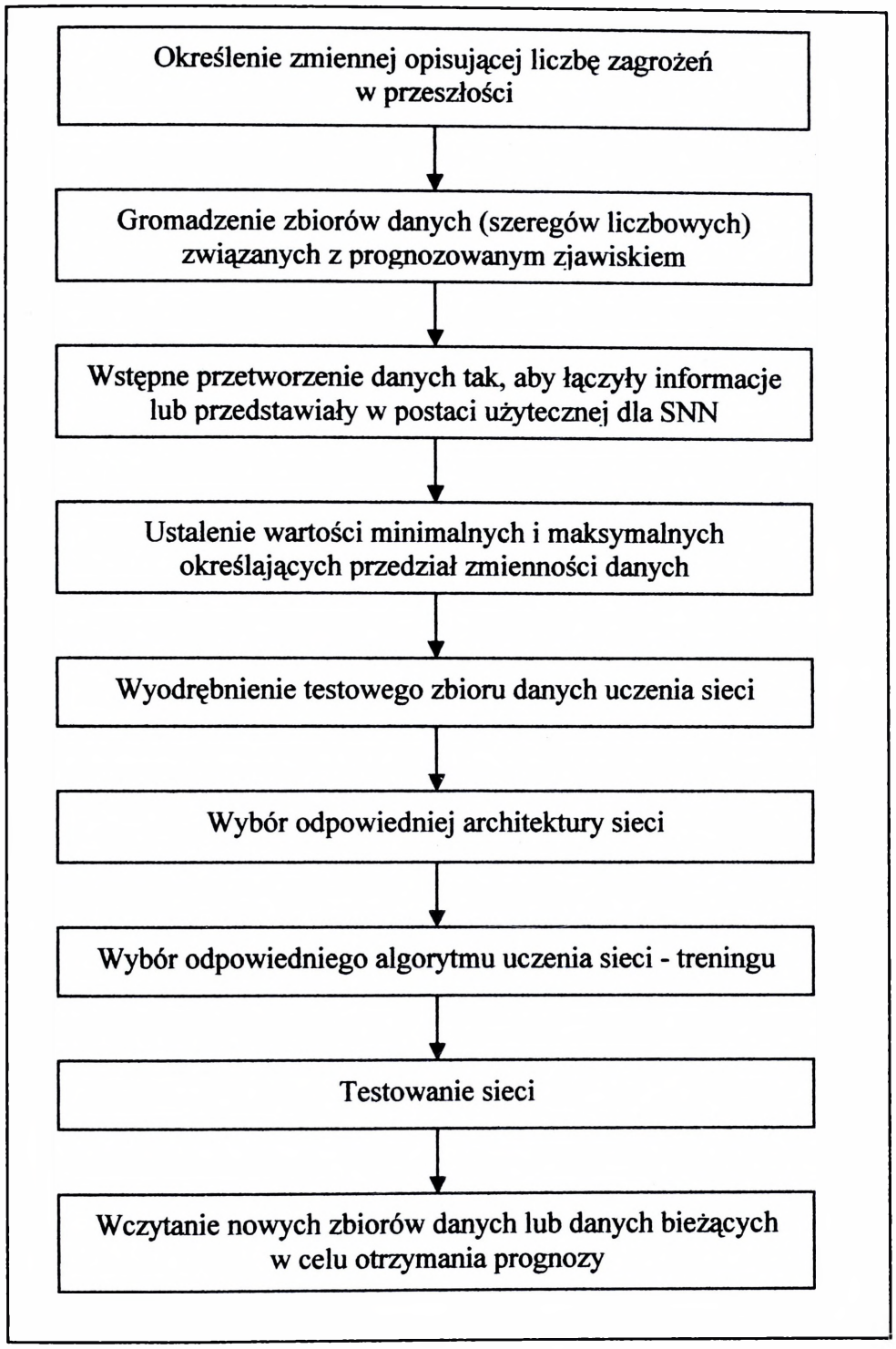
---

[166] Kluczowym elementem w procesie uczenia są wagi wejść poszczególnych neuronów. Jeśli zmienią się wartości wag – neuron zacznie pełnić innego rodzaju funkcję w sieci, a co za tym idzie cała sieć zacznie inaczej działać. Uczenie sieci polega więc na tym, by dobrać wagi, aby wszystkie neurony wykonywały dokładnie takie czynności, jakich się od nich wymaga.

[167] U podstaw większości algorytmów uczenia z nauczycielem leży reguła Delta wprowadzona przez Widrowa i Hoffa. Polega ona na tym, że każdy neuron po otrzymaniu na swoich wejściach określonych sygnałów wyznacza swój sygnał wyjściowy, wykorzystując posiadaną wiedzę w postaci wcześniej ustalonych wartości współczynników wagowych wszystkich wejść oraz progu. Wartość sygnału wyjściowego, wyznaczonego przez neuron na danym kroku procesu uczenia porównywana jest z odpowiedzią wzorcową podaną przez nauczyciela w ciągu uczącym. Jeśli występuje rozbieżność – neuron wyznacza różnicę pomiędzy swoim sygnałem wyjściowym a tą wartością sygnału, która byłaby – według nauczyciela prawidłowa. Ta różnica oznaczana jest zwykle symbolem greckiej litery Δ i stąd nazwa opisywanej metody.

[168] Uczenie bez nauczyciela polega na tym, że sieci pokazuje się kolejne przykłady sygnałów wejściowych, nie udostępniając żadnych informacji o tym, co z tymi sygnałami powinno się zrobić. Sieć obserwuje otoczenie i przyjmuje różne sygnały. Na podstawie obserwacji występujących sygnałów, sieć etapami sama odkrywa, jakie jest ich znaczenie i jednocześnie sama ustala zachodzące między sygnałami zależności.

nia według specjalnego schematu działania złożonego z wielu etapów (rysunek 3-32). Realizacja każdego z nich wpływa na powodzenie całości.



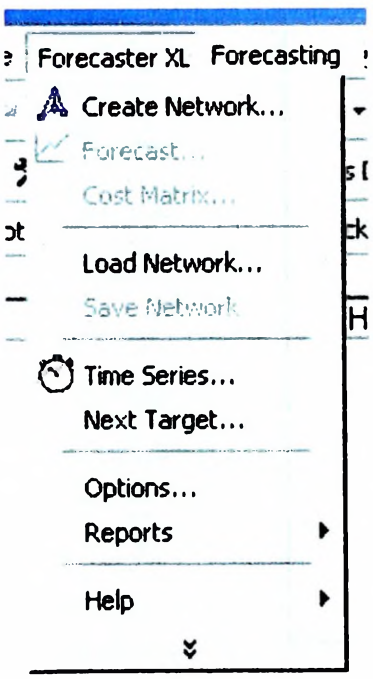
Rysunek 3-32. Schemat procesu prognozowania za pomocą sztucznej sieci neuronowej
Źródło: opracowanie własne na podstawie: E.Gatley, *Sieci neutronowe*. Op.cit.

Wybór zmiennej prognozowanej zależy od horyzontu czasowego prognozy i jakości danych. Za zmienną przyjęto liczbę prognozowanych ataków na bezpieczeństwo w sieci teleinformatycznej: robak sieciowy, trojan, spam.[169] Dane, reprezentowały (w każdym z przypad-

[169] Przygotowano dane, na podstawie raportów i statystyk sporządzonych przez CERT (*Computer Emergency Response Team*) dotyczące przypadków naruszenia bezpieczeństwa teleinformatycznego w polskich sieciach. Ze względu na zbyt duże błędy prognozy, horyzont czasowy prognozy ograniczono do roku 2009.

ków) ciąg zaobserwowanych stanów zmiennej Y (reprezentującą poszczególne zagrożenia) uporządkowanych według wartości zmiennej czasowej t, zachowując postać jednowymiarowego szeregu czasowego.

Badanie prowadzono w kilku etapach podzielonych na sesje, podczas których sprawdzano zachowanie się sieci w zależności od zastosowanego modelu dla określonych danych. W dwóch sesjach zastosowano sieć wielomianową, w sześciu sesjach posłużono się modelem sieci *time series* (serie czasowe). Kolejne trzy sesje służyły wykonaniu prognoz. Zastosowano program Generated by Alyuda Forecaster XL[170], który jest w istocie automatyczną siecią neuronową. Stosowany jest w tym programie wybór architektury sieci i parametrów (rysunek 3-33). W sytuacji brakujących lub niekompletnych czy nieprawidłowych danych można posłużyć się automatyczną metodą uzupełniania danych (średnia z danych, najniższą lub najwyższa wartością w szeregu). Ponieważ dane, które posłużyły do badań były kompletne - bowiem wstępna ich analiza wykazała 100 procent ich ważności - nie stosowno tej opcji. Wyjątek stanowił szereg czasowy zawierający realizację zmiennej „robak sieciowy". W roku 2005 nastąpił gwałtowny wzrost tego typu zagrożeń. Po usunięciu danej, która zniekształciłby trend, program automatycznie uzupełnił brakującą wartość.[171] Dane wprowadzono do arkusza kalkulacyjnego programu Microsoft Excel.



Rysunek 3-33. Menu programu Forecaster XL

Większość problemów rozwiązuje się za pomocą sieci trzywarstwowej opartej na algorytmie wstecznej propagacji błędu. Oznacza to, że sieć porównuje prognozę z wartością rzeczywistą.[172] Uzyskana różnica jest bazą służącą do korygowania siły powiązań między neuronami.

W badaniu wykorzystano sieci jedno, dwu i trzywarstwowe, wykorzystując modele sieci rekurencyjnej i sieci realizującej regresję uogólnioną (załącznik IV). W pierwszym etapie, w fazie uczenia sieci, do treningu wykorzystano dane z roku 1997 przedstawiające informacje dotyczące ilości mie-

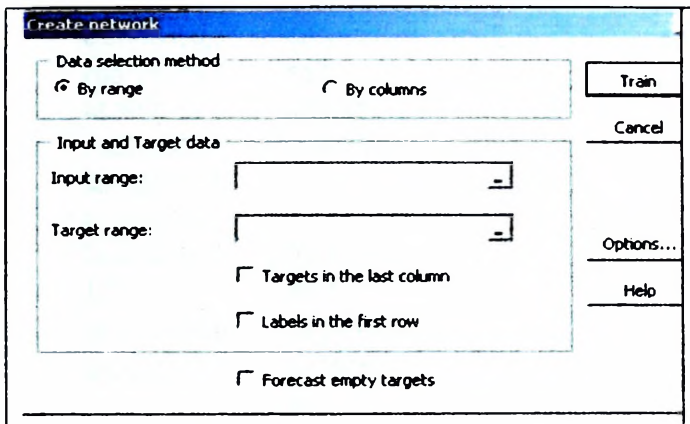
[170] Program dostępny w wersji testowej na stronie: http://www.alyuda.com/forecasting-tool-for-excel.htm.

[171] Ta metoda oblicza Środek i odchylenie standardowe dla danej numerycznej kolumny i wtedy usuwa wszystkie wartości, które wykazują silne odchylenia

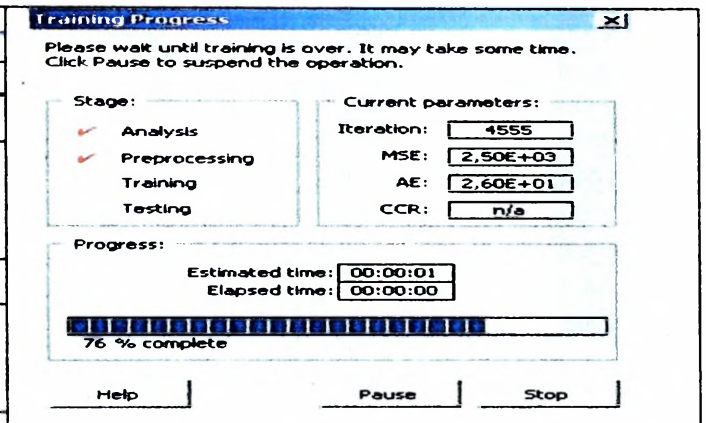
[172] Każdy neuron w warstwie ukrytej *n* jest połączony z wszystkimi neuronami warstwy *n+1*.Odwracamy przebieg sygnału – wartość błędu z warstwy *n+1* jest propagowana na warstwę *n*, począwszy od warstwy wyjściowej o znanym błędzie. Propagowany błąd neuronu w warstwie *n* zależy od błędów wszystkich neuronów warstwy *n+1* pomnożonych przez wagi odpowiednich połączeń miedzy neuronami.

sięcznych ataków poszczególnych typów zagrożeń, a więc liczbę określającą ilość zarejestrowanych incydentów (załącznik IV, sesja 1, przykład 1,2,3).

W procesie wstępnego przetworzenia, program modelujący bada dane oraz określa minimalną i maksymalną wartość zmiennych wejściowych i wyjściowych. Celem jest wyskalowanie do przedziału akceptowanego prze sieć. W badaniu posłużono się wartością średnią z dokładnością do 0,05 i MSE (błędem średnio kwadratowym) z dokładnością 0,05. Domyślnie, minimum i maksimum są obliczone automatycznie używając wartości kolumny (rysunek 3-34, 3-35).



Rysunek 3-34 Menu programu tworzenie sieci



Rysunek 3-35. Menu programu, trenowanie sieci

W wyniku analizy danych i wstępnego przetworzenia, otrzymujemy raport z tabelą wyników sprawdzenia poprawności danych, a także wyniki ich wstępnego przetworzenia (tabela 3-20 i 3-21). Model prognozowania oparty jest na regresji.

Tabela 3-20. Raport wstępnego przetworzenia danych (robaki sieciowe)

Summary
2 columns and 16 rows analysed.
2 columns and 16 rows are accepted for neural network training.
The following columns recognized as numeric:
ROK,
ROBAKI SIECIOWE.
3 values recognized as missing.
Data analysis and preprocessing successfully completed.

Źródło: opracowanie własne.

Tabela 3-21. Wyniki analizy poprawności danych oraz wstępnego przetworzenia (robaki sieciowe)

Analysis Details

Input	Target
ROK	ROBAKI SIECIOWE
numeric	numeric
1993	10
1994	36
1995	44
1996	62
1997	79
1998	88
1999	95
2000	120
2001	138
2002	149
2003	161
2004	170
2005	178
2006	
2007	
2008	

LEGEND

- Input values
- Target values
- Removed rows and columns
- Missing values
- Outliers

Preprocessing Details

Input	Target
ROK	ROBAKI SIECIOWE
[n]	[n]
min: 1993	min: 10
max: 2008	max: 178
-0,4	-0,4
-0,346667	-0,276190476
-0,293333	-0,238095238
-0,24	-0,152380952
-0,186667	-0,071428571
-0,133333	-0,028571429
-0,08	0,004761905
-0,026667	0,123809524
0,0266667	0,20952381
0,08	0,261904762
0,1333333	0,319047619
0,1866667	0,361904762
0,24	0,4
0,2933333	-0,447619048
0,3466667	-0,447619048
0,4	

Źródło: opracowanie własne.

W modelu sieci wielomianowej, w procesie wstępnego przetworzenia dane zapisywane są w kolumnach (załącznik IV sesja 1). Po wprowadzeniu danych do arkusza kalkulacyjnego, wstępnym przetworzeniu, ustaleniu wartości minimalnych i maksymalnych, wyborze architektury sieci, sieć poddawana jest uczeniu (rysunki 3-34 i 3-35).

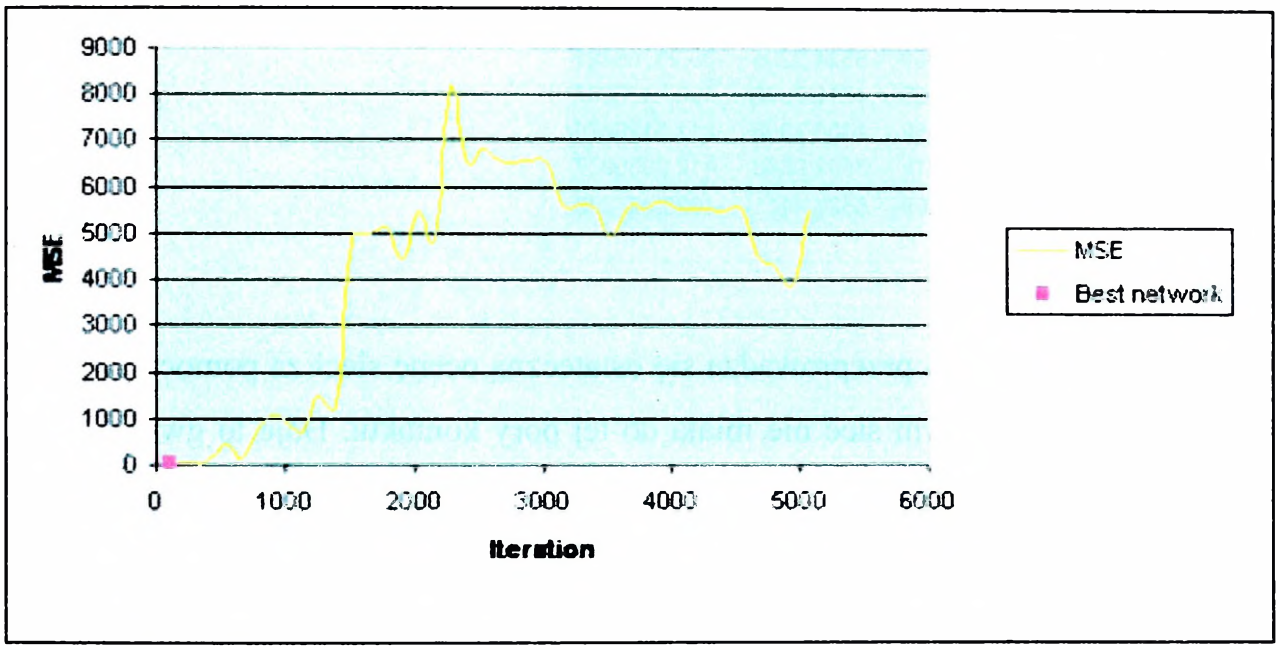
W programie stosowane są iteracyjne procedury uczące (tabela 3-22). W trakcie pracy monitorowane są poprzez wykreślanie błędu dla ciągu uczącego i niezależnego ciągu walidacyjnego (rysunek 3-36, tabela 3-23). Procedura uczenia może być w dowolnej chwili przerwana przez użytkownika. Nie ma żadnej praktycznej reguły dla zatrzymywania szkolonych sieci; tylko przez eksperymentowanie z różnymi zestawami danych i sieci możemy otrzymać najlepsze rezultaty. Można też podać warunki przerwania algorytmu uczącego; na przykład po obniżeniu się wartości błędu uczenia poniżej określonego poziomu lub, gdy błąd dla ciągu walidacyjnego zwiększa swą wartość przez określoną liczbę epok (wystąpienie tego zjawiska wskazuje na przeuczenie sieci).

Tabela 3-22. Raport uczenia sieci dla zagrożenia „robaki sieciowe"

Summary
Problem type: regression
STOP TRAINING CONDITIONS
Training stops automatically.
Training stop reason: maximum number of iterations was achieved.
TRAINING RESULTS
Iterations trained: 5067
The best network was restored.

Źródło: opracowanie własne

Stosowany model prognozowania: regresja. Wykonano 5067 iteracji. Najlepszą sieć, spełniającą założone kryteria osiągnięto przy 101 iteracji.



Rysunek 3-36. Wykres średniego błędu kwadratowego trenowanej sieci robaki sieciowe (*Training Error Graph*)

Tabela 3-23. Zestawienie błędów uczonej sieci robaki sieciowe

Training Error Table

Iteration No.	AE	AE improv.	MSE	MSE improv.
[best] - 101	3,7630253	0	30,514055	0
227	4,3963857	-0,6333604	37,642372	-7,12831758
376	5,2137735	-0,8173878	71,934029	-34,29165633
542	15,372439	-10,158666	438,01904	-366,0850112
668	7,9741344	7,39830467	142,98831	295,0307283
802	18,284032	-10,309898	861,13099	-718,1426765
939	22,566518	-4,2824861	1096,6898	-235,558773
1129	13,544153	9,02236481	669,47194	427,2178161
1255	28,826641	-15,282487	1505,86	-836,3880643
1395	22,242958	6,58368288	1252,1611	253,6989053
1521	35,707113	-13,464155	4895,6368	-3643,475695
1654	38,985469	-3,2783555	4996,023	-100,3861545
1780	36,039482	2,94598692	5144,4671	-148,4441957
1906	32,936907	3,10257499	4440,104	704,3631423

2032	42,127749	-9,1908422	5501,5523	-1061,448314
2158	31,528274	10,5994754	4827,8311	673,7212064
2284	69,540789	-38,012515	8179,3197	-3351,488577
2410	43,502467	26,0383215	6520,374	1658,945683
2536	52,074679	-8,5722117	6843,9497	-323,5756618
2662	44,648685	7,42599338	6553,8637	290,0859623
2788	44,942425	-0,2937397	6546,8914	6,972278821
2914	46,959809	-2,0173834	6573,3756	-26,48418481
3040	43,355387	3,60442116	6518,7381	54,63753243
3166	42,770797	0,58459075	5593,0309	925,7071738
3292	42,769873	0,00092359	5613,1398	-20,1089366
3418	37,94013	4,82974296	5523,2876	89,85219543
3544	38,01395	-0,0738198	4925,2397	598,0479569
3670	41,758431	-3,7444807	5579,48	-654,2403057
3796	38,334886	3,4235442	5524,8682	54,61184057
3922	44,854695	-6,5198088	5696,7433	-171,8751249
4048	38,073302	6,78139328	5522,4511	174,2921337
4174	37,775598	0,2977039	5522,6174	-0,166300056
4300	37,99148	-0,2158822	5526,1433	-3,525832066
4426	38,542544	-0,5510633	5484,9536	41,1897093
4552	38,258215	0,28432909	5524,2206	-39,26705421
4678	41,852497	-3,5942823	4516,7938	1007,426867
4812	32,765276	9,08722059	4305,2808	211,5129375
4938	28,206716	4,55856019	3892,9868	412,2939937
5067	37,279197	-9,0724809	5521,4111	-1628,424223

Źródło: opracowanie własne.

Po zakończeniu uczenia przeprowadza się ostateczną ocenę sieci za pomocą niezależnego zbioru testowego, z którym sieć nie miała do tej pory kontaktu. Daje to gwarancję, że sieć nauczyła się wykonywać zadanie z oczekiwaną dokładnością. Założono, że błąd wynosić może 10%. W załączniku IV (sesja 2 i 3) zawarto wyniki otrzymane podczas kolejnych eksperymentów uczenia sieci i weryfikowania badań dla różnych danych. Proces uczenia dla obu metod, zatrzymywany był automatycznie w chwili osiągnięcia maksymalnego numeru iteracji.

Raport zbiorczy dla danych empirycznych i uzyskanych prognoz zawiera obliczone wartości statystyk (tabela 3-25) takie, jak: średnia, odchylenie standardowe z próby, a także bardzo istotny wskaźnik r Pearsona[173] określający siłę związku pomiędzy zbiorem danych empirycznych i uzyskanych z modelu, a który przyjęto jako kryterium wyboru najlepszego

---

[173] $r = \sqrt{1 - \frac{s_0^2}{s_y^2}}, s_0 = \sqrt{\frac{\sum_{y_i-1}^{p} (y_i - y_{ip})^2}{n-2}}, \quad s_y = \sqrt{\frac{\sum y_i^2}{n} - \bar{y}_i^2}$, gdzie: y_i – wartość eksperymentalna, y_i^p – wartość przewidziana przez sieć, n- liczba próbek, y_i^2- średnia wartość eksperymentalna. Wartość współczynnika korelacji mieści się w przedziale (-1,1>. Im wyższa bezwzględna wartość współczynnika determinacji, tym silniejsza zależność liniowa między cechami, oznacza to większą dokładność prognoz.

modelu neuronowego dla regresji. Poniżej zestawiono wyniki badań dla wykonanych prognoz wraz z wykresami (tabela 3-24).

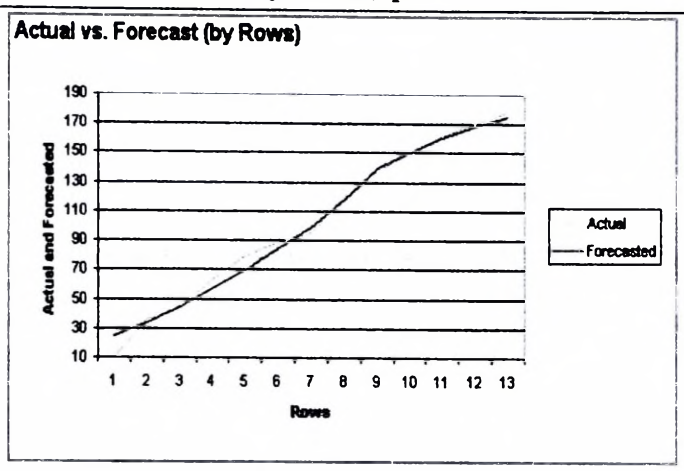
Tabela 3-24. Raport statystyk dla zagrożeń: „robak sieciowy", koń trojański, „spam"

Summary

	Training set	Test set
# of rows:	11	2
CCR:	n/a	n/a
Average AE:	2,7759173	10,156578
Average MSE:	12,906743	124,88423
Tolerance type:	Relative	Relative
Tolerance:	10%	30%
# of Good forecasts:	10 (91%)	1 (50%)
# of Bad forecasts:	1 (9%)	1 (50%)

RSquared: 0,9892
Correlation: 0,9948

Podsumowanie wyników treningu i testowania sieci dla zagrożenia „robak sieciowy"



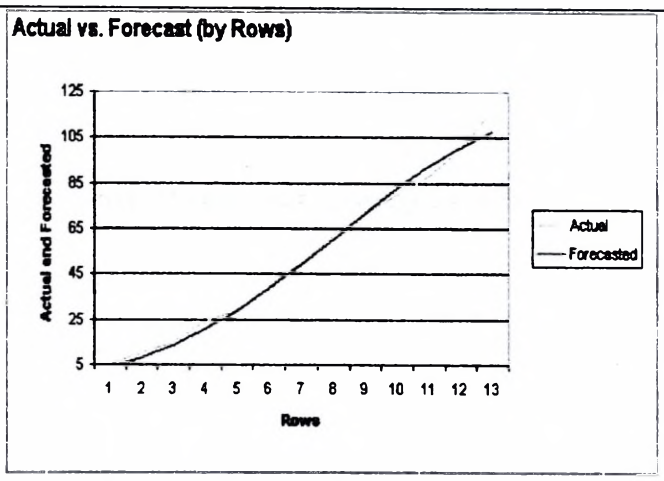
Bezwzględne wartości wejściowej kolumny zagrożenia „robak sieciowy" i przewidywane wartości

Summary

	Training set	Test set
# of rows:	11	2
CCR:	n/a	n/a
Average AE:	2,3990653	1,1771088
Average MSE:	11,779633	1,896793
Tolerance type:	Relative	Relative
Tolerance:	10%	30%
# of Good forecasts:	9 (82%)	2 (100%)
# of Bad forecasts:	2 (18%)	0 (0%)

RSquared: 0,9916
Correlation: 0,9961

Podsumowanie wyników treningu i testowania sieci dla zagrożenia „Koń trojański"



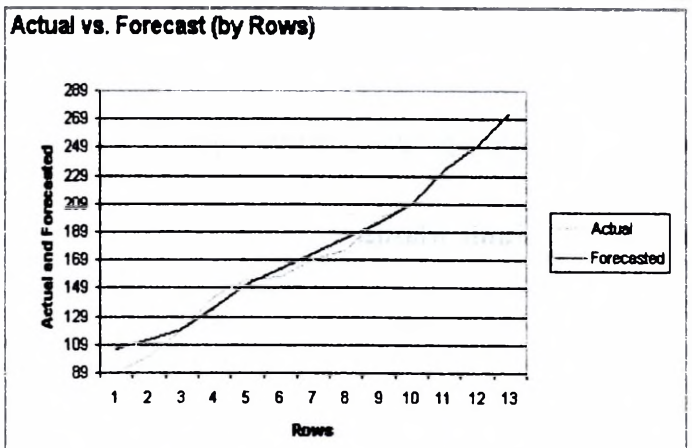
Bezwzględne wartości wejściowej kolumny dla zagrożenia „koń trojański" i przewidywane wartości

Summary

	Training set	Test set
# of rows:	11	2
CCR:	n/a	n/a
Average AE:	4,0774279	10,602182
Average MSE:	31,688133	149,62365
Tolerance type:	Relative	Relative
Tolerance:	10%	30%
# of Good forecasts:	10 (91%)	2 (100%)
# of Bad forecasts:	1 (9%)	0 (0%)

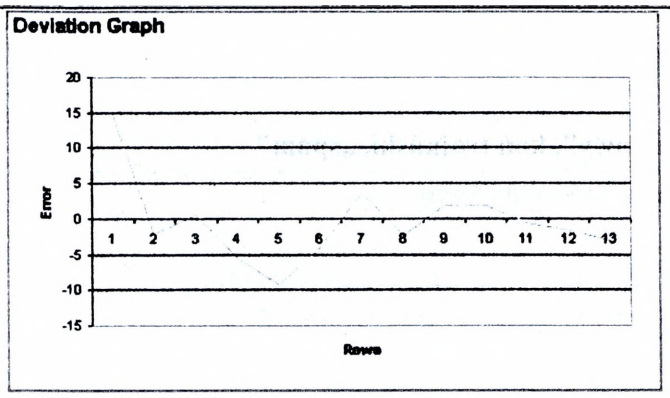
RSquared: 0,9832
Correlation: 0,9938

Podsumowanie wyników treningu i testowania sieci dla zagrożenia „spam"

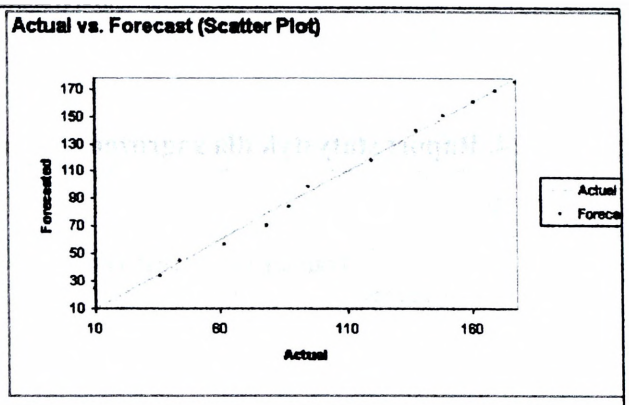


Bezwzględne wartości wejściowej kolumny dla zagrożenia „spam" i przewidywane wartości

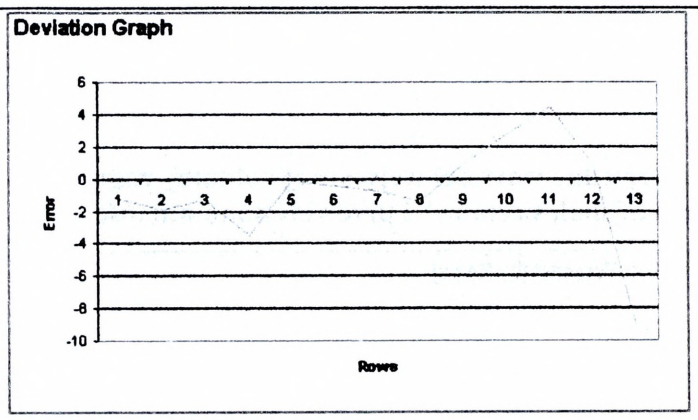
Tabela cd. Zestawienie wyników prognozowania ciąg dalszy



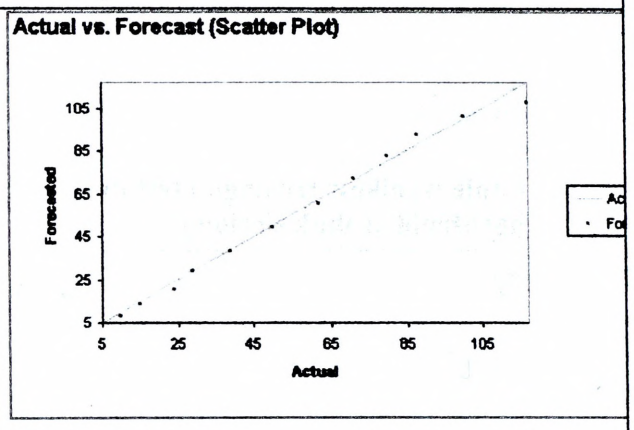
Odchylenia błędów prognozowania „robak sieciowy"



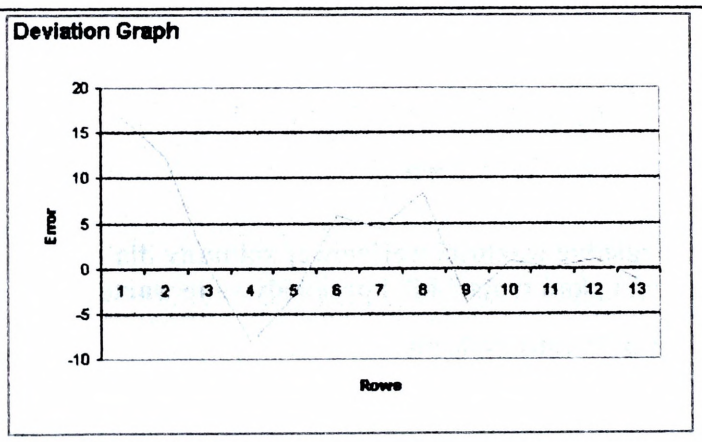
Mapa punktowa rozrzucenia prognoz „robak sieciowy"



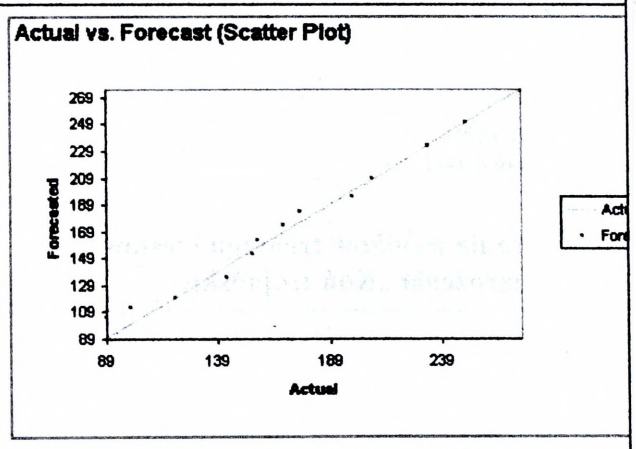
Odchylenia błędów prognozowania „koń trojański"



Mapa punktowa rozrzucenia prognoz „koń trojański"



Odchylenia błędów prognozowania „spam"



Mapa punktowa rozrzucenia prognoz „spam"

Źródło: opracowanie własne.

Tabela 3-25. Zestawienie prognoz dla zagrożeń: „spam", robaki sieciowe", „koń trojański"

Rok	Spam	Robaki sieciowe	Koń trojański
1993	89	10	5
1994	100	36	10
1995	120	44	15
1996	143	62	24
1997	155	79	29
1998	157	88	39
1999	169	95	50
2000	176	120	62
2001	199	138	71
2002	208	149	80
2003	233	161	88
2004	250	170	100
2005	275	178	117
2006	278,0735742	180,3197479	113,5276296
2007	281,2683965	184,5437861	117,9421175
2008	283,988909	187,868246	121,329292
2009	286,297727	190,4615707	123,8870755

Źródło: opracowanie własne.

Tabela 3-26. Zalety i wady sieci neuronowych

Zalety	Wady
Zdolność do adaptacji i samoorganizacji. Łatwość programowania sieci poprzez uczenie. Odporność na uszkodzenia poszczególnych elementów. Zdolność przetwarzania danych niekompletnych, rozmytych, chaotycznych, a nawet sprzecznych. Szybkie i efektywne przetwarzanie dużych ilości danych. Przetwarzanie rozproszone i równoległe. Skojarzeniowy dostęp do informacji zawartej w sieci (tzw. pamięć skojarzeniowa).	Trudność w objaśnianiu wyników. Kłopotliwe dla niedoświadczonego użytkownika, jeśli sam ustala algorytm, parametry algorytmu oraz architekturę sieci. Niebezpieczeństwo przetrenowania sieci lub niedouczenia sieci.

Źródło: D.Dżega, *Metoda oceny ryzyka projektów informatycznych*. Praca doktorska. Politechnika Szczecińska, Szczecin 2008.

3.4. Analiza społecznej percepcji zagrożeń informacyjnych[174]

Wprowadzenie

Wszechstronne badania opinii publicznej, pozwalają wychwycić różnice dotyczące ważnych kwestii bezpieczeństwa, nie tylko politycznych, które mogą obciążać stosunki wewnątrz społeczeństwa jak i stosunki międzynarodowe. Dostarczają wskazań dla decydentów, w jaki sposób należy kształtować kulturę bezpieczeństwa, oraz jakie braki edukacyjne i potrzeby występują w społeczeństwie, w obszarze bezpieczeństwa.

Decydujący wpływ na postrzeganie ryzyka ma wiedza i dostęp do informacji na temat istniejących, czy możliwych i prawdopodobnych zagrożeń, ich skutków oraz możliwości ochrony (obrony, postępowania, podejmowania). Ogromną rolę w zakresie percepcji spełniają media, głównie elektroniczne oraz w coraz większym stopniu Internet. Znane są już przypadki manipulowania informacją dla wzmocnienia „zamówionych" efektów. Coraz częściej przekaz opiera się na emocjach, i manipulacji a nie rzetelnej informacji.[175] W kontekście nadmiaru niesprawdzalnej informacji, pisze się o „bombie informacyjnej", którą uważa się nawet za groźniejszą dla przetrwania ludzkości niż bomba atomowa, bo uniemożliwia postrzeganie tego, co się dzieje w sposób umożliwiający podejmowanie racjonalnych decyzji.[176] Nadmiar informacji o przeszłych zdarzeniach utrudnia diagnozę, a w konsekwencji podjęcie racjonalnej decyzji. Na podstawie dotychczasowych badań przyjmuje się pewne sytuacyjne uwarunkowania postrzegania ryzyka. Wyróżnia się kryteria oceny zagrożeń, które pozwalają przewidzieć, w jaki sposób wartościowane jest ryzyko (tabela 3-27).

Oczywiście, stanowi to tylko przesłanki dla oceny percepcji ryzyka w rzeczywistych sytuacjach problemowych. Zagadnienie jest o wiele bardziej złożone, gdyż, na co dzień posługujemy się heurystykami („drogą na skróty") używając wzorców czy matryc standardowych zachowań, doświadczeń, a także tzw. złudzeń poznawczych.[177]

Niepewne sytuacje problemowe wyrażają trudność w jednoznacznym określeniu stanu jakichś zjawisk (obiektów, procesów), nieoznaczoność parametrów (własności) jakichś obiektów, czy nieprzewidywalność ich zachowania. Przyczynami niepewności mogą być: brak in-

---

[174] Jest to wydzielony fragment wyników badań empirycznych dotyczących postrzegania ryzyka pt. *Społeczna percepcja zagrożeń bezpieczeństwa obywateli w warunkach GSI.* Wykonanej pod kierunkiem P.Sienkiewicza, AON, Warszawa 2009.

[175] Np. osoba przekazująca (lektor) informację, pretenduje do roli komentatora uprawnionego do opiniowania wydarzeń.

[176] Paul Virilio, *Bomba informacyjna*. Sic! Warszawa 2005.

[177] Szerzej: P.Sienkiewicz, H.Świeboda, *Percepcja zagrożeń bezpieczeństwa w społeczeństwie ryzyka.* [W:] *Edukacja w społeczeństwie „ryzyka". Bezpieczeństwo jako wartość.* M.Gwoździcka-Piotrowska i in. Wydawnictwo Wyższej Szkoły Bezpieczeństwa, Poznań 2007, s.100 –117.

formacji, nieznany stopień nieścisłości dostępnych informacji, brak możliwości uzyskania potrzebnych informacji, brak wykonania jakichś istotnych pomiarów itp. (tabela 3-28).

Tabela 3-27. Kryteria oceny w postrzeganiu ryzyka

KRYTERIUM OCENY	PERCEPCJA RYZYKA
Dobrowolność	Zachowania podejmowane dobrowolnie oceniane są jako mniej ryzykowne, wyższy jest również poziom ryzyka uznawanego za akceptowalne w tym przypadku.
Szybkość konsekwencji	Ryzyko związane z natychmiastowymi konsekwencjami jest postrzegane jako większe niż w sytuacji, kiedy straty są odroczone w czasie.
Katastroficzność konsekwencji	Ryzyko, którego wynikiem mogą być skutki o charakterze katastroficznym (np. katastrofa lotnicza) jest postrzegane jako większe niż ryzyko związane ze skutkami chronicznymi.
Stopień kontroli	Ryzyko związane z działaniami postrzeganymi jako kontrolowalne, zależne od jednostki (np. jazda samochodem) jest oceniane jako mniejsze niż ryzyko postrzegane jako niekontrolowalne (np. pożar).
Nowość	Ryzyko nowe oceniane jest jako większe niż ryzyko, z którym jednostka miała kontakt wcześniej.
Poziom wiedzy	Ryzyko, które jest mało rozpoznane (nieznane są wszystkie możliwe konsekwencje, jakie ze sobą niesie) jest postrzegane jako większe.
Pozom lęku	Im większy jest lęk przed określonymi zagrożeniami, tym ryzyko z nimi związane postrzegane jest jako większe.

Źródło: M. Milczek, *Kultura bezpieczeństwa*, WWW.ciop.pl/10563 [on line], [dostępna: 20.04.2005].

Bezpieczeństwo jest naturalną potrzebą ludzi, traktowana jako wartość egzystencjalna, a także, jako – po prostu brak zagrożeń. Poczucie bezpieczeństwa jest siłą pozwalająca funkcjonować i rozwijać się. Poczucie zagrożeń, ich percepcja może okazać się barierą paraliżującą aktywność (rysunek 3-37).[178]

Obywatel społeczeństwa informacyjnego korzystający z Internetu ma obecnie możliwość dużo większej dynamiki i zakresu działalności, o ile należy do grona ludzi „Galaktyki Internetu".[179] Wchodząc w różnorodne relacje w cyberprzestrzeni, poszerza swoją infosferę, może skutecznie w ramach „społeczności internetowych" przeciwstawiać się traumie, a także ograniczać uzależnienie od państwa i rynku. Środowisko sieci sprzyja samodzielnemu reali-

[178] P.Sienkiewicz, H.Świeboda, *Percepcja zagrożeń bezpieczeństwa w społeczeństwie ryzyka.* [W:] *Edukacja w społeczeństwie „ryzyka". Bezpieczeństwo jako wartość.* M.Gwoździcka-Piotrowska i in.,Wydawnictwo Wyższej Szkoły Bezpieczeństwa, Poznań 2007, s.100 –117.

[179] M.Castells, Galaktyka Internetu, refleksje nad Internetem biznesem i społeczeństwem, Rebis, Poznań 2003.

zowaniu własnych potrzeb, interesów i zainteresowań w oparciu o zasadę wzajemności,[180] może stać się źródłem wsparcia procesów demokracji, a demokracji bezpośredniej w szczególności, może być również narzędziem nieposłuszeństwa obywatelskiego.[181] Może być także miarą „społecznego wzburzenia" uwzględnianą w analizach zagrożeń, w sytuacjach decyzyjnych.

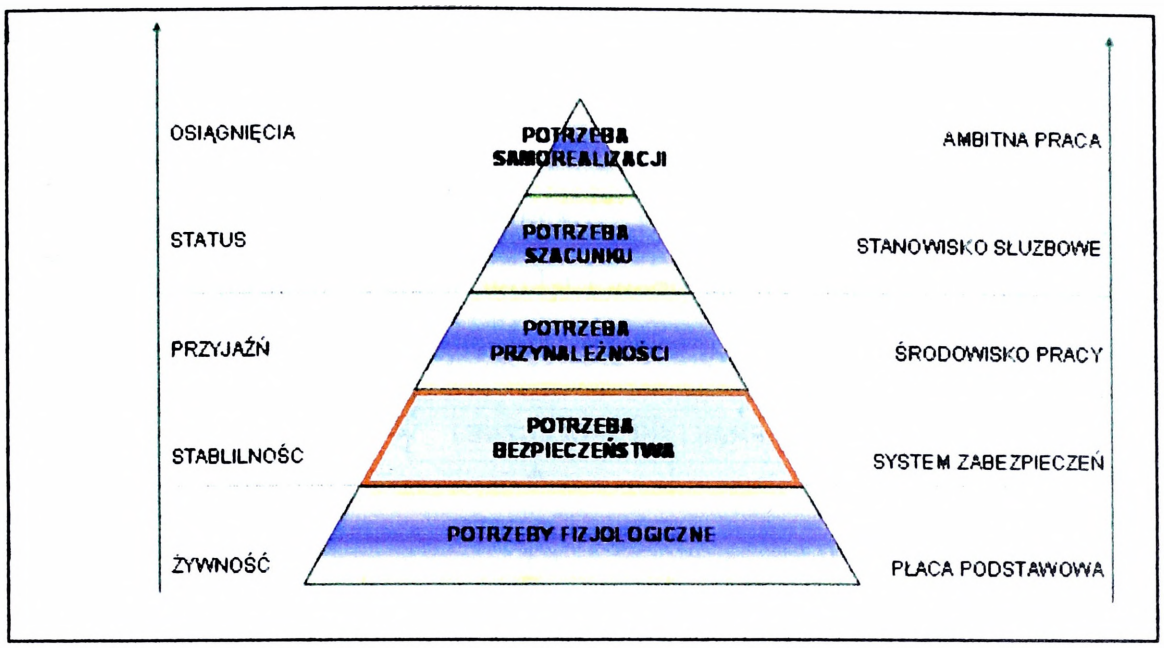
Tabela 3-28. Analiza systemowa determinant niepewności i ryzyka

LP	DETERMINANTY NIEPEWNOŚCI	CHARAKTERYSTYKA	SKUTEK
1	**Homogeniczność otoczenia**	Jednakowe własności elementów i relacji między nimi	Zwiększenie powoduje zmniejszenie niepewności
2	**Stabilność otoczenia**	Trwałość elementów systemu i otoczenia jak i związków między nimi	Redukcja niepewności
3	**Iteracyjność (powtarzalność)**	Cyklicznie powtarzane zmiany stanów otoczenia lub zmian zachodzących wewnątrz systemu	Kompresja niepewności
4	**Strukturyzacja otoczenia**	Identyfikacja związków, sprzężeń zwrotnych między elementami systemu a otoczeniem	Zmniejszenie niepewności
5	**Dezintegracja otoczenia**	Rozpad, dekompozycja struktur systemu	Wzrost niepewności
6	**Złożoność otoczenia**	Wzrost elementów systemu i otoczenia oraz sprzężeń zwrotnych między nimi	Wzrost niepewności
7	**Adaptacyjność**	Zdolność dostosowawcza systemu do zmian w otoczeniu	Zmniejszenie niepewności
8	**Przewidywalność**	Możliwość prognozowania zmian systemu i otocznia	Redukcja niepewności
9	**Sterowalność**	Zdolność osiągania pożądanych stanów	Redukcja niepewności

Źródło: opracowanie własne.

[180] Zagadnienie więzi społecznych analizowane jest w pracy doktorskiej J.Bierówki pt.: *Zasada wzajemności w formującym się społeczeństwie informacyjnym*". Rozprawa doktorska, Uniwersytet Jagielloński, Instytut Socjologii, Kraków 2006.

[181] Szerzej [w:] H.Świeboda, Postrzeganie demokracji w społeczeństwie informacyjnym w świetle opinii społecznej. Transformacje, Warszawa, 2009 (w druku). Także, P.Sienkiewicz, Zagrożenia dla demokracji w społeczeństwie informacyjnym. Transformacje, Warszawa, 2009 (w druku).



Rysunek 3-37. Klasyczna hierarchia potrzeb według Maslowa
Źródło: P.Sienkiewicz, H.Świeboda, *Percepcja zagrożeń bezpieczeństwa w społeczeństwie ryzyka.* [w:] *Edukacja w społeczeństwie „ryzyka". Bezpieczeństwo jako wartość.* M.Gwoździcka-Piotrowska i in. Wydawnictwo Wyższej Szkoły Bezpieczeństwa, Poznań 2007, s.100 –11.

Opis badań

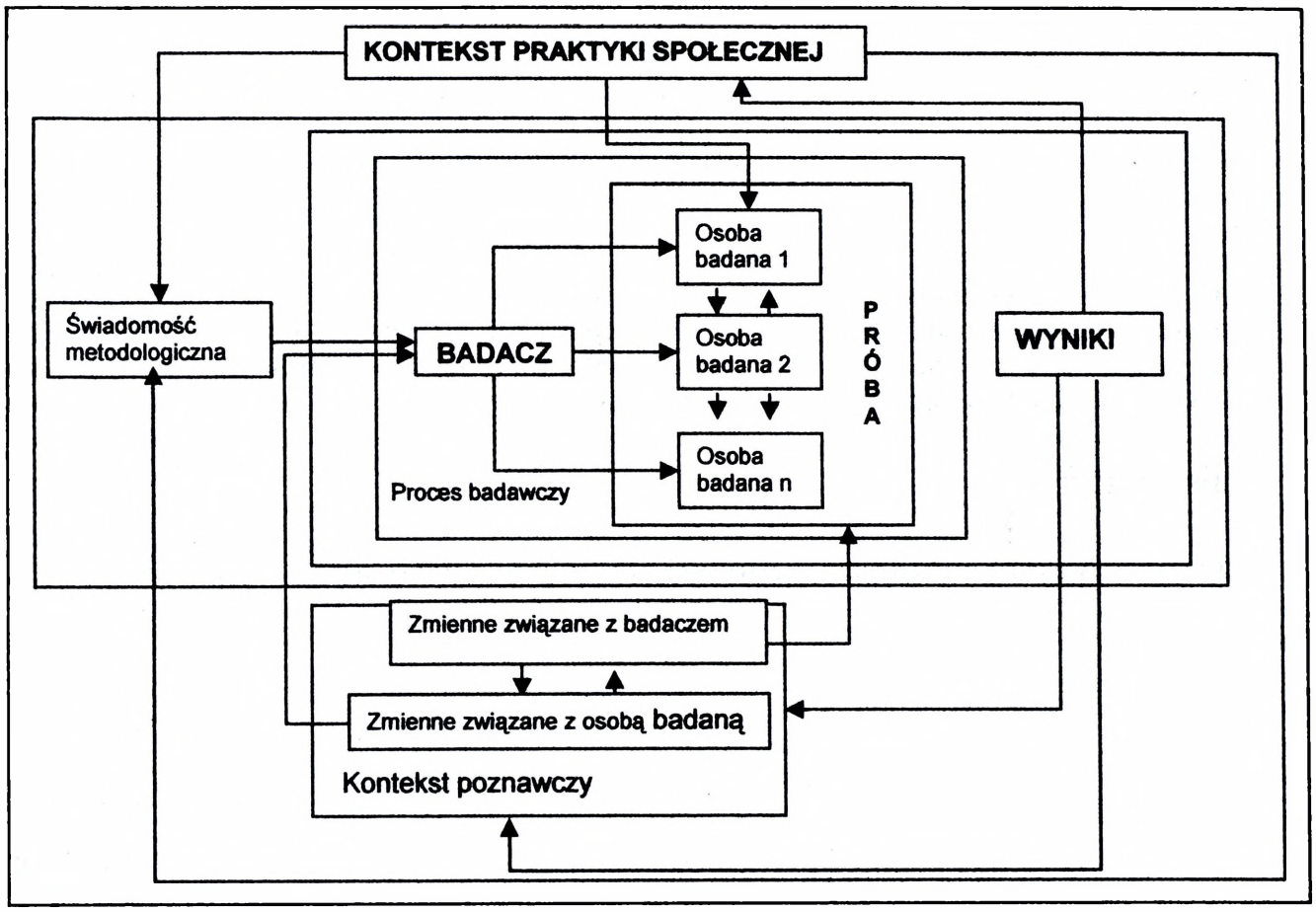
W badaniach eksploracyjnych często wykorzystywaną metodą jest sondaż. Pozwala na racjonalne zbadanie opinii i postaw przedstawicieli danej populacji, w celu odkrycia zachodzących w niej zjawisk. Techniką, która została użyta w sondażu była ankieta audytoryjna składająca się z czterech części (załącznik IX). Ankieta składa się z czterech części oraz części metrykalnej. Pierwsza cześć A[182] stanowi źródło informacji o percepcji intensywności zjawisk dotyczących rozwoju społeczeństwa informacyjnego. Zawierała pytania najczęściej pojawiające się w dyskusjach dotyczących rozwoju społeczeństwa informacyjnego oraz jego konsekwencji społecznych, ekonomicznych i politycznych (w kontekście szans, zagrożeń i wyzwań)[183]. Pytanie brzmiało: Czy wyróżniona cecha wzrośnie czy zmaleje, bądź trudno powiedzieć, w wyniku rozwoju społeczeństwa informacyjnego?

Część ankiety B, pozwoliła określić stopień postrzegania zagrożeń dla bezpieczeństwa narodowego RP w kontekście współczesnych niebezpieczeństw związanych z rozwojem technologii, jak również z globalnymi zmianami społeczno-politycznymi i konfliktami na świecie, w kontekście możliwych i prawdopodobnych zagrożeń. Część C ankiety poświęcono percepcji zagrożeń w kontekście bezpieczeństwa osobistego, obejmujących również zagrożenia informacyjne. Części te stanowiły kontekst dla części D ankiety, którą poświęcono ocenie

[182] Cześć A, B i C stanowi podstawę odrębnego opracowania, (P.Sienkiewicz, H.Swieboda, *Społeczna percepcja zagrożeń bezpieczeństwa obywateli w warunkach globalnego społeczeństwa informacyjnego.* AON Warszawa 2009, miała jednak znaczenie przy interpretacji niektórych wyników i wyciąganiu wniosków.

[183] Wykorzystano zestaw pytań opracowanych przez profesorów: socjologa A.Sicińskiego i inżyniera J.Lubacza.

skutków rozwoju technologii informacyjnych w aspekcie bezpieczeństwa informacyjnego RP. Jednocześnie uzupełniały wiedzę o percepcji zagrożeń w różnych sferach bezpieczeństwa narodowego (rysunek 3-38). Część Da zawierała wyszczególnione konkretne, możliwe i prawdopodobne zagrożenia informacyjne.[184] Zamieszczono w niej pytania pozwalające na określenie częstości pojawiających się obaw i lęków, a także wskazanie wartości uniwersalnych, które respondenci cenią sobie najbardziej. Ankietę zakończyły pytania metrykalne.



Rysunek 3-38. Schemat procesu badawczego

Źródło: opracowanie własne.

Badanie pozwoliło określić skutki rozwoju globalnego społeczeństwa informacyjnego oraz antycypację zmian społecznych zachodzących pod wpływem technologii ICT. Założono, że w skomplikowanej sytuacji wynikającej z globalizacji, kryzysu gospodarczego, także – odczuwalnych nadal skutków transformacji systemowej i zmian ustrojowych, reform społeczno-gospodarczych itp., której immanentną cechą jest dynamiczny rozwój technologii ICT, postrzeganie przez badanych asocjacji i różnego rodzaju sprzężeń, może być zakłócane nie tylko dużą ilością zdarzeń, ale i własnymi ograniczeniami.

Głównym celem badawczym było poznanie stopnia percepcji społecznej zagrożeń związanych z coraz powszechniej stosowanymi technologiami informacyjno-komunikacyjnymi.

[184] Część D stanowi treść niniejszego opracowania.

W badaniu uczestniczyło 687 osób w 2007/2008 roku. Wszystkie dane o licznościach prób obejmują przypadki, które znalazły się w bazie danych, a nie wszystkie przypadki przebadane. Część przebadanych przypadków ze względu na wadliwie wypełnione ankiety lub problemy z identyfikacją odpowiedzi, nie została wprowadzona do bazy danych. Badania ankietowe uzupełnione były pogłębionymi wywiadami prowadzonymi w ramach wykładanego przedmiotu (np.: „Problemy społeczeństwa informacyjnego", „Gospodarka Oparta na Wiedzy", „Prognozowanie zagrożeń dla bezpieczeństwa narodowego").

Należy podkreślić, że prezentowane tu badania stanowią jedynie egzemplifikację rozważań teoretycznych, któremu poświęcono odrębne opracowanie.[185]

Dane pochodzące z tego sondowania opracowano komputerowo z wykorzystaniem pakietu Statistica i Excel. Ich analiza stanowiła podstawę do weryfikacji postawionych na wstępie hipotez i do opracowania czwartej części pracy poświęconej modelowi zarządzania bezpieczeństwem informacyjnym.

Do sprawdzenia stopnia niezależności par cech wykorzystano test nieparametryczny Pearsona oparty na rozkładzie χ^2. Rozkład ten umożliwia sprawdzenie, jak często zachodzą wyróżnione zdarzenia. Hipotezę zerową odrzucano, gdy prawdopodobieństwo uzyskania danego wyniku było mniejsze od przyjętego poziomu α. W badaniu przyjęto poziom istotności równy 0,05 w niektórych przypadkach 0,01 i 0,001. W przypadku określania zgodności współzależności więcej niż dwóch uporządkowań, używano współczynnika zgodności Kendalla *W*. Liczba wartości miary inwersji S była większa niż 10. Dokonano więcej niż 5 par pomiarów. Wartość korelacji τ interpretowano za pomocą rozkładu standaryzowanego, reprezentowanego równaniem:

$$z = \frac{|S| - 1}{\sqrt{N(N-1)(2N+5)/18}} \tag{3-35}$$

O istotności współczynnika decydowano na podstawie wyniku testu χ^2. Ponadto posłużono się statystyką opisową. Do liczenia rozkładu liczebności wyróżnionych kategorii odpowiedzi zastosowano test χ^2. Otrzymane wartości okazały się istotne na poziomie $p<0,01$ potwierdzając, że istnieje związek pomiędzy wybieranym rodzajem odpowiedzi, a postrzeganiem zagrożenia.

Charakterystyka próby

[185] P.Sienkiewicz, H.Świeboda, *Percepcja zagrożeń,...*,2007, op.cit.

Badaniem sondażowym objęto 687 studentów, zarówno studiów dziennych jak i zaocznych Akademii Obrony Narodowej i Warszawskiej Wyższej Szkoły Informatyki. Do bazy danych wprowadzono 481 ankiet poprawnie zidentyfikowanych i odczytanych. Charakterystykę próby przedstawia tabela 2-29.

Osiemdziesiąt siedem procent wyróżnionej grupy badawczej stanowili mężczyźni. Jest to odzwierciedlenie preferencji przez mężczyzn technicznych kierunków studiów.

W grupie badawczej, ze względu na sposób prowadzania badań, zarówno na studiach dziennych jak i zaocznych, określono przedziały wieku: (1) do 20 lat, (2) 20-30 lat, (3) 30-40 lat, (4) powyżej 40 lat. Najliczniejszą grupę stanowili studenci z przedziału wiekowego drugiego (tabela 3-30-2) natomiast średnia wieku dla całości badanej próby wynosiła 20 lat.

Ze względu na uczelnie reprezentowane w badaniu kierunki studiów sklasyfikowano: (1) ekonomiczne, 2) techniczne, (3) menadżerskie, (4) wojskowe, (5) humanistyczne. Najliczniejszą grupę stanowili studenci kierunków technicznych 80%, kierunki ekonomiczne reprezentowało 9%, a reprezentanci humanistycznych kierunków stanowili 10 procent ankietowanych. Niewielki procent próby badawczej stanowili studenci wojskowi i menadżerowie (1%).

W badanej grupie, która należy do zamożnej, ponieważ dochody powyżej 3000 tys. zł podało 331 osób, co stanowi 69% grupy. Grupa do 1000 PLN stanowiła 25% badanej zbiorowości. Dochody do 500 PLN podało tylko 6 % ankietowanych. Chociaż w dużej części grupę badawczą stanowili studenci dzienni, można przypuszczać, że są to osoby pracujące, lub pochodzące z zamożnych domów.

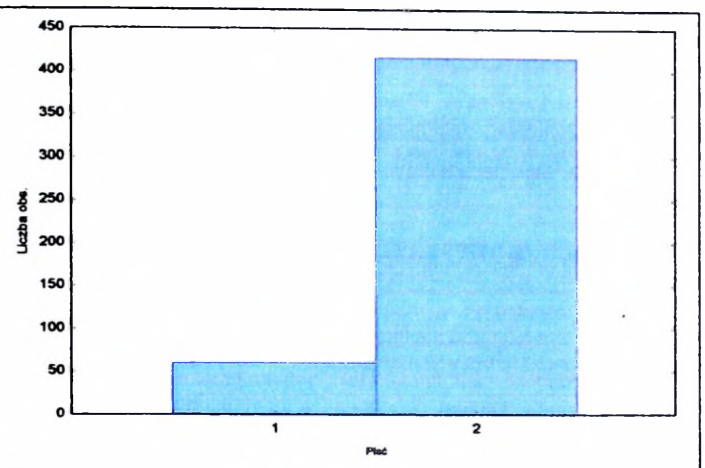
W pytaniach metrykalnych wyróżniono również klasyfikacje osób badanych ze względu na miejsce zamieszkiwania. W grupie respondentów mieszkańcy miasta powyżej 500 tys. stanowili najliczniejszą grupę (57%). Drugą, co do liczność grupę reprezentowali mieszkańcy miast do 100 tys., (19%), trzecią mieszkańcy wsi (10%), czwartą najmniej liczną reprezentowali mieszkańcy miast do 500 tys. (9%) i 5% stanowili mieszkańcy miast do 100 tys. W badanej próbie, z racji miejsca prowadzonego badania, najwięcej respondentów zamieszkiwało w aglomeracji Warszawa.

Wśród badanych osób wszystkie dysponowały dostępem do Internetu, a 85% badanych miała stałe łącza. Ponadto wyposażeni byli w telefony komórkowe (niektórzy posiadali więcej niż jeden telefon), 65% z dostępem do Internetu, 87% badanych korzystało z komunikatorów internetowych, a 100% badanych posiadało internetowe konta bankowe. Ponad połowa badanych aktywnie wykorzystuje sieć uczestnicząc w forach dyskusyjnych, a także robiąc zakupy w sklepach internetowych.

Tabela 3-29. Charakterystyka próby

Płeć badanych

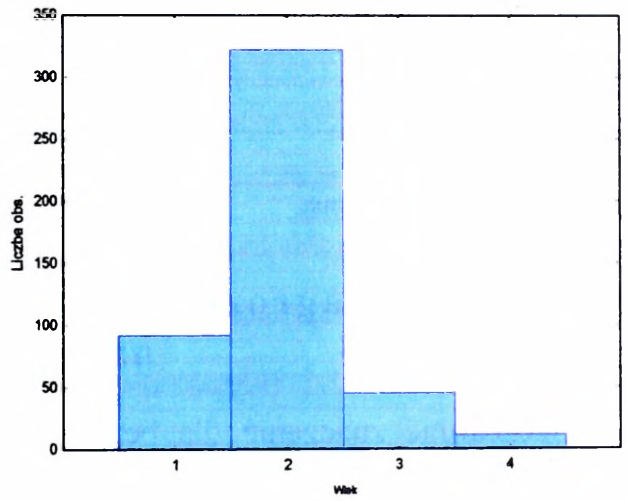
Płeć	N=481	
	n	%
Mężczyźni	419	87
Kobiety	62	12,8



Płeć badanych

Ankietowani w podziale na grupy wiekowe

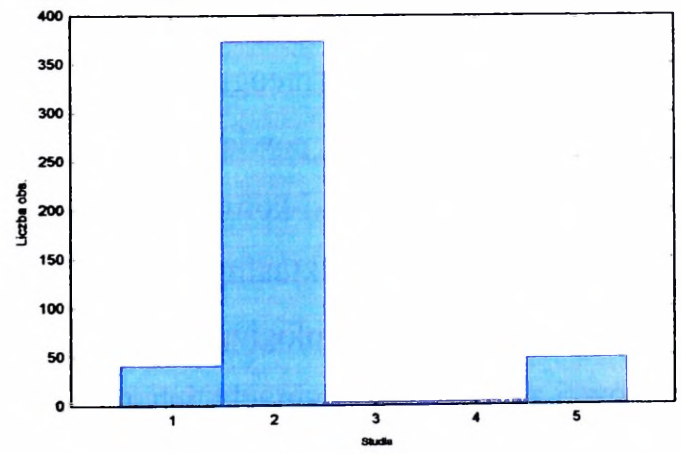
Przedział wieku	N=481	
	n	%
Do 20 lat	94	20
20-30 lat	328	68
30-40 lat	48	10
Powyżej 40 lat	11	2
suma	481	100



Wiek badanych

Kierunek studiów

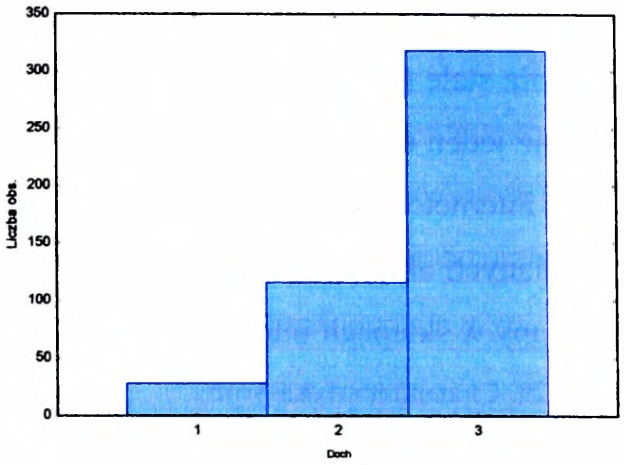
Kierunek studiów	N	
	n	%
Ekonomiczne	43	8,93
Techniczne	385	80,0
Menadżerskie	3	0,62
Wojskowe	3	0,62
Humanistyczne	47	9,77
	481	99,94



Kierunek studiów

Dochody badanych

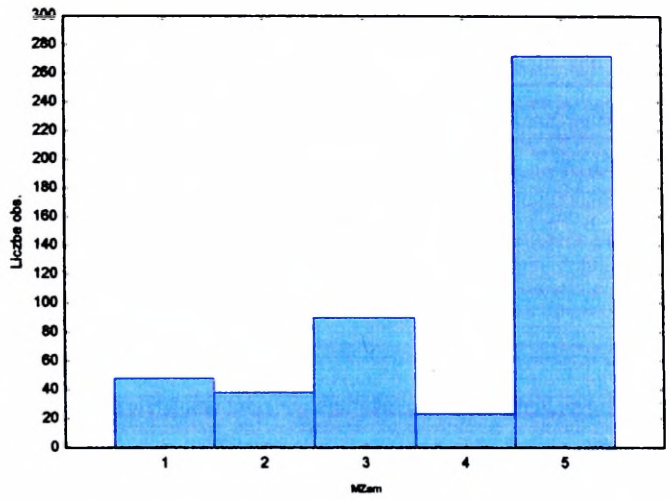
Dochody	N=481	
	n	%
powyżej 500PLN	29	6,0
do 1000PLN	125	25,98
powyżej 1000PLN	327	67,9
	481	99,88



Kategoria dochodów reprezentowana przez badanych

Miejsce zamieszkania

Miejsce zamieszkania	N	
	n	%
Wieś	49	10,18
Miasto do 20 tyś. mieszk.	43	8,93
Miasto do 100 tyś. mieszk.	93	19,33
Miasto do 500 tyś. mieszk.	24	4,98
Miasto powyżej 500 tyś. mieszk.	272	56,54
	481	99,96



Miejsce zamieszkania respondentów

Źródło: opracowanie własne.

Percepcja zagrożeń informacyjnych dla bezpieczeństwa narodowego RP

Szczególne znaczenie dla bezpieczeństwa narodowego ma wymiar technologiczny związany z wysoką dynamiką zmian w sferze komunikacji i informacji oraz postępującą integracją systemów informatycznych i telekomunikacyjnych. Powstały nowe obszary aktywności ludzkiej w zasadzie nieograniczone czasem i przestrzenią, pozwalające także zachować anonimowość. Rozwój powiązań społecznych, gospodarczych i politycznych z udziałem technologii informacyjno-komunikacyjnych spowodował powstanie cyberprzestrzeni, której granice wyznaczane są aktualnym poziomem rozwoju techniki informacyjno-komunikacyjnej. Wraz z rozwojem technologicznym wystąpiła konieczność zapewnienia bezpieczeństwa systemów i sieci informacyjnych, ich poufności, integralności i nienaruszalności. Zagrożenia informacyjne mają również wpływ na jakość życia obywateli.

Różnorodność przestępstw komputerowych i motywów działania sprawców oraz świadomość braku doskonałych zabezpieczeń powoduje, że antycypacja zagrożeń oraz ich percepcja, często wspomagana medialnym przekazem, powoduje frustracje i niechęć do korzystania

z nowoczesnych technologii. Postrzeganie i ewaluacja zagrożeń związanych z rozwojem społeczeństwa informacyjnego w kontekście bezpieczeństwa narodowego ma szeroki kontekst globalny spraw i uwarunkowań społeczno-politycznych.

Dla przykładu, jeżeli spam[186] stanowi przede wszystkim dużą dokuczliwość dla indywidualnych użytkowników sieci, to w przypadku korporacji, urzędów państwowych może grozić blokadą informacyjną, przechwytywaniem danych[187], może być jednym ze sposobów blokady serwerów. Świadomość, percepcja a także antycypacja zagrożeń, sprzyja racjonalizacji działania i umiejętności obrony przed niebezpieczeństwami. Znajomość zagrożeń neutralizuje wyolbrzymiane przez media informacje, skupiające się wyłącznie na negatywnych aspektach bezpieczeństwa.

W badaniu oceny skutków rozwoju technologii informacyjnych, w aspekcie bezpieczeństwa narodowego, głównym założeniem było poznanie postrzegania i rozpoznawania działań jako zagrożeń. **Czy arbitralnie dobrana grupa studentów, dla której współczesne media informacyjno-komunikacyjne nie stanowią nowości, dostrzega niebezpieczeństwa, którym te media sprzyjają i w jakim stopniu stanowi to zagrożenie?**

Wszelkie działania mogą być postrzegane i oceniane w zależności od perspektywy percepcyjnej i dystansu psychologicznego[188] (sprawcy, obserwatora, pokrzywdzonego). Badaniom towarzyszyły pogłębione wywiady stanowiące typ „scenariuszy", opisujące poszczególne rodzaje zagrożeń np. technologicznych, które mogłyby doprowadzić do niekorzystnych skutków. Analiza opisów pozwala rozpoznać zagrożenia funkcjonujące w świadomości badanych, jak również poznać aspekty charakterystyczne podejmowanych działań w czasie wystąpienia zagrożenia.

Badani poproszeni byli o ocenę zagrożeń odpowiednio do postrzegania zjawiska, przydzielając punkty w skali od 0-5, gdzie 0 oznaczało brak zagrożenia lub zagrożenie pomijalne, natomiast 5 oznaczało wysoki stopień zagrożenia. Listę zagrożeń można było uzupełnić o własną propozycję. W obszarze zagrożeń informacyjnych dla bezpieczeństwa narodowego wyróżniono zagrożenia przedstawione w tabeli 3-30.

---

[186] Spam stanowił 82,1% wszystkich wiadomości e-mail, o 2,1% więcej niż w 2007r. Wzrosła ilość spamu kierowanego do użytkowników portali społecznościowych oraz ilość spamu na takich portalach. Wzrosła popularność spamu zachęcającego użytkowników do wysyłania kosztownych wiadomości tekstowych na krótkie numery.

[187] Dzięki stosowaniu np. technik inżynierii społecznej.

[188] M.Goszczyńska, Człowiek wobec zagrożeń. Uwarunkowania oceny i akceptacji ryzyka. Wyd. Żak, Warszawa 1997, s.128.

Tabela 3-30. Zagrożenia bezpieczeństwa narodowego w obszarze informacyjnym

LP.	ZAGROŻENIA
1	Cyberteroryzm (infoteroryzm)
2	Zakłócenia krytycznej infrastruktury państwa RP
3	Hackerstwo
4	Przechwytywanie danych
5	Oszustwa bankowe
6	Ograniczony dostęp do informacji
7	Spam - rozsyłanie niechcianej poczty elektroniczne
8	"Wojny (cybernetyczne) hakerskie" (np.Estonia) (cyberwar)
9	Cybernetyczny atak na szczeblu państwowym
10	Blokady serwerów rządowych RP
11	Podsłuchiwanie transmisji w sieci
12	Trojan / konie trojańskie
13	Sabotaż komputerowy
14	Zniszczenie danych lub programów komputerowych
15	Atak na serwer (WWW, DNS, inne...)
16	Atak na system operacyjny
17	Inżynieria społeczna *(Social engineering)*

Źródło: opracowanie własne.

Do analizy wzajemnych zależności posłużono się współczynnikami korelacji. Do testowania istotności wykorzystano rozkład t studenta oraz χ^2. Intencją tego pytania była chęć poznania czy w świadomości badanych istnieje pojęcie bezpieczeństwa informacyjnego i czy niepokoje związane z zagrożeniami informacyjnymi wywołują zaniepokojenie. Wśród badanych 50% wyraża niewielkie obawy o stan bezpieczeństwa informacyjnego, natomiast 39% duże, po 4% badanej populacji wyraziło zarówno bardzo duże obawy jak i brak obaw. 4% było nie zdecydowanych.

Tabela 3-31. Osobiste niepokoje - procentowy rozkład odpowiedzi

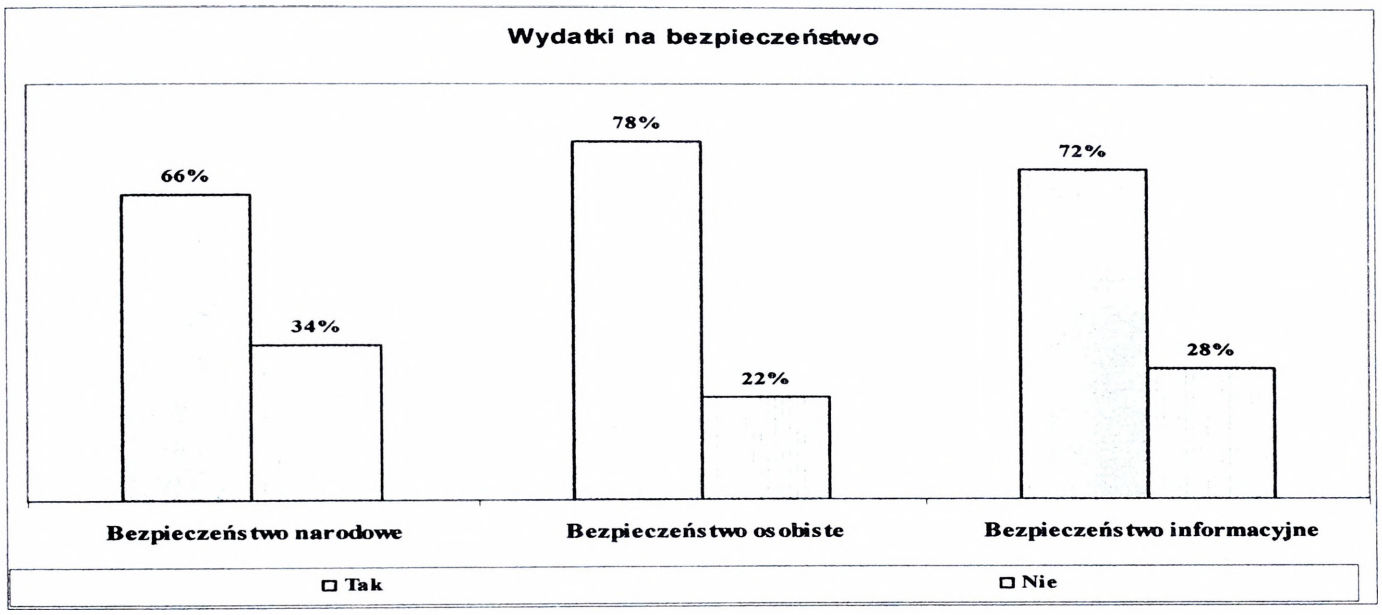
Czy pana(i) obawy i niepokoje o stan bezpieczeństwa informacyjnego są:	N=480
Bardzo duże obawy i niepokoje	4%
Duże obawy i niepokoje	39%
Niewielkie obawy niepokoje	50%
Brak obaw i niepokojów	4%
Trudno powiedzieć	4%

Źródło: opracowanie własne.

Wpływ rodzajów studiów reprezentowanych przez badanych na wyrażanie obaw i niepokojów okazał się niewielki. Tylko w grupie badanych reprezentujących studia techniczne

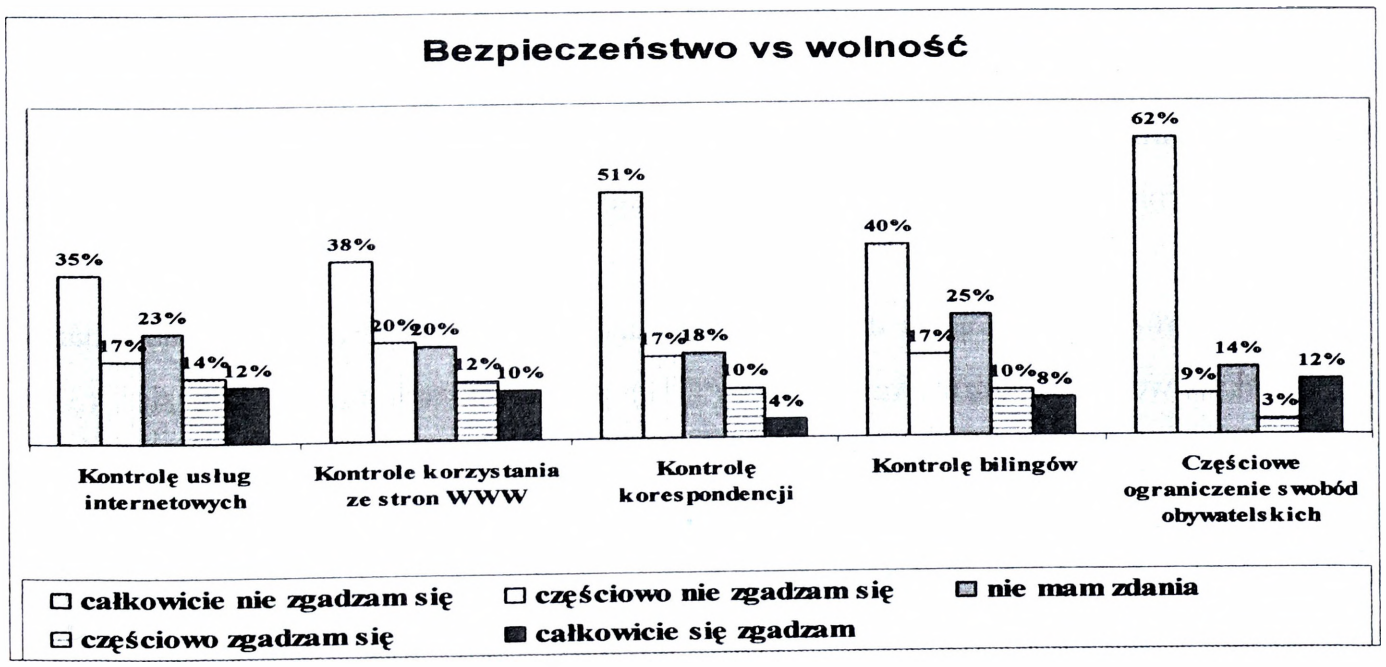
rozpoznawalność zagrożeń (p<0,1, *df*=20) była większa niż w przypadku badanych kierunków studiów humanistycznych.

Pomimo, iż 50% badanych ujawniło, że w niewielkim stopniu wyraża obawy o stan bezpieczeństwa to w odpowiedzi na pytanie: czy w zamian za zwiększenie poczucia bezpieczeństwa uznał(a)by Pan(i) za słuszne zwiększenie wydatków na bezpieczeństwo, badani byli zgodni, co do tego, że ponieśliby wydatki (rysunek 3-39).



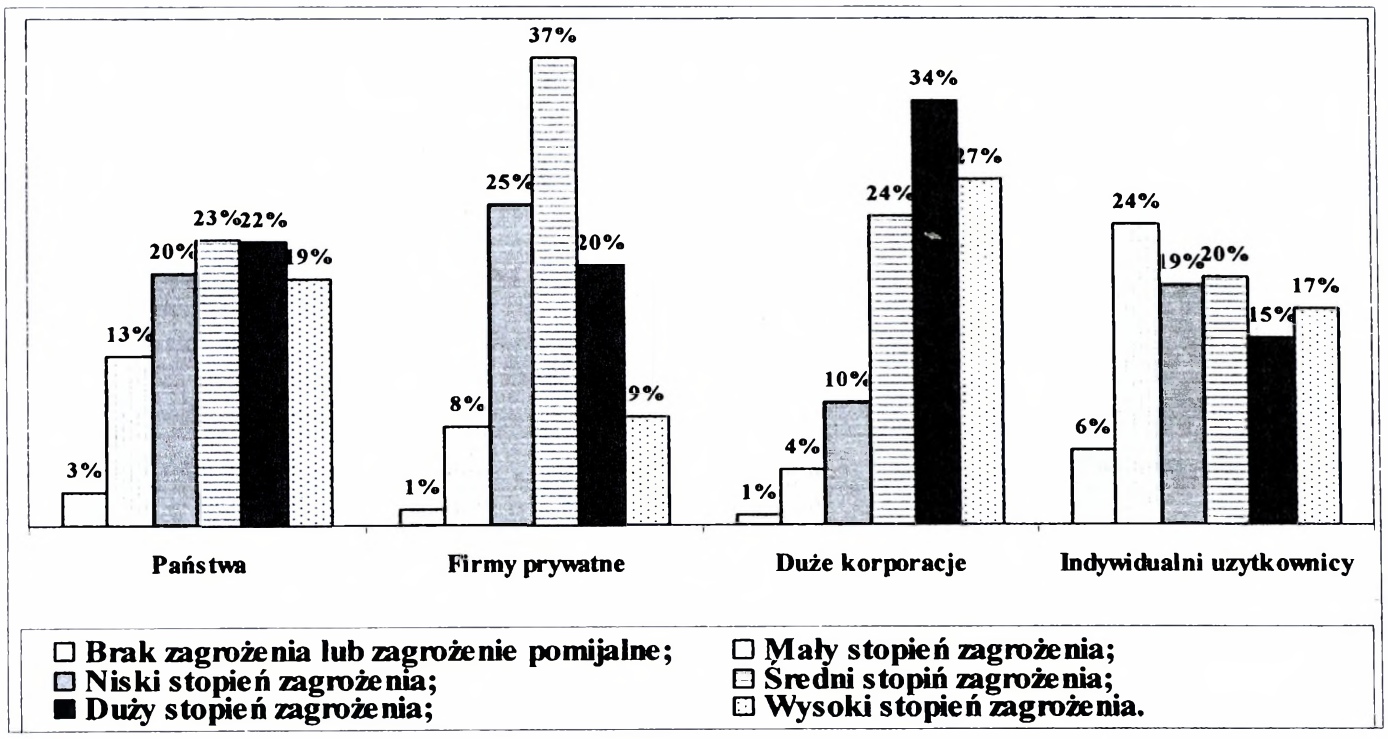
Rysunek 3-39. Procentowy rozkład odpowiedzi wydatki na bezpieczeństwo
Źródło: opracowanie własne.

W imię bezpieczeństwa badani skłonni byliby na ograniczenia: 62% badanych zgodziłoby się na częściowe ograniczenie swobód obywatelskich (12% byłoby całkowicie przeciwnych), 51% na kontrolę korespondencji, 40% na kontrolę bilingów, 38% kontrolę korzystania ze stron WWW, a 35% kontrolę usług internetowych (rysunek 3-40).



Rysunek 3-40. Procentowa analiza odpowiedzi o wyrażenie zgody na ograniczenia
Źródło: opracowanie własne.

Na zagrożenia informacyjne najbardziej narażone są duże korporacje: 34% badanych wyraziło taką opinię, a 27% uznało, że korporacje są w wysokim stopniu narażone na ataki. Firmom prywatnym przypisano średni stopień zagrożenia (37%), ¼ badanych uznała za stopień niski. W przypadku indywidualnych użytkowników badani najczęściej wybierali odpowiedź, że zagrożenia te są w małym stopniu dokuczliwe. W przypadku zagrożeń, w stosunku do państwa, po około 20% badanych udzieliło odpowiedzi przypisując zagrożenia zarówno: niskiemu, średniemu, dużemu i wysokiemu stopniowi (rysunek 3-41).

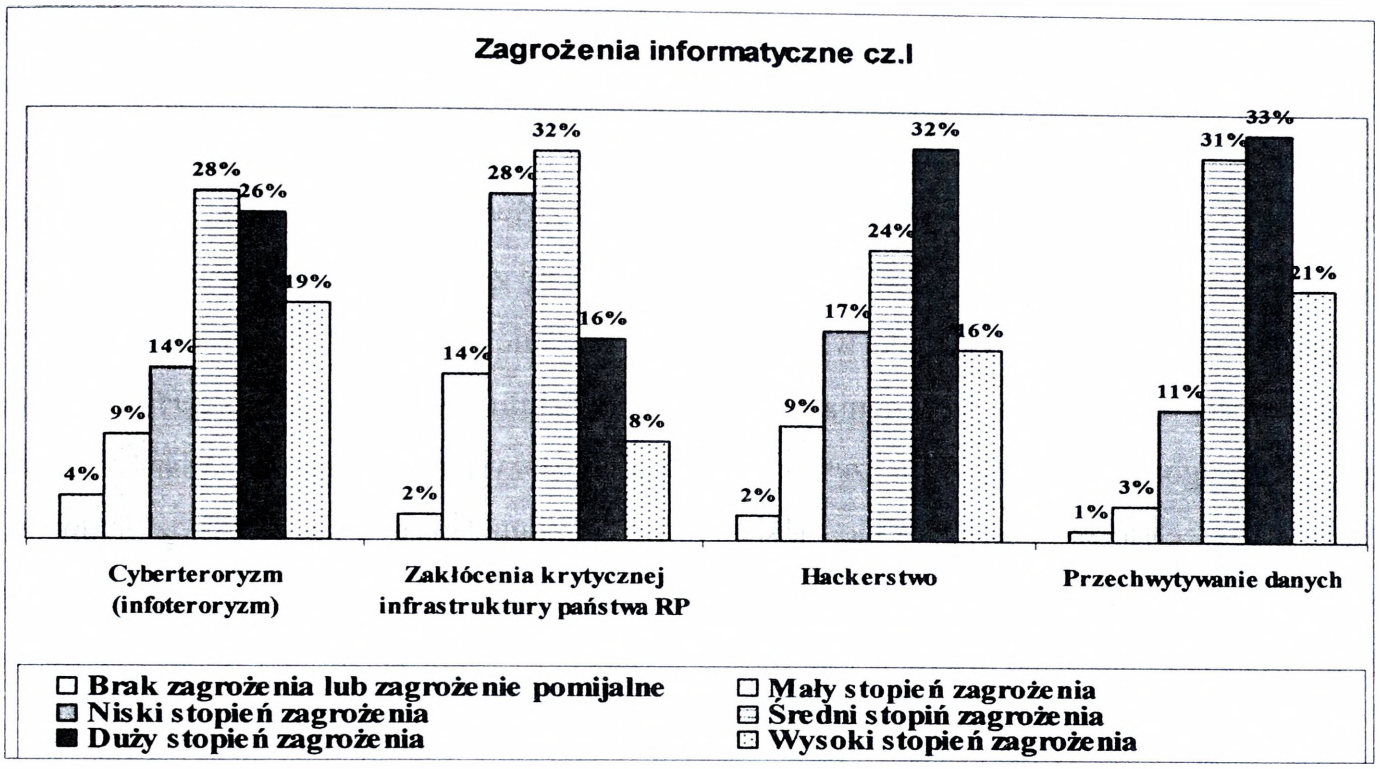


Rysunek 3-41. Analiza procentowa odpowiedzi o instytucje, które najbardziej narażone są na ataki
Źródło: opracowanie własne.

Wśród wyspecyfikowanych zagrożeń za niebezpieczne w wysokim stopniu badani uznali spam, czyli rozsyłanie niechcianej poczty elektronicznej. Zagrożenie jest szczególnie dokuczliwe i powszechne. Ze spamem ludzie mają do czynienia, na co dzień, są to nie tylko niechciane informacje, występuje coraz więcej listów, które nie są reklamami, ale oszustwami z zakresu inżynierii społecznej bazującej na cechach ludzkiego charakteru: ciekawości czy chciwości.

Za zagrożenia w stopniu dużym, badani uznali takie jak: przechwytywanie danych (33%), hakerstwo (32%), oszustwa bankowe (33%), podsłuchiwanie transmisji w sieci (37%), złośliwe oprogramowanie w formie koni trojanów (27%), cybernetyczny atak na szczeblu państwowym (26%), zniszczenie danych lub programów komputerowych (37%), ataki na serwer WWW, DNS, i inne (30%). Ataki na system operacyjny w celu przejęcia kontroli nad nimi również został zaklasyfikowany do ataków o dużym stopniu niebezpieczeństwa.

Cyberterroryzm (28%), zakłócenia krytycznej infrastruktury państwa RP (32%), ograniczony dostęp do informacji (26%), blokady serwerów rządowych (25%), wojny (cybernetyczne) hakerskie (32%), sabotaż komputerowy (33%), social engineering (30%), postrzegane są w średnim stopniu zagrożenia (rysunki 3-42, 3-43 i 3-44).



Rysunek 3-42. Rozkład procentowy postrzeganie zagrożeń informatycznych cz. 1
Źródło: opracowanie własne.

Rozpatrując rozkład odpowiedzi w badaniu dotyczącym cyberterroryzmu, należy zauważyć, że chociaż najczęstszą odpowiedzią był wybór średniego stopnia zagrożenia (tabela 3-32), daje się zauważyć, że w przypadku 26% zagrożenie to postrzegane jest w stopniu dużym, a dla 19% w stopniu wysokim. Cyberterroryzm jest coraz częściej postrzegany jako zagrożenia nie tylko dla bezpieczeństwa narodowego, ale również jako niebezpieczeństwo dla indywidualnego członka społeczności internetowej. Unieruchomienie banków, instytucji państwowych grozi paraliżem obsługi klientów i stratą finansową np. z powodu niemożności wykonywania pracy.

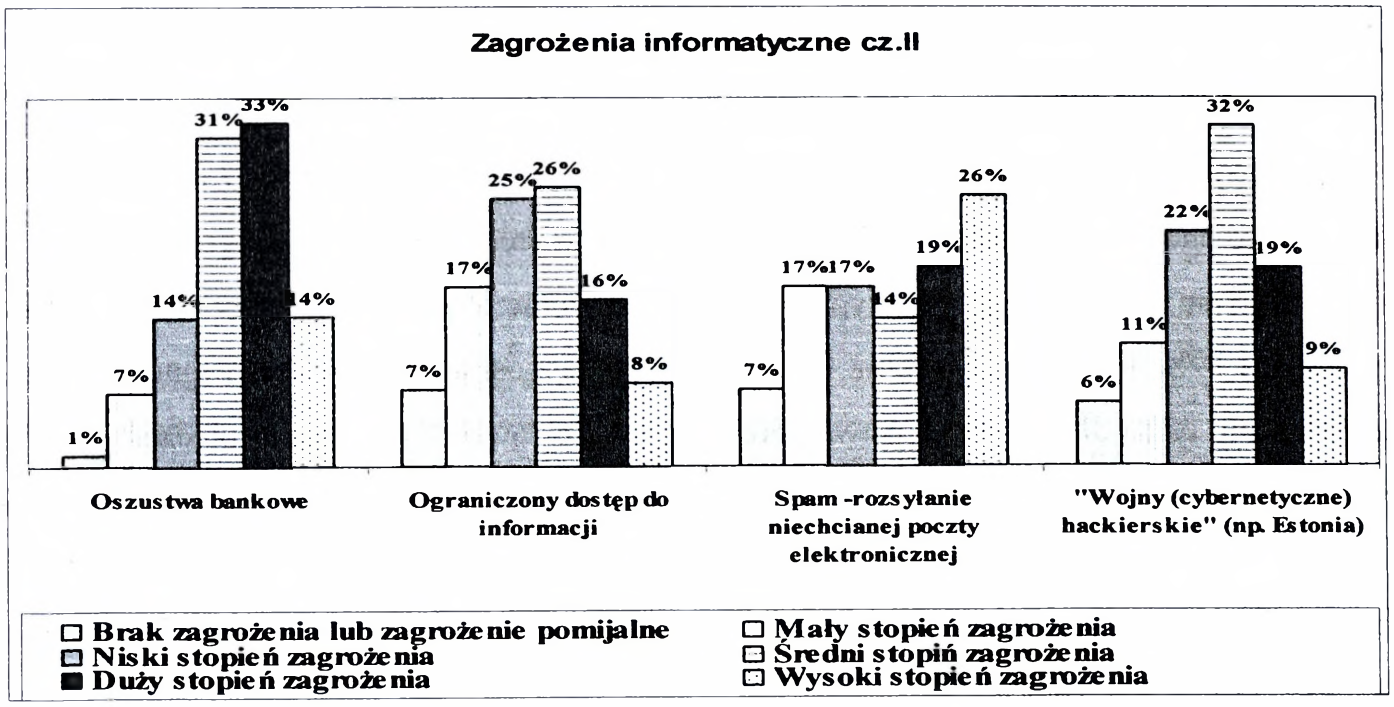
Tabela 3-32. Modalna dla zagrożenia cyberterroryzm

	Cyberterroryzm (infoterroryzm)
Nr ankiety	1
Średnia	3,23
Modalna	3

Stwierdzono istotny związek występowania hakerstwa z ograniczonym dostępem do informacji (df=25, p=0,02), a także ograniczonego dostępu do informacji a atakiem na serwer (df=25, p=0,01). Wzrost przestępstw związanych z hakerstwem powoduje wzrost ograniczenia dostępu do informacji. Wzrost ataków na serwer również skutkuje ograniczonym dostępem do informacji. Zależności występują również w wy-

padku spamu i ataku cybernetycznego na szczeblu państwowym (df=25, p=0,02), także spamu i blokady serwerów rządowych RP(df=25, p=0,02) (spam uznawany jest za narzędzie wykonywania ataku cybernetycznego, wzrost może sugerować atak). Wzrost spamu może skutkować blokadą serwerów rządowych.[189]

W rozkładzie chi kwadrat występuje również istotna zależność spamu i *social engineeringu* (df=25, p=0,01). W inżynierii społecznej jako instrumentu wywierania wpływu, wykorzystuje się spam odwołując się do natury człowieka. Zagrożenia, którym częściej ulęgają badani są lepiej postrzegane niż zagrożenia, o których mówi się mniej lub jest to wiedza dostępna wąskiemu gronu specjalistów. Osoby stykające się z określonymi zagrożeniami, mają skłonność do postrzegania przede wszystkim tych właśnie zagrożeń. Należy uznać za brak świadomości u badanych niedocenianie zagrożenia, jakim jest *social engineering*. Rodzaj ataku opartego na spamie jest najczęstszym sposobem pozyskiwania danych. Warto tutaj zaznaczyć, że celem socjotechnika nie musi być firma, mogą nim być np. banki czy jednostki samorządu terytorialnego, agendy rządowe, instytucje unijne oraz instytucje, które zgodnie z ich przeznaczeniem, powinny te informacje chronić. W wielu badaniach podkreśla się, że człowiek to najsłabsze ogniwo systemu bezpieczeństwa.[190]



Rysunek 3-43. Rozkład zagrożeń informatycznych cz. II

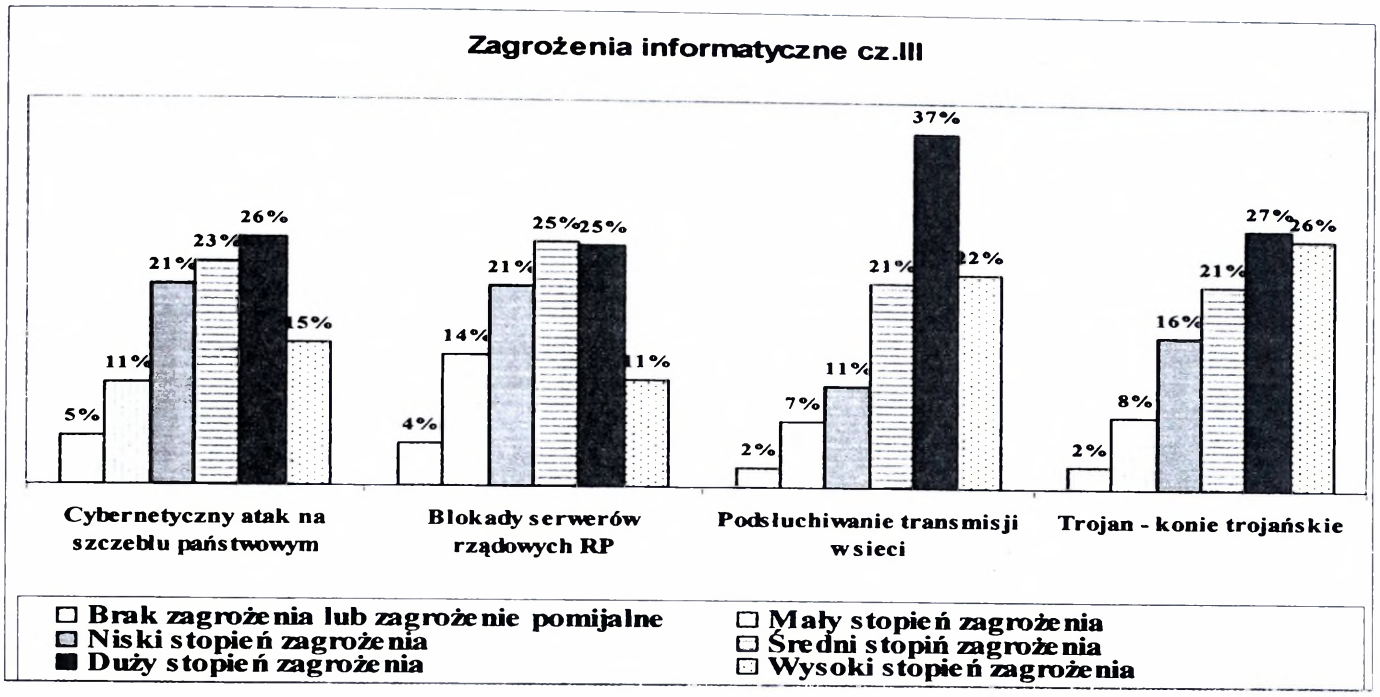
Źródło: opracowanie własne.

---

[189] Z taką sytuacja mieliśmy do czynienia w czasie konfliktu Rosja – Łotwa, Rosja – Gruzja, także podczas konfliktu Kossowskiego gdzie wystąpiły blokady serwerów NATO.

[190] Wiele firm np. Mcfee, F-Secure, Megapanel, Internetstat, Gemius dokonują regularnych badań nad rozwojem i bezpieczeństwem Internetu. Firma Trend Micro prowadzi i publikuje badaniach na temat bezpieczeństwa również na temat poczucia bezpieczeństwa w Internecie. Analizując wyniki stwierdziłam, że wskaźnik ilości użytkowników, którzy uważają korzystanie z Internetu za bezpieczne, waha się około 40 do 45% w państwach badanych (USA, Francja, Japonia i Niemcy). Od roku 2007 obserwuje się spadek zaufania do Internetu i wynosi około 35% (średnia dla wszystkich badanych państw).

Ograniczony dostęp do informacji przez 25% badanych postrzegany jest w stopniu niskim szkodliwości, a przez 26% w średnim stopniu szkodliwości w małym przez 17%, przy czym tylko dla 16% w dużym i 8% wysokim stopniu zagrożenia. Osoby, które zetknęły się z utrudnionym dostępem do sieci, znacznie częściej podkreślają wystąpienie tego ryzyka jako dotkliwego.



Rysunek 3-44. Rozkład zagrożeń informatycznych cz. III
Źródło: opracowanie własne.

Trojany od pojawienia się w sieci, przeszły podobnie jak inne zagrożenia ewolucję. Są szczególnie niebezpieczne,[191] zwłaszcza trojany bankowe, ponieważ powodują poważne straty wśród użytkowników finansowych usług internetowych na całym świecie. Stąd też w ocenie badanych przez 27% zagrożenie to zostało określone w dużym stopniu jako szkodliwe, przez 26% za wysoce szkodliwe, a 21% określiło to zagrożenie, w stopniu średnim.

Niebezpieczeństwo związane z podsłuchem transmisji danych w sieci[192] nie jest duże, a najbardziej narażeni na podsłuch są użytkownicy dużych sieci lokalnych (np. sieci osiedlowych).[193] Nie mniej jednak znajdują coraz bardziej niekonwencjonalne zastosowania (takie

---

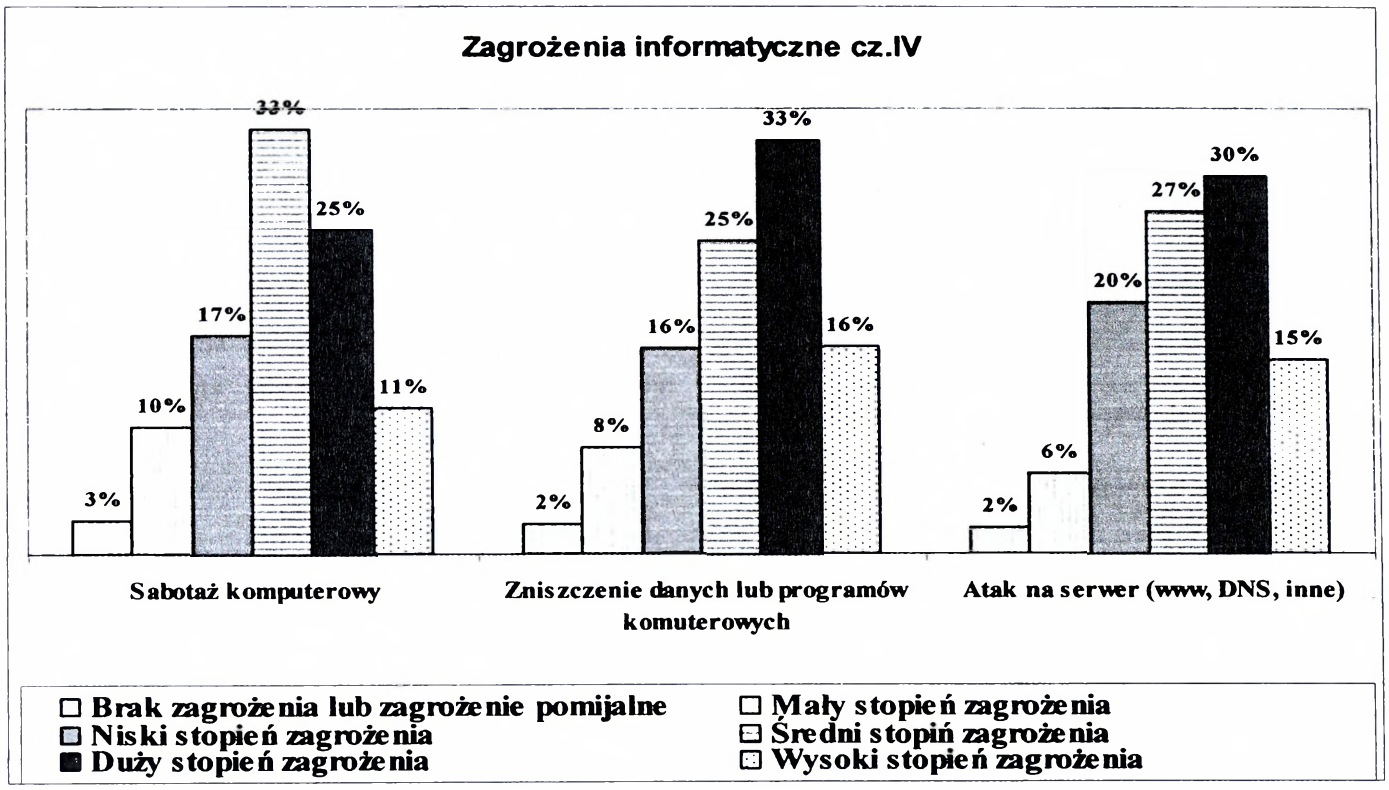
[191] Warto zaznaczyć, że trojany nie rozprzestrzeniają się na komputery ofiary samodzielnie. Mogą zostać zainstalowane przez złośliwe oprogramowanie, które jest już obecne w systemie, lub może przeniknąć przez luki w zabezpieczeniu przeglądarki.

[192] Znacznie większe niebezpieczeństwo stwarza posługiwanie SMS. Za pośrednictwem SMS prowadzi się komunikację biznesową, ujawnia podatną na przechwycenie informację (hasła, numery PIN itp.), czy też przesyła poufne raporty. Zastanawiający jest fakt dużego zaufania, jakie abonenci sieci komórkowych pokładają w usłudze SMS, bowiem zwykły SMS jest mechanizmem transmisyjnym całkowicie pozbawionym zabezpieczeń. Sytuacja taka wynika głównie z braku znajomości podstaw realizacji tej usługi wśród zwykłych użytkowników

[193] Zagrożenia dla Twojej prywatności w sieci [dostęp on line 20.03.2009] tp.pl/prt/pl/tpcert/bezpieczenstwo/zagrozenia/prywatnosc/prywatnosc_ogolne.

jak np. sterowanie botnetem, opisywane na łamach DI.[194] Zagrożenie podsłuchem 37% badanych określiło jako bardzo niebezpieczne, a 22% wysoce niebezpieczne i 21% postrzega to zagrożenie w średnim stopniu.

Postrzeganie zagrożenia, jakie stanowią blokady serwerów rządowych, wykazują bardzo regularny rozrzut odpowiedzi. Nasze społeczeństwo nie wykorzystuje w swojej działalności możliwości, jakie mogłaby wykorzystać, gdyby na stronach urzędów, agend, instytucji dostępna była bieżąca, wiarygodna informacja, jak również większość usług.



Rysunek 3-45. Rozkład zagrożeń informatycznych cz. IV
Źródło: opracowanie własne.

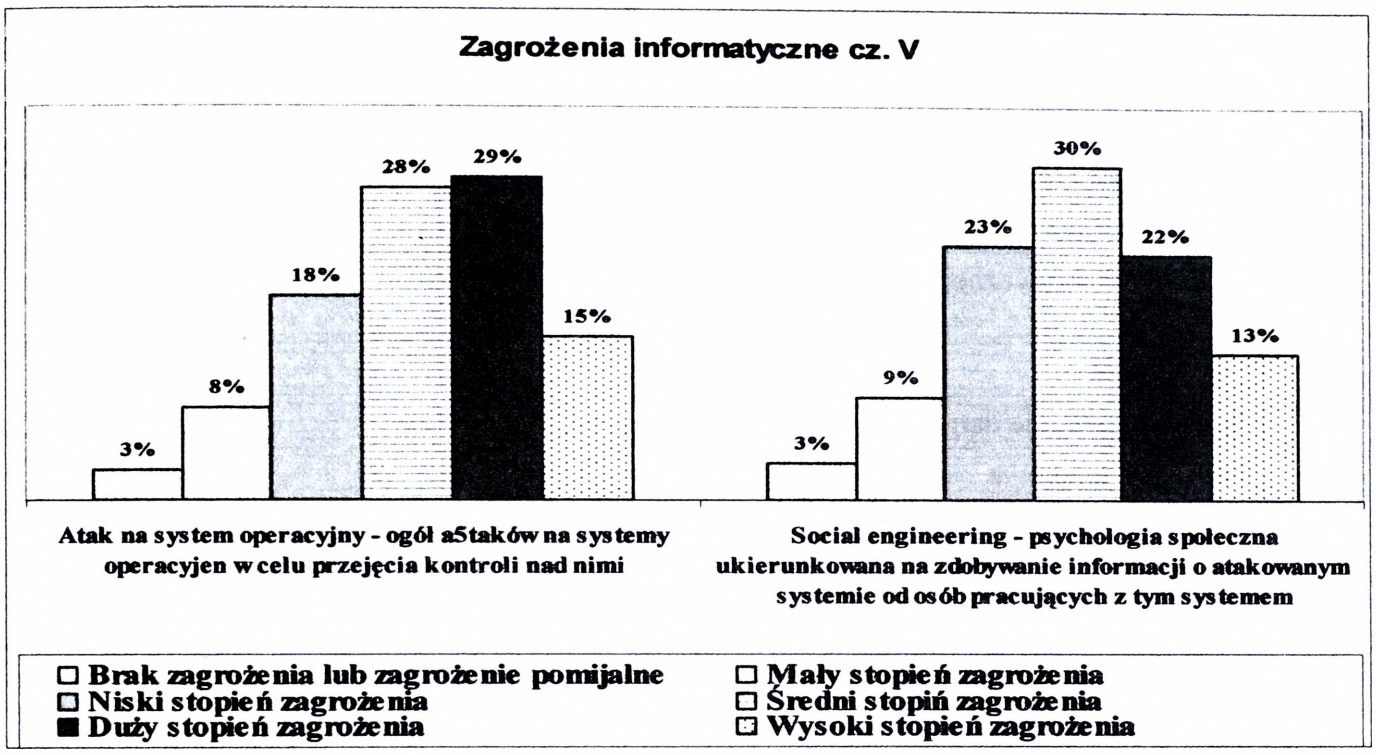
Sabotaż komputerowy jest jednym z najgroźniejszych ryzyk, związanych z wrogim działaniem zatrudnionych pracowników. Każda forma sabotażu jest dla organizacji wysoce szkodliwa, niezależnie od tego, czy jest to kradzież, czy ośmieszanie, zniechęcanie klientów, czy zaniechanie jakiejś czynności, która powinna być wykonana, czy też mechaniczne zniszczenie. W takiej sytuacji system monitorowania jest jednym ze skuteczniejszych sposobów zabezpieczeń. Przez 33% badanych sabotaż postrzegany jest jako średnie zagrożenie, przez 25% jako zagrożenie duże (rysunek 3-45).

Ataki na serwer WWW[195], ograniczające dostęp do informacji, DNS[196] postrzegane są przez 30% jako w dużym stopniu zagrażające, tylko 15% badanych uważa je za wysoce niebezpieczne, a dla 20% stanowią niski stopień zagrożenia.

---

[194] http://di.com.pl/news/12634,0.html. Usługi telefonii internetowej (VoIP) mogą pomagać internetowym przestępcom przy wysyłaniu spamu i atakach DoS.

Zniszczenie danych i programów komputerowych dla 33% stanowi duże zagrożenie, dla 16% wysokie, a dla 25% średnie.



Rysunek 3-46. Rozkład zagrożeń informatycznych cz. V
Źródło: opracowanie własne.

Rozkład opinii dotyczącej ataków na system operacyjny pokrywa się z ocenami ataków na serwer WWW, DNS i jest potwierdzeniem normalności rozkładu. Rozkład dotyczący oceny zjawiska *social engineering* jest podobny do rozkładu (rozkład normalny) opinii nt. sabotażu (rysunek 3-46). Modalna (3) określa najczęściej wybieraną odpowiedź, czyli średni stopień zagrożenia (tabela 3-33). Dla 22% zjawisko postrzegane jest w dużym stopniu zagrożenia, a przez 13% w wysokim.

Tabela 3-33. Modalna dla social engineering

	social engineering
Nr ankiety	17
Średnia	2,97
Modalna	3

Źródło: opracowanie własne.

Na podstawie otrzymanych wyników badań dokonano klasyfikacji zagrożeń w opaciu o najczęściej wybieraną odpowiedź. Uszeregowano zagrożenia jednocześnie przypisując im prawdopodobieństwa wystąpienia. Przykład jest propozycja wykorzystania badania sondażo-

---

[195] Może być to podmiana strony, zablokowanie serwisu – jest dokuczliwe ale nie takie groźne.

[196] Taki atak może polegać na zatruwaniu pamięci serwera DNS (ang. *cache poisoning*), co umożliwia cyberprzestępcy przekierowanie nieświadomego internauty pod fałszywy adres IP, aby wyłudzić od niego poufne dane lub zainfekować jego maszynę szkodliwym oprogramowaniem.

wego do budowania skal prawdopodobieństwa zdarzeń, które można wykorzystać w prognozowaniu scenariuszowym. Przyjmując, że stwierdzone[197] prawidłowości mają najwyższy stopień prawdopodobieństwa[198], arbitralnie przypisano je odpowiedzią (tabela 3-34).

Tabela 3-34. Wyznaczanie prawdopodobieństwa w oparciu o częstość występowania zagrożenia

LP.	ZAGROŻENIA	CZĘSTOŚĆ	PRAWDOPODOBIEŃSTWO
1	Cyberteroryzm (infoteroryzm)	3	0,7
2	Zakłócenia krytycznej infrastruktury państwa RP	3	0,7
3	Hackerstwo	4	0,9
4	Przechwytywanie danych	4	0,9
5	Oszustwa bankowe	4	0,9
6	Ograniczony dostęp do informacji	3	0,7
7	Spam - rozsyłanie niechcianej poczty elektroniczne	5	1
8	"Wojny (cybernetyczne) hakerskie" (np.Estonia) (cyberwar)	3	0,7
9	Cybernetyczny atak na szczeblu państwowym	3	0,7
10	Blokady serwerów rządowych RP	4	0,9
11	Podsłuchiwanie transmisji w sieci	3	0,7
12	Trojan / konie trojańskie	4	0,9
13	Sabotaż komputerowy	3	0,7
14	Zniszczenie danych lub programów komputerowych	4	0,9
15	Atak na serwer (WWW, DNS, inne...)	4	0,9
16	Atak na system operacyjny	4	0,9
17	Inżynieria społeczna *(Social engineering)*	3	0,3

Źródło: opracowanie własne.

Świadomość niebezpieczeństw informacyjnych oraz skutków realizacji tych ryzyk jest dalece niewystarczająca. Potwierdzają to badania prowadzone przez wyspecjalizowane firmy jak np. Security Standard, która w raporcie o zagrożeniach bezpieczeństwa pochodzących z Internetu dla Polski, w 2007 roku opublikowała ranking. Ranking nie dość, że potwierdza istniejące zagrożenia, to potwierdza również, że Polska „internetowa" jest również niebezpieczna dla innych indywidualnych, instytucjonalnych i państwowych użytkowników sieci (tabela 3-35).

[197] W odniesieniu do przeprowadzonego sondażu.
[198] Ograniczone doborem próby.

Tabela 3-35. Miejsce Polski w rankingu zagrożeń

LP	MIEJSCE W RANKINGU	ZAGROŻENIE
1	1 miejsce	(86%) wśród krajów odbierających największą ilość spamu;
2	2 miejsce	(11%) wśród krajów o największej intensywności destrukcyjnej działalności przypadającej na jednego użytkownika Internetu. Pierwsze miejsce przypadło Izraelowi (19%);
3	2 miejsce	(11%) wśród krajów o największej ilości komputerów-zombie. Pierwsze miejsce przypadło dla Niemiec (17%);
4	3 miejsce	(8%) wśród krajów, z których pochodzi największa ilość wysyłanego spamu. Na pierwszym miejscu znalazły się wszystkie niezidentyfikowane kraje z regionu EMEA (21%);
5	6 miejsce	(5%) wśród krajów o największej intensywności destrukcyjnej działalności. Pierwsze miejsce zajęły Niemcy (19%);
6	6 miejsce	(4%) wśród krajów przechowujących na serwerach strony służące do ataków typu „phishing". Pierwsze miejsce dla Niemiec (22%)
7	7 miejsce	(6%) wśród krajów zainfekowanych sieciami bot. Na pierwszym miejscu znalazły się Niemcy (23%);
8	8, 9 i 10 miejsce	odpowiednio dla Warszawy, Katowic oraz Poznania jako miast z największą ilością komputerów-zombie. Pierwsze miejsce przypadło Madrytowi (Hiszpania);
9	9 miejsce	dla Warszawy jako miasta z największą ilością komputerów zainfekowanych sieciami bot. Pierwsze miejsce przypadło Madrytowi (Hiszpania);
10	10 miejsce	(1%) wśród krajów, z którego pochodzi największa ilość ataków skierowanych na region EMEA. Pierwsze miejsce zajęły Stany Zjednoczone (35%);
11	10 miejsce	(2%) wśród krajów, w które wymierzano ataki typu „odmowa usługi" (*Denial of Service*). Pierwsze miejsce przypadło Wielkiej Brytanii (46%).

Źródło: *http://securitystandard.pl/katalog/katalog.asp?c=313*

3.5. Scenariusze zagrożeń informacyjnych[199]

Jedną istotnych metod radzenia sobie z trudno przewidywalnymi zagrożeniami jest metoda prognozowania scenariuszowego. Metoda oprócz antycypacyjnego myślenia może służyć w edukacji jako czynnik nabywania kompetencji w rozpoznawaniu sytuacji zagrożeń, budowaniu strategii przeciwdziałania lub strategii postępowania w sytuacji wystąpienia ryzyka.

Pierwotnie metoda budowania scenariuszy pojawiła się jako narzędzie planowania strategicznego w pracach C.Von Clausewtiz'a i Moltke[200]. Współczesną formę przedstawiania przyszłości zaproponował H. Kahna (1967 r.) pod nazwą „pisania scenariuszy" (ang. *Scenariowritting*), opartych na logice intuicyjnej (ang. *Intuitive Logics*). Równolegle rozwijana była

---

[199] Wykorzystano autorski podrozdział 9 pt. *Metody scenariuszowe*. [w:] pracy naukowo-badawczej pod red. P.Sienkiewicza nt. *Wybrane metody naukowych badań nad bezpieczeństwem i obronnością. Studium metodologiczne.* AON, Warszawa 2008, s.219-237.

[200] K.Czaplicka, N.Howaniec, A.Smoliński, *Budowa scenariuszy dla potrzeb forsieghtu technologicznego*. [dostęp online:] http://www.foresightenergetyczny.pl/

metoda budowania scenariuszy w oparciu o tzw. probabilistyczną modyfikację trendów PMT (ang. *The probabilistic modified trends school*) oraz metody wykorzystujące symulację komputerową. Praktyka stosowania tych metod przyniosła wiele różnych technik budowania scenariuszy. Chociaż metoda scenariuszowa wywodzi się z badań wojskowych obecnie z powodzeniem stosowana jest: w prognozowaniu ekonomicznym, w zarządzaniu kryzysowym, polityce społecznej, edukacji i biznesie.

Wynikiem końcowym w metodzie opartej na logice intuicyjnej jest zestaw scenariuszy, jednakowo prawdopodobnych, zaś w metodzie opartej na PMT otrzymuje się zestaw scenariuszy najbardziej prawdopodobnych. Istota metody zawiera się w projekcji (zbioru obrazów) dowolnego systemu lub przewidywanych sytuacji. Wielu autorów sugeruje potrzebę, przygotowywania wielu rozmaitych wersji scenariuszy oraz budowania dla każdego z nich wariantów planu rozwoju (strategii działania). Sposób podejścia do budowy scenariuszy pozwala wyróżnić cztery postawy wobec przyszłości: (1) bierną, (2) adaptacyjną, (3) prognostyczną, (4) kreatywną (tabela 3-36)[201]. Za wyjątkiem postawy biernej pozostałe uzupełniają się - są komplementarne.

Istota metody

Metoda opiera się na założeniu, że przyszłości nie da się przewidzieć z całą pewnością, lecz należy ją projektować. Metoda scenariuszy stanowi specyficzną kombinację różnych technik, stosowanych indywidualnie dla każdego zadania prognostycznego, przy czym łączą je pewne ogólne zasady[202].

Tabela 3-36. Postawy wobec przyszłości w technice pisania scenariuszy

POSTAWA WOBEC PRZYSZŁOŚCI	CHARAKTERYSTYKA POSTAWY
Bierna (oportunistyczna)	Poddająca się całkowicie biegowi wydarzeń, będąca w pewnym sensie wyrazem filozofii fatalistycznej.
Adaptacyjna	Polegająca na optymalizowaniu aktualnego działania, tak aby efekty były lepiej przystosowane do przewidywanej przyszłości.
Prognostyczna	Polega na ekstrapolacji możliwego stanu rzeczy, w danym przyszłym momencie, przy założeniu kontynuacji aktualnych tendencji.
Kreatywna	Planowanie wielu wizji przyszłości.

Źródło: na podstawie: A. Stabryła, *Zarządzanie projektami ekonomicznymi i organizacyjnymi*, PWN, Warszawa 2006.

[201] Zob. A.Stabryła, Zarządzanie projektami ekonomicznymi i organizacyjnymi, PWN, Warszawa 2006, s.258.

[202] Zob. M. Cieślak (red. nauk.), *Prognozowanie gospodarcze. Metody i zastosowania*, PWN, Warszawa 1997.

W podejściu twórczym (wg. H. Khana) stosujemy słowną formą przekazu treści scenariusza, której istotą jest tworzenie modelu myślowego (wizji) poddawanego intuicyjnej symulacji przyszłych zdarzeń. W rezultacie uwaga koncentruje się na opisie prawdopodobnych zdarzeń i ich logicznych następstwach (rozwoju systemu, organizacji, procesu) dla których buduje się alternatywne ciągi zdarzeń. Natomiast istota podejścia opartego na modelach formalnych, polega na wyodrębnieniu zbioru zmiennych charakteryzujących dynamikę zmian badanego obiektu (systemu), oraz identyfikacji zbioru zdarzeń. Istotne zmiany wartości zmiennych łączone są parami w logiczne ciągi, z określeniem prawdopodobieństwa ich wystąpienia (najczęściej przez ekspertów, a więc prawdopodobieństwa subiektywnego). Następnie dokonuje się szacowania (obliczania) prawdopodobieństwa łącznego zajścia par zdarzeń lub ich całych ciągów (np. za pomocą metody Bayesa).

Prognozy wyznaczone metodą scenariuszy charakteryzują takie cechy, jak:

– złożoność obiektów - przedmiotów scenariuszy czyli duża liczba opisujących je zmiennych (endo- i egzogenicznych);

– uwzględnianie wpływu otoczenia na zmienne wewnętrzne obiektu;

– wielowariantowość (wieloaspektowość), alternatywne spojrzenie na przyszłość;

– bogaty zestaw stosowanych technik diagnostycznych i prognostycznych;

– jakościowy opis obiektu w przyjętym horyzoncie czasowym, (chociaż dopuszczalne są np. ilościowe metody przyczynowo-skutkowe typu ekonometrycznego).

Pojęcie scenariusza

Scenariusz jest opisem przyszłej, możliwej i prawdopodobnej sytuacji charakteryzującej zjawiska (obiekt, system, proces), stanowiące obiekt badań. Przedstawia on ciąg stanów (zdarzeń), który prowadzi do przewidywanej sytuacji. Ukazuje możliwości zaistnienia pewnych stanów i rozwoju zdarzeń (zmiennych zależnych), które warunkują przyszłe stany obiektu (systemu) i jego możliwe zachowanie (funkcjonowanie) w otoczeniu. Scenariusz to uporządkowany i spójny opis możliwej lub pożądanej przyszłości badanego obiektu, skonstruowany przy pomocy logicznego ciągu zdarzeń i procesów. Zwraca się uwagę na rozróżnienie między scenariuszem możliwym, a scenariuszem pożądanym, bowiem scenariusze możliwe nie zawsze będą pożądane, a pożądane nie zawsze będą miały szansę powodzenia[203].

Scenariusze zawierają informacje o: (1) hipotetycznych sytuacjach jakie mogą wystąpić w kolejnych etapach (fazach); (2) istniejących (rekomendowanych) wariantach następstw dla każdego zdarzenia, i w każdej fazie analizy itp.

---

[203] P. Sienkiewicz, *Analiza systemowa*...., AGH, op.cit.

Typologię scenariuszy zaproponowano w opracowaniu: *Budowa scenariuszy dla potrzeb Foresightu technologicznego*[204]. Typologia ta stanowi treść załącznika IX.

Rodzaje metod scenariuszowych

Wśród scenariuszy wyróżnia się cztery podstawowe typy, których kombinacje (tabela 3-37), umożliwiają wyróżnienie scenariuszy o charakterze mieszanym, można je z powodzeniem wykorzystać w fazie badania otoczenia, formułowania strategii czy sprawdzania poprawności analizy.

Tabela 3-37. Kombinacje scenariuszy

SCENARIUSZ	EKSPLORACYJNY (BADAWCZY, ODKRYWCZE)	ANTYCYPACYJNY
DESKRYPTYWNY (OPISOWY)	dla danych przyczyn → jakie będą efekty?	dla danych efektów → jakie są przyczyny?
NORMATYWNY (WARTOŚCIUJĄCY)	dla danych środków → jakie cele będą osiągnięte?	dla danych celów → jakich środków powinniśmy użyć?

Źródło: M. Cieślak (Red.), Prognozowanie gospodarcze. Metody i zastosowania. PWN, Warszawa, s. 192, z drobnymi zmianami.

W ujęciu systemowym z założenia prospektywnym preferowane jest „pisanie przyszłości", z kolei scenariusze eksploracyjne odpowiadają scenariuszom prospektywnym, zaś scenariusze antycypacyjne - retrospektywnym (tabela 3-38).

Tabela 3-38. Typologia scenariuszy

PODEJŚCIE	RODZAJE SCENARIUSZY	CELE BUDOWY	ZAŁOŻENIA WIODĄCE	CECHY PROCEDURY
Prospektywne pisanie scenariusza „do przodu"	Scenariusz projekcyjny Scenariusz alternatywnych „dopuszczalnych" wariantów przyszłości	Określenie najbardziej prawdopodobnej przyszłości. Określenie ograniczeń w przestrzeni możliwych rozwiązań.	Dominacja dotychczasowych tendencji rozwojowych	Analiza trendów i mechanizmów je generujących. Wprowadzanie krańcowych hipotez o kształtowaniu się parametrów trendów.
Retrospektywne pisanie scenariusza „do tyłu"	Scenariusz normatywny Scenariusz kontrapunktowy	Określenie pożądanej i możliwej przyszłości oraz dróg realizacji Określenie cech przyszłości w punktach granicznych	W momencie wyjściowym można określić osiągane cele W momencie wyjściowym można określić relacje celów pożądanych do możliwych.	Synteza celów i identyfikacja relacji między teraźniejszością pożądaną (zakładaną) przyszłością)

Źródło: J.Kisielnicki *„Metody systemowe"*, s.159.

[204] K.Czaplicka i in., *Budowa*,..., op.cit. (http://www.foresightenergetyczny.pl/)

Praca nad scenariuszami wymaga analizy dotychczasowego rozwoju zjawiska (obiektu, systemu) w celu identyfikacji występujących w nim prawidłowości, poznania ich logiki i opisu możliwych stanów przyszłości, także w sytuacji, gdy dotychczasowe tendencje rozwojowe zostaną zakłócone. Scenariusz jest w znacznym stopniu koncepcyjnym opisem przyszłości przedstawianej w formie zależności przyczynowo-skutkowych, formalno-prawnych, czasowego następstwa, prawdopodobieństwa warunkowego, niepewności, konieczności i ryzyka).

Punktem wyjścia do sporządzenia scenariuszy może być, np. sytuacja bieżąca i dominujące tendencje na rynku (scenariusze eksploracyjne), lub pożądany obraz przyszłości (scenariusze antycypacyjne). Scenariuszami przyszłości są również te, które obiektywnie opisują sekwencje możliwych zdarzeń, niezależnie od tego, czy są one pożądane, czy nie (scenariusze deskryptywne) oraz te, które skupiają się na wartościowaniu zakładanych zdarzeń (scenariusze normatywne).

W praktyce prognostycznej stosuje się różne rodzaje i typy scenariuszy, których konstrukcje są odmienne zaś dobór ich do badań zależy przede wszystkim od charakteru (specyfiki) badanych obiektów (systemu, procesów), a także innych uwarunkowań np. finansowych, politycznych, technologicznych.

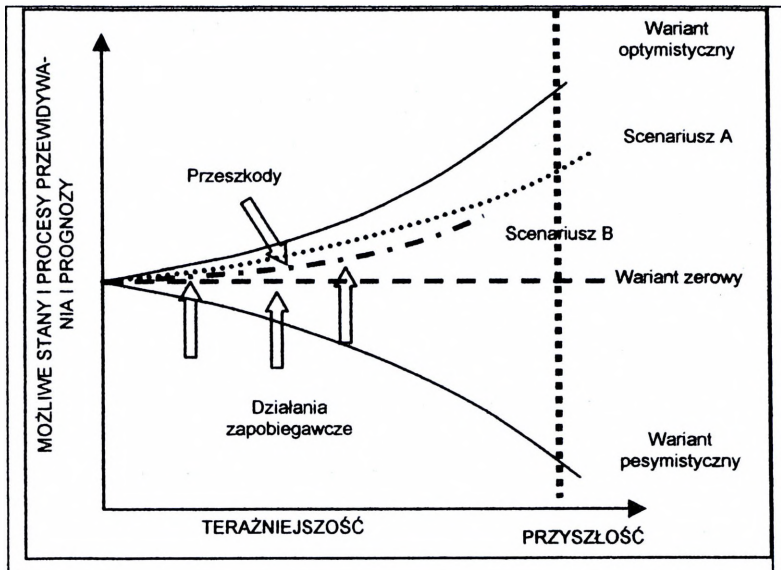
Ze względu na stopień prawdopodobieństwa lub skalę preferencji można dokonać podziału scenariuszy na (tabela 3-39):

Tabela 3-39. Charakterystyka scenariuszy

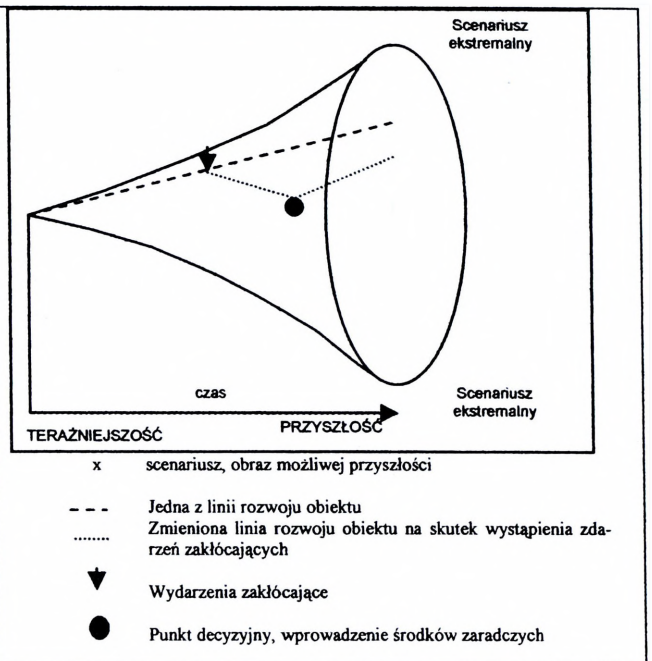
SCENARIUSZ	CHARAKTERYSTYKA
scenariusze optymistyczne	bierze on pod uwagę najwyżej ocenioną tendencję zmian każdego czynnika
scenariusze pesymistyczne	bierze pod uwagę najniżej ocenioną tendencje zmian każdego czynnika
scenariusze najbardziej prawdopodobne	bierze pod uwagę taką tendencję zmian, której przypisano najwyższe prawdopodobieństwo wystąpienia;
scenariusz „niespodziankowy"	bierze pod uwagę ten trend, dla którego określono najmniejsze prawdopodobieństwo wystąpienia

Źródło: opracowanie własne.

„Lejek scenariusza" pokazuje, że wychodząc od stanu aktualnego można otrzymać wiele różnych scenariuszy opisujących przyszłość. Mogą to być scenariusze ekstremalne (optymistyczny lub pesymistyczny), leżące na brzegu lejka i scenariusze pośrednie, ujmujące różnorodne zakłócenia na ścieżce rozwoju obiektu, zawierające jednocześnie środki zaradcze przeciwdziałające tym zakłóceniom (rysunek 3-47 i 3-48).



Rysunek 3-47. Scenariusze rozwoju otoczenia
Źródło: P.Sienkiewicz, *Analiza Systemowa*. 2003



Rysunek 3-48. Lejek scenariusza
Źródło: M.Cieślak (red.), *Prognozowanie,.. op.cit.*

Konstruowanie scenariusza[205]

Ogólne zasady pisania scenariuszy (etapy) pozostają niezmienne dla wszystkich metod (tabela 3-40).[206]

Tabela 3-40. Etapy konstruowania scenariusza

ETAP 1	Model wnętrza obiektu	Zdefiniowanie obiektu, określenie jego elementów i powiązań między nimi, określenie zakresu scenariusza (wybór zjawisk zachodzących w obiekcie i uwzględnianych w scenariuszu, redukcja zbioru zmiennych pierwotnych poprzez zamianę na zmienne syntetyczne lub stosując metody formalne lub opinię ekspertów). Występujące powiązania zdefiniować za pomocą modeli ekonometrycznych.
ETAP 2	Model wpływów otoczenia na obiekt	Identyfikacja zjawisk należących do otoczenia danego obiektu (tzw. obszarów oddziaływania) i wpływających na jego rozwój oraz określenie powiązań między zmiennymi należącymi do różnych obszarów oddziaływania i zmiennymi wnętrza obiektu. (Wykorzystujemy modele ekonometryczne i opinie ekspertów).
ETAP 3	Ilościowy opis powiązań między elementami obiektu oraz między obiektem a jego otoczeniem w teraźniejszości, czyli w chwili, w której przygotowuje się scenariusz.	
ETAP 4	Konstruowanie prognoz zmiennych należących do otoczenia obiektu i wpływających nań	oddziaływujących na badany obiekt. W predykcji możemy stosować dowolną metodę np. ekstrapolację szeregów czasowych lub korzystać z opinii ekspertów a także prognoz demograficznych, prognoz koniunktury gospodarczej, prognoz inflacji.

[205] W konstruowaniu scenariuszy jako narzędzi wspomagających można stosować różne techniki np. QUEST (Quick Environmental Scanning Technique) i PEST (akronim czterech kategorii czynników zmian: *Political, Economic, Social, Technological*).

[206] M. Cieślak, Prognozowanie,...,op.cit.

ETAP 5	Opracowanie prescenariuszy	Konstruuje się prognozy zmiennych należących do obiektu. Jakościowy opis wybranych wariantów przyszłości obiektu to prescenariusz. Jest tworzony na podstawie wielowariantowego opisu rozwoju obiektu przy czym analizuje się alternatywy, czyli bada się różne warianty przyszłości ze względu na ich spoistość, zgodność, logikę.
ETAP 6	Identyfikacja czynników zakłócających proces rozwoju obiektu	Ocenia się wpływ zdarzeń, występujących nagle bez cech katastroficznych ale istotnie wpływających na obiekt. Jest to moment określania działań : działanie przeciwdziałające - zakłócenie negatywne działanie przystosowawcze - zakłócenie pozytywne
Etap 7	Sporządzenie scenariusza	Uwzględnienie czynników zakłócających i ich skutków prowadzi do otrzymania scenariusza. Otrzymujemy syntetyczny opis rozwoju i stanu badanego obiektu w przyszłości, uwzględniający zmiany ilościowe i jakościowe występujące zarówno w obiekcie jak i w jego otoczeniu.

Źródło: opracowanie własne na podstawie: M.Cieślak, *Prognozowanie gospodarcze. Metody i zastosowania*, PWN, Warszawa 2000, s. 194-197.

Zbudowany według powyższych zasad scenariusz obejmuje system będący przedmiotem analizy prognostycznej, ponadto analizie diagnostycznej poddawane jest otoczenie, w takim zakresie, w jakim może ono oddziaływać bezpośrednio lub pośrednio na elementy systemu.[207]

Przykładowy scenariusze ataku cyberterrorystycznego dla Polski

Wprowadzenie

Potencjalnego ataku cyberterrorystycznego może spodziewać się również Polska, jako kraj popierający politykę USA, a także jako uczestnik w operacji w Afganistanie. Również narażeni jesteśmy na ataki ze strony Rosji. 16 lipca 2008 roku media podały informację o możliwym cyberataku Rosji na Polskę.[208] Miała być to odpowiedź na budowę elementów tarczy antyrakietowej na terenie Polski. I chociaż do niego niedoszło to jest to zdarzenie możliwe i prawdopodobne. Możliwe i prawdopodobne są również ataki Al-Kaidy. Portal izrael-

[207] W zależności od przyjętych kryteriów wśród technik wykorzystywanych w procesie budowy scenariuszy wyróżnić możemy:
a) metody jakościowe: metoda Delphi, „burza mózgów", analiza SWOT (*Strengths, Weaknesses, Opportunities, and Threats*), konsultacje społeczne, panel ekspercki itp.;
b) metody ilościowe: analiza szeregów czasowych i ekstrapolacja trendów, modelowanie systemowe, krzyżowa analiza wpływów, techniki predykcji, metoda Bayesa, sztuczne sieci neuronowe itp.
Podczas formułowania syntetycznej diagnozy lub rekomendowanej alternatywy strategicznej można stosować wielokryterialną analizę porównawczą (WAP), w szczególności wybraną technikę aksonometryczną.

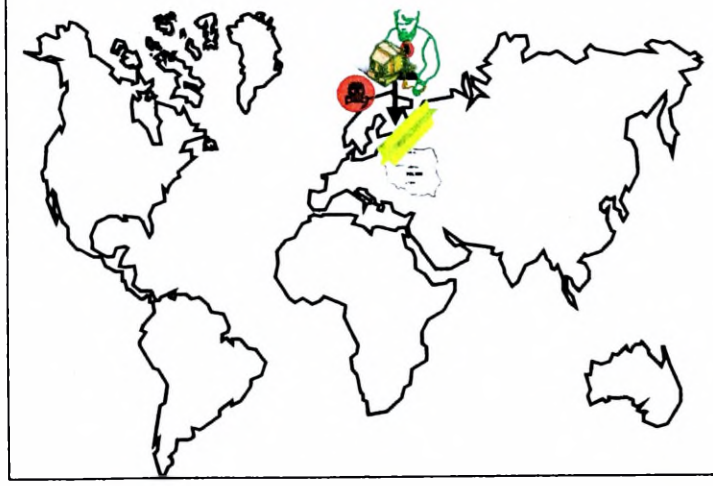
[208] http://wiadomościonet.pl/1788837,11,item.html.

skiego serwisu DEBKAfile[209] podał, że zamierzają oni przenieść wojnę do cyberprzestrzeni ponieważ coraz dłużej udaje się im utrzymać strony.

Kolejne badania zagrożeń bezpieczeństwa pochodzących z Internetu potwierdzają istniejące zagrożenia.[210] Komputery polskich użytkowników zawierają wirusy rozsyłane przez hakerów w postaci trojanów (niekiedy są to bomby logiczne), które pojawiają się w pamięci komputera, przejmując nad nim kontrolę (bez wiedzy właściciela lub użytkownika) stając się uczestnikiem sieci „zombie"[211] (Załącznik V). Uaktywniają się na wyraźny sygnał agresora i rozpoczynają destrukcję.

W opracowanym scenariuszu cyberataku na Polskę, za najprawdopodobniejszy przyjęto atak typu DDoS (*distributed denial-of-service*), w którym wykorzystywane są sieci lub serwery „zombie". W atakach, prowadzonych w sposób rozproszony, skierowany na wybrany przez hakera cel, nadmierny strumień informacji blokuje komputer „ofiarę" doprowadzając do całkowitej utraty funkcjonalności. Ponieważ napastnik często korzysta z „pośrednika" dysponującego „siecią zombie" identyfikacja atakującego jest bardzo utrudniona. Przygotowanie ataku ułatwia możliwość „wynajęcia" on-line „sieci zombie" jak i bonetów.[212] Wśród rozpoznanych typów ataków wyróżnić możemy (tabela 3-41):

Tabela 3-41. Typologia ataków

Atak pojedynczy	**charakterystyka**
	Ataku dokonuje pojedynczy napastnik na pojedynczy obiekt, lub różne obiekty. Napastnikami często są wynajęci hakerzy włamujący się na zlecenie na strony różnych firm, których celem jest kradzież danych np. bazy klientów.

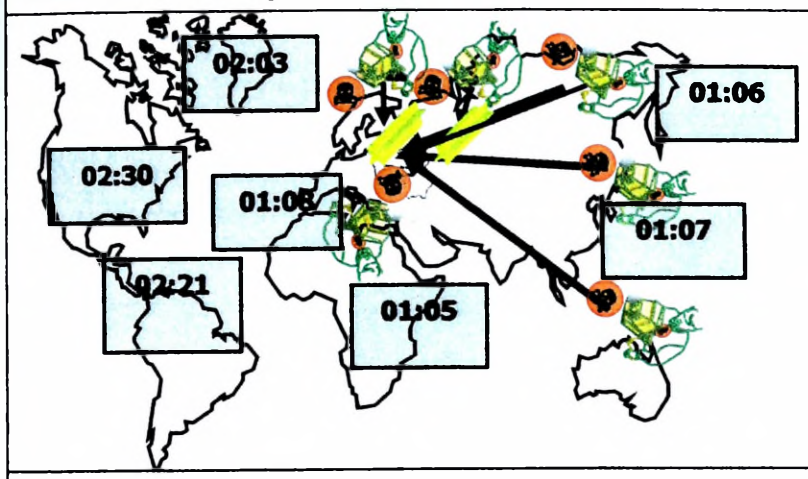
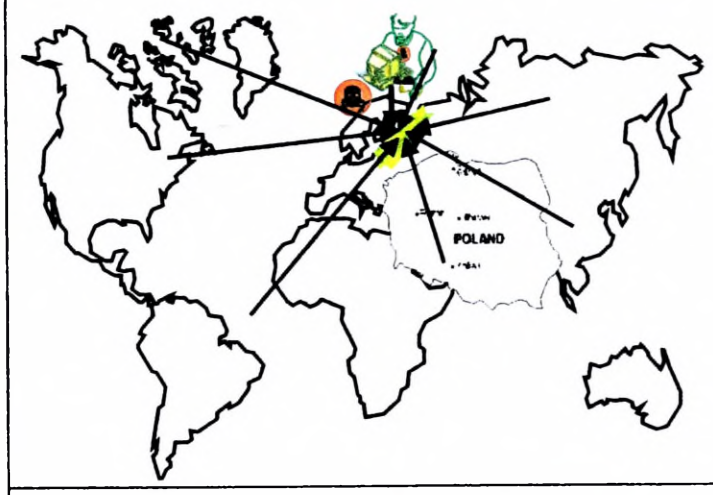
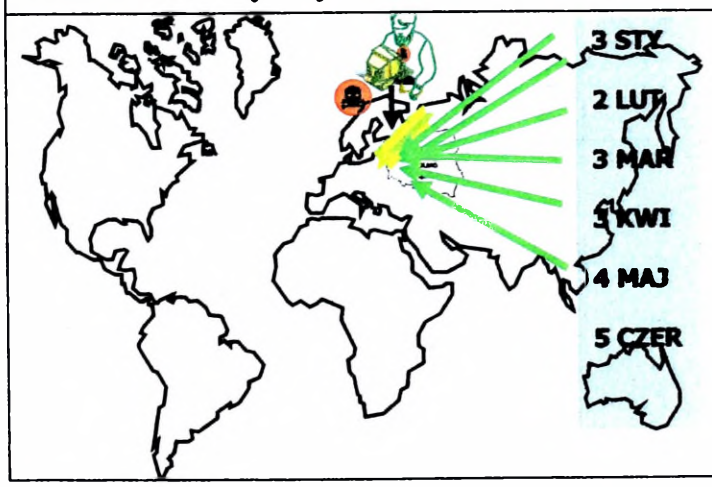
[209] http://www.debka.com/index1.php.

[210] Badania firmy Security Standard o zagrożeniach bezpieczeństwa pochodzących z Internetu dla Polski w 2007. Polska zajmuje 2 miejsce (11%) wśród krajów o największej ilości komputerów-zombie, 6 miejsce (4%) wśród krajów przechowujących na serwerach strony służące do ataków typu „*phishing*"(tabela 3-33).

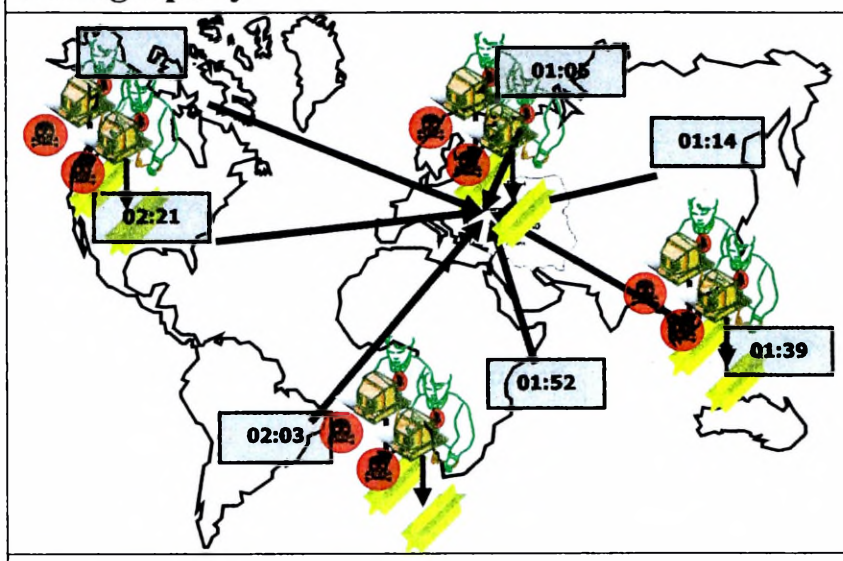
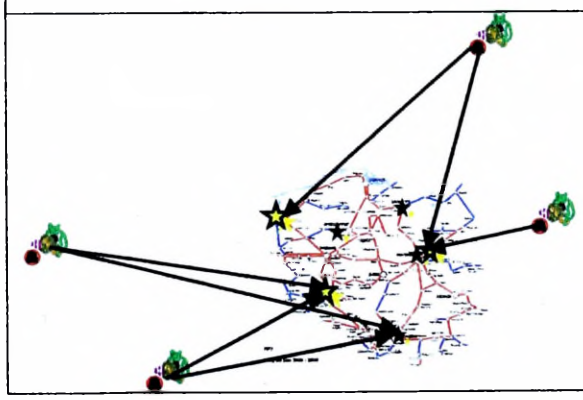
[211] Powodem jest stosownie np. nielegalnego oprogramowania, ale także uleganie pułapkom stosowanym w inżynierii społecznej wykorzystującej ludzkie słabości.

[212] Z takiego pośrednictwa korzystali napastnicy w czasie ataków na Estonię w 2007r.

Cd.

Atak zmasowany	**charakterystyka**
	Atak, w którym uczestniczyć może pojedynczy napastnik korzystający z bonetu. Mogą uczestnikami ataku być internauci zachęceni do wzięcia udziału w blokowaniu stron. Ma charakter ataku ciągłego (trwającego wiele godzin). Serwer zasypywany dużą liczbą odwołań powodujących blokadę systemu.
Atak wielokrotny	**charakterystyka**
	Atak powtarzany wielokrotnie na te same obiekty. Sprawcami mogą być niepowiązane ze sobą grupy internautów.
Atak konsekutywny	**charakterystyka**
	Ataki następują po sobie w określonym interwale czasowym.

Cd.

Atak grupowy	**charakterystyka**
	Atak prowadzony przez zmieniające się grupy napastników. Grupy atakują w określonych interwałach Może być: czasowych i przestrzennych, i w porozumieniu.
Atak synchroniczny	**charakterystyka**
	Atak jednoczesny, w którym zdarzenia zachodzą w tym samym czasie. Może być przeprowadzany z wykorzystaniem botnetów, przez pojedynczego napastnika lub np. ze wsparciem chętnych internautów, zachęconych do korzystania z narzędzi poleconych przez napastnika(ów) na stronach WWW.
	Z przeprowadzonych analiz ataków, których ofiarami były między innymi systemy ICT w Estonii, Gruzji wynika, że ataki łączą w sobie wiele form. Często przybierają postać e-zamieszek, czyli przypominają działania „rozjuszonego tłumu" tylko, że w wersji internetowej.

Źrodło: International Scientific And Educational Conference „Terrorism and security of mass events", H.Swieboda, P.Sienkiewicz, *Cyberterrorism as a threat to the security of mass.* and P.Sienkiewicz, *Methods of analysis of the risk of terrorist threats events.* Waplewo, November 13-15, 2008

SCENARIUSZ I

Mistrzostwa Europy w Piłce Nożnej 2012, organizowane wspólnie przez dwa państwa: Polskę i Ukrainę mogą stać się możliwym i prawdopodobnym celem ataku terrorystów.

Ranga imprezy, duże skupiska ludzi i wszechobecne media gwarantują odpowiednie nagłośnienie zajścia, wywołanie paniki wśród ludzi.

Przewidywany (w chwili pisania scenariusza) nieoficjalny termin przeprowadzenia finałów to okres od 9 czerwca 2012 roku (mecz otwarcia w Warszawie) do 1 lipca 2012 (spotkanie finałowe). Organizacja tak dużej imprezy jest wyzwaniem logistycznym, szczególnie w zakresie zapewnienia bezpieczeństwa. Problem komplikuje fakt wschodniej granicy Polski, która jest granicą Unii Europejskiej. Nawet w sytuacji wzmożonej ochrony[213] trudno przewidzieć wszystkie sytuacje i zabezpieczyć się przed wszystkimi możliwymi i prawdopodobnymi zdarzeniami.

Celem ataku był paraliż systemu komunikacyjnego Warszawy, wywołanie chaosu, nie wykluczono ofiar śmiertelnych. Wywołanie niezadowolenia społecznego, strat materialnych i ofiar może mieć wpływ np. na decyzję o wycofaniu wojsk z Afganistanu.

Hipotetyczny scenariusz – najbardziej prawdopodobny

W okresie przed zbliżającymi się Mistrzostwami grupa hakerów (wynajętych i opłaconych przez terrorystów) wprowadziła wirusy do wielu prywatnych komputerów (przygotowując sieć komputerów zombie), z zamiarem wykorzystania ich w przeprowadzeniu skoordynowanego ataku na systemy najważniejszych instytucji rządowych i komercyjnych (banki). Wśród form ataków wyróżnia się między innymi (tabela 2-4, 2-5, rysunek 2-6, załącznik V):

W dniu „meczu otwarcia" nastąpił zmasowany atak na strony parlamentu, prezydenta, i partii politycznych. Wykorzystano „sieci bonetów"[214] co w początkowej fazie nie wywołało zaniepokojenia. Był obserwowany tylko zwiększony ruch w sieci.

Po kilku godzinach na stronie prezydenta i parlamentu pojawiły się treści ośmieszające i wulgarne. Ruch internetowy wzrósł jeszcze bardziej, na stronach rządowych pojawiły się wezwania aktywizujące ludzi do zgromadzenia się w różnych miejscach Warszawy.

W tym samym czasie strony mediów zostały zaatakowane i podmienione. Pojawiły się komunikaty wzywające do zgromadzenia się ludzi w miejscach, które podane były na stronach rządowych. W konsekwencji doprowadzono do wyłączenia stron. Zablokowano internetowe banki. Zlokalizowano miejsca skąd pochodziły ataki: niektóre pochodziły z obszaru Polski, dużo z Pakistanu, Chin i Rosji. Na stronach w krajach skąd pochodziły ataki, na platfor-

[213] Polska odpowiada za opracowanie Zintegrowanej Koncepcji Bezpieczeństwa EURO 2012.

[214] Co utrudniło identyfikację napastników, ponadto do zarządzania siecią złożoną nawet z miliona komputerów wystarczy jeden człowiek. Ataki zwykle trwają kilka godzin, zanim służby odpowiedzialne zorientują „co dzieje się"

mach dyskusyjnych, i forach internetowych, pojawiły się instrukcje dla chcących wziąć udział w cyberataku. Nastąpiło odpieranie ataków wzniesiono dodatkowe zapory firewhole.

Wystąpił chaos informacyjny, ludzie zaczęli przemieszczać się w różne kierunki w sposób sprzyjający panice. Nastąpił atak na Centralną Dyspozytornię linii metra (stacja metro „Politechnika"). Zagłuszono sygnały nadawcze anteny (brak było łączności pomiędzy stacjami metra) oraz wyłączono energię zasilającą linie metra.

Scenariusz najbardziej prawdopodobny: pasażerowie nie wpadli w panikę, sprawnie działające służby opanowały sytuację. Ludzi wyprowadzono z tunelu. Wśród poszkodowanych były tylko przypadki zasłabnięcia i omdlenia. Trzeba było wezwać służby ratownicze.

Scenariusz katastroficzny (Ia): panika wśród pasażerów, powielana informacja o rozpyleniu wąglika powoduje zamieszanie i próbę szybkiego opuszczenia tunelu przez część pasażerów. W wyniku czego były osoby zgniecione przez tłum poruszający się w ciemnościach. Konieczność wezwana dużych sił ratowniczych. Zarządzanie państwem jest w pełni z destabilizowane. Brak informacji lub media podają zafałszowane komunikaty.

W katastroficznym scenariuszu można przewidzieć użycie bomb typu EMP (*Electro-Magnetic Pulse*[215].), emitujących promieniowanie elektromagnetyczne. Jednoczesne użycie ich w kilku miejscach stolicy, np. w śródmieściu i okolicy lotniska Okęcie – lub kilku miastach – spowodowałoby zniszczenie urządzeń elektronicznych w promieniu kilkuset metrów. Oprócz zniszczeń jako efektu pierwszej fazy ataku do dalszych konsekwencji dołączą:

– sparaliżowanie sieci teleinformatycznych: wstrzymane operacje bankowe i handlowe,

– paraliż sygnalizacji świetlnej, kolizje i stłuczki,

– blokada lub niszczenie systemów alarmowych 911 i 112[216], brak możliwość wezwania służb ratowniczych,

– wyłączenie urządzeń lotniska – może dojść do katastrof,

– blokada mediów, nadawanie fałszywych komunikatów, wzywających do zbiórek i manifestacji.

Organizacja takiego ataku wymaga ludzi i środków rozpoznania i dobrej koordynacji działań. Atak w sieci jest wydajniejszy, i tańszy oraz trudniejszy do wykrycia, można wykorzystać chęć zwykłych internautów w ataku oferując im narzędzia, praktycznie napastnicy są

---

[215] D.Verton, *Black Ice. Niewidzialna groźba cyberterroryzmu*, Wydawnictwo Helion SA, Gliwice 2004, s.46.

[216] Istnieją potwierdzone przypadki takich działań. A.Pietrzak, *Nowe oblicza terroryzmu*. Dostęp online: www.paneuropa.l.pl

trudno identyfikowalni, a jeśli już to bark jest odpowiednich mechanizmów prawnych aby pociągnąć do odpowiedzialności uczestników akcji z innych państw.

SCENARIUSZ II

Tabela 3-42. Syntetyczny scenariusz II

DZIEŃ	TYP ATAKU	CEL	SKUTKI BLIŻSZE	SKUTKI DALSZE
1	DDoS	Internetowe strony rządowe	Nierozpoznany przez dobę	
2	Wzrost ruchu w sieci			
3	DDoS	Strona parlamentu	Pierwsze sygnały o utrudnieniach	
4,5,6	DDoS	Systematyczny atak na strony rządowe Blokada stron partii politycznych	Początkowo ośmieszające treści, później brak dostępu do stron	Konsekwencje nie załatwienia spraw terminowych
	spaming[217]	główne strony mediów	Wzywanie do nieposłuszeństwa obywatelskiego, nawoływanie do demonstracji, wieców ulicznych, wywołanie niepokojów	Niepokoje społeczne Zniszczenia materialne, koszty napraw, remonty, dodatkowe sprawy sądowe
7	DDoS	Całkowita blokada stron rządowych, parlamentu, partii politycznych	Brak informacji	Niepokoje społeczne, demonstracje
8	DDoS	Atak na strony głównych mediów	Brak informacji	Niepokoje społeczne
9	Rozpoznanie skąd prowadzone ataki – z różnych stron z zagranicy, atak zmasowany, sprawcy nieznani			
10	DDoS	Atak na strony głównych mediów	Brak informacji wychodzącej, brak informacji o sytuacji wewnątrz kraju	Zamieszki, demonstracje Są poszkodowani w wiecach i demonstracjach ulicznych
	Próby normowania sytuacji: blokowanie ruchu przychodzącego przez media			
11	Utrzymują się zmasowane ataki na strony rządowe i mediów, trudna sytuacja wewnętrzna			
12	Zmasowany atak na system bankowy DDoS	System bankowy bank centralny, systemy płatnicze, sieci bankomatowe, giełda, centra rozliczeniowe kart kredytowych	Zakłócenia swobodnego przepływu środków pieniężnych, Manipulowanie notowaniami kursowymi bądź giełdo-	Dotkliwe skutki dla społeczeństwa Straty finansowe Nieczynne bankomaty Zerwanie łączności z zagranicą

[217] Przejęcie transmisji i zastąpienie pokazywanego obrazu swoim własnym.

			wymi Zaprzestanie prowadzania usług on-line Straty finansowe	Brak możliwości autoryzacji kart płatniczych osób poza granicami Straty finansowe Dezorganizacja pracy przedsiębiorstw Utrata zaufania do banków
13	Ataki ustały			

Źródło: opracowanie własne.

Najpoważniejszymi zagrożeniami dla kraju są ataki typu *sniffing*[218], *brute force*[219], *dictionary attac*[220], *port skaning*, *spoofing*[221] czy *backdoors*. Zastosowanie tego typu ataków umożliwiłoby penetrację systemów komputerowych elektrowni, lotnisk, wodociągów, a więc wszystkich systemów stanowiących obszar tzw. krytycznej infrastruktury. Do sterowania urządzeniami automatyki przemysłowej i zbierania danych o ich funkcjonowaniu służą systemy SCADA (*Supervisory Control and Data Acquisition*). Są powszechnie stosowane w elektrowniach, rafineriach, gazociągach, oczyszczalniach ścieków i zakładach przemysłowych.[222]

Udany cyberatak na system sterownia elektrowni może spowodować przerwy w zasilaniu w energię elektryczną powodując olbrzymie straty finansowe zarówno w wielu obszarach gospodarki, a także u indywidualnych odbiorców energii.[223]

Przewidywanie możliwych scenariuszy dla systemów, z obszaru KIP, których zaatakowanie może zagrozić bezpieczeństwu narodowemu, na skutek konsekwencji jakie mogą

---

[218] Program komputerowy lub urządzenie, którego zadaniem jest przechwytywanie i ewentualne analizowanie danych przepływających w sieci. Bywa stosowany do monitorowania aktywności sieciowej osób trzecich, co jest w większości przypadków niezgodne z prawem. Źródło: http://pl.wikpedia.org.

[219] W bezpieczeństwie pojęcie *ataku brute force* używane jest do opisania przeprowadzanych przez człowieka lub program komputerowy prób przełamania zabezpieczeń – na przykład odgadnięcia hasła – przez sukcesywne sprawdzanie wszystkich możliwości. Źródło: http://pl.wikpedia.org.

[220] Ataki, które wykorzystują słownik haseł. Źródło: http://www.digipedia.pl/def/833822646-dictionary-attack.html.

[221] Termin określający fałszowanie źródłowego adresu IP w wysyłanym przez komputer pakiecie sieciowym. Takie działanie może służyć ukryciu tożsamości atakującego. Źródło: http://pl.wikpedia.org.

[222] Opublikowany 5 września 2008r. *exploit* wykorzystuje upublicznioną 11 czerwca 2008 roku lukę w systemie CitectSCADA firmy Citect, jednym z popularniejszych systemów tego typu (w 80 krajach sprzedanych łącznie ponad 150 tysięcy licencji). Oprogramowanie to jest uruchomione na standardowych komputerach z systemem Microsoft Windows. Odkryta luka pozwala na zdalne przeprowadzenie ataku DoS lub wykonanie dowolnego kodu na zaatakowanym systemie. Jedynym warunkiem jest możliwość połączenia do zdalnego systemu na port 20222/TCP.

[223] Podobne zdarzenie, chociaż nie spowodowane cyberatakiem, miało miejsce na północno-wschodnim obszarze USA 14 sierpnia 2003. Straty finansowe oszacowano na 6 miliardów USD. Z podobna sytuacją mieliśmy do czynienia w 2008r. w Szczecinie w czasie awarii systemu energetycznego spowodowanego obfitymi opadami śniegu.

wystąpić w przypadku ich realizacji. Oczywiście należałoby rozpatrywać każdy przypadek indywidualnie, bowiem inne ryzyko grozi systemom standardowym podłączonym bezpośrednio do internetu a inne występuje w systemach wysoce zabezpieczonych systemach sterownia posiadającymi wielopoziomowe zabezpieczenia. Niemniej jednak zagrożenie jest możliwe i prawdopodobne.

Tabela 3-43. Zagrożenia dla KIP

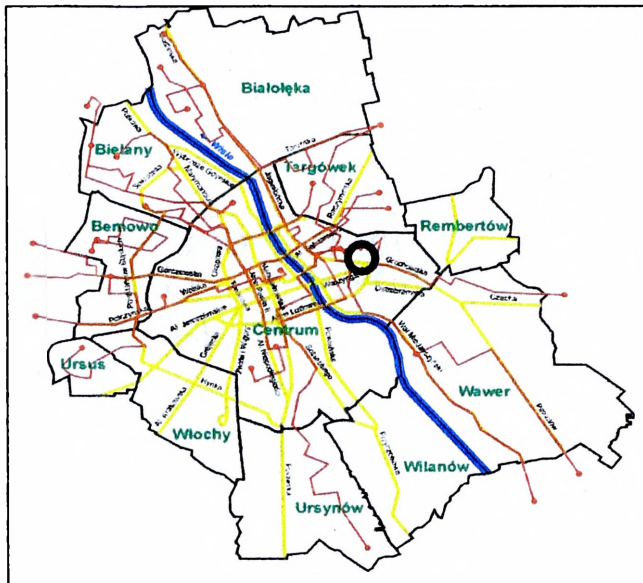
ZAGROŻENIE DLA ELEMENTÓW KIP	ZAGROŻENIA	SKUTKI	PODATNOŚĆ	OCENA RYZYKA
Zagrożenia specyficzne dla danego sektora	prawdopodobne	katastrofalne	mała	średnie
Potencjalne zagrożenie eksplozją	prawdopodobne	katastrofalne	mała	małe
Przerwanie nadzoru procesu technologicznego	prawdopodobne	katastrofalne	mała	małe
Zmiany w recepturach	prawdopodobne	katastrofalne	mała	małe
Uwolnienie do środowiska substancji używanych do produkcji	prawdopodobne	katastrofalne	mała	średnie
Zniszczenie urządzeń	prawdopodobne	katastrofalne	mała	małe
Utrata danych historycznych	prawdopodobne	katastrofalne	mała	średnie
Ograniczenie zdolności produkcyjnych	prawdopodobne	katastrofalne	mała	średnie

Źródło: opracowanie własne.

SCENARIUSZ III

Analiza scenariuszy uwzględniająca atak cyberterrorystyczny, w obliczu zbliżających się Mistrzostw Europy EURO 2012, jest jak najbardziej potrzebna. Cyberatak na system, telekomunikacyjny lub energetyczny byłby wydarzeniem, które przyniósłby wielomilionowe straty. W miejscach imprez masowych powinny być zidentyfikowane punkty najbardziej podatne na uszkodzenia, których awaria, destrukcja powodowałby największe straty. Ten typ analizy nakazuje szczegółowe rozważenie jak są zaprojektowane urządzenia, systemy obsługi i jakie operacje w nich występują. Konsekwencje docierają daleko poza czas i miejsce bezpośredniego ataku i lokalizują się w sektorach odległych gospodarki czy społeczeństwa. Bezpośrednie konsekwencje obserwujemy natychmiast. W zależności od powagi ataku mogą to być: ilość zabitych, rannych i straty materialne. Konsekwencje mogą rozchodzić się przez połączenia infrastruktur a także społecznego odbioru ryzyka. Takim pierwszoplanowym, możliwym i prawdopodobnym zagrożeniem jest zakłócenie zasilania. Wobec tego podstawowym pyta-

niem pozostaje przygotowanie społeczeństwa na traumatyczne przeżycia. Dodatkowy wysiłek należy skoncentrować na skutecznym informowaniu w czasie incydentu decyduje to bowiem o sprawności akcji ratowniczej w przypadku wystąpienia zakłóceń.



Rysunek 3-49. Mapa Warszawy
Źródło:
http://www.frontreklamowy.com.pl/img/mapa/horiz/mapa%20warszawy.jpg

Rysunek 3-50. Mapa okolicy Stadionu Narodowego
Źródło:www.Yahoo.com

Uważne przestudiowanie mapy w szczególności okolic miejsca gdzie ma stanąć Stadion Narodowy pozawala zauważyć małą liczbę dróg, dojazdowych, co może być powodem trudności komunikacyjnych nie tylko w sytuacji kryzysowej.[224]

W internecie dostępne są adresy oraz dane wszystkich typów elektrowni istniejących, a także planowanych. W przykładowym scenariuszu ataku dokonano włamania do komputerów kontrolujących klimatyzację pomieszczeń, w którym umieszczone są komputery z systemami sterującymi urządzeniami energetycznymi, omijając ich dobre zabezpieczenie. Włamanie daje napastnikowi możliwość sterowania temperaturą, powodując jej wzrost do poziomu zniszczenia urządzeń. W efekcie doprowadziłoby do zakłóceń w dostawie prądu.

Tabela 3-44. Scenariusz IV

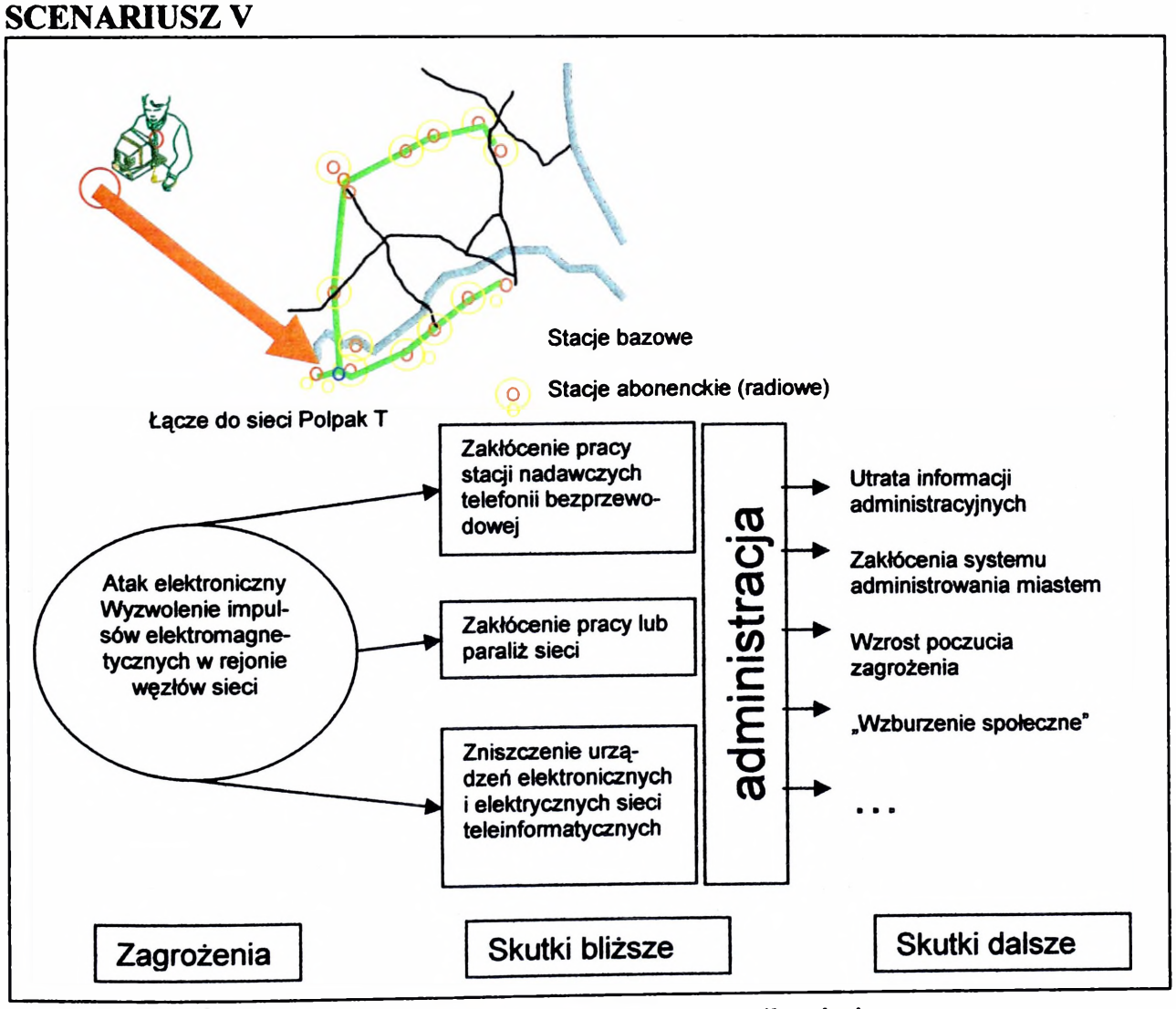
DZIEŃ	TYP ATAKU	CEL	SKUTKI BLIŻSZE	SKUTKI DALSZE
1	dictionary attack	Komputery kontrolujące klimatyzacje pomieszczeń z urządzeniami sterującymi	Wzrost temperatury w pomieszczeniu	
2			Zakłócenia w dostawie prądu	
3			Nie działają systemy informatyczne i telekomuni-	Skutki odczuwane poza aglomeracją war-

[224] Trudności z opuszczeniem miejsca koncertu Madonny.

			kacyjne, brak informacji o tym co się dzieje	szawską
4			Zaniepokojeni uczestnicy imprezy usiłują opuścić stadion	
5			Nie działa sygnalizacja świetlna, na ulicach tworzą się korki – dochodzi do wypadków Nie działają komórki, nie można powiadomić policji i pogotowia	Straty finansowe z powodu niemożności transmitowania meczów Wpłaty odszkodowań dla osób poszkodowanych Nakłady na likwidację skutków rozbojów, zniszczeń wywołanych rozróbami oraz kradzieży
6			Staje metro a w nim pozostają uwięzieni pasażerowie	
7	przeciwdziałanie			

Źródło: opracowanie własne.

SCENARIUSZ V



Rysunek 3-51. Hipotetyczny scenariusz ataku na łącze sieci telekomunikacyjnej

Źródło: opracowanie własne.

Tabela 3-45. Przykładowy ogólny scenariusz zagrożeń na szczeblu państwa

TYP ATAKU	SKUTKI BLIŻSZE	SKUTKI DALASZE	PRZECIWDZIAŁANIE
Atak elektroniczny Wyzwolenie impulsów elekromagnetycznych w rejonach węzłów sieci; Uruchomienie urządzeń zakłócających pracę nadajników łączności bezprzewodowej.	Zniszczenie urządzeń elektronicznych i elektrycznych sieci teleinformatycznych – zakłócenie pracy lub paraliż tych sieci; Zniszczenie stacji nadawczych telefonii komórkowej zakłócenia w pracy sieci; Zakłócenie pracy stacji nadawczych telefonii bezprzewodowej.	Utrata informacji administracyjnych; Zakłócenie pracy lub paraliż systemu administrowania miastem. Wzrost poczucia zagrożenia i niezadowolenia społecznego.	Wykrywanie i ocena zagrożeń; Uodpornienie urządzeń i pomieszczeń na atak elektromagnetyczny; Zorganizowanie systemu odtwarzania sprawności systemu po ataku.
Atak ogniowy Zdetonowanie ładunków wybuchowych w obrębie węzłów sieci; Przerywanie linii magistralnych sieci.	Zniszczenie central telefonicznych i serwerowni – paraliż pracy sieci; Zakłócenie pracy lub paraliż systemu administrowania miastem.	Utrata informacji administracyjnych; Zakłócenie pracy systemu administrowania państwem. Wzrost poczucia zagrożenia i niezadowolenia społecznego.	Wykrywanie i ocena zagrożeń; Fizyczne uodpornienie sieci na atak ogniowy; Zorganizowanie systemu odtwarzania sprawności systemu po ataku.
Działania psychologiczne Inżynieria społeczna - pozyskiwanie personelu urzędów do współuczestnictwa w atakach.	Umożliwienie dostępu do sieci informatycznej systemów administrowania państwem, ujawnienie niejawnej informacji; Sabotaż wewnętrzny ze strony pozyskanego personelu; Defraudacje finansowe dokonywane przez pracowników administracji.	Zewnętrzny atak informatyczny na sieć; Zagrożenie bezpieczeństwa informacyjnego państwa; Kradzież niejawnych informacji (np. danych osobowych czy finansowych); Pogorszenie bezpieczeństwa finansowego; Zakłócenia w administrowaniu państwem; Wzrost poczucia zagrożenia i niezadowolenia społecznego.	Wykrywanie i ocena zagrożeń; Podnoszenie świadomości stanów osobowych; Doskonalenie procedur kontroli dostępu do informacji.
Dezinformacja Rozsyłanie fałszywych informacji pocztą elektroniczną oraz przez inne środki komunikowania społecznego.	Kwestionowanie uczciwych zamiarów władz i kierownictw organizacji systemu administrowania państwem; Podważanie wiarygodności oraz kwalifikacji wybranych grup personelu; Rozpowszechnianie fałszywych informacji o zamiarach władz państwa; Podawanie fałszywych informacji o pracy na rzecz interesów obcych państw i organizacji przez przedstawicieli władz.	Wywoływanie zaniepokojenia, pogarszanie nastrojów, próby wywoływania paniki, pogarszanie jakości funkcjonowania państwa. Próby zachwiania stabilnością finansową i płynnością finansową państwa. Wzrost poczucia zagrożenia i niezadowolenia społecznego.	Szybka reakcja władz na fałszywe informacje; Sprawne docieranie do ludności i personelu firm z obiektywną informacją; Zachowywanie prawdy w informowaniu; Wykrywanie i napiętnowanie dezinformatorów.

Źródło: opracowanie własne na podstawie: R.Szpyra, *Scenariusze zagrożeń.* [w:] T.Jemioło,(kier.) *Modelowanie zagrożeń dla bezpieczeństwa informacyjnego państwa. Teoria walki informacyjnej.* AON, Warszawa 2004, s.52.

Każdy hipotetyczny atak można rozpatrywać poddając analizie dziedziny Krytycznej Infrastruktury Państwa starając się określić podatność oraz możliwe zagrożenia.

Tabela 3-46. Scenariusz możliwych prawdopodobnych zagrożeń dla dziadziny telekomunikacji

DZIEDZINA: TELEKOMUNIKACJA			
ELEMENT	**SYSTEM**	**MOŻLIWE ZAGROŻENIA INFORMACYJNE**	**PODATNOŚĆ**
stacje bazowe punkty dostępowe centra zarządzania	telefonia bezprzewodowa GSM (ERA, PLUS, IDEA)	przejęcie kontroli nad centrum zarządzania atak fizyczny lub elektromagnetyczny na centrum zarządzania lub stacje bazowe podsłuch transmisji	L M M
centrale abonenckie łącza transmisyjne telewizja kablowa	telefonia przewodowa (TPSA, NETIA, ASTER CITY, UPC, PKP, ENERGETYKA, SZ RP)	atak fizyczny lub elektromagnetyczny na elementy systemu blokada usług telekomunikacyjnych podsłuch transmisji przekierowanie transmisji	H H H H
centra usług satelitarnych satelity komunikacyjne terminale satelitarne	telefonia satelitarna (Centrum Usług Satelitarnych PSARY, NASK)	przejęcie kontroli nad centrum zarządzania atak fizyczny lub elektromagnetyczny na elementy systemu podsłuch transmisji	L M L
zestawy nadawczo-odbiorcze radiolinie	łączność radiowa (MSWiA, SZ RP, komercyjna, prywatna)	przejęcie kontroli nad elementami systemu atak fizyczny lub elektromagnetyczny na elementy systemu zakłócanie transmisji podsłuch transmisji podszywanie się w systemie (dezinformacja)	L (rząd.) H (cyw.) M H L (rząd.) H (cyw.) L (rząd.) H (cyw.)
polska sieć szkieletowa; serwery, punkty dostępowe,	internet (sieci WAN, MAN)	atak fizyczny lub elektromagnetyczny na elementy sieci spowolnienie lub blokada usług poprzez: spam, wirusy, robaki, konie trojańskie, ataki hakerów przejęcie kontroli na portalami i dezinformacja przejęcie kontroli nad elementami infrastruktury krytycznej za pomocą sieci Internet	H H H M
zestawy nadawczo-odbiorcze stacje przekaźnikowe centra zarządzania studia TV	Radio i Telewizja (publiczne, komercyjne)	atak fizyczny lub elektromagnetyczny na elementy sieci zakłócanie transmisji przejęcie kontroli nad elementem systemu w celu dezinformacji i propagandy	H H M

Źródło: opracowanie własne.

Tabela 3-47. Scenariusz możliwych i prawdopodobnych zagrożeń dla energetyki

ELEMENT	SYSTEM	MOŻLIWE ZAGROŻENIA INFORMACYJNE	PODATNOŚĆ
Gospodarstwo domowe	Powiadamiania o uszkodzeniach i przerwach w dostawie energii	Uszkodzenie sieci telefonicznej	Średnia
Linia energetyczna	Przesyłowy Nadzoru Awaryjny	Przerwanie linii Zwarcie linii Uszkodzenie elementów systemu nadzoru dostaw energii	Średnia
Podstacja lokalna		Włamanie do podstacji Zniszczenie podstacji Uszkodzenie elementów systemu nadzoru dostaw energii	Wysoka
Rozdzielnia miejska		Zajęcie rozdzielni Uszkodzenie systemu nadzoru i przyjmowania zgłoszeń Uszkodzenie elementów rozdzielni	Wysoka
Rozdzielnia powiatowa		Zajęcie rozdzielni Uszkodzenie systemu nadzoru i przyjmowania zgłoszeń Uszkodzenie elementów rozdzielni	Wysoka
Elektrownia	Przesyłowy Nadzoru Awaryjny Zarządzania	Zajęcie elektrowni Uszkodzenie systemu nadzoru i przyjmowania zgłoszeń Ataki hakerskie na systemy sterujące pracą elektrowni Uszkodzenie elementów elektrowni	Średnia
Sieć transmisyjna	Przesyłowy Nadzoru Zarządzania	Przerwanie (zwarcie) sieci transmisyjnych Zakłócenia elektromagnetyczne Ataki hakerskie	Wysoka

Źródło: opracowanie własne.

Tabela 3-48. Tabela scenariusze dla systemów na różnych stopniach zarządzania administracyjnego przewidzianych dla dziedziny transportu

DZIEDZINA: TRANSPORT			
ELEMENT	**SYSTEM**	**MOŻLIWE ZAGROŻENIA INFORMACYJNE**	**PODATNOŚĆ**
GMINA, POWIAT. WOJEWÓDZTWO	System monitorowania ruchu drogowego	brak stacjonarnej łączności telefonicznej, komórkowej, brak możliwości dotarcia do osoby kierującej zespołem w danym miejscu, zniszczenie lub sabotaż węzłów monitorujących (kamery, czujki), awaria serwera bazodanowego, niewykwalifikowana kadra,	Krytyczna Krytyczna Krytyczna Krytyczna
GMINA, POWIAT. WOJEWÓDZTWO	System powiadamiania o utrudnieniach w ruchu drogowym	brak stacjonarnej łączności telefonicznej, komórkowej, brak możliwości dotarcia do mediów, zniszczenie lub sabotaż węzłów przekaźnikowych (Masmedia); niewykwalifikowana kadra, wydłużony czas na powiadomienia na informację (NIEAKTUALNOŚC INFORMACJI)	Krytyczna Krytyczna Krytyczna Krytyczna Krytyczna

WOJEWÓDZTWO	System monitorowania ruchu kolejowego	brak stacjonarnej łączności telefonicznej, komórkowej, brak możliwości dotarcia do osoby kierującej zespołem w danym miejscu, opóźnienie w przesyłaniu informacji z poszczególnych węzłów kolejowych, awaria serwera bazodanowego, niewykwalifikowana kadra,	Katastrofalna Katastrofalna Katastrofalna
WOJEWÓDZ-TWO	System powiadamiania o utrudnieniach w ruchu kolejowym	brak stacjonarnej łączności telefonicznej, komórkowej. brak możliwości dotarcia do mediów, zniszczenie lub sabotaż węzłów przekaźnikowych (Massmedia), niewykwalifikowana kadra, wydłużony czas na powiadomienia na informację (NIEAKTUALNOŚC INFORMACJI)	Katastrofalna Katastrofalna Katastrofalna
WOJEWÓDZ-TWO	System monitorowania stanu jakości tras kolejowych	brak stacjonarnej łączności telefonicznej, komórkowej. brak możliwości dotarcia do mediów, zniszczenie lub sabotaż węzłów przekaźnikowych (Masmedia), niewykwalifikowana kadra, wydłużony czas na powiadomienia na informację (NIEAKTUALNOŚC INFORMACJI)	Katastrofalna Katastrofalna Katastrofalna Katastrofalna
WOJEWÓDZ-TWO	System monitorowania ruchu lotniczego	brak stacjonarnej łączności telefonicznej, komórkowej, radiowej brak możliwości dotarcia do osoby koordynującej zespołem w danym miejscu, awaria serwera bazodanowego, pomyłka kontrolera ruchu,	Krytyczna Krytyczna Krytyczna Krytyczna
WOJEWÓDZTWO	System powiadamiania o utrudnieniach w ruchu lotniczym	brak stacjonarnej łączności telefonicznej, komórkowej, radiowej brak możliwości dotarcia do osoby koordynującej zespołem w danym miejscu, zniszczenie lub sabotaż węzłów monitorujących, nawigacyjnych, awaria systemów kierowania, pomyłka kontrolera ruchu,	Katastrofalna Katastrofalna Katastrofalna Katastrofalna Katastrofalna
GMINA, POWIAT. WOJE-WÓDZ-TWO	System gromadzenia informacji o stanach nawierzchni drogowej	niewłaściwie przeprowadzony audit nawierzchni, błędne wskazania urządzeń pomiarowych,	Marginalna Marginalna
GMINA, POWIAT. WOJE-WÓDZ-TWO	System powiadamiania służb drogowych o krytycznym stanie nawierzchni dróg	brak stacjonarnej łączności telefonicznej, komórkowej, brak możliwości dotarcia do osoby kierującej zespołem w danym miejscu, niewykwalifikowana kadra,	Krytyczna Krytyczna marginalna
WOJE-WÓDZ-TWO	System oznaczania węzłów krytycznych w komunikacji drogowej	awaria systemu sygnalizacji świetlnej lub jej brak, sabotaż, błędnie zinterpretowana informacja	Krytyczna Krytyczna

WOJE-WÓDZ-TWO	System oznaczania węzłów krytycznych w komunikacji kolejowej	awaria systemu sygnalizacji świetlnej lub jej brak, błędnie zinterpretowana informacja	Krytyczna Krytyczna
WOJE-WÓDZ-TWO GMINA, POWIAT.	System monitorowania warunków atmosferycznych	błędne prognozy synoptyków, brak łączności m.in. satelitarnej itd.,	Krytyczna Krytyczna
WOJE-WÓDZ-TWO	System powiadamiania o warunkach atmosferycznych	zbyt późne informacje o pogorszeniach pogody, nadchodzących kataklizmach, brak łączności satelitarnej, awarie stacji meteo, itd.,	Katastrofalna Katastrofalna Krytyczna
GMINA, POWIAT	System ostrzegania o krytycznej liczbie niesprawnego sprzętu w publicznej komunikacji miejskiej i podmiejskiej	błędy obliczeniowe urządzeń, niekompetencja użytkowników, przetrzymywanie informacji przez komórki źródłowe,	Krytyczna Krytyczna Krytyczna
WOJEWÓDZ-TWO GMINA, POWIAT	Prywatne zrzeszenia taksówkarzy	brak stacjonarnej łączności telefonicznej, komórkowej, brak płynnego przepływu informacji, brak zaangażowania prywatnych przewoźników, strajki,	Krytyczna Krytyczna Katastrofalna Krytyczna
WOJE-WÓDZ-TWO	System prognozowania wykorzystania infrastruktury transportowej	brak przepływu informacji, błędnie podjęte decyzje, błędne prognozy symulacji, brak zaangażowania decydentów,	Katastrofalna Katastrofalna Katastrofalna Katastrofalna

Źródło: opracowanie własne.

Tabela 3-49. Scenariusz dla dziedziny komunikacji z podaniem podatności wg. Skali 1-6

DZIEDZINA: TELEKOMUNIKACJA				
Infrastruktura telekomunikacyjna	**Element**	**System**	**Zagrożenia**	**Podatność**
	Węzły łączności	Telefonia i usługi faksowe	Zakłócenia funkcjonowania linii abonenckich, Ataki hackerów na systemy teleinformatyczne, Kradzież informacji przesyłanych drogą elektroniczną, Zakłócenie systemów kierowania, powiadamiania i alarmowania, Zablokowanie rozliczeń i rozrachunków międzybankowych za pomocą elektronicznych nośników	3
		Internet		6
		Transmisja danych		5
		Centrum zarządzania Bazy danych		4
		Wymiana danych w systemach bankowych a w tym: - bankomaty		2

		- kasy fiskalne - transakcje bankowe	informacji, , Kradzież środków finansowych, Zawieranie nielegalnych transakcji Zakłócenia systemu sygnalizacji świetlnej w aglomeracjach miejskich	2 1
	Kanalizacje kablowe (Linie łączności)	System abonencki	Awarie usług telefonicznych Awarie usług teletransmisyjnych brak zasilania urządzeń telekomunikacyjnych	6
		Transmisja danych		3
		Internet		
		Zasilanie		3
	Słupy wieże, Nadajniki radiowe	Telefonia komórkowa	Zakłócenia usług telefonii komórkowej	2
		Telewizja	Wojna informacyjna	4
		Radio	Dezinformacja	5
		Naziemne stacje satelitarne (transpondery, wozy satelitarne)	Zakłócenie w systemie kierowania ruchem lotniczym	4
		System powiadamiana drogą radiową (pagery)	Zakłócenia systemu sygnalizacji świetlnej w aglomeracjach miejskich	2

Źródło: opracowanie własne.

Wśród zaproponowanych różnych scenariuszy występują zarówno te najbardziej prawdopodobne jak i te mało prawdopodobne. Projektując rozwój wypadków dla ewentualnego wystąpienia zagrożenia, możemy projektować strategię postępowania. Jest to żmudna i trudna praca ale w sytuacji krytycznej efektem jest dobre zorganizowanie zarówno zapobiegania jak i rodzenia sobie z kryzysem.

Scenariusze są dobrą metodą uczenia antycypacji i postrzegania zagrożeń a także prospektywnego, kreatywnego myślenia. Ponadto uczy przewidywania pomaga opanować zdolność przydziału sił i środków w trudnych sytuacjach (kryzys).

Tabela 3-50. Scenariusz z wyróżnieniem form ataku dla infrastruktury komunikacyjnej[225]

Rodzaj ataku	Skutki bliższe	Skutki dalsze	Przeciwdziałanie
Atak informatyczny włamanie do sieci sterowania sygnalizacją świetlną węzłów kolejowych Warszawa - Zachodnia , Warszawa – Wschodnia, Siedlce zawirusowanie baz danych spowodowanie wadliwego działania sygnalizacji świetlnej	Całkowite zablokowanie ruchu kolejowego w wymienionych węzłach, doszło do kilku wypadków z ofiarami w ludziach. Przejęcie kontroli nad jak największą liczbą komputerów, które będą wykorzystane do sparaliżowania systemu rezerwacji biletów na loty z (do) Warszawy. Wprowadzenie zmian w systemie międzynarodowej rezerwacji biletów.	Zademonstrowanie możliwości ataku i żądanie okupu – szantaż; Zademonstrowanie możliwości ataku i żądanie okupu – szantaż; Utrata ważnych zasobów informacyjnych. Utrata zaufania klientów do największej polskiej firmy lotniczej, spadek notowań na giełdzie, przejecie Lotu przez konkurencję.	Zorganizowanie lub doskonalenie systemu bezpieczeństwa informatycznego a w tym: Przeprowadzenie analizy ryzyka (przegląd spraw takich, jak: dotychczasowa polityka, zarządzanie ryzykiem; zarządzanie i kontrola nad kontami użytkowników; sterowanie konfiguracją sprzętową i programową; kontrola sesji; bezpieczeństwo sieci; dostęp zdalny; administrowanie systemem; ocena techniczna; reakcja na incydent; audyt; ochrona antywirusowa; planowanie reakcji na przypadkowe zdarzenia; kopie bezpieczeństwa i odzyskiwanie; konserwacja, utrzymanie sprzętu; bezpieczeństwo fizyczne; bezpieczeństwo osobowe; przywracanie funkcji po incydentach). Określenie polityki bezpieczeństwa (określenie procedur i dokumentów operacyjnych. Zorganizowanie ochrony i wdrożenie procedur polityki: Ochrona fizyczna i środowiskowa (kontrola dostępu; ochrona przed pożarami, awariami systemów zasilania i obsługi; ochrona przed przechwyceniem danych); Ochrona informatyczna: filtry i zapory sieciowe (ochrona wewnętrznej sieci informatycznej organizacji przed nieautoryzowanym dostępem z zewnątrz; ochrona przed próbami ataku z sieci zewnętrznej, jak również przed próbami zmodyfikowania jej konfiguracji z wewnętrznej sieci organizacji; ochrona poufności i integralności informacji przechowywanych i przesyłanych w systemie informatycznym organizacji; ochrona przed atakami na dostępność – przed przepełnieniem; ochrona przed atakami wykorzystującymi sfałszowanie adresów urządzeń informatycznych oraz wykorzystującymi luki w bezpieczeństwie oprogramowania; ochrona przed rozpoznaniem – szyfrowanie i hasła); obserwacja sieci, programy antywirusowe, oprogramowanie zabezpieczające. Monitorowanie i doskonalenie systemu bezpieczeństwa informatycznego (reagowanie na incydenty; odtwarzanie informacji i sprawności systemu; zarządzanie ryzykiem; szkolenie personelu; modyfikowanie systemu adekwatne do zmian zagrożeń.

[225] Podane formy ataku za: R. Szpyra, *Scenariusze zagrożeń* [w] T. Jemioło (red.), *Modelowanie walki informacyjnej*. T.II AON, Warszawa 2004, s. 52

Atak elektroniczny Detonacja bomby elekromagnetycznej w rejonie lotniska Okęcie	Zniszczenie urządzeń elektronicznych i elektrycznych sieci; Zniszczenie systemu kontroli ruchu lotniczego.	Całkowite wyeliminowanie sieci informatycznych w budynku portu lotniczego. Odwołanie lotów z Warszawy na 2 tygodnie.	Wykrywanie i ocena zagrożeń; Uodpornienie urządzeń i pomieszczeń na atak elektromagnetyczny. Zorganizowanie kontroli pojazdów wjeżdżających na teren bezpośrednio przylegających do lotniska. Zorganizowanie systemu odtwarzania sprawności systemu po ataku.
Atak ogniowy Zdetonowanie ładunków wybuchowych w jednej ze stacji przepompowującej ropę naftową rurociągu „Przyjaźń"	Zniszczenie urządzeń przepompowujących, spowodowanie wycieku, pożaru i skażenia środowiska na obszarze około 20 ha.	Przerwanie dostaw ropy przez około 2 tygodnie.	Wykrywanie i ocena zagrożeń; Fizyczne uodpornienie sieci na atak ogniowy; Zorganizowanie systemu odtwarzania sprawności systemu po ataku.
Działania psychologiczne Rozpowszechnienie informacji przez media	Umożliwienie dostępu do sieci informatycznej oraz dostępu do niejawnej informacji przez media i osoby nieupoważnione	Zewnętrzny atak informatyczny na sieć; Kradzież niejawnych informacji (np. danych osobowych czy finansowych).	Wykrywanie i ocena zagrożeń; Podnoszenie świadomości stanów osobowych; Doskonalenie procedur kontroli dostępu do informacji.
Dezinformacja Rozsyłanie fałszywych informacji pocztą elektroniczną oraz za pośrednictwem innych środków masowej komunikacji.	Kwestionowanie uczciwych zamiarów przywództwa i kierownictw organizacji i firm oraz kierownictw ich komórek organizacyjnych; Podważanie wiarygodności oraz kwalifikacji wybranych grup personelu.	Wywoływanie zaniepokojenia, pogarszanie nastrojów, próby wywoływania paniki, pogarszanie jakości funkcjonowania miasta.	Szybka reakcja władz miasta i zarządów firm na fałszywe informacje; Sprawne docieranie do mieszkańców miasta i personelu firm z obiektywną informacją; Zachowywanie prawdy w informowaniu; Wykrywanie i napiętnowanie dezinformatorów.

Tabela 3-51. Scenariusz z podaniem form ataku dla obszaru administracji

Rodzaj ataku	Bezpośrednie efekty ataku	Dalsze skutki ataku	Przeciwdziałanie
Atak informatyczny	Blokowanie połączeń – ograniczenie przepustowości łączy sieciowych; Przejęcie kontroli nad systemem – zablokowanie funkcjonowania sieci; Przejęcie kontroli nad jak największą liczbą komputerów, które będą później wykorzystane podczas ataku typu DDoS na inne obiekty prowadzonego za pomocą zainstalowanego skrycie	Kradzież informacji - każda informacja może być celem takiego ataku. Przejęcie numerów kont bankowych, kart kredytowych, danych osobowych, własności intelektualnej; Zademonstrowanie możliwości ataku i żądanie okupu – szantaż.	Zorganizowanie lub doskonalenie systemu bezpieczeństwa informatycznego a w tym: Przeprowadzenie analizy ryzyka (przegląd spraw takich, jak: dotychczasowa polityka, zarządzanie ryzykiem; zarządzanie i kontrola nad kontami użytkowników; sterowanie konfiguracją sprzętową i programową; kontrola sesji; bezpieczeństwo sieci; dostęp zdalny; administrowanie systemem; ocena techniczna; reakcja na incydent; audyt; ochrona antywirusowa; planowanie reakcji na przypadkowe zdarzenia; kopie bezpieczeństwa i odzyskiwanie; konserwacja, utrzymanie sprzętu; bezpieczeństwo fizyczne; bezpieczeństwo osobowe; przywracanie funkcji po incydentach). Określenie polityki bezpieczeństwa (określenie procedur i dokumentów

	oprogramowania; Wykasowanie informacji przechowywanych na dyskach komputerów, niszczenie dysków komputerowych i innych podzespołów stacji roboczych i serwerów.		operacyjnych. Zorganizowanie ochrony i wdrożenie procedur polityki: Ochrona fizyczna i środowiskowa (kontrola dostępu; ochrona przed pożarami, awariami systemów zasilania i obsługi; ochrona przed przechwyceniem danych); Ochrona informatyczna: filtry i zapory sieciowe (ochrona wewnętrznej sieci informatycznej organizacji przed nieautoryzowanym dostępem z zewnątrz; ochrona przed próbami ataku z sieci zewnętrznej, jak również przed próbami zmodyfikowania jej konfiguracji z wewnętrznej sieci organizacji; ochrona poufności i integralności informacji przechowywanych i przesyłanych w systemie informatycznym organizacji; ochrona przed atakami na dostępność – przed przepełnieniem; ochrona przed atakami wykorzystującymi sfałszowanie adresów urządzeń informatycznych oraz wykorzystującymi luki w bezpieczeństwie oprogramowania; ochrona przed rozpoznaniem – szyfrowanie i hasła); obserwacja sieci, programy antywirusowe, oprogramowanie zabezpieczające. Monitorowanie i doskonalenie systemu bezpieczeństwa informatycznego (reagowanie na incydenty; odtwarzanie informacji i sprawności systemu; zarządzanie ryzykiem; szkolenie personelu; modyfikowanie systemu adekwatne do zmian zagrożeń.
Atak elektroniczny Wyzwolenie impulsów elekromagnetycznych w rejonie węzłów sieci;	Zniszczenie urządzeń elektronicznych i elektrycznych; Zniszczenie centrali telefonicznej.	Paraliż sieci informatycznych; Paraliż sieci telefonicznej;	Wykrywanie i ocena zagrożeń; Uodpornienie urządzeń i pomieszczeń na atak elektromagnetyczny; Zorganizowanie systemu odtwarzania sprawności systemu po ataku.
Atak ogniowy Zdetonowanie ładunków wybuchowych w obrębie węzłów sieci; Przerywanie linii magistralnych sieci łączności.	Zniszczenie centrali telefonicznej i serwerowi;	Zakłócenie pracy sieci informatycznych i łączności. Paraliż pracy sieci informatycznych i łączności;	Wykrywanie i ocena zagrożeń; Fizyczne uodpornienie sieci na atak ogniowy; Zorganizowanie systemu odtwarzania sprawności systemu po ataku.
Dezinformacja Rozsyłanie fałszywych informacji kanałami społecznego komunikowania.	Kwestionowanie trafności decyzji podejmowanych przez administrację Podważanie wiarygodności oraz kwalifikacji wybranych grup personelu uczelni;	Wywoływanie zaniepokojenia, pogarszanie nastrojów, panika.	Szybka reakcja informacyjna władz Wykorzystanie samorządu i personelu Zachowywanie prawdy w informowaniu; Wykrywanie i napiętnowanie dezinformatorów.

Metoda ekspercka

Uzupełnieniem badań opinii publicznej, również wykorzystywanej przy budowie scenariuszy, jest metoda badań eksperckich prowadzonych techniką delficką[226] (rysunek 3-52). Dla potrzeb zaprojektowanych badań technikę delficką dostosowano do rozwiązania przyjętych problemów oceny scenariuszy i oceny ryzyka zagrożeń.

Opinie ekspertów opracowywano w oparciu o regułę największej wiarygodności. Prognozą jest opinia najczęstsza wyznaczona ze zbioru opinii powstałego po odrzuceniu opinii skrajnych. Jakość prognoz wyznaczonych na podstawie metod heurystycznych może być określana przez niezależnych ekspertów lub przez wykorzystanie błędów ex post.

Czterech ekspertów poproszono o opinie dotyczące sformułowanych scenariuszy. Zadaniem ekspertów było przypisanie rang, oceniających kolejność według szans wystąpienia określonego scenariusza. (skala rang od 1-5) (tabela 3-52). Oznacza to, że w sumie może przyznać 15 punktów (1+2+3+4+5=15). Średnia suma rang przypadające na jeden scenariusz wynosi 12.

Tabela 3-52. Zestawienie rang dla scenariuszy

Warianty	ekspert				Suma rang
	I	II	III	IV	
Scenariusz I	5	5	5	5	20
Scenariusz Ia	3	2	4	4	13
Scenariusz III	2	4	1	2	9
Scenariusz IV	4	3	2	1	10
Scenariusz V	1	1	3	3	8

Źródło: opracowanie własne.

W celu określenia przeciętnego stopnia zgodności ekspertów (zastosowano skalę porządkową) posłużono się współczynnik zgodności Kendalla, wymaga to obliczenia dwóch statystyk S otrzymanej i maksymalnej. Statystyka S jest sumą kwadratów odchyleń sumy rang przyznanych każdemu ze scenariuszy od średniej sumy rang przypadającej na scenariusz.

---

[226] Metoda delficka została opracowana w latach czterdziestych XX wieku w firmie RAND Corporation przez O. Helmera i N. Dalkey'a (*http://pespmc1.vub.ac.be/ASC/Delphi_metho.html. Delphi Method. Principia Cybernetica Web.)*. Początkowo była to technika przewidywania przyszłych wydarzeń. Z biegiem czasu metoda ta ewoluowała i ostatecznie została zdefiniowana, jako struktura komunikacji grupowej, umożliwiająca rozwiązywanie określonych zadań (C. Jones. *Estimating Software Costs*. McGraw-Hill, New York, 1998.). Jest ona przede wszystkim wycelowana w szczegółową, krytyczną analizę i dyskusję, nie zaś w dążenie za wszelką cenę do osiągnięcia szybkiego kompromisu.

$S = \sum_{j=1}^{k}\left(\sum_{i=1}^{n} x_{ij} - \bar{x}\right)^2$, gdzie ***k***- liczbą scenariuszy, ***n*** jest liczba ekspertów, $\bar{x}$ jest średnią wartością sumy rang dla wszystkich scenariuszy obliczoną ze wzoru: $\bar{x} = \frac{1}{k}\sum_{i=1}^{n}\sum_{j=1}^{k} x_{ij} = 12$. Wobec tego S=82, natomiast wartość maksymalną obliczono ze wzoru: $S_{\max} = \frac{N^2(k^3 - k)}{12} = 160$. Współczynnik zgodności W Kendalla jest stosunkiem uzyskanej wartości S do S_{max}: $W = \frac{S}{S_{\max}} = 0{,}5125$.

Współczynnik pozwala na ocenę zgodności co do kolejności prawdopodobieństwa zrealizowania się poszczególnych scenariuszy. O istotności współczynnika zgodności W decyduje test χ^2 wyrażający się wzorem: χ^2=N(k-1)*W, gdzie N- liczba ekspertów, k- liczba scenariuszy. Wartości testu wynosi χ^2=8,2.

Krytyczna wartość testu χ^2, dla przyjętego stopnia istotności α=0,05 i df=4, wynosi 9,49. Otrzymana wartość χ^2= 8,2 jest mniejsza od wartości krytycznej, co oznacza, że nie można odrzucić hipotezy zerowej o braku związku pomiędzy ocenami scenariuszy ocenianymi przez ekspertów. Należy uznać, że eksperci byli zgodni w wyborze najbardziej prawdopodobnego scenariusza.

Z uporządkowania rang łącznych przypisanych poszczególnym scenariuszom wynika, że największe szanse na realizacje ma scenariusz I, następnie II, IV, III, V jako scenariusz najbardziej prawdopodobny.

W drugim badaniu zastosowano zmodyfikowaną wersje techniki delfickiej dla oceny ryzyka zagrożeń. Zaproponowana autorska metoda określenia ryzyka najgroźniejszych zagrożeń informacyjnych przy pomocy techniki delfickiej wymaga zgromadzania w badaniu ekspertów posiadających duże doświadczenie z obszaru zagrożeń informacyjnych. Sposób postępowania w przypadku analizy ryzyka dokonywanej tą metodą jest następujący:

1) przedstawionym do oceny zagrożeniom przypisuje się kolejne numery;
2) posłużono się pięcioma osobami – ekspertami;
3) każdy ekspert, nie konfrontując swoich ocen z innymi tworzy własną listę rankingową, przypisując poziom ryzyka dla każdego zagrożenia;

4) ustalono, (w założeniach badawczych), że zagrożenie, które powinno być zrealizowane jako pierwsze (największe ryzyko) otrzymuje liczbę punktów równą liczbie ocenionych zagrożeń;
5) każde kolejne otrzymuje o jeden punkt mniej – ostatnie zadanie na liście otrzymuje 1 punkt;
6) punkty przyznane przez każdego eksperta są sumowane i tworzony jest ranking zadań począwszy od tego, które otrzymało najwięcej punktów;
7) aby wyrazić otrzymany wynik w procentach dzieli się liczbę punktów, które otrzymało każde zagrożenie łącznie przez liczbę punktów, którą otrzymało zagrożenie pierwsze na liście;
8) pierwsze na liście zagrożenie ma ryzyko równe 1 (100%), każde następne ma mniej niż 1 (100%). Jest możliwe uzyskanie przez dwa lub więcej zagrożeń takiego samego wyniku punktowego.

Eksperci do oceny otrzymali zestaw zagrożeń dla bezpieczeństwa narodowego z obszaru zagrożeń informacyjnych. Zestaw zagrożeń stanowił podstawę badania postrzegania ryzyka (rozdział III, tabela 3-32).

Założenia ustalenia ryzyka zagrożeń informacyjnych z zastosowaniem metody delfickiej przy założeniu, że:

- grupa wyznaczona do oceny ryzyka liczy 5 osób,
- ocenie poddaje się 17 zagrożeń informacyjnych,
- ranking zagrożeń ustalono według punktu 8.

Tabela 3-53. Delficka metoda analizy ryzyka

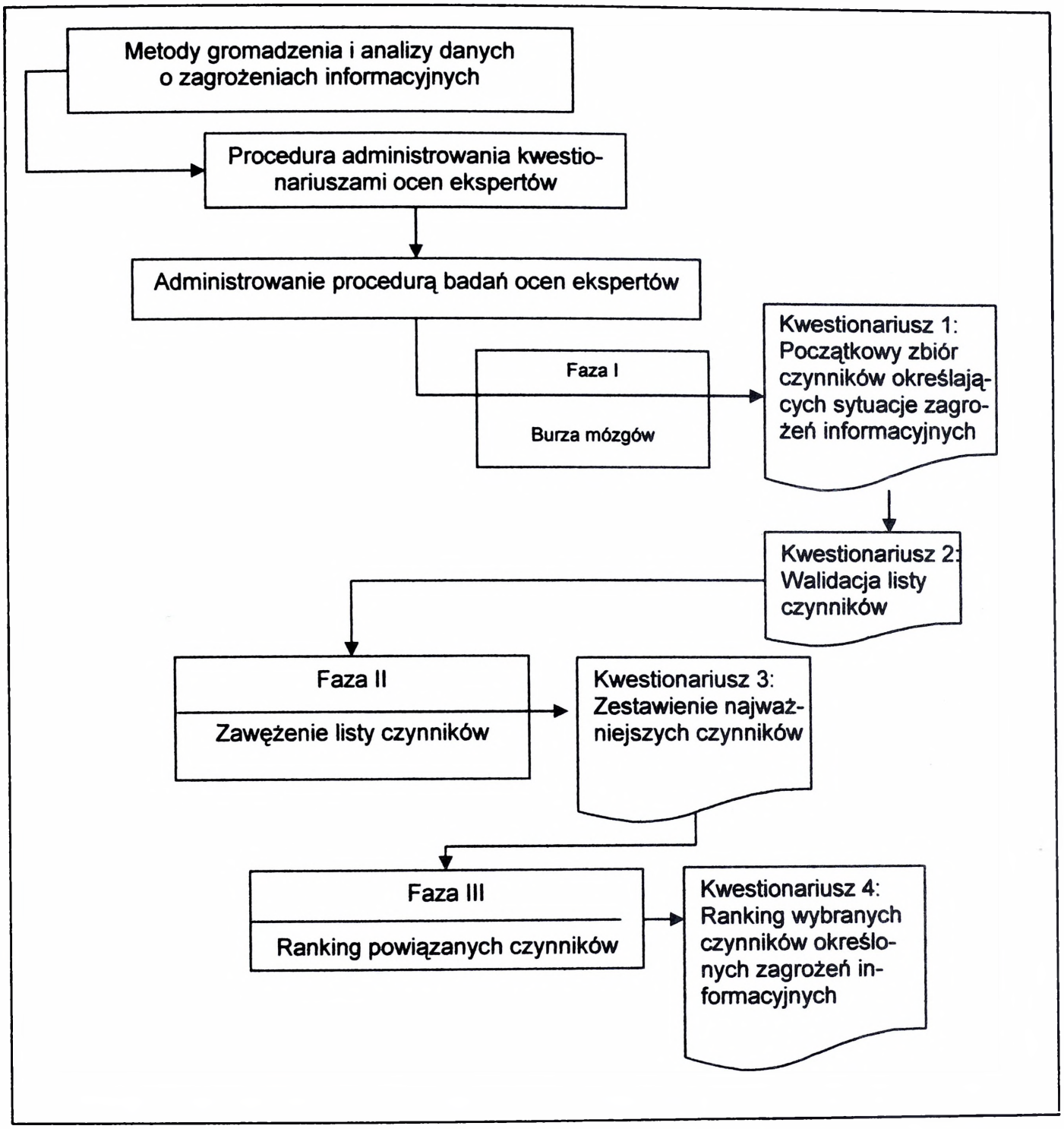
Lp	Zagrożenia	Eksperci					Suma uzyskanych punktów	Pozycja w rankingu	Ocena ryzyka
		I	II	III	IV	V			
1	Cyberteroryzm (infoteroryzm)	3	3	2	2	4	14	15	21%
2	Zakłócenia krytycznej infrastruktury państwa RP	4	4	4	1	2	15	14	22%
3	Hackerstwo	5	5	3	4	1	18	12	27%
4	Przechwytywanie danych	2	9	8	5	5	29	10	43%
5	Oszustwa bankowe	9	6	7	3	3	28	11	42%
6	Ograniczony dostęp do informacji	1	1	2	6	6	16	13	24%
7	Spam - rozsyłanie niechcianej poczty elektroniczne	7	2	5	7	9	30	9	45%
8	"Wojny (cybernetyczne) hakerskie" (np.Estonia) (cybe-	15	8	9	9	10	51	6	76%

Lp	Zagrożenia	Eksperci					Suma uzyskanych punktów	Pozycja w rankingu	Ocena ryzyka
		I	II	III	IV	V			
	rwar)								
9	Cybernetyczny atak na szczeblu państwowym	6	14	6	8	15	49	8	73%
10	Blokady serwerów rządowych RP	12	10	12	10	6	50	7	75%
11	Podsłuchiwanie transmisji w sieci	11	14	11	14	10	60	3	90%
12	Trojan / konie trojańskie	10	11	10	11	11	53	5	79%
13	Sabotaż komputerowy	14	13	13	13	14	67	1	100%
14	Zniszczenie danych lub programów komputerowych	13	12	14	12	13	64	2	96%
15	Atak na serwer (WWW, DNS, inne...)	8	7	15	14	12	56	4	84%
16	Atak na system operacyjny	12	14	15	7	8	56	4	84%
17	Inżynieria społeczna *(Social engineering)*	14	13	13	13	14	67	1	100%

Źródło: opracowanie własne.

Interpretacja wyniku:

Za zagrożenia o najwyższym ryzyku uznano: inżynierię społeczną, sabotaż komputerowy, podsłuchiwanie transmisji w sieci, ataki na serwery (WWW, DNS), ataki na system operacyjny.



Rysunek 3-52. Proces gromadzenia oraz analizy danych o zagrożeniach informacyjnych za pomocą techniki delfickiej

Źródło: opracowanie własne.

3.5. Wnioski

Prognozy stanowią podstawę podejmowania racjonalnych decyzji. Ma to szczególne znaczenie w przypadku zagrożeń informacyjnych, których obiektem mogą być systemy krytycznej infrastruktury państwa (KIP). Celem prognozowania jest określenie kierunku i dynamiki zmian badanych wielkości w przyszłości oraz przygotowanie działań wspomagających przedsięwzięcia planistyczne, w systemie zarządzania bezpieczeństwem państwa.

Przeprowadzone badania nad przydatnością, modeli zarówno ilościowych jak i jakościowych, do prognozowania zagrożeń informacyjnych, pozwoliło na wyciągnięcie

wniosków, zarówno natury ogólnej, jak i bardzo szczegółowych dotyczących poszczególnych metod prognozowania. Ponadto badanie społecznej percepcji zagrożeń informacyjnych (sondaż) pozwoliło na uszeregowanie, według przyjętego kryterium „wagi" ryzyka ich pojawiania się w kontekście „wzburzenia społecznego". Prognozowanie scenariuszowe jest przykładem antycypacyjnego projektowania przyszłości w sytuacjach trudno przewidywalnych, incydentalnych.

Każda z zastosowanych metod prognozowania podlega pewnym ograniczeniom, które wynikają z istoty przyjętego modelu, jak i długości horyzontu prognozy a także z podejścia do problemu prognoz ściśle związanego z teorią podejmowania decyzji.[227] Głównym jednak warunkiem musi być założenie o stałości otocznia, a także braku zmian w zjawisku poddawanym predykcji. Zastrzeżenie „stałości otoczenia" dotyczy również stosowania sztucznych sieci neuronowych, jak i każdej innej ilościowej metody. Natomiast nie ma to znaczenia w prognozowaniu z wykorzystaniem modeli jakościowych.

Zwykle w zjawiskach występują „ewolucyjne" transpozycje, niosąc zmiany w prawidłowościach występowania pewnych tendencji (wzrostu, spadku). Wiele zagrożeń ma charakter masowy, a to pozwala na wykorzystanie metod opartych na analizie szeregów czasowych i sztucznych sieci neuronowych. Przy czym wymagana jest dobra znajomość zarówno prognozowego zjawiska, jak i otoczenia. Wiedza ta pomocna jest w interpretacji otrzymanej prognozy, pozwala ustalić wpływ niektórych czynników z otoczenia na przebieg zjawiska.[228] Zasada ta dotyczy również prognozowania modeli jakościowych. Niektóre z zagrożeń występują incydentalnie. W takich sytuacjach klasyczne prognozowanie pozostaje bezradne. Pomocą w podejmowaniu decyzji mogą służyć metody projektowania przyszłości: scenariusze, a przede wszystkim prognozowanie typu Foresight[229]. Metody te pozwalają: w przypadku scenariuszy, na budowanie różnych (odpowiednich) strategii postępowania w zależności od rodzaju scenariusza, a w drugim przypadku obok prognozowania, projektuje się działania wywierające wpływ na prognozowane zjawiska. W metodzie scenariuszy wykorzystuje się techniki oparte na wiedzy ekspertów (Delphi, AWOT,

---

[227] Według tej teorii prognoza powinna być tak zbudowana by zabezpieczała przed ponoszeniem zbyt dużych strat W myśl tej koncepcji staramy się odpowiedzieć na pytanie, jakie są koszty popełnianej pomyłki. Wynika to z tego, że w zbiorze dopuszczalnych decyzji mogą istnieć decyzje „fałszywe", których podjęcie naraża na mniejsze lub większe straty.

[228] Np. zasadność takiego twierdzenia możemy odnieść do problemu, jaki wystąpił w przypadku prognozowania zagrożenia informacyjnego typu „ogólna liczba incydentów". W analizie danych w 2005 roku nastąpił gwałtowny spadek incydentów poczym nastąpił gwałtowny wzrost. Zmianę można wytłumaczyć zwiększeniem skuteczności zabezpieczeń.

[229] Foresight, pojęcie nie ma polskiego odpowiednika, jest to systematyczny sposób budowania średnio- i długookresowej wizji rozwoju zjawiska. Według tej metodologii realizowany jest Narodowy Program Foresight „Polska 2020" prowadzony z inicjatywy MNiSzW

PEST), metody ilościowe (ekstrapolacja trendów, modelowanie) oraz służące do identyfikacji działań projektujących wpływ na prognozowane zjawiska (np.: drzewo odniesień).

Wnioski ogólne dotyczące procesu prognozowania:

- zdecydowanie lepsze prognozy otrzymujemy w prognozowaniu krótkookresowym.
- W prognozowaniu zagrożeń informacyjnych, (na przebieg zjawiska może mieć wpływ sytuacja polityczna) niezbędna jest potrzeba dobrej znajomości otoczenia i samego zjawiska.
- Aby prognozy mogły powstawać, system zbierania informacji powinien być wszechstronnie rozwinięty i ciągle doskonalony.
- Gnoseologiczne podstawy prognozowania związane z narastającą wiedzą o zjawiskach (zagrożeniach) pozwalają sądzić, że prognozy w miarę postępu nauki będą coraz lepsze tzn. trafniejsze i dokładniejsze.

Wnioski dotyczące prognozowania z zastosowaniem modeli adaptacyjnych

- Model prostego wygładzania wykładniczego może być stosowany przy założeniu, że wartości stałej wygładzania danego szeregu czasowego, dobiera się każdorazowo dla danego szeregu czasowego. Ponadto może być stosowany do prognozowania krótkookresowego.
- Najlepsze wyniki w sensie założonego błędu prognozy, osiągnięto stosując model Holta.
- Prognozowanie z wykorzystaniem modelu średniej ruchomej i średniej ruchomej ważonej, bardziej nadaje się do wygładzania szeregu, bowiem prognozy punktowe w świetle przyjętych kryteriów, obarczone są dużym błędem. Jest to natomiast doskonałe narzędzie do rozpoznawania tendencji
- W przypadku dużej ilości danych, sprawdzają się modele Wintersa - multiplikatywny i addytywny - przy założeniu każdorazowego ustalania wartości stałych wygładzania.

Wnioski dotyczące prognozowania w oparciu o sztuczne sieci neuronowe:

- Głównym problemem jest właściwe określenie czasu trwania procesu uczenia.
- Ze względu na dynamiczny charakter szeregów czasowych, potrzebne jest posiadanie nieliniowych narzędzi w celu rozpoznawania zależności wśród danych.
- Sieci neuronowe radzą sobie z niepełnymi lub zakłóconymi (odstającymi) danymi.

- Sieci neuronowe szybko wykazywały oznaki przeuczenia dopasowując się do danych.
- W stosunku do prognoz otrzymanych z modeli adaptacyjnych, prognozy wykazują większe odchylenia od danych empirycznych, większe są również błędy prognozy.
- Ponieważ prognozowanie szeregów czasowych za pomocą sztucznych sieci neuronowych z wykorzystaniem *time series*, w których nie są stosowne metody klasyfikacji (na zasadzie podobieństw) wyznaczone prognozy były obarczone większymi błędami.[230] Nie dyskwalifikuje to sztucznych sieci neuronowych w prognozowaniu. Obie metody mogą być skutecznymi narzędziami prognozowania. Można wykorzystywać je do wzajemnych weryfikacji prognoz.

Wyniki badań społecznej percepcji zagrożeń informacyjnych bezpieczeństwa:

- Badana grupa w ogólnej ocenie poczucia bezpieczeństwa, reprezentuje średni stopień odczuwania zagrożenia. Tylko w niektórych przypadkach zjawiska odbierane są jako niebezpieczne w dużym i wysokim stopniu zagrożenia. Zagrożenia w dużym stopniu, postrzegane są przez około 40% badanej grupy.
- Za szczególnie niebezpieczne dla bezpieczeństwa narodowego badani uznali zagrożenia globalnym kryzysem energetycznym oraz cyberterroryzm.
- Badani najbardziej obawiają się manipulacji informacją w mediach (w stopniu dużym 37% i wysokim 27%).
- Dla wzrostu bezpieczeństwa badani ponieśliby dodatkowe obciążenia, rezygnując na rzecz bezpieczeństwa z części wolności. Na częściowe ograniczenie swobód obywatelskich zgodziłoby się 62% badanych.
- Cyberterroryzm bywa kojarzony z ogółem przestępstw w cyberprzestrzeni.
- Zagrożenia informatyczne w większości postrzegane są w dużym stopniu zagrożenia, szczególnie w odniesieniu do przestępstw bankowych.
- Podsłuch sieci jest zagrożeniem, którego szczególnie obawiają się badani.
- Badani wykazują małą obawę przed *social engineering*, obecnie najbardziej niebezpiecznego narzędzia stosownego w pozyskiwaniu danych nastawionego na wykorzystywanie słabości ludzkich.
- Za zagrożenia o dużym stopniu ryzyka badani uznali takie, jak: przechwytywanie danych (33%), hakerstwo (32%), oszustwa bankowe (33%), podsłuchiwanie

[230] Sieci neuronowe stosowne jako oprogramowanie w monitoringu, radzą sobie doskonale z rozpoznawaniem zagrożeń na zasadzie porównywania zdarzeń.

transmisji w sieci (37%), złośliwe oprogramowanie w formie koni trojanów (27%), cybernetyczny atak na szczeblu państwowym (26%), zniszczenie danych lub programów komputerowych (37%), ataki na serwer WWW, DNS, i inne (30%). Ataki na system operacyjny w celu przejęcia nad nim kontroli, również zostały zaklasyfikowane do ataków o dużym stopniu niebezpieczeństwa.

Wnioski z badań społecznej percepcji zagrożeń informacyjnych dla bezpieczeństwa

- Świadomość zarówno występujących zagrożeń, jak i ryzyk, a także sposobów przeciwdziałania, czy zabezpieczania się, jest dalece niewystarczająca.
- Z analizy wyników badania wynika, że badani bardziej kojarzą zjawiska z częstością ich występowania, niż ze skutkami ich wystąpienia.
- Badani bardziej skłonni są akceptować zagrożenia występujące częściej z mniejszymi skutkami tych zdarzeń, niż z występującymi rzadziej, ale z dotkliwszymi konsekwencjami.
- Postrzegane są zagrożenia częściej występujące lub, o których szerzej się informuje, albo, z którym badani osobiście się zetknęli.
- Percepcja badanych zależy przede wszystkim od stopnia doświadczenia, umiejętności i wiedzy.
- Im większe poczucie zagrożenia, tym częściej ludzie uciekają się do praktyk zabobonów, myślenia magicznego.

Wnioski z prognozowania scenariuszowego

- Sprawdzają się w prognozowania zagrożeń incydentalnych i trudno przewidywalnych.
- Dają możliwość nauki antycypacyjnego przewidywania zagrożeń oraz prospektywnego modelownia przyszłości.
- Stwarzają możliwość nauki optymalnego rozdziału sił i środków w sytuacjach kryzysowych.
- Uczą planowania i oswajają z ewentualnym wystąpieniem sytuacji kryzysowych.

Tabela 3-54. Zbiorcze zestawienie charakterystyki modeli prognostycznych

Prognozy / Model prognostyczny		Charakterystyka					
		Horyzont czasowy	**Stopień szczegółowości**	**Cel prognozy**	**Metoda opracowania**	**Charakter lub struktura**	**Ocena**
Adaptacyjne modele trendu	Średnie ruchome proste i ważone	Krótkoterminowa, operacyjna	Szczegółowe dotyczące pewnego aspektu zagrożeń	Ostrzegawcze, badawcze, stanowiące podstawę podejmowania decyzji	Prognozy czyste, pierwotne, modelowe. Ekstrapolacja zaobserwowanego trendu badanego zjawiska	Ilościowe	Przydatne jeśli spełniają warunki podane we wnioskach
	Proste wygładzanie wykładnicze	Krótkoterminowa, operacyjna					
	Holt	Średnioterminowa, Operacyjna					
	Winters	Długoterminowa, operacyjna					
Sztuczne sieci neuronowe		Krótkoterminowa, operacyjna	Szczegółowe		Prognozy czyste, pierwotne Ekstrapolacja trendu modelowe	Ilościowe	Przydatne w określonych warunkach
Sondaż		Perspektywiczna, strategiczna	Szczegółowe/ ogólne		Projektowane	Jakościowe	Przydatne jako uzupełnienie metod ilościowych
Scenariusze		Długoterminowa, perspektywiczna, strategiczna	Szczegółowe/ ogólne		Projektowane	Jakościowe	Przydatne jako uzupełnienie metod ilościowych

Źródło: opracowanie własne.

Rozdział 4

MODEL ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACYJNYM RP

4.1. Wprowadzenie

Współcześnie jednym z krytycznych problemów zarządzania bezpieczeństwem narodowym jest zapewnienie bezpieczeństwa informacyjnego, na każdym szczeblu zarządzania, we wszystkich organizacjach bez względu na ich status prawny. Na władzach ustawodawczych i wykonawczych spoczywa obowiązek określenia wymaganego poziomu bezpieczeństwa informacyjnego oraz warunków jego spełnienia. Szczególne znaczenie przypada podmiotom realizującym zadania publiczne, w których następuje wymiana informacji w formie elektronicznej pomiędzy, np.: administracją a obywatelami, administracją a podmiotami gospodarczymi i organizacjami (np. uczelniami, instytutami itp.), pomiędzy różnymi organizacjami administracji publicznej, rządowej i samorządowej oraz administracją kraju a administracjami, UE lub innych państw. Wynika stąd nie tylko potrzeba zorganizowanego zapewniania bezpieczeństwa informacyjnego, ale również potrzeba interoperacyjności, czyli „zdolności do współdziałania".[231] Interoperacyjność powinna być realizowana w trzech oddziaływujących płaszczyznach: organizacyjnej, informacyjnej i technicznej.[232]

Procesom zapewniania bezpieczeństwa, jak i wszystkim społecznym działaniom, towarzyszy ryzyko, które jest atrybutem realnych sytuacji decyzyjnych. Jest nierozerwalnie związane z bezpieczeństwem, definiowanym np. jako brak zagrożeń. Niedoskonałość definicji ryzyka, a także utopijność tak abstrakcyjnej sytuacji, jak teza o „całkowitym braku ryzyka" („wyzerowaniu ryzyka") skłania do ustalenia bezpieczeństwa jako stanu otoczenia cywilizacyjnego i środowiska naturalnego dowolnej społeczności, który określony jest przez poziom całościowego ryzyka w nich występującego.[233] Dlatego też wyrazem bezpieczeństwa jest zapewnienie swoistej równowagi między zagrożeniami a zabezpieczeniami (rysunek 4-1).[234]

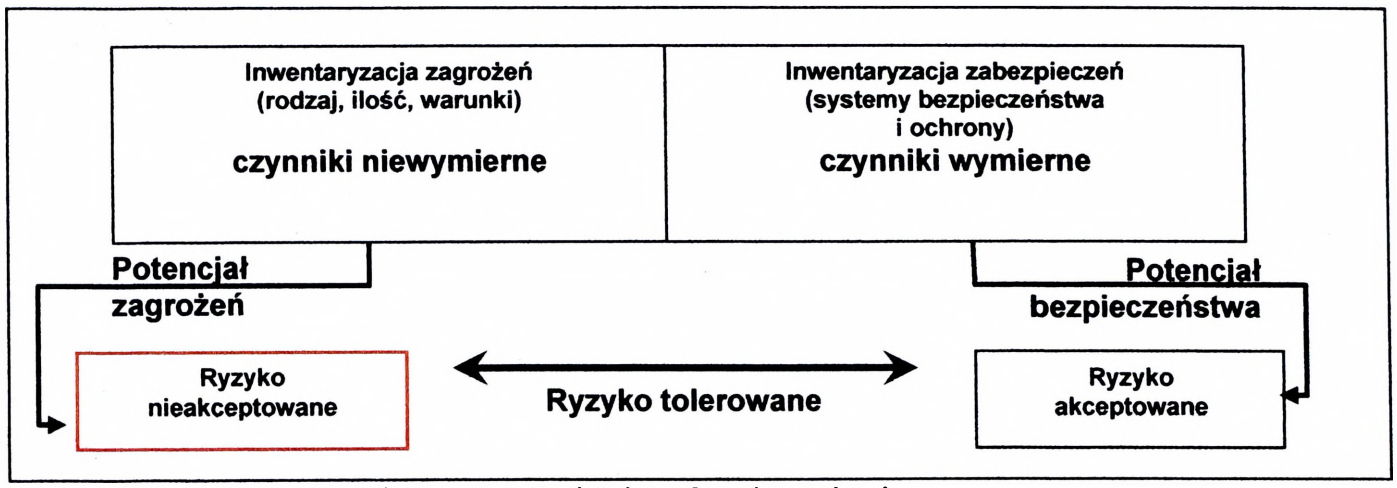
---

[231] Problemy interoperacyjności w obszarze sił zbrojnych szczegółowo omawia J.Dereń w pracy doktorskiej. Op.cit.

[232] Zob. B.Szafrański (red.), *Interoperacyjność i bezpieczeństwo systemów informatycznych.* PTI Oddział Górnośląski, Katowice 2006.

[233] P. Sienkiewicz (red), *Zarządzanie ryzykiem,...,* 2006,op.cit., s. 43.

[234] P. Sienkiewicz, Bezpieczeństwo i wolność w globalnym społeczeństwie informacyjnym. AGH, Kraków 2007.



Rysunek 4-1. Równowaga między zagrożeniami a zabezpieczeniami

Źródło: P. Sienkiewicz, (red), *Zarządzanie ryzykiem w sytuacjach kryzysowych*. AON, Warszawa 2006, s.70.

W sytuacji zapewnienia bezpieczeństwa podstawową klasą systemów problemowych są sytuacje decyzyjne, czyli wyboru wariantu działania spośród wariantów dopuszczalnych.

Podczas objaśniania realnych sytuacji problemowych rozpatruje się na ogół:[235]

- ryzyko obejmujące zjawiska (procesy) dokonujące się poza człowiekiem w jego otoczeniu, ale wskutek jego udziału wywołujące niepożądane skutki;
- ryzyko jako niebezpieczne przedsięwzięcie podjęte przez człowieka i charakteryzujące jego odwagę.

Ze względu na charakter informacji o możliwych i prawdopodobnych stanach rzeczy (natury, otoczenia) wyróżnia się (rysunek 4-2):[236] sytuacje pewne, sytuacje niepewne, sytuacje ryzykowne. Ryzykiem jest zatem zespół czynników, działań (przedsięwzięć) lub czynności, powodujących szkody lub straty (materialne), bądź skutki negatywne (odmienne od zamierzonych, pożądanych, oczekiwanych). [237]

4.2. Zarządzanie ryzykiem

Skuteczny system bezpieczeństwa wymaga sprawnego zarządzania ryzykiem zagrożeń informacyjnych, dlatego najistotniejszym wymaganiem stała się identyfikacja i taksonomia ryzyka bowiem od poprawności ich identyfikacji zagrożeń zależy właściwy wybór efektywnych środków przeciwdziałania. Interdyscyplinarne podstawy metodologii analizy ryzyka pozwalają na implementację metod do specyficznych potrzeb takiej analizy. W procesie identyfikacji i opisu szczególną uwagę należy zwrócić na odróżnienie zagrożenia, przyczyny jego

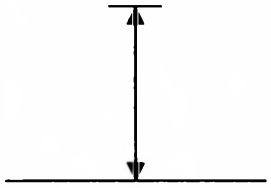
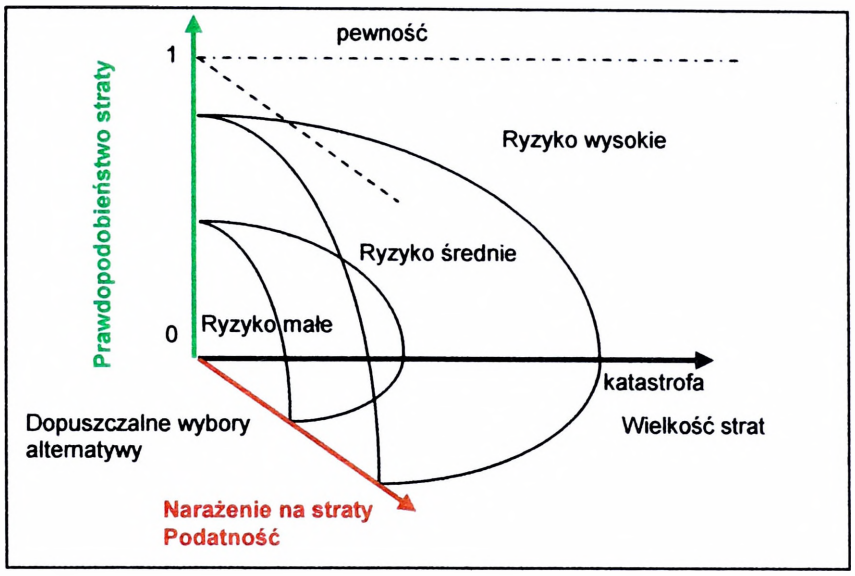
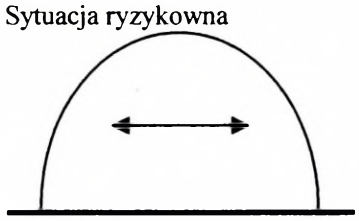
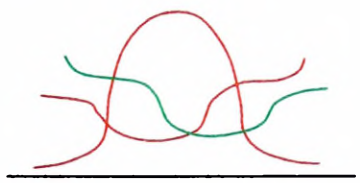
---

[235] T.Kaczmarek, *Ryzyko i zarządzanie ryzykiem*, Difin, Warszawa 2006.

[236] P.Sienkiewicz, *Inżynieria systemów*. MON, Warszawa 1983; *Analiza systemowa*, Bellona, Warszawa 1995; *Teoretyczne podstawy zarządzania ryzykiem*. ZN 4(68) AON, 2007.

[237] Ryzyko różni się od niebezpieczeństwa, które oznacza raczej pewne bezpośrednie zagrożenie, czyli pewna strata nie jest ryzykiem. Jednakże najczęściej przyjmuje się, że o bezpieczeństwie jest sens mówić, gdy istnieje niebezpieczeństwo, a więc występuje zagrożenie, a wtedy pojawia się kwestia ryzyka.

powstania od skutku jego realizacji, aby uniknąć działań typu „walka ze skutkami, lecz nie z przyczynami".

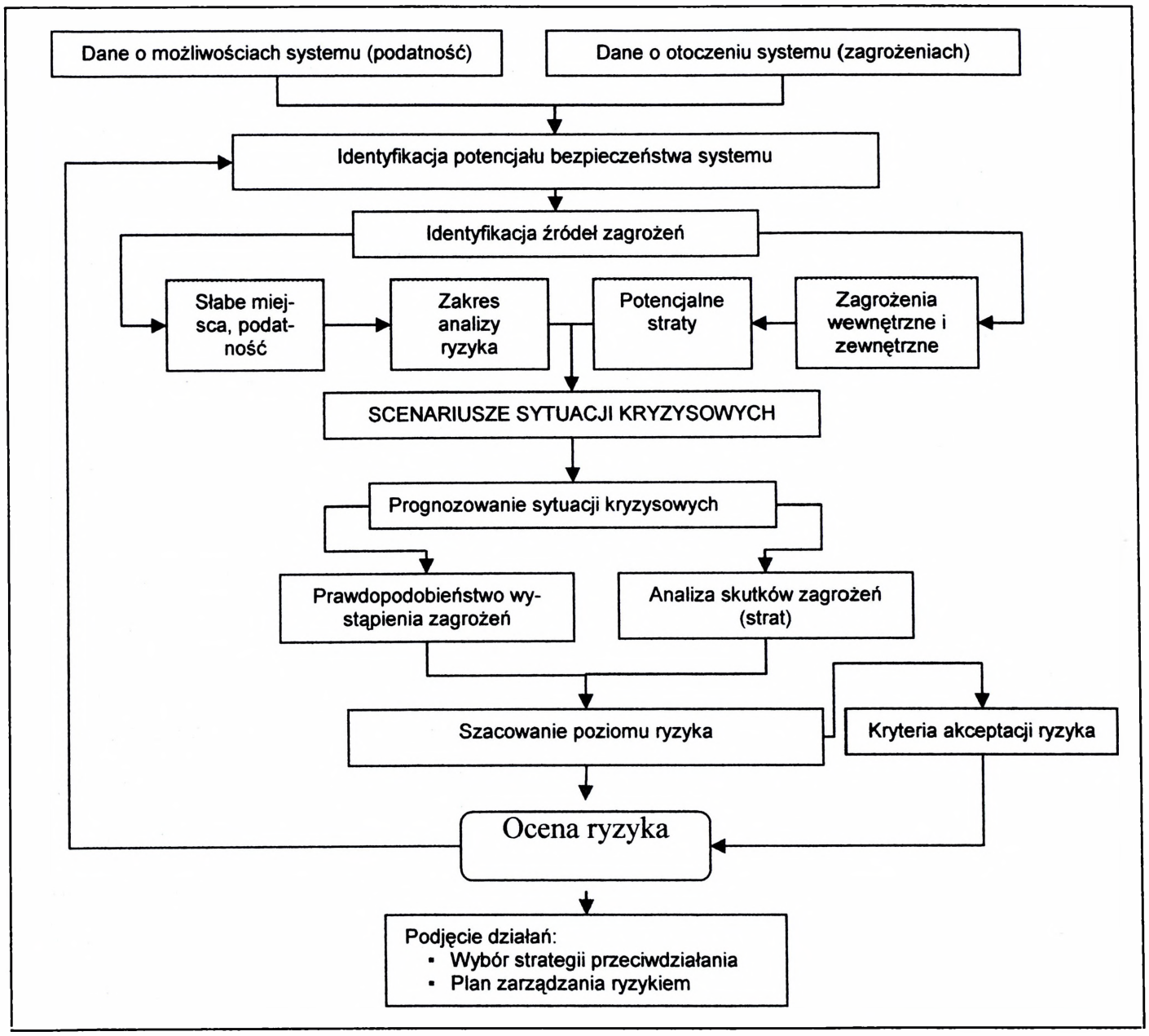
LP	SYTUACJA DECYZYJNA	EWALUACJA RYZYKA
1	Sytuacja pewna Prawdopodobieństwo = 1  zdarzenie	
2	Sytuacja ryzykowna  zdarzenie	
3	Sytuacja niepewna  zdarzenie	

Rysunek 4-2. Sytuacje decyzyjne i charakter sytuacji
Źródło: P.Sienkiewicz, *Ewaluacja ryzyka w zarządzaniu kryzysowym.* AON, 2009 (w druku).

Drugim bardzo istotnym założeniem jest oddzielenie zagrożenia od podatności systemu (wrażliwości). Oceny ryzyka dokonuje się za pomocą metod jakościowych lub ilościowych. W przypadku metod jakościowych efekty analizy uzyskuje się w postaci opisowej, np. ryzyko niskie, średnie, duże lub większe niż,..., mniejsze niż,.... itp. W przypadku metod ilościowych wyniki stanowią konkretne jednostki miar, np. kwoty pieniężne lub prawdopodobieństwo, wariancja, współczynnik zmienności itp. Istotą ewaluacji ryzyka jest oszacowanie prawdopodobieństwa wystąpienia zdarzeń oraz zbadanie związków przyczynowo-skutkowych między kolejnymi zdarzeniami (korelacje). Ryzyko obliczeniowe traktuje się jako funkcję prawdopodobieństwa wystąpienia zagrożeń oraz wartości możliwych strat powstałych jako rezultat zagrożeń. Trudności kumulują się, gdy między kolejnymi zdarzeniami istnieją zależności statystyczne oraz gdy ocenie poddajemy zdarzenia określane według formuły, dla których przyjęto, że ryzyko jest funkcją ryzyka obliczeniowego i „społecznego

wzburzenia", czyli ryzyka uwzględniającego społeczne postrzeganie. Społeczne wzburzenie jest tak samo rzeczywiste jak ryzyko obliczeniowe.[238]

Niezależnie od segmentu, w którym funkcjonuje organizacja czy podejmowane są działania a także niezależnie od szczegółowości analizy - analiza ryzyka przebiega według uniwersalnego schematu (rysunek 4-3). Na każdym z poziomów analizy odbywa się dokumentowanie wyników wnioskowania.



Rysunek 4-3. Model oceny ryzyka w sytuacjach kryzysowych

Źródło: na podstawie: P.Sienkiewicz (red.), *Zarządzanie ryzykiem w sytuacjach kryzysowych*. AON, Warszawa 2006, s. 43.

W przypadku obiektów o szczególnym znaczeniu należy uwzględnić szczegółową analizę otoczenia, to znaczy zwrócić uwagę na obiekty położone w bliskim otoczeniu oraz na to, w jaki sposób mogą one wpłynąć na nasze bezpieczeństwo. Ma to istotne znaczenie w przypadku realizacji ryzyka, gdy następuje jego rozprzestrzenianie się (efekt domina).

[238] P. Sandman, Responding to Community Outrage: Strategies for effective Risk Communication. American Industrial Hyguene Association Fairfax. 1997.

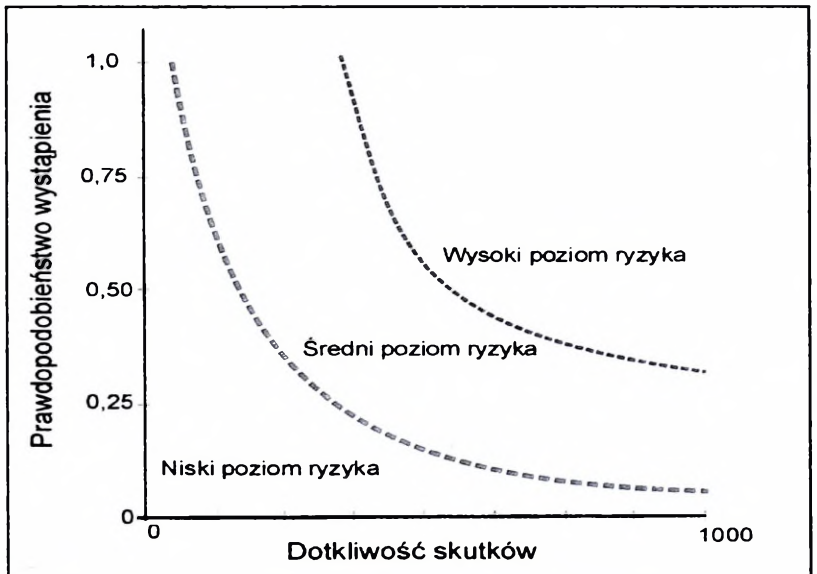
Wśród źródeł, z których należy czerpać informacje, a które dotyczą poziomu zagrożeń należy uwzględniać oceny poziomu zagrożeń formułowane przez instytucje między innymi takie, jak np.: odpowiedzialne za bezpieczeństwo (instytucjonalnie), firmy ubezpieczeniowe, ochrony, media, inne instytucje analityczne.

Należy zauważyć, że nie ma jednej uniwersalnej i „absolutnie doskonałej" klasyfikacji ryzyka. Ze względu na różnorodność spotykanych rodzajów ryzyka, dynamikę ich zmian, jak również aktualne wymagania analiz, odmienne kryteria klasyfikacji mogą stanowić podstawę ich podziału. Nie są to podziały rozłączne, wręcz przeciwne, poszczególne ryzyka mogą być zaszeregowane do kilku różnych klas. Stwarza to dodatkowe trudności analityczne, wobec których metody ilościowe są mało użyteczne.

Potocznie ryzyko rozumiane jest jako możliwość niepowodzenia, straty.[239]

Ryzyko	=	*Prawdopodobieństwo wystąpienia straty*	x	*Wartość straty*

Wtedy prawdopodobieństwo określa liczbę zdarzeń powodujących straty w ciągu roku, a wartość starty jest stratą pojedynczego wystąpienia ryzyka. Skutek i prawdopodobieństwo są wielkościami całkowicie od siebie nie zależnymi, dlatego też wymagają odrębnej analizy (rysunek 4-4). W analizach ryzyka najczęściej używa się prawdopodobieństwa w sensie częstości występowania zjawiska w określonym czasie lub prawdopodobieństw subiektywnych. Ryzyko ma wiele znaczeń, np. w technice kojarzone jest z pojęciem hazardu[240], w ubezpieczeniach łączone jest ze szkodami wywołanymi siłami przyrody, w ekonomii z niepewnymi inwestycjami.



Rysunek 4-4. Prawdopodobieństwo jako funkcja niepowodzeń i wielkości straty

Źródło: P.Sienkiewicz, *Analiza zarządzania ryzykiem projektów*, konferencja Rynia 2005.

[239] W literaturze a także w dokumencie wydanym przez ISO (Międzynarodową Organizację Normalizacyjną) „Zalecenia ISO/IEC nr 73. Zarządzanie ryzykiem – Słownictwo – Wytyczne dla norm definiuje się je w sensie funkcji: „dwóch zmiennych prawdopodobieństwa niepowodzenia i wielkości straty".

[240] Hazard – to ryzykowne przedsięwzięcie, którego wynik zależy wyłącznie od przypadku, także narażenie się na niebezpieczeństwo.

W ocenie ryzyka do jego szacowania przyjęto dwie grupy metod: kwantyfikatywne (ilościowe) i kwalifikatywne (jakościowe). Ilościowe wykorzystują obliczenia matematyczne operując danymi statystycznymi i historycznymi, a jakościowe korzystają z wiedzy i ocen ekspertów stosując miary opisowe.[241] Prawdopodobieństwa wyznacza się w oparciu o dane statystyczne, oszacowania ekspertów w tym oszacowania z zastosowaniem metody delfickiej. Wśród metod jakościowych stosuje się techniki takie, jak: HAZOP, FMEA, metoda drzewa błędów, metoda drzewa zdarzeń wiele innych.

W systemach informatycznych aby ocenić ryzyko musimy „wycenić" chronione zasoby, które stanowią o dotkliwości skutków.[242] W przypadku złożonych systemów korzystamy z modelu, w którym uwzględnimy wartość chronionych zasobów oraz podatność systemu na zagrożenia. Wówczas ryzyko jest iloczynem trzech wartości: prawdopodobieństwa zagrożeń, prawdopodobieństwa podatności systemu[243] i wartości potencjalnych strat: $R(z)=P(z)*V(z)*C(z)$.

Zarządzanie ryzykiem można określić jako podejmowanie decyzji w sposób zapewniający jak najwyższy poziom bezpieczeństwa, realizowany poprzez ograniczanie wpływu przewidywalnych czynników zagrożeń. Stąd zarządzanie ryzykiem koncentruje się na zapobieganiu szkodom i ich ograniczaniu. W procesie zarządzania ryzykiem wyróżnia się dwie fazy[244]: (1) analizy ryzyka oraz (2) zarządzania ryzykiem (rysunek 4-5).

W fazie zarządzania następuje opracowanie zasad postępowania z ryzykiem.[245] Zapewnieniu bezpieczeństwa sprzyja konstruowanie map zagrożeń, które mogą stanowić pod-

---

[241] Podstawowe elementy procesu zarządzania ryzykiem (w kontekście ryzyka informacyjnego) oparte są o uznane standardy: brytyjski standard Risk Management Standard (4360 Standard promowany jest przez FERMA (*Federation of European Risk Management Asssociatios*)) i australijski AS/NZS.

[242] W wycenie uwzględniamy np. wartość zasobów dla właściciela, koszt odtworzenia lub odzyskania zasobu, koszt pośredni np. utrata klientów, naruszenie dobrej opinii firmy, straty wynikające z zablokowania pracy systemu.

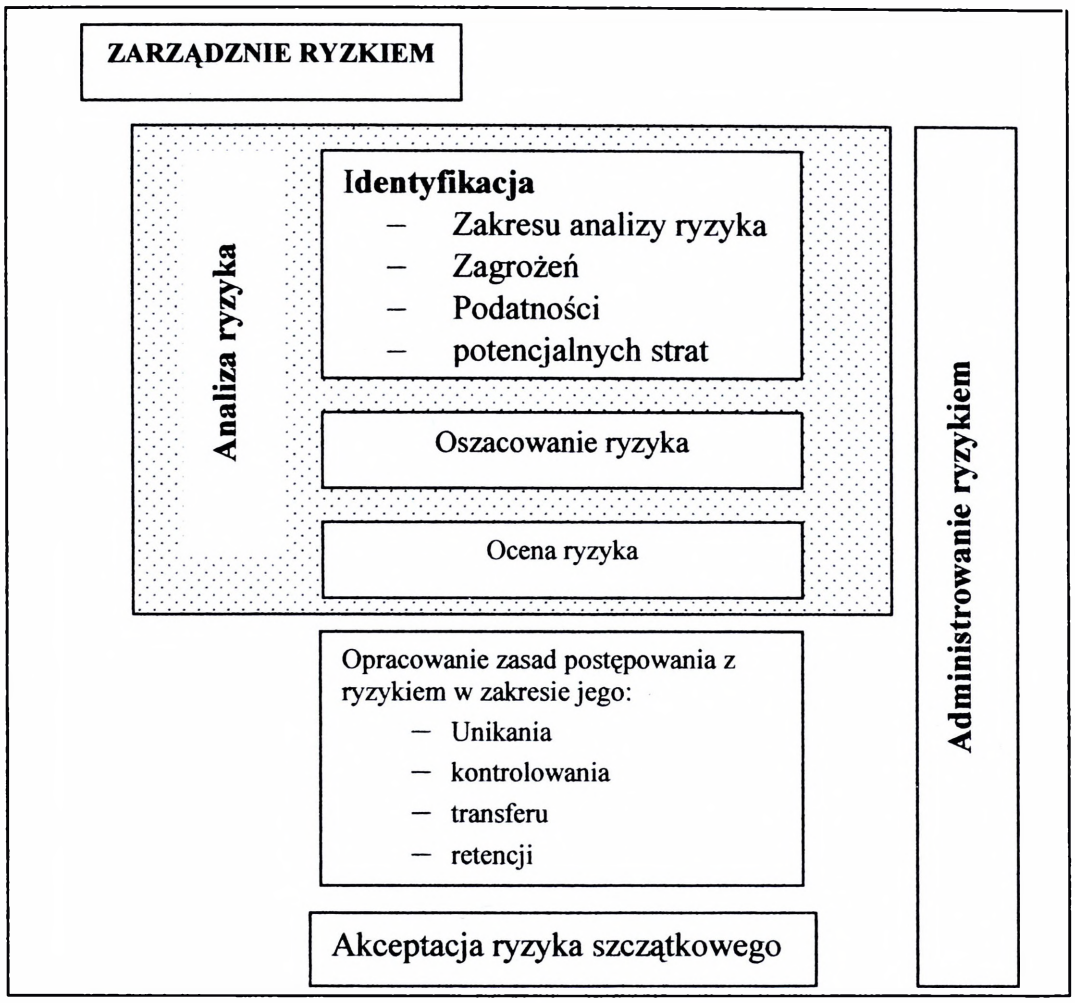
[243] Często występujące podatności to np. niestabilna sieć zasilająca, wrażliwość na zmiany temperatury, „dziury" w oprogramowaniu, niewłaściwe zarządzie hasłami, brak kontroli, kopii zapasowych, niewłaściwa ochrona połączeń, brak uwierzytelniania i identyfikacji nadawcy/odbiorcy, nie chronione podłączenie z siecią, publiczną, niewłaściwa obsługa, brak szkoleń, świadomości, niefrasobliwość pracowników, celowe działania na szkodę.

[244] P. Sienkiewicz, *Analiza zarządzania op.cit.,* Rynia 2005.

[245] Postępowanie wobec ryzyka następująco:

- Redukcja możliwości – oddziaływanie na skutek realizacji ryzyka (zmniejszenie jego maksymalnej wielkości);
- Prewencja – oddziaływanie na prawdopodobieństwo a więc przyczyny i mechanizmy prowadzące do realizacji ryzyka;
- Retencja – inaczej zatrzymanie ryzyka; jest świadomą decyzją organizacji o wzięciu na siebie konsekwencji zdarzeń losowych w przypadku ich realizacji. Najczęściej decyzja taka podejmowana jest w przypadku, kiedy zarówno redukcja ryzyka jak i jego transfer są niemożliwe lub nieopłacalne z finansowego punktu widzenia.
- Transfer – przekazanie ryzyka podmiotowi, który potrafi nim zarządzać (autsourcing, ubezpieczenie ryzyka);
- Unikanie - wśród sposobów minimalizacji ryzyka najbardziej ograniczony sposób.

stawy efektywnego systemu bezpieczeństwa dla obiektów różnej wielkości, w szczególności związanych z krytyczną infrastrukturą. W przypadku zagrożeń wynikających ze stosowania nowoczesnych technologii a więc odnoszących się do technosfery możemy przyjąć, że zagrożenie informacyjne generuje ryzyko w chwili stwierdzenia podatności danego systemu na to zagrożenie. Szacując negatywne skutki realizacji ryzyka możemy ustalić wielkość poniesionych strat.



Rysunek 4-5. Podstawowe elementy procesu zarządzania ryzykiem
Źródło: K.Liderman, *Analiza ryzyka i ochrona informacji w systemach komputerowych*. PWN Warszawa, 2008, s.79.

Technika budowania map ryzyka

Podstawą wyboru strategii dla postępowania wobec ryzyka w zarządzaniu kryzysowym jest analiza ryzyka, na fundamentach, której powinny być planowane pod konkretne przedsięwzięcia organizacyjno-technologiczne określone w polityce bezpieczeństwa. Analizę ryzyka poprzedza metodyczna identyfikacja wszystkich obszarów działania pod kątem występowania możliwych i prawdopodobnych zagrożeń, ze szczególnym uwzględnieniem domen krytycznych (tabela 4-1). Rozpoznane ryzyko są katalogowane w formie opisu zawartego w tabeli lub tabelach (tab.4-2).

Tabela 4-1. Identyfikacja obszarów ryzyka oraz możliwych zagrożeń

Obszar zagrożenia				
Rozpoznanie zagrożenia				
Możliwe zdarzenia	Przyczyna wystąpienia	miejsce wystąpienia	czas wystąpienia	Konsekwencje wystąpienia

Tabela 4-2. Opis zidentyfikowanego ryzyka

1	Nazwa ryzyka	.....
2	Zakres ryzyka	Opis jakościowy zdarzeń – skala, rodzaj, liczba Także zdarzeń pochodnych
3	Charakter ryzyka	Np. technologiczne, strategiczne, finansowe, związane z zarządzaniem wiedzą lub zgodnością z przepisami
4	Grupy nacisku	Grupy nacisku i ich oczekiwania
5	Opis ilościowy ryzyka	Znaczenie i prawdopodobieństwo
6	Tolerancja w zakresie ryzyka (poziom akceptowanego ryzyka)	Potencjalna wielkość strat i skutki finansowe realizacji ryzyka Zagrożone aktywa Prawdopodobieństwo i wielkość potencjalnych szkód/korzyści Cele w zakresie kontrolowania ryzyka i optymalne wyniki
7	Działania względem ryzyka i mechanizmy kontroli	Podstawowe środki stosowane obecnie do zarządzania danym ryzykiem Poziom pewności przy obecnych mechanizmach kontroli Istniejące procedury monitorowania i analiza systemu
8	Potencjalne możliwości poprawy sytuacji	Zalecenia służące zmniejszeniu ryzyka
9	Opracowanie strategii i planów krótkookresowych	Określenie pionu odpowiedzialnego za opracowanie strategii i planów krótkookresowych

Źródło: AIRMIC, ALARM, IRM:2002, translation copyright FERMA: 2003 [w:] P.Sienkiewicz (red.), *Zarządzanie ryzykiem w sytuacjach kryzysowych*. AON, Warszawa 2007.

Opis jest strukturalizowanym przedstawieniem cech zagrożenia i wynikającego z nich ryzyka, umożliwiającym ich porównanie i hierarchizację. Zdefiniowane i zestawione w tabeli ryzyka pozwalają ustalić priorytety i wybrać te ryzyka, które należy poddać dalszej analizie. Dla każdego obszaru, organizacji, przedsięwzięcia katalog ryzyk będzie oryginalny, bowiem zaprojektowany i uwzględniający istotę ryzyka oraz charakter „właściciela ryzyka". Analiza identyfikacyjna pozwala ujawnić charakter ryzyk, który często układa się w ciąg przyczynowo-skutkowy. Z tego też względu trzeba posługiwać się analizą równoległą jednocześnie szacując wartość przyjętej miary ryzyka.

Typy i poziomy ryzyka zmieniają się i zależą od charakteru organizacji (systemu), którego dotyczą, a także od preferencji ryzyka. Profil ryzyka jest specyficzny i przynależny danemu systemowi. Podstawowym problemem jest wybranie konwencji jednolitych zasad oceny zjawisk i własności zagrożeń w szczególności dotyczące następstw, które nie zawsze

można wyrazić w jednostkach pieniężnych. Stosuje się wartości umowne, do których przypisane są wartości kwotowe.

Mapa ryzyka jest bazowym dokumentem, określającym warunki brzegowe związane z ustaleniem wskaźników stopnia akceptacji poszczególnych ryzyk. Głównym zadaniem przy tworzeniu map zagrożeń jest konieczność kompleksowej analizy chronionych zasobów, według określonej hierarchii kryteriów, np.: (1) ludzie, (2) mienie, (3) maszyny i urządzania techniczne, (4) informacje, (5) procesy (np. przesyłanie, produkcja, dostawa, procesy krytyczne). Często bagatelizowanym zasobem są informacje i procesy tak istotne w warunkach rozwoju systemów teleinformatycznych.

Tworząc skalę wartości zasobów można wykorzystać metodę macierzy predefiniowanych[246] wartości przyjmując założenie, że podatność i zagrożenia można wyrazić np. na trójstopniowej skali (tabela 4-3). Zasobom przypisuje się wartości w skali od 0-5, a ryzyko szacowne będzie na skali 10-stopniowej.

Tabela 4-3. Macierz predefiniowanych wartości zasobów

	zagrożenie	**Niskie**			**Średnie**			**wysokie**		
	podatność	Niska	Średnia	wysoka	Niska	Średnia	wysoka	Niska	Średnia	wysoka
Wartość zasobu	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8
	5	5	6	7	6	7	8	7	8	9

Źródło: A. Białas, Bezpieczeństwo informacji i usług. WNT, Warszawa 2006, s.98.

W procesie zarządzania ryzykiem występuje często potrzeba wskazania priorytetowych ryzyk. Do uporządkowania ryzyk ze względu na „powagę" zagrożenia analizie poddajemy zarówno straty, jak i podatności na ryzyko, przypisując wartości według umownej skali np. 1-5 (tabela 4 -4).

W przypadku oceny środowiska zagrożeń (organizacji, instytucji), w którym występują zasoby o różnej wartości zachodzi potrzeba określenia częstości zagrożeń, która wyraża realność i wielkość zjawisk niekorzystnych, w oderwaniu od potencjalnych skutków.

Aby ustalić skalę częstości zdarzeń założono 3-poziomową skalę dla podatności oraz 4-poziomową dla zagrożeń (tabela 4-5).

[246] Uprzednio zdefiniowanych skal.

Tabela 4-4. Metoda porządkowania zagrożeń

zagrożenia	Wartość zasobu	Podatność	Ryzyko	Uporządkowanie ryzyk
Zagrożenie 1	1	2	2	5
Zagrożenie 2	4	3	12	3
Zagrożenie 3	3	5	15	2
Zagrożenie 4	5	5	25	1
Zagrożenie 5	5	1	5	4

Źródło: A. Białas, op.cit, s.98.

Tabela 4-5. Metoda wyznania częstości zagrożeń

Zagrożenie	Niskie			Średnie			Wysokie			Bardzo wysokie		
Podatność	Niska	Średnia	wysoka	Niska	Średnia	wysoka	Niska	Średnia	wysoka	Niska	Średnia	wysoka
Częstość zagrożeń	0	1	2	1	2	3	2	3	4	3	4	5

Źródło: A. Białas, op.cit. s.98.

Na podstawie częstości zagrożeń oraz wartości zasobów (potencjalnych szkód) ustalana jest szacunkowa wartość ryzyka wyrażająca wielkość potencjalnych strat.

Tabela 4-6. Metoda wyznaczania szacunkowej wielkości potencjalnych strat

Wartość zasobu	0	1	2	3	4	5
Częstość zagrożeń						
0	0	1	2	3	4	5
1	1	2	3	4	5	6
2	2	3	4	5	6	7
3	3	4	5	6	7	8
4	4	5	6	7	8	9
5	5	6	7	8	9	10

Źródło: A. Białas, op.cit. s.98.

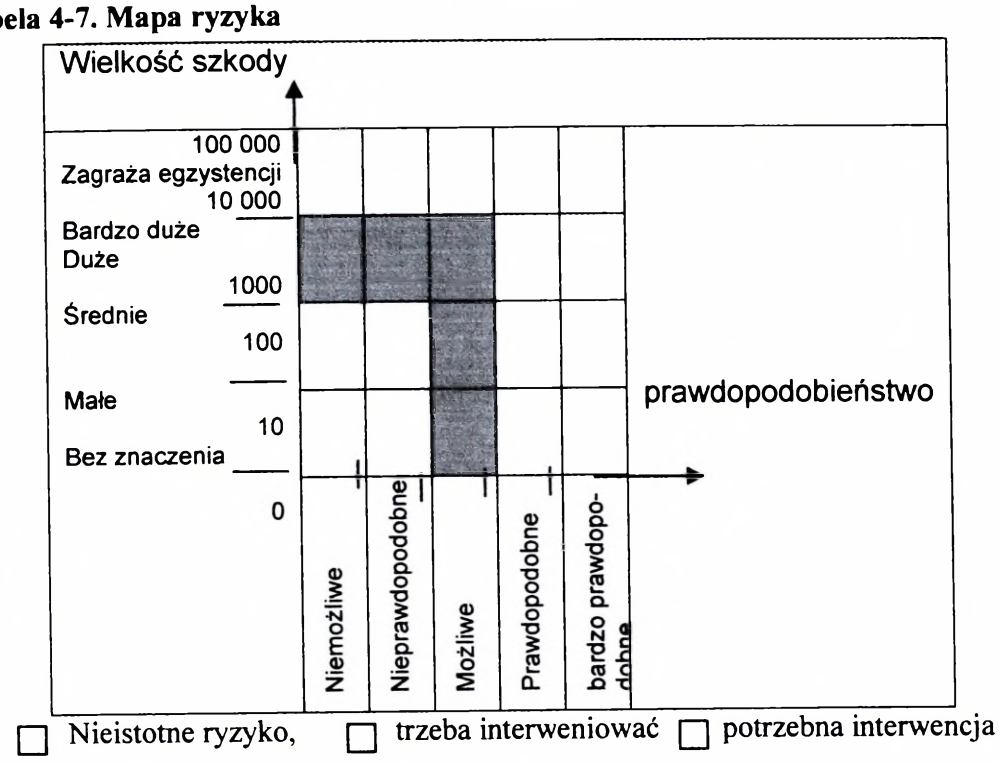
Na jakość map ryzyka składa się wiele czynników. Jest ona bowiem pochodną danych uzyskanych z instytucji profesjonalnie zajmujących się bezpieczeństwem. Zależy również od znajomości sytuacji operacyjnej otoczenia obiektu (obiektów), w którym znajdują się chronione zasoby, od trafnego określenia prawdopodobieństwa wystąpienia incydentów zagrażających bezpieczeństwu.

Prawdopodobieństwa zagrożeń można wyznaczać na podstawie danych statystycznych[247] lub ocen ekspertów. Badania potwierdzają, że szacownie zdarzeń incydentalnych jest obarczone dużymi błędami powodowanymi ograniczeniami ekspertów w postrzeganiu zagro-

[247] Dane takie gromadzone są przez CERT, Komendę Główną Straży Pożarnej, Komendę Główna Policji niestety jakość danych jest ograniczona niespójnymi metodami klasyfikacji.

żeń. Na postrzeganie wpływ mają środki masowego komunikowania, niejednokrotnie przekazując informacje nieadekwatnie do zagrożenia.

Tabela 4-7. Mapa ryzyka



Źródło: opracowanie własne.

Szacowanie prawdopodobieństwa i skutków wystąpienia ryzyka

Poniżej przedstawiono przykładowe tabele ułatwiające ocenę ryzyka w kategoriach prawdopodobieństwa i skutków. Do oceny prawdopodobieństwa zastosowano skalę procentową. Prawdopodobieństwo wystąpienia większego od 50% oznacza zdarzenie pewne i oznaczane jest przez A.

Tabela 4-8. Ocena prawdopodobieństwa wystąpienia ryzyka

Poziom ryzyka	Prawdopodobieństwo	Miara prawdopodobieństwa	Charakterystyka
A	Pewne	>50%	Zdarzenie wystąpi
B	Prawdopodobne	20%-50%	Jest wysoce prawdopodobne, że zdarzenie wystąpi
C	Możliwe	10-20%	Tylko w niektórych przypadkach zdarzenie może wystąpić
D	Mało prawdopodobne	1-10%	Tylko przy zbiegu różnych okoliczności, zwykle nie występujących razem
E	Niemożliwe	<1%	Zdarzenie nie wystąpi

Źródło: opracowanie własne

Do opisu skali skutków wystąpienia określonego ryzyka użyto cyfr od 1-5, skutek katastrofalny przypisano cyfrze 5.

Tabela 4-9. Przykładowa ocena skutków wystąpienia ryzyka

Poziom ryzyka	Skutek	Charakterystyka	Koszt
1	Nieznaczny	Brak szkód	0
2	Mało znaczący	Pojedyncze przypadki zranień	10 000
3	Umiarkowany	Pojedyncze przypadki zranień, liczne przypadki lekkich zranień	100 000
4	Poważny/krytyczny	Pojedyncze przypadki śmiertelne	1 000 000
5	katastrofalny	Wiele ofiar śmiertelnych	10 000 000

Źródło: opracowanie własne.

Tabela 4-10. Szacowanie poziomu ryzyka

Prawdopodobieństwo wystąpienia ryzyka P_z / **Kategoria strat S_z**	**M – mało prawdopodobne $P_Z < 0,3$**	**P – prawdopodobne $0,3 \leq P_Z < 0,7$**	**W – wysoce prawdopodobne $P_Z \geq 0,7$**
	Stopień ryzyka		
Ma – marginalne	N	N	S
Kr – krytyczne	N	S	W
Ka – katastrofalne	S	W	W

N – niski, S – średni, W – wysoki

Źródło: opracowanie własne na podstawie wykładu P.Sienkiewicza pt. *Zarządzanie w stanach kryzysowych*. Wykłady otwarte grudzień 2003.

Prawdopodobieństwo zagrożeń możemy również ustalać w punktach. Wszystko podyktowane jest nieobligatoryjnym wyborem skal, które w toku dalszej analizy należy konsekwentnie stosować.

Tabela 4-11. Procedura probabilistycznej analizy ryzyka zagrożeń informacyjnych dla bezpieczeństwa organizacji/instytucji

Faza 1

Probabilistyczny ranking ryzyka	
ranga	**prawdopodobieństwo**
5	**0,80-0,99**
4	**0,60-0,79**
3	**0,40-0,59**
2	**0,20-0,39**
1	**0,01-0,19**

Faza 2

Tabela 4-12. Określenie głównych konsekwencji zagrożeń dla informacyjnego bezpieczeństwa organizacji (instytucji)

Wpływ ryzyka na działanie organizacji (instytucji)						
Wpływ		**1**	**2**	**4**	**8**	**16**
założenia	Czas realizacji planowanych przedsięwzięć	Niewielkie opóźnienia	Opóźnienia do jednego kwartału	Opóźnienia przekraczają jeden kwartał	Opóźnienia przekraczają więcej niż jeden kwartał	Opóźnienia przekraczają rok budżetowy
	Koszt realizacji planowanych przedsięwzięć	Niewielki wzrost kosztów	<5% wzrost kosztów	5-10% wzrost kosztów	10-20% wzrost kosztów	>20% wzrost kosztów
	Zakres działania organizacji/ instytucji	Niezauważalne różnice w planie	Zmiany w planie albo uwzględnienie <5% wzrostu kosztów	Zmiany w planach albo uwzględnienie 5-10% wzrostu kosztów	Przesłanki o celowości dalszych prac	Utrata znaczenia i potrzeby

Faza 3 na podstawie informacji zawartych w fazie 1 i 2 opracowano macierz prawdopodobieństwa i wpływu ryzyka na główne działania.

Tabela 4-13. Rangowanie ryzyka

Punktacja	Ryzyko
1-6	Niskie
7-14	Umiarkowane
Pow. 15	wysokie

Źródło: opracowanie własne.

Tabela 4-14. Czas, koszt, zakres działania

prawdopodobieństwo					
5	5	10	20	40	80
4	4	8	16	32	64
3	3	6	12	24	48
2	2	4	8	16	32
1	1	2	4	8	16
	1	2	4	8	16
	Wpływ ryzyka na bezpieczeństwo informacyjne organizacji				

Tabela 4-15. Przykład kategorii prawdopodobieństwa i szkód dla cyberataków

PRAWDOPODOBIEŃSTWO		
OZNACZENIE KATEGORII KLASA RYZYKA	**OPIS KATEGORII CZĘSTOŚCI**	**DEFINICJA/PARAMETRY KATEGORII**
A	często	Prawdopodobieństwo częstego występowania
B	prawdopodobne	Może występować wiele razy
C	okazjonalnie	Może występować kilka razy
D	mało prawdopodobne	Możliwe wystąpienie zdarzenia
E	nieprawdopodobne	Prawdopodobieństwo, pozwalające zakładać, że zdarzenie nie wystąpi
Szkoda		
	kategoria	**opis**
1	katastroficzna	W skutek blokady straty finansowe, utrata płynności, utrata wizerunku, klientów – bankructwo, sankcje prawne wynikające z braku należytej ochrony danych, niezrealizowanie ważnych lub krytycznych dla organizacji zadań, utrata strategicznych planów,
2	poważna	Utrata wiarygodności lub reputacji, brak obsługi klientów – straty finansowe
3	marginalna	Krótkotrwałe przerwy w obsłudze klientów
4	pomijalna	uszkodzenia systemu tak małe, że mogą być tolerowane

Źródło: opracowane własne.

Wpływ na jakość mapy ma również obserwacja bieżących zmian w konfiguracji obiektów z chronionymi zasobami a także obserwacja ich wpływu na stan bezpieczeństwa. Istotna rolę ma również aspekt rozpoznania zagrożeń wewnętrznych.

Tabela 4-16. Przykład analizy

OBSZAR ZAGROŻENIA	STRONA WWW ORGANIZACJI X			
Rozpoznanie zagrożenia	Nieautoryzowana modyfikacja strony internetowej na serwerze www			
Możliwe zdarzenia	Przyczyna wystąpienia	miejsce wystąpienia	czas wystąpienia	Konsekwencje wystąpienia
	Atak hakerski	System operacyjny serwera WWW Strona www	Zarejestrowana data	Utrata integralności i dostępności

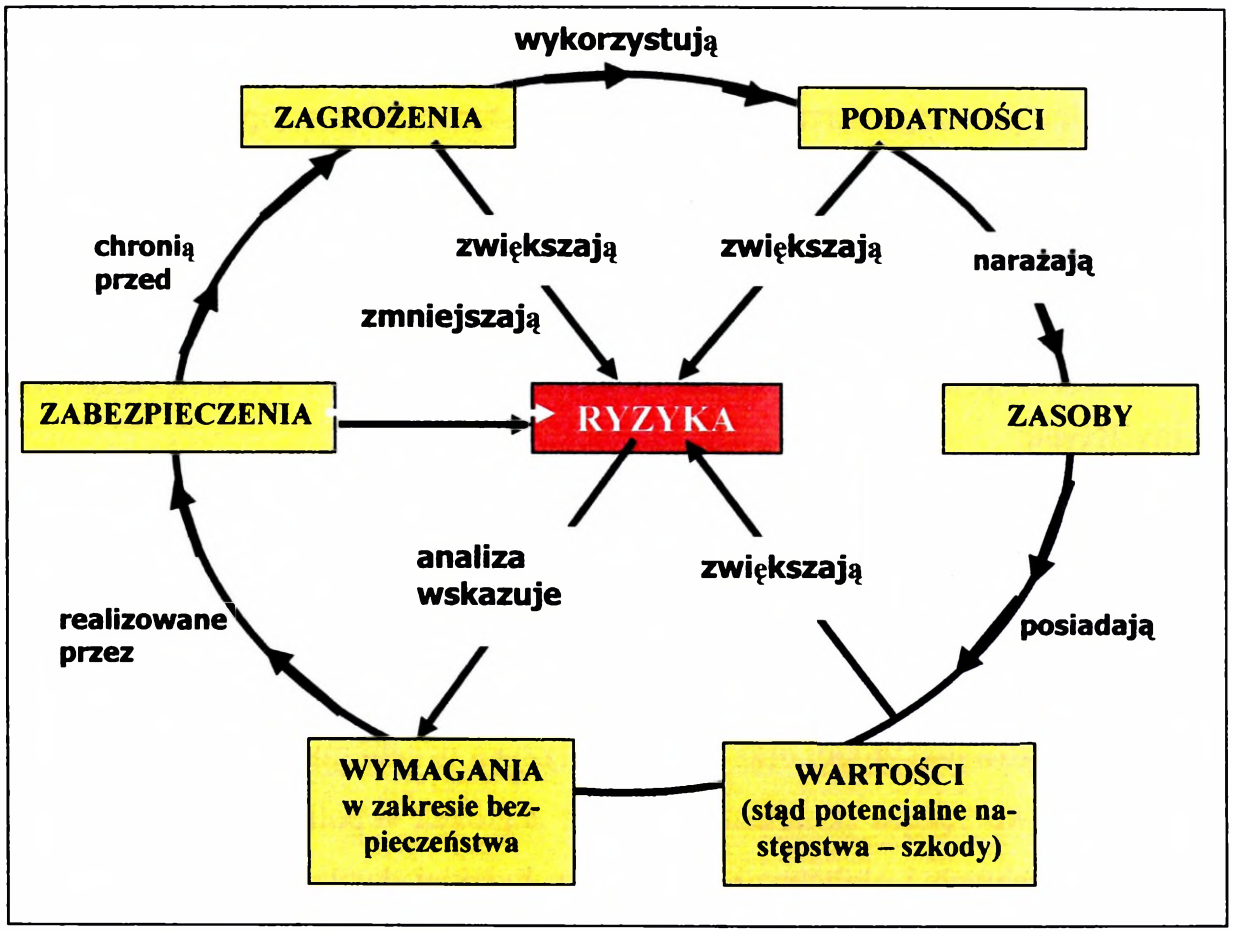
Identyfikacja i określenie podatności systemu	**Określenie wielkości wpływu na system z wykorzystania podatności systemu**
Wysokie – 1,0 Średnie – 0,5 Niskie – 0,1	Wysokie – 100 Średnie – 50 Niskie - 10

Tabela 4 -17. Wyznaczenie macierzy poziomu ryzyka

		Straty wywołane wykorzystaniem podatności		
		Niskie (10)	Średnie (50)	Wysokie (100)
Prawdopodobieństwo wystąpienia podatności	Wysokie (1,0)	Niskie 10*1,0=10	Średnie 50*1,0=50	Wysokie 100*1,0=100
	Średnie (0,5)	Niskie 10*0,5=5	Średnie 50*0,5=25	Średnie 100*0,5=50
	Niskie (0,1)	Niskie 10*0,1=1	Niskie 50*0,1=5	Niskie 100*0,1=10

Źródło: opracowanie własne

Wzajemne relacje między elementami bezpieczeństwa i zagrożeń regulują zasady porządkujące kolejność działań prowadzących do efektywnego zarządzania ryzykiem (rysunek 4-6).



Rysunek 4-6. Zależności między elementami bezpieczeństwa i zagrożeń w kontekście zarządzania ryzykiem.

Źródło: M.Łacheta, M.Molski, *Bezpieczeństwo i audyt systemów informatycznych*. Bydgoszcz 2009, s.22.

Zagrożenia informacyjne dla bezpieczeństwa państwa mogą realizować się jako działania destrukcyjne w systemach teleinformatycznych, a także same systemy mogą ulegać destrukcji w wyniku terrorystycznego ataku. Skutki działania kumulują się w obszarze ekonomicznych podstaw gospodarki, nawet jeżeli są to tylko działania przestępcze na szkodę oby-

wateli. Wynikiem, oprócz strat wymiernych finansowo, może być „wzburzenie społeczne" czy chaos polityczny.

Główne znaczenie w kontekście bezpieczeństwa narodowego ma kwestia podatności struktur administracyjnych i wojskowych, gospodarczych i społecznych na zagrożenia wynikające z działań prowadzonych w cyberprzestrzeni, których skutki odczuwane są w krytycznej infrastrukturze.

W analizach ryzyka na potrzeby zarządzania kryzysowego zwraca się uwagę na istnienie poważnej rozbieżności pomiędzy ekspercką oceną wagi ryzyka, a jego oceną społeczną.[248] Zmodyfikowana definicja ryzyka uwzględnia, oprócz „ryzyka obliczeniowego", czynnik społecznego wzburzenia, określającego stosunek społeczności lokalnej do danego rodzaju ryzyka. „Społeczne wzburzenie" podobnie jak ryzyko obliczeniowe ma następujące właściwości: jest rzeczywiste i mierzalne, poddaje się zarządzaniu i jest równoważnym składnikiem ryzyka. Uważa się, że niedocenianie „społecznego wzburzenia" powoduje, że społeczność lokalna postrzega zarządzanie bezpieczeństwem tylko w oparciu o ryzyko obliczeniowe jako złe zarządzanie.[249]

Analiza ryzyka pozwala na identyfikację i ewaluację istniejących zagrożeń, jak również określenie obszarów potencjalnie zagrożonych. Powinna być procesem ciągłym, który stanowi kluczowy problem zarządzenia bezpieczeństwem. Jest niezbędny przy dylematach decyzyjnych typu:

- **inwestować w środki bezpieczeństwa czy akceptować możliwość strat lub zniszczeń?**
- **które z wymagań bezpieczeństwa mają najwyższy priorytet?**[250]

Warunkiem skutecznego przeciwdziałania zagrożeniom jest wdrożenie metod prawidłowego identyfikowania źródeł oraz ewaluacji ryzyka w celu minimalizowania strat i szkód. Sytuacje kryzysowe będące skutkiem kumulacji zagrożeń w polityce i biznesie stały immanentną cechą lokalnych i globalnych przejawów ludzkiej działalności. „Utrzymanie ryzyka w ryzach" stało się imperatywem racjonalnego działania wszelkich systemów. [251]

---

[248] P.Sandman, *Responding*,..., op.cit.

[249] J. Wolanin, *Zarys*,..., op.cit.

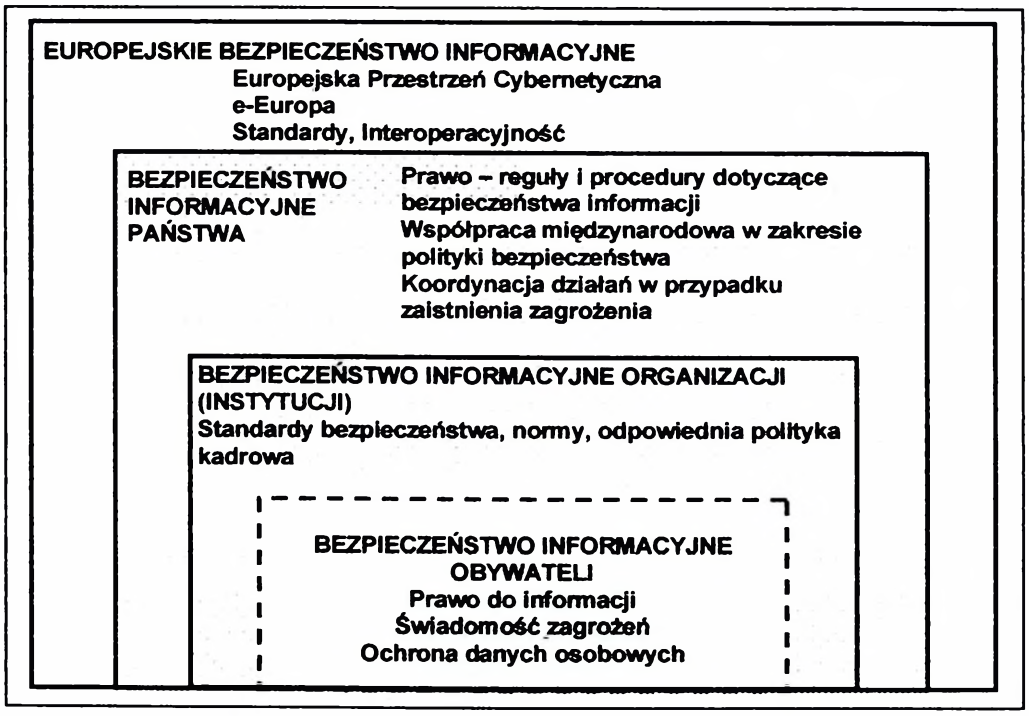
[250] Ze względu na wysokie i stale rosnące koszt zabezpieczeń racjonalne jest przeznaczanie sił i środków na zabezpieczenia przed zagrożeniami informacyjnymi tylko tych obiektów, które posiadają szczególną wartość społeczną (polityczną, obronną, itp.).

[251] Dla potrzeb identyfikacji zagrożeń, badania odporności systemów a także „nauczenia radzenia z zagrożeniami" są prowadzone w Wielkiej Brytanii operacje *Cyber Storm* jako ćwiczenia symulacyjne, w których udział biorą publiczne i prywatne podmioty, banki, elektrownie firmy z branży IT. Również akademie wojskowe i uniwersytety w Stanach Zjednoczonych po raz szósty sprawdzały umiejętności studentów w obronie przeciw działaniom intruzów w sieci.

Zdolność do unikania zbyt wielkich szkód można osiągnąć dzięki przewidywaniu (prognozowaniu), niebezpieczeństw i zagrożeń wesprze to osiągnięcie pożądanego stanu bezpieczeństwa państwa, w którym strategie zabezpieczeń krytycznych zasobów zrównoważone zostaną ze skłonnością do podejmowania ryzyka i z dopuszczalnym ryzykiem.

4.3. Model systemu zarządzania bezpieczeństwem informacyjnym

Zarządzanie bezpieczeństwem jest bardzo złożonym problemem bowiem dotyczy obszaru bezpieczeństwa informacyjnego, który jest, w obecnej skali dziedziną nową *in statu nascendi.* Kontrowersje powstają także w związku z dużym zróżnicowaniem pojęciowym dotyczącym obszaru bezpieczeństwa informacyjnego. Warto podkreślić, że w ujęciu szerokim bezpieczeństwo informacyjne jest *traktowane jako dział bezpieczeństwa, uznający wzrost roli informacji w podtrzymywaniu stabilności gospodarek i systemów społecznych współczesnych państw.*[252] Obejmuje bardzo zróżnicowane podmioty ze względu na: wielkość, formę prawną zorganizowania (państwo, podmioty gospodarcze w tym państwowe, prywatne, spółki, organizacje non profit), celami działania (od producentów po konsumentów). Mnogość i wielopoziomowość powiązań gospodarczych, rozproszenie odpowiedzialności za bezpieczeństwo, stawia państwo w roli naczelnego koordynatora działań zapewniających bezpieczeństwo informacyjne (rysunek 4-7).



Rysunek 4-7. Płaszczyzny bezpieczeństwa informacyjnego

Źródło: P.Sienkiewicz, H.Świeboda, *Bezpieczeństwo europejskiej przestrzeni cybernetycznej.* AMW, Gdynia 2009 (w druku).

---

[252] A.Bógdal-Brzeźińska, M.Gawrycki, op.cit.

Transgraniczny charakter zagrożeń informacyjnych wymaga współpracy z innymi państwami, w celu ujednolicenia definicji i uregulowań prawnych dotyczących zarówno cyberprzestępczości, jaki i cyberterroryzmu.

W strategii amerykańskiej precyzyjnie wyznaczono współużytkownikom cyberprzestrzeni zakresy odpowiedzialności. [253]

Tabela 4-18. Podział ról i odpowiedzialności w procesie zabezpieczania cyberprzestrzeni

POZIOM	NARODOWY SYSTEM ODPOWIEDZI NA ATAKI W CYBERPRZESTRZENI	PROGRAM REDUKOWANIA ZAGROŻEŃ I OBNIŻANIA WRAŻLIWOŚCI SYSTEMÓW	PROGRAMY OSTRZEGANIA I SZKOLENIA	BEZPIECZEŃSTWO RZĄDOWEJ CYBERPRZESTRZENI	BEZPIECZEŃSTWO NARODOWE WSPÓŁPRACA MIĘDZYNARODOWA W ZAKRESIE OCHRONY CYBERPRZESTRZENI
Użytkownicy domowi/ małe firmy		X	X		
Duże firmy	X	X	X	X	
Infrastruktura krytyczna	X	X	X	X	X
Bezpieczeństwo narodowe Wrażliwość systemów	X	X	X	X	X

Źródło: na podstawie: The National Strategy to Secure Cyberspace Publisher: Morgan James Publishing (February 1, 2003); [online]:http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf

Powstał również polski Program,[254] adresowany jest do wszystkich obywateli ze szczególnym wyróżnieniem: 1) administracji publicznej i innych podmiotów zarządzających zasobami krytycznej infrastruktury teleinformatycznej państwa; b) beneficjentów systemów, sieci i usług teleinformatycznych stanowiących KITP. Program jest pierwszym rządowym dokumentem całościowo obejmującym kwestie bezpieczeństwa przestrzeni cybernetycznej państwa. Zaletą dokumentu jest jednoznaczne określenie celów i kierunków działań stanowią-

---

[253] USA ochronę cyberprzestrzeni uregulowała po wydarzeniach z 11 września 2001. W Narodowej Strategii Bezpieczeństwa Krajowego (2003) założono trzy cele: (1) zabezpieczenie amerykańskiej infrastruktury krytycznej przed atakami; (2) wzmocnienie odporności systemów na ataki; (3) ograniczanie szkód i czasu odtwarzania zasobów i zdolności. W każdym z dokumentów podkreśla się edukację z zakresu bezpieczeństwa cybernetycznego.

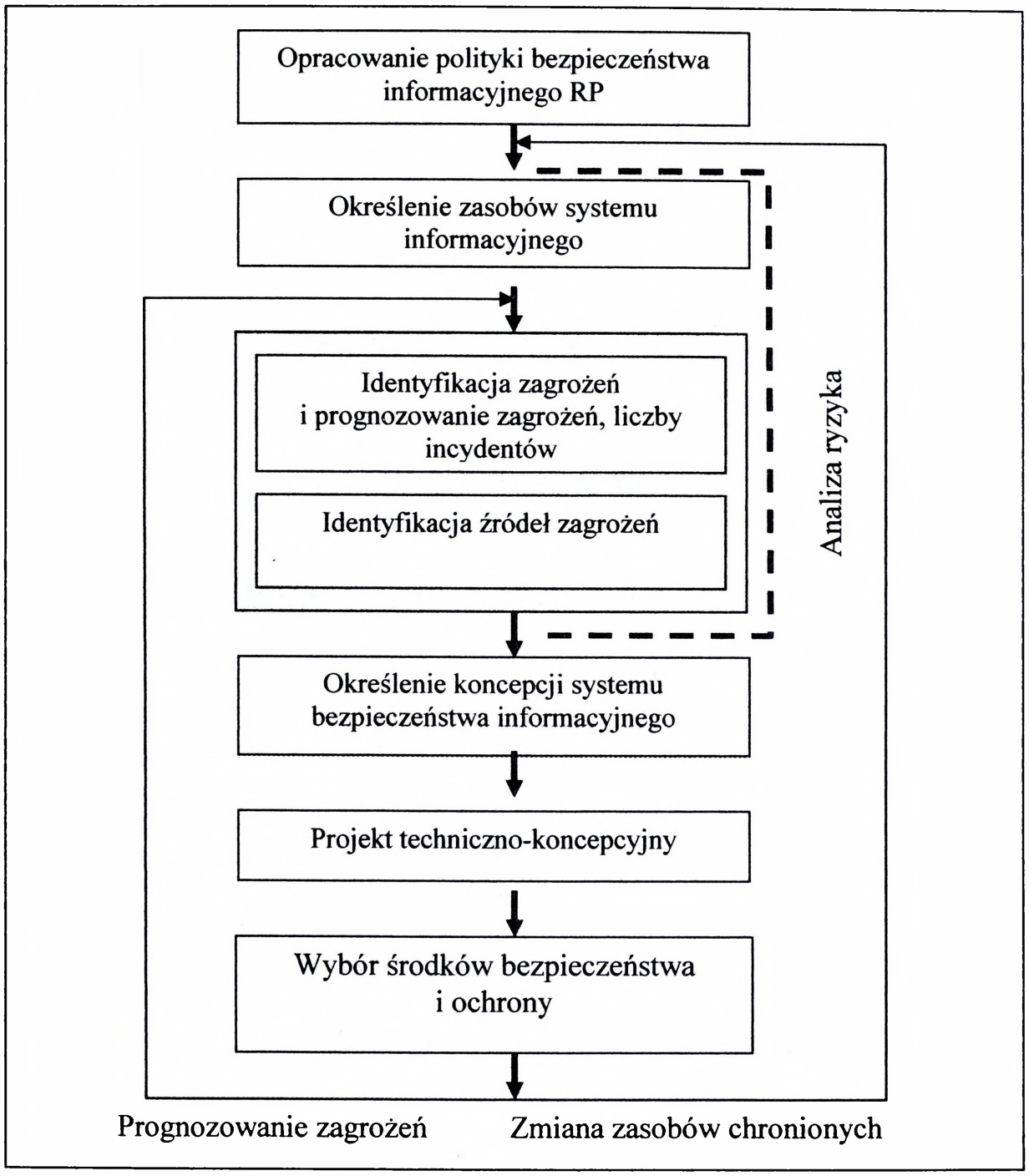
[254] Rządowy Program Ochrony Cyberprzestrzeni RP na lata 2009-2011., op.cit. dostęp online: www.mswia.gov.pl. Program opracowano przez MSWiA i ABW, jako odpowiedź na zwiększające się ryzyko zagrożeń w cyberprzestrzeni. Podstawę systemowego uregulowania bezpieczeństwa cyberprzestrzeni państw sojuszniczych, był atak na Estonię w 2007 roku i całkowita blokada funkcjonowania państwa.

Sytuacja ta była również czynnikiem, który legitymizował powołanie przez siedem krajów NATO centrum badawczego, którego celem będzie poprawienie zabezpieczeń Sojuszu przed cyberatakami. Umowę podpisali szefowie sztabów generalnych Estonii, Łotwy, Litwy, Niemiec, Włoch, Hiszpanii i Słowacji. Zobowiązali się oni do dostarczenia personelu i funduszy dla centrum z siedzibą w stolicy Estonii, Tallinie.

cych ramy realizacji Programu oraz podmiotów odpowiedzialnych za koordynację i realizację.

Plan projektowania systemu bezpieczeństwa wymaga określenia zasobów, zdefiniowania pojęć w sensie prawnym, wyodrębnienia działań i infrastruktur a także określenia roli i zadań dla podmiotów uczestniczących w procesie ochrony cyberprzestrzeni RP oraz krytycznej infrastruktury (rysunek 4-8).

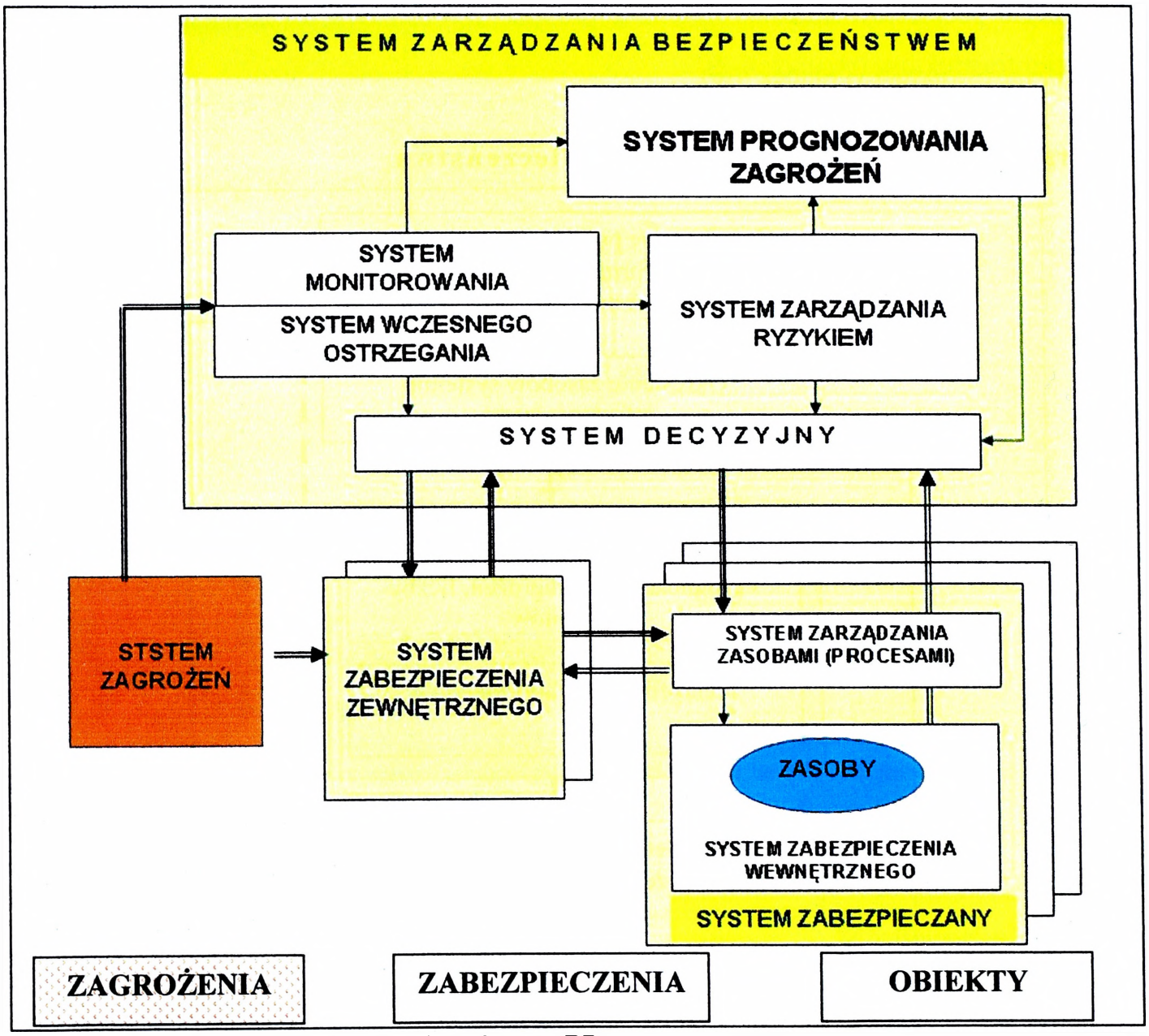
I. Etap projektowania systemu bezpieczeństwa



Rysunek 4-8. Proces projektowania systemu bezpieczeństwa
Źródło: opracowanie własne.

Istotnym elementem systemu bezpieczeństwa jest analiza ryzyka obejmująca identyfikacje zagrożeń oraz ich prognozowanie wraz z identyfikacją źródeł zagrożeń.

Proponowany model przedstawia strukturę systemu dwupoziomowego sterowania (zarządzania) (rysunek 4-9).[255] Lokalny poziom tworzą obiekty (zasoby, aktywa) zagrożeń informacyjnych posiadające autonomiczne zabezpieczenia (system zabezpieczania wewnętrznego).



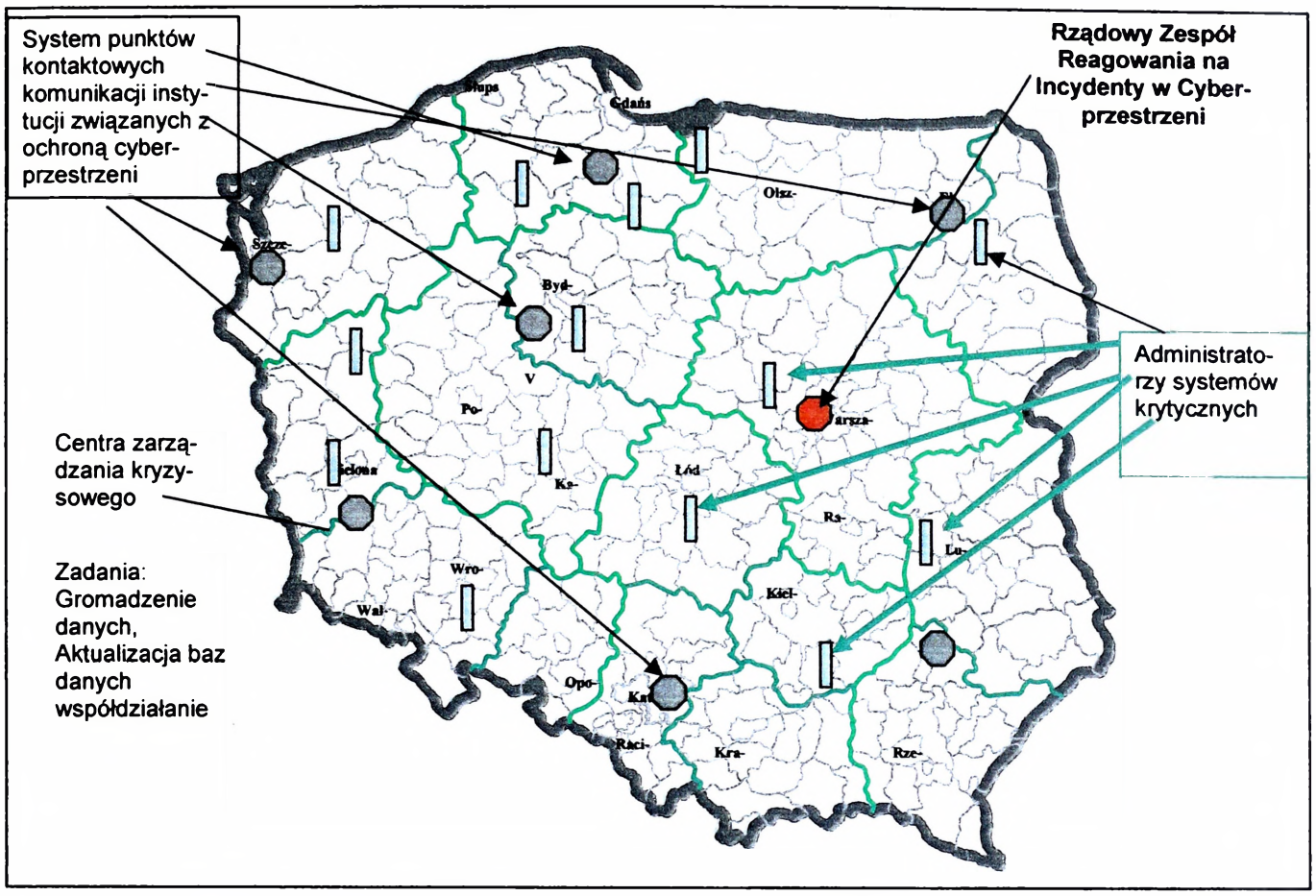
Rysunek 4-9. System zarządzania bezpieczeństwem RP
Źródło: opracowanie własne.

Każdy z obiektów zagrożeń może korzystać z sił i środków tworzących system zabezpieczenia zewnętrznego (np. agencje ochrony, służby itp.). Nadrzędny poziom zarządzania tworzy system zarządzania bezpieczeństwem jako centralny koordynator, który jest głównym dysponentem środków systemu zabezpieczenia zewnętrznego.

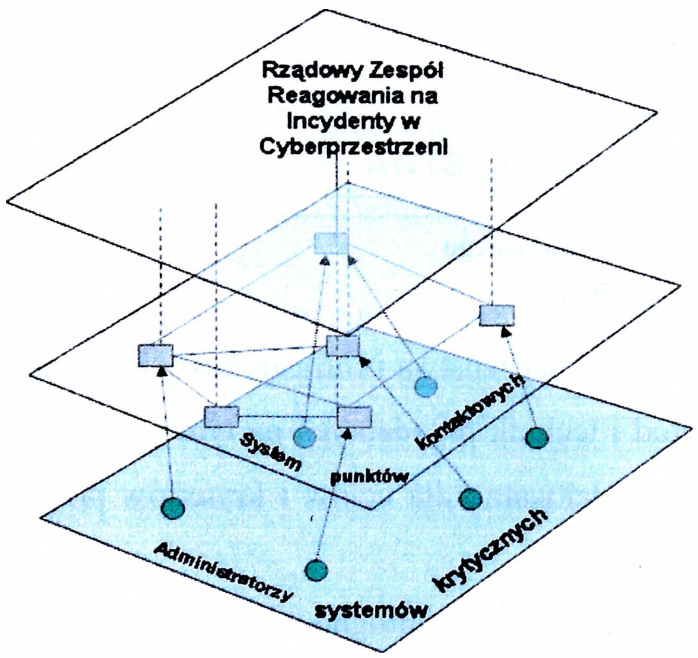
Efektywna koordynacja wymaga: systemu monitorowania wraz z systemem wczesnego ostrzegania, stanowiącego platformę dla pozyskiwania danych jako podstawy dla prognozowania możliwych i prawdopodobnych zagrożeń, a także ewaluacji ryzyka (system zarzą-

[255] Jest to klasyczny problem teorii systemów.

dzania ryzykiem). Na obszarze Polski proponuje się utworzenie systemu punktów kontaktowych służących komunikacji z jednoczesnym opracowaniem (segmentowym, wydzielonego obszaru cyberprzestrzeni) prognoz, instytucji związanych z ochroną cyberprzestrzeni (sieć).



Rysunek 4-10. Struktura systemu monitorowania zagrożeń bezpieczeństwa informacyjnego RP
Źródło: opracowanie własne.

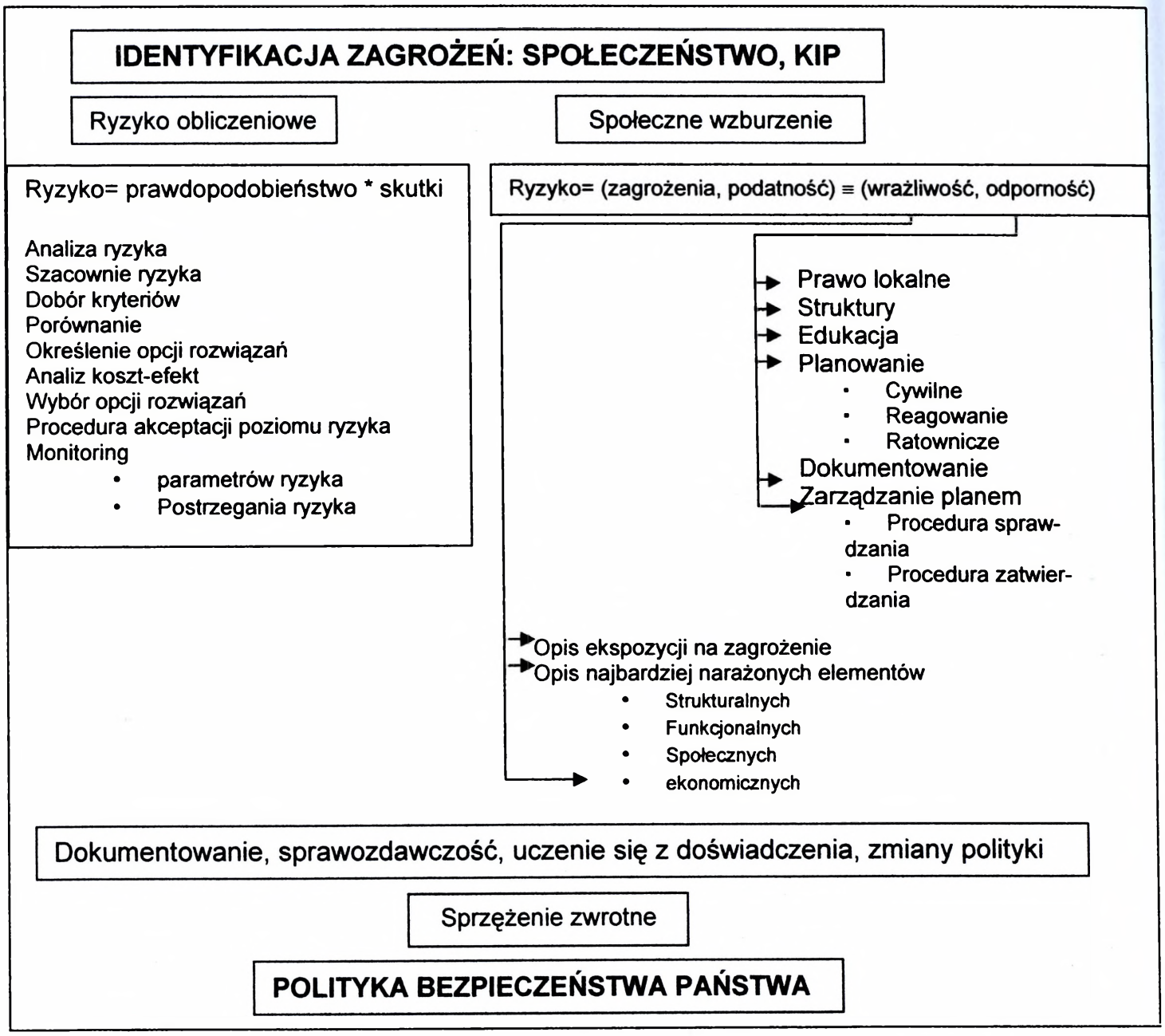


Rysunek 4-11. System prognozowania zagrożeń
Źródło: opracowanie własne.

W punktach kontaktowych (komunikacji instytucji związanych z ochroną cyberprzestrzeni) proponuje się utworzenie stanowisk ekspercckich (zdalnych) do dokonywania oceny zagrożeń na podstawie danych statystycznych i otrzymanych w badaniu eksperckim (według szablonów) prognoz. Dla rozpoznanych rodzajów ataków zaproponowanych w zbiorczej tabeli eksperci oceniają prawdopodobieństwo w skali 0-1 i ilość prawdopodobnych ataków z oceną ich ewentualnych skutków

z uwzględnieniem oceny eksperckiej i oceny „społecznego wzburzenia" (np. według technik zaproponowanych w rozdziale III).

II. Etap identyfikacji zasobów systemu informacyjnego



Rysunek 4-12. Schemat identyfikacji zasobów systemu informacyjnego
Źródło: J. Wolanin, *Zarys teorii bezpieczeństwa obywateli.* 2005.

Ogólny schemat identyfikacji zagrożeń dla społeczeństwa i infrastruktury informacyjnej państwa stanowi syntetyczny przegląd metod i technik przydatnych na tym etapie. Z zaproponowanych technik wybieramy, te które są adekwatne dla celów i kryteriów przyjętej analizy.

W zależności od zidentyfikowanego typu zagrożeń, w prognozowaniu możemy wykorzystać: szeregi czasowe, symulację, scenariusze. Rozpoznanie i klasyfikacja zidentyfiko-

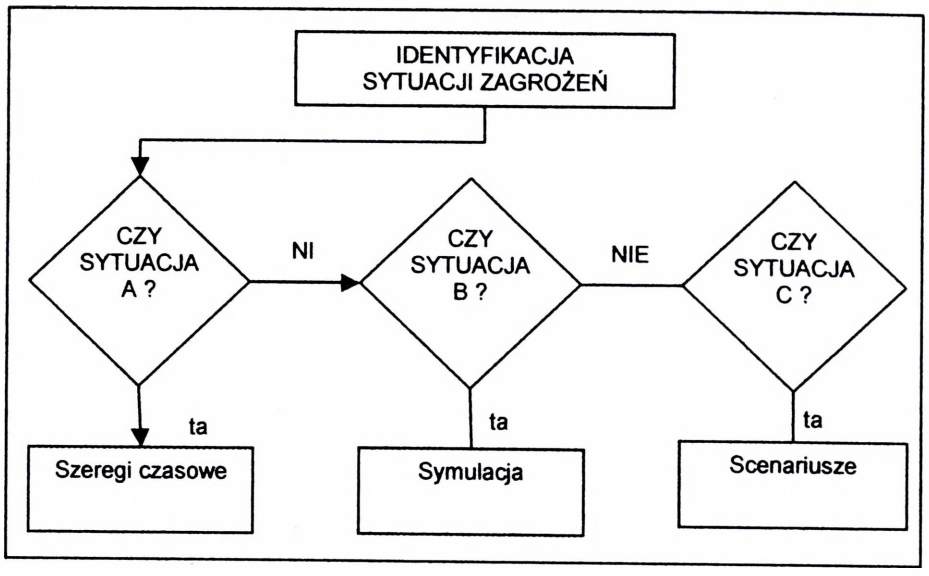
wanego zagrożenia pozwala na zaszeregowanie go do jednej z wyszczególnionych grup. Jeżeli mamy do czynienia z zagrożeniami typu:[256]

A - sytuacja problemowa dobrze ustrukturyzowna (dominują, cechami ilościowymi);

B – sytuacja problemowa średnio ustruturyzowna (występują cechy ilościowe i jakościowe);

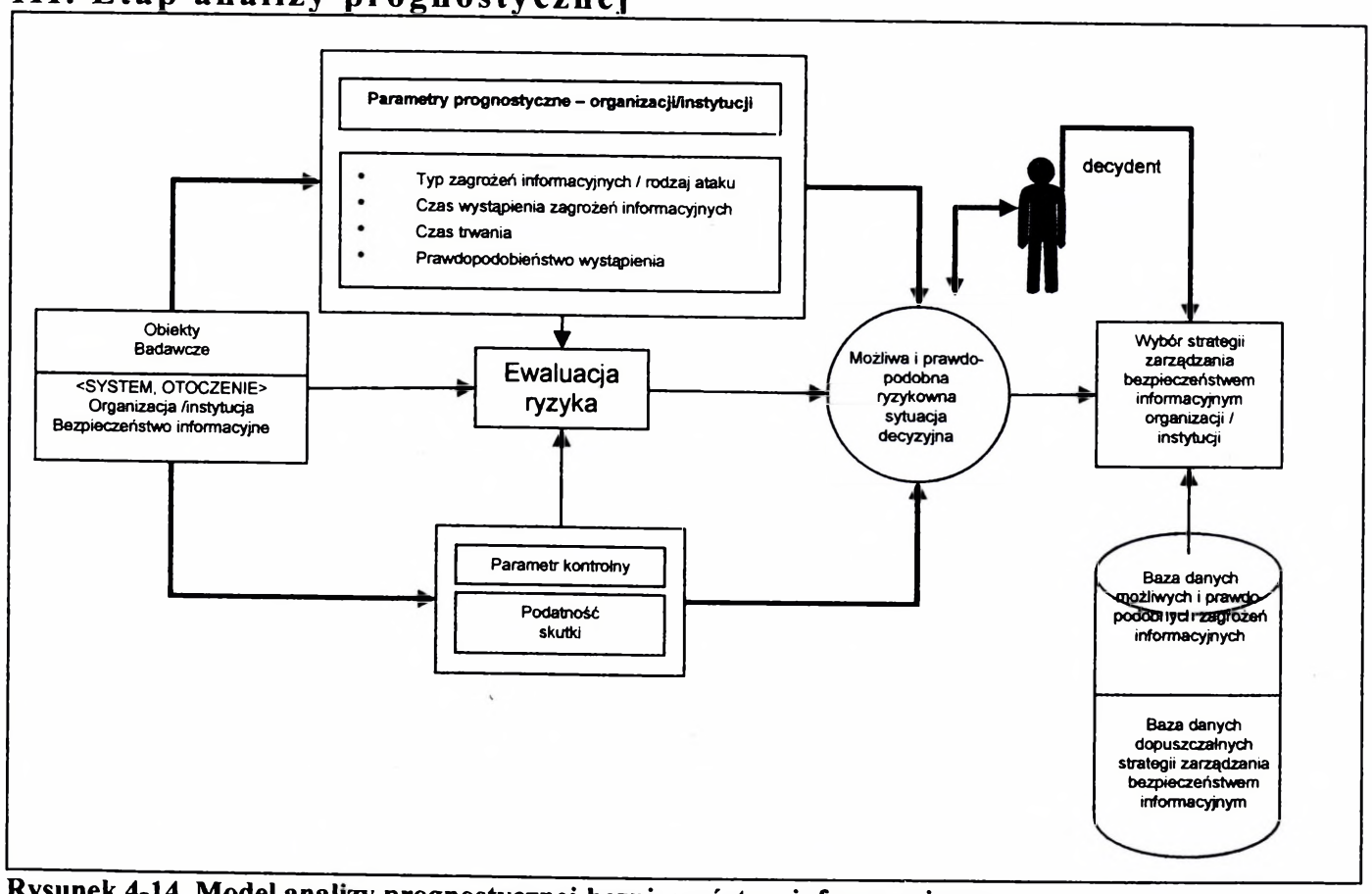
C - sytuacja problemowa słabo ustruturyzowna (dominują cechy jakościowe);

posługujemy się jedną z metod prognozowania zagrożeń (rysunek 4-13).



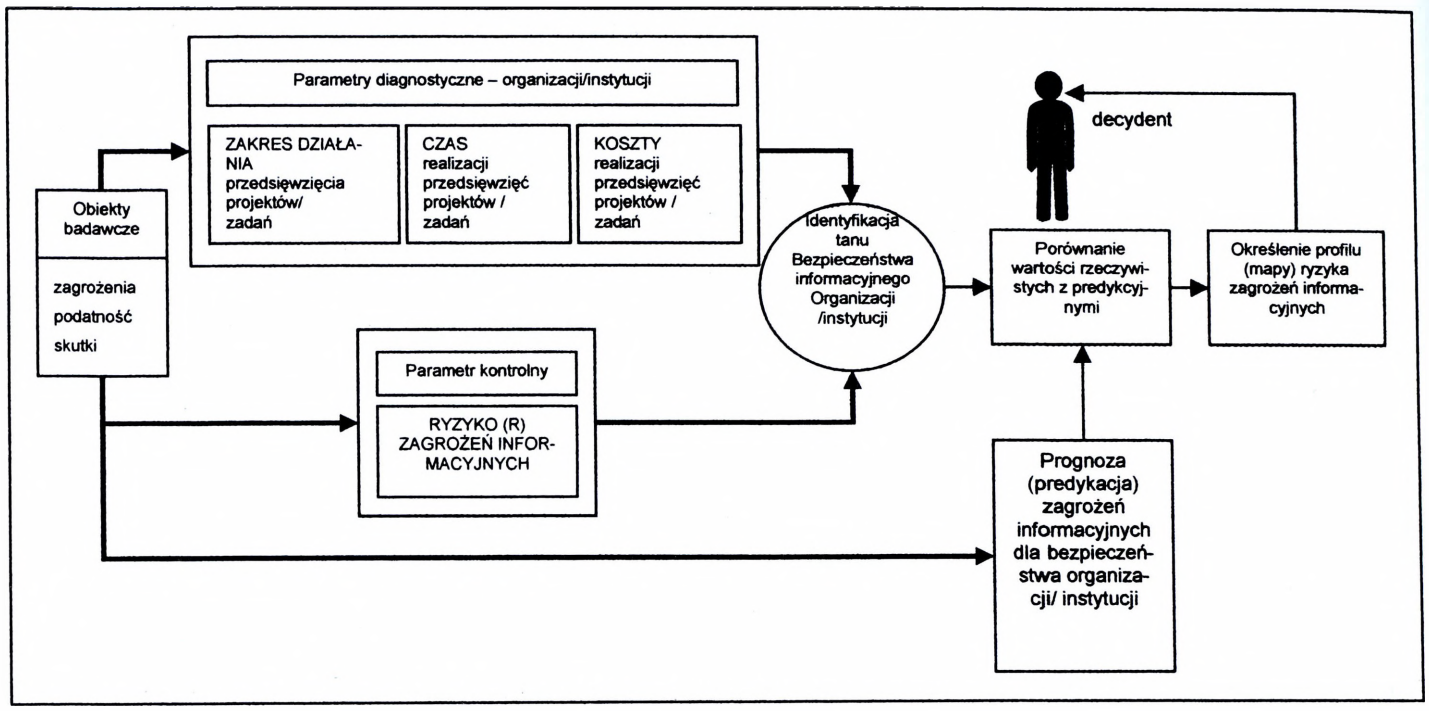
Rysunek 4-13. Makroalgorytm identyfikacji sytuacji zagrożeń
Źródło: opracowanie własne.

III. Etap analizy prognostycznej



Rysunek 4-14. Model analizy prognostycznej bezpieczeństwa informacyjnego
Źródło: opracowanie własne.

[256] H.A.Simon, *Podejmowanie decyzji kierowniczych*. Nowe nurty. Warszawa 1982, s.126.



Rysunek 4-15. Model procesu zarządzania bezpieczeństwem informacyjnym (z wykorzystaniem metody wielowymiarowej oceny ryzyka zagrożeń informacyjnych

Źródło: opracowanie własne.

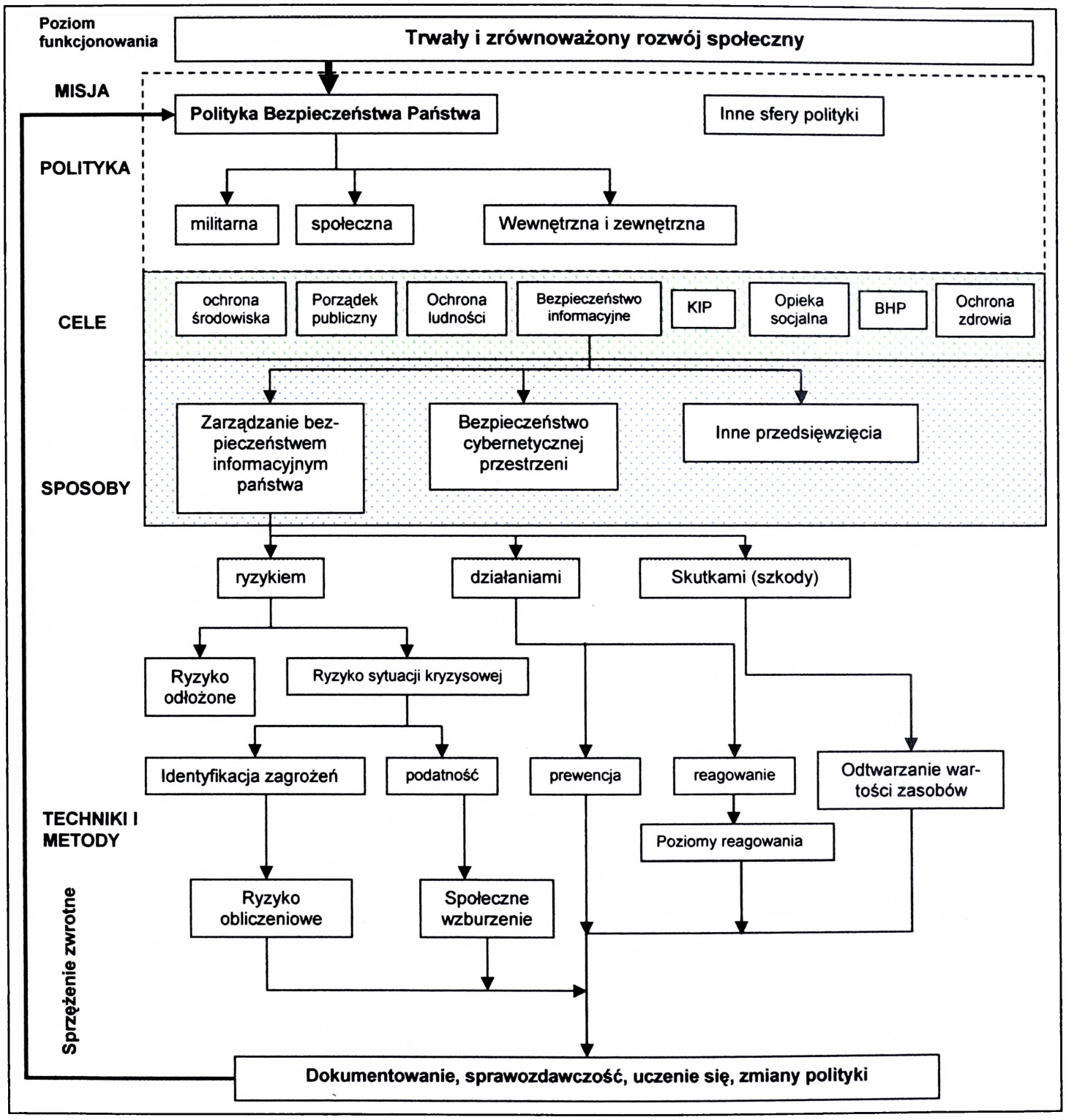
Należy zauważyć, że problem zarządzania bezpieczeństwem systemu, można sprowadzić do problemu: (1) minimalizacji funkcji ryzyka pod warunkiem, że wartość efektów (użyteczności) uzyskiwanych dzięki funkcjonowaniu systemu będą nie mniejsze od wartości granicznej (pożądanej) albo (2) maksymalizacji funkcji efektywności systemu pod warunkiem, że funkcja ryzyka nie przekroczy wartości dopuszczalnej. Jest to jeden z warunków racjonalnych i ekonomicznych podstaw zarządzania wyrażonych w modelu funkcjonalno-strukturalnym (rysunek 4-16).

4.4. Wnioski

Stworzenie efektywnego i skutecznego systemu zarządzania bezpieczeństwem informacyjnym jest zadaniem złożonym i wymaga współpracy wielu instytucji. Podstawą powinny być działania organizacyjno-prawne, a przede wszystkim prawne zdefiniowanie pojęć z zakresu bezpieczeństwa informacyjnego, a także uregulowanie współpracy z podmiotami prywatnymi, które pozostają właścicielami części infrastruktury krytycznej państwa. Ochrona narodowej cyberprzestrzeni musi korespondować z ochroną europejskiej cyberprzestrzeni a także natowską i globalną.

Istotna sprawą jest rozbudowa systemu wczesnego ostrzegania i prognozowanie zagrożeń.[257] Dynamiczne wskaźniki ryzyka wynikające z rozwoju technologii mogą powodować koszty przy braku ciągłej ich obserwacji.

V. Model funkcjonalno-strukturalny



Rysunek 4-16. Model funkcjonalno-strukturalny zarządzania
Źródło: opracowanie własne na podstawie J. Wolanian, *Zarys teorii bezpieczeństwa obywateli.* Wydawnictwo Edura, 2005.

---

[257] Obecnie w 50 jednostkach organizacji administracji publicznej zainstalowano sensory na styku sieci „produkcyjnej" z Internetem tworzą system wykrywający i opisujący pojawiające się zagrożenia. System nosi nazwę ARAKIS_GOV. Odpowiedzialną jednostka jest CERT (*Computer Emergency Response Team*) Polska jest zespołem powołanym do reagowania na zdarzenia naruszające bezpieczeństwo w sieci Internet.

ZAKOŃCZENIE

Efektem końcowym dysertacji, będącym realizacją głównego celu badań, jest koncepcja modelu zarządzania bezpieczeństwem informacyjnym. W modelu tym wykorzystano podstawowe ilościowe i jakościowe metody prognozowania oraz oryginalną metodykę ewaluacji ryzyka zagrożeń informacyjnych. Propozycja jest jednym z elementów wspomagania procesów decyzyjnych przy planowaniu polityki bezpieczeństwa informacyjnego. Może także stanowić podstawę dla edukacji w zakresie bezpieczeństwa i polityki informacyjnej.[258] Ponadto wyraźnie koresponduje ze znacznie później powstałym „Programem ochrony cyberprzestrzeni RP"[259]

Własne badania i analizy pozwoliły na pozytywne zweryfikowanie głównej tezy rozprawy, a mianowicie: **zagrożenia informacyjne w coraz większym stopniu wpływają na poziom bezpieczeństwa narodowego RP. Wykazano, że za pomocą zarówno technik ilościowych, jak i jakościowych można oceniać ryzyko zagrożeń informacyjnych i prognozować wystąpienie możliwych i prawdopodobnych zagrożeń informacyjnych RP.**

Aby prognozy mogły powstawać, system zbierania informacji o zagrożeniach powinien być wszechstronne rozwinięty i ciągle doskonalony. Dotychczasowe doświadczenia wskazują, że prognozy krótkookresowe są wiarygodne gdy istnieje dobrze skwantyfikowana historia prognozowanego zjawiska. Prognozy długookresowe (np. do 2015) mogą być tworzone jedynie w warunkach dobrze zorganizowanego systemu doradczo-eksperckiego. Należy podkreślić, że pomimo zastrzeżeń (kontrowersji) metodologicznych oraz trudności wynikających z dysponowania niepełnymi i niepewnymi informacjami prognozy musza być sporządzane, gdyż w istocie stanowią podstawę podejmowania decyzji. Daje to podstawę dla kolejnego bardzo ważnego wniosku: **konieczne są dalsze badania z zastosowaniem różnych modeli ilościowych i jakościowych do prognozowania zagrożeń oraz poszukiwanie metod i modeli adekwatnych do swoistych cech prognozowanego zjawiska..**

Poszczególne tezy robocze znalazły potwierdzenie w analizach, których wyniki zaprezentowano w rozdziale II, co stanowi odpowiedź na szczegółowe zagadnienia problemowe (pytania) sformułowane w rozdziale pierwszym poświeconym metodologicznym podstawom badań , nad współczesnymi zagrożeniami informacyjnymi dla bezpieczeństwa narodowego.

---

[258] Wiele propozycji stanowiących treść niniejszej dysertacji wykorzystywane było w ramach prowadzonych zajęć z przedmiotu bezpieczeństwo informacyjne na studiach w AON.

[259] „Program,..., op.cit.

Wyniki szczegółowych analiz prognostycznych dotyczących zagrożeń informacyjnych przedstawiono w rozdziale III gdzie przykłady prognozowania z zastosowaniem szeregów czasowych i sztucznych sieci neuronowych. Wykazano użyteczność tych metod, ale również wskazano na ograniczenia i mankamenty. Ponadto zaprezentowano wyniki badań opinii społecznej (poprawnych w sensie statystycznym) oraz zasady budowy scenariuszy możliwych i prawdopodobnych sytuacji zagrożeń.

W rozdziale IV omówiono podstawy zarządzania ryzykiem zagrożeń informacyjnych dla bezpieczeństwa narodowego, wraz z propozycją oryginalnej metodyki ewaluacji ryzyka. Swoistą syntezę propozycji z zakresu prognozowania zagrożeń i zarządzania ryzykiem stanowi koncepcja modelu systemu zarządzania bezpieczeństwem informacyjnym RP.

Na podstawie przeprowadzonych badań i analiz przyjęte hipotezy robocze zweryfikowano pozytywnie:

dla hipotez ogólnych:

8. Wzrost zagrożeń informacyjnych powoduje obniżenie poziomu bezpieczeństwa informacyjnego państwa.

Zasadnicza większość zagrożeń informacyjnych w sposób bezpośredni wpływa na stan bezpieczeństwa narodowego. Istnieją jednak również zagrożenia, które mogą oddziaływać pośrednio na pozostałe podstawowe dziedziny bezpieczeństwa narodowego (tabela 4-19).

Tabela 4-19. Wpływ zagrożeń informacyjnych na bezpieczeństwo państwa RP (PRZYKŁAD)

DZIEDZINY BEZPIECZEŃSTWA PAŃSTWA	RODZAJ ZAGROŻEŃ	SKUTKI DLA BEZPIECZEŃSTWA PAŃSTWA
BEZPIECZEŃSTWO NARODOWE[260]	Terroryzm, cyberterroryzm	Osłabienie zdolności obronnych i rozwojowych państwa
BEZPIECZEŃSTWO MILITARNE	Niedostateczny poziom rozwoju systemu ochrony cyberprzestrzeni.(wysoka podatność na zagrożenia) Terroryzm, cyberterroryzm	Osłabienie zdolności obronnych i rozwojowych państwa oraz KIP. Obniżenie zdolności prowadzenia własnych i sojuszniczych operacji informacyjnych
STOSUNKI MIĘDZYNARODOWE	Brak strategii ochrony cyberprzestrzeni; Brak zdolności współpracy z podmiotami zagranicznymi w dziedzinie bezpieczeństwa cyberprzestrzeni UE, NATO	Osłabienie wizerunku państwa i wiarygodności jako partnera i sojusznika; Obniżenie poziomu bezpieczeństwa systemów komunikacyjnych

[260] Według pojęcia bezpieczeństwa narodowego utożsamiane jako bezpieczeństwo państwa, którego składnikami są bezpieczeństwo wewnętrzne i zewnętrzne. Podział, jak zaznaczono w pierwszym rozdziale nie jest ostry.

STOSUNKI DYPLOMATYCZNE	Możliwość infiltracji przechwytywania wiadomości, podsłuchu sieci itp.	Obniżenie zaufania między partnerami oraz rangi międzynarodowej
EKONOMIA	Destabilizacja rynku finansowego, monetarnego, giełdy papierów wartościowych, duża liczba kradzieży internetowych itp.	Wzrost kosztów usuwania skutków zagrożeń itp. Zwiększanie nakładów na systemy bezpieczeństwa
OPINIA PUBLICZNA (SPOŁECZNA)	Dezinformowanie, parainformowanie, pseudoinformowanie społeczeństwa, nadmiar informacji, smog informacyjny, tabloidyzacja mediów itp.	Wzrost „wzburzenia społecznego", wycofania społecznego, apatia, itp.
SPRAWNOŚĆ OPERACYJNA	Blokowanie stron WWW, zniekształcanie informacji w systemach informacyjnych administracji państwowej i samorządowej. Propaganda informacyjna	Utrata sprawnej łączność w sferze publicznej oraz rządowej I samorządowej, w czasie pokoju, jak i w stanie wyjątkowym
NAUKA, TECHNIKA, TECHNOLOGIA	Kradzież własności intelektualnej Szpiegostwo przemysłowe, wykorzystujące luki w bezpieczeństwie komunikacyjnym	Obniżenie zdolności rozwoju Intelektualnego obywateli oraz rozwoju cywilizacyjnego

Źródło: opracowanie własne.

9. Obniżenie poziomu bezpieczeństwa informacyjnego państwa powoduje obniżenie poziomu bezpieczeństwa narodowego.
10. Bezpieczeństwo informacyjne jest istotnym czynnikiem jakości życia obywateli.

System bezpieczeństwa informacyjnego państwa nie może ograniczać się tylko do bezpieczeństwa teleinformatycznego, gdyż musi odnosić się do całości infosfery (procesów informacyjnych zachodzących w państwie), a także w jego otoczeniu (UE, NATO).

dla hipotez dotyczących diagnozy polskiego systemu bezpieczeństwa informacyjnego:

11. Występują braki w świadomości społecznej zagrożeń informacyjnych - jest to przyczyna najczęściej powodująca szkody („człowiek najsłabsze ogniwo"). Zagrożenia szybko ewoluują, rozwiązania prawne, organizacyjne i techniczne nie nadążają za zmianami technologicznymi.

12. Dla obrony przed zagrożeniami informacyjnymi, ze względu na ich ilość i różnorodność, rosną wymagania bezpieczeństwa, które nie wszyscy użytkownicy sieci mogą spełnić z powodów ekonomicznych (finansowych).
13. Zastosowanie nowoczesnych metod pomiaru, analizy i oceny jakości bezpieczeństwa informacyjnego stwarza podstawy dla racjonalnej polityki bezpieczeństwa oraz zapewnienia pożądanego poziomu bezpieczeństwa informacyjnego państwa.
14. Upowszechnienie nowoczesnych metod i narzędzi pomiaru, analizy i oceny zagrożeń bezpieczeństwa informacyjnego, przy jednoczesnym właściwym doborze treści, form i środków kształcenia i szkolenia jest jednym z podstawowych warunków zapewnienia bezpieczeństwa informacyjnego państwa.
15. Przyjęty wariant analizy systemowej odpowiada wymaganiom ogólnej sytuacji problemowej wynikającej z obecnego i przyszłego stanu realnych zjawisk zwianych z występowaniem zagrożeń informacyjnych w bliższym i dalszym otoczeniu systemowym państwa. Wariant ten umożliwił:
    - Analizę identyfikacyjną zagrożeń informacyjnych (źródła, symptomy, przyczyn, możliwe skutki);
    - Opracowanie metodyki zarządzania ryzykiem zagrożeń informacyjnych na potrzeby budowy modelu zarządzania bezpieczeństwem narodowym;
    - Opracowanie scenariuszy możliwych i prawdopodobnych sytuacji zagrożeń dla bezpieczeństwa informacyjnego wraz z generowaniem strategii przeciwdziałania sytuacjami zagrożeń dla bezpieczeństwa informacyjnego;

<u>wśród ogólnych wniosków z przeprowadzonych analiz do najważnieiszych należą:</u>

- Problematyka bezpieczeństwa systemów jest problematyką interdyscyplinarną, jej znaczenie będzie wzrastać szczególnie w obszarze technologii oraz systemów ICT.
- Bezpieczeństwo jest kategoria systemową, gdyż dotyczy cechy obiektów złożonych (technicznych, społecznych) rozpatrywanych jako ustrukturyzowne całości aktywne w aktywnym otoczeniu funkcjonujące.
- Bezpieczeństwo systemu jest pojęciem względnym (zawsze relatywizowanym do ogólnej sytuacji zewnętrznej), a ponadto może oznaczać zarówno brak zagrożenia (stan obiektywny), jak i brak poczucia zagrożenia (stan subiektywny)
- Bezpieczeństwo jest procesem, który wymaga sprawnej koordynacji przez państwowe.

- Systemy ICT stanowią immanentną część społecznej infrastruktury, a także krytycznej infrastruktury państwa (organizacji, instytucji).
- Bezpieczeństwo systemu zależy zarówno od wielkości zagrożenia (intensywność) jak i od efektywności systemu zabezpieczeń (ochrony, podatności).
- Źródłem zagrożeń są różni użytkownicy cyberprzestrzeni (organizacje państwowe i międzynarodowe, organizacje przestępcze i podmioty bezpaństwowe, terroryści, wandale itp.)
- Bezpieczeństwo musi być uwzględniane w procesie projektowania i eksploatowania systemów ICT, w każdej fazie przesyłania, przetwarzania, przechowywania i dystrybucji informacji;
- Bezpieczeństwo informacyjne ze względu na mnogość interakcji powinno być analizowane na kilku płaszczyznach bezpieczeństwa: systemu państwa, bezpieczeństwa organizacji i obywatela.
- Bezpieczeństwo informacyjne należy rozpatrywać w kontekście organizacyjnym, technicznym oraz prawnym, a także od strony własności systemów informacyjnych, albowiem w znacznej części właścicielami systemów komunikacyjnych pozostają podmioty niepaństwowe.
- Bezpieczeństwo informacyjne odnieść należy do obszarów:
  - bezpieczeństwo informacji (zasobów informacyjnych): odnoszące się do ochrony danych, poufności danych, informacji niejawnych o charakterze strategicznym;
  - cyberbezpieczeństwo: rozumiane jako zabezpieczenie przed cyberprzestępstwami i cyberterroryzmem (bezpieczeństwo cyberprzestrzeni);
  - bezpieczeństwo teleinformatyczne: jako pojęcie, określające ochronę zinformatyzowanych działów strategicznych, do których można dotrzeć przy pomocy szeroko pojmowanych połączeń sieciowych;
  - polityki bezpieczeństwa informacyjnego państwa;
  - bezpieczeństwo odnoszące się do praw obywatelskich;
  - doktryny walki informacyjnej, stosowanej przez współczesne armie.

W kontekście tak zweryfikowanych hipotez osiągnięto główny cel badań: opracowano koncepcję modelu zarządzania bezpieczeństwem informacyjnym, wykorzystującego analizę systemową sytuacji zagrożeń informacyjnych, wraz z metodami prognozowania i ewaluacji ryzyka.

Konkluzja

Istnieje potrzeba badań systemowych nad zagrożeniami informacyjnymi i bezpieczeństwem informacyjnym i jego wpływem na bezpieczeństwo państwa. Bezpieczeństwo jest procesem, a wobec zmian w technologiach, które wywierają wpływ na środowisko bezpieczeństwa narodowego i międzynarodowego jest konieczna ciągła eksploracja tego obszaru.

Bezpieczeństwo w cyberprzestrzeni zależy od sposobów ochrony zasobów informacji każdego kraju, każdej firmy i każdego użytkownika korzystającego z sieci teleinformatycznych. Aby ochronić się przed wyrafinowanymi technikami specjalnie tworzonymi przez cyberprzestępców, konieczne jest stworzenie globalnej kultury bezpiecznych zachowań w cyberprzestrzeni. Wymaga to prawnych i prewencyjnych działań, ale także bardzo wysokiego poziomu świadomości społecznej istniejących zagrożeń.

Kierunki dalszych badań

Zagrożenia informacyjne i problem bezpieczeństwa informacyjnego jest w istocie problemem, który będzie stale generował nowe szczegółowe problemy, gdyż będą pojawiały się nowe zagrożenia. Skuteczne przeciwdziałanie zagrożeniom informacyjnym wymaga skoordynowanych działań różnych organów i służb administracji publicznej (nie tylko rządowej), ale przedsiębiorstw prywatnych i innych.

Wynika stąd konieczność doskonalenia:

1) metod identyfikacji zagrożeń informacyjnych;
2) metod oceny podatności obiektów na zagrożenia;
3) metod oszacowania szkód (strat) obiektów spowodowanych zagrożeniami informacyjnymi;
4) metod prognozowania zagrożeń informacyjnych zarówno masowych, jak i incydentalnych (zaprezentowane modele formalne nie wyczerpują zastosowań innych jeszcze nie zbadanych);
5) metod ewaluacji ryzyka zagrożeń informacyjnych w aspekcie bezpieczeństwa narodowego;
6) integracji systemów monitoringu, wczesnego ostrzegania i analizy zagrożeń (obecnie tylko rozpoznajemy zagrożenia);
7) rozwoju metod i modeli systemów zarządzania bezpieczeństwem informacyjnym na potrzeby systemu zarządzania bezpieczeństwem narodowym RP;

8) Stałej współpracy międzynarodowej i wymiany informacji w ramach programu bezpieczeństwa europejskiej cyberprzestrzeni;
9) konieczność budowy centrum (instytucji koordynującej) całość zagadnień związanych z zarządzaniem bezpieczeństwem w cyberprzestrzeni i jednocześnie nadzorującej i zlecającej programy badawcze oraz nadzorującej programy kształcenia.

Zagrożenie „wojną cybernetyczną" staje się możliwe i prawdopodobne. Na podatność państwa na zagrożenia informacyjne ma zapewne wpływ stanu niemal całkowitego braku wytycznych polityki państwowej oraz odpowiednich przepisów prawa międzynarodowego i traktatów. Brakuje porozumienia, co do kwalifikacji prawnej ataku cybernetycznego (akt wojny czy przestępstwo pospolite). Obecnie można pokładać nadzieję w realizacji, niektórych postulatów dotyczących ochrony cyberprzestrzeni w związku z przyjęciem w dniu 9 mara 2009 roku przez Komitet Stały Rady Ministrów dokumentu pt. „Rządowy program ochrony cyberprzestrzeni RP na lata 2009-2011". Być może największym osiągnięciem będzie stworzenie partnerstwa publiczno-prywatnego w ochronie cyberprzestrzeni.

Literatura

Adamski A., *Cyberterroryzm*, [w:] Kwiatkowska-Darul V., (red.), *Terroryzm*. Materiały z sesji naukowej, Wydawnictwo Naukowe Uniwersytetu Mikołaja Kopernika w Toruniu, Toruń 11.04.2002.

AIRMIC, ALARM, IRM:2002, translation copyright FERMA: 2003.

Alberts David S., John J. Garstka, Frederick P. Stein, *Network Centric Warfare – Developing and Leveraging Information Superiority*, 2-nd Edition of CCRP, ISBN 1-57906-019-6, August 1999.

Anderson R., *Inżynieria zabezpieczenia*. WNT, Warszawa 2005.

Apanowicz J., *Metodologia nauk*. Wyd. „DOM ORGANIZATORA", Toruń 2003.

Arguilla I. , Ronfeldt D., *Cyberwar is Coming*" , Comparative Strategy, 12, 1993; end *In Athena's Camp: Preparing for Conflict in the Information Age*, Santa Monica 1997.

Attali J., *Słownik XXI wieku*, Wyd. Dolnośląskie, Wrocław 2002.

Barczak A., Sidoruk T., *Bezpieczeństwo systemów informatycznych*, Wyd. Akademii Podlaskiej, Siedlce 2002.

Baylis J., Wirtz J., Gray C., Cohen E., *Strategia we współczesnym świecie*. Wyd. UJ, Kraków 2009.

Bączek P., *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Wyd. Adam Marszałek, Toruń 2005.

Beck U., *Społeczeństwo ryzyka. W drodze do innej nowoczesności*, Wyd. SCHOLAR, Warszawa 2004.

Bendyk E., *Miłość, wojna, rewolucja*. Wyd. W.A.B., Warszawa 2009.

Bernstein P.L., *Przeciw bogom. Niezwykłe dzieje ryzyka*. WIG PRESS, Warszawa 1997.

Białas A., *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*. WNT, Warszawa 2006.

Birówka J., *Zasada wzajemności w formującym się społeczeństwie informacyjnym*, Rozpraw doktorska, UJ, Kraków 2007.

Bódgał-Brzeźińska A., Gawrycki M.F., *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*. Wyd. Fundacja Studiów Międzynarodowych, Warszawa 2003.

Brian A. Jackson, Lloyd Dixon, Victoria A.Greenfield, *Economically Targeted Terrorism, A Review of the Literature and a Framework for Considering Defensive Approaches*. RAND, 2007.

Brzeziński J., *Metodologia badań psychologicznych*, PWN, Warszawa 2006.

Campen A., *The First Information War*, NY, 1991.

Castells M., *Społeczeństwo sieci*. PWN Warszawa 2008.

Christopher G. Pernin, Katherine Comanor, Lance Menthe, Louis R. Moore, Tim Andersen, *Allocation of Forces, Fires, and Effects Using Genetic Algorithms*. RAND, 2008.

Ciborowski L., *Walka informacyjna*, Toruń 1999.

Ciecierski M., *Ochrona informacji niejawnych i biznesowych*, Materiały IV Kongresu KSOIN, Uniwersytet Śląski, Katowice 2008.

Cieciura M., *Jak skutecznie studiować*?, Wyd. VIZJA PRESS&IT, Warszawa 2007.

Cieślak M. (red.), *Prognozowanie gospodarcze*. PWN Warszawa 2000.

Czapiński J., Panek T. (red.), *Diagnoza społeczna 2007. Warunki życia Polaków*. Raport. Rada Monitoringu Społecznego. Warszawa 2007.

Czechowski R., Sienkiewicz P., *Przestępcze oblicza komputerów*. PWN, Warszawa 1993.

Darilek R., Perry W., Bracken J., Gordon J. Nichiporuk B. *Measures of Effectivness for the Information-Age Army*. Rand, Santa Monica 2001.

Denning D. E., *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool For Influencing Foreign Policy*, [w:] J. Arquilla, D. Ronfeldt (red.), *Networks and Netwars: The future of terror, crime and militancy*, Santa Monica 2001.

Denning D.E., *Wojna informacyjna i bezpieczeństwo informacji*. Wydawnictwa Naukowo-Techniczne. Warszawa 2002.

Devlin K. *Żegnaj Kartezjuszu. Rozstanie z logiką w poszukiwaniu nowej kosmologii umysłu*. Wyd. Prószyński i S-ka, Warszawa 1997.

Dżega D., *Metoda oceny ryzyka projektów informatycznych*. Praca doktorska. Politechnika Szczecińska, Szczecin 2008.

Elszkowski M., *Cyberprzestępczość zagrożeniem XXI wieku – oszustwo internetowe*, Szczytno 2004.

Ferguson G. A., Takane Y., *Analiza statystyczna w psychologii i pedagogice*. PWN, Warszawa 2005.

Findeisen W., (red.), *Analiza systemowa – podstawy i metodologia.* WNT, Warszawa 1985.

Frankfort-Nachmias C., Nachmias D., *Metody badawcze w naukach społecznych*, Wyd. Zysk i S-ka, Poznań 2001.

Gajda J.B., Prognozowanie i symulacja a decyzje gospodarcze. Wyd. C.H.Beck, Warszawa 2001.

Garstka John J., *Network Centric Warfare: An Overview of Emerging Theory.* PHALANX. December 2000.

Gately E., *Sieci neuronowe. Prognozowanie finansowe i projektowanie systemów transakcyjnych.* Wig Press, Warszawa 1999.

Gawliczek P., *Asymetria w środowisku bezpieczeństwa. Rozprawa habilitacyjna.* AON, Warszawa 2009.

Gębski B., *Wprowadzenie do metodologii badań społecznych.* Wyd. I, Wyd. WWSP TWP, Warszawa 2008.

Gilgam M.M., *Information warfare: Combating the threat in the 21st century.* 1997.

Goban-Klas T., *Media i komunikowanie masowe – teoria i analizy prasy, radia, telewizji i Internetu.* Warszawa 2004.

Goban-Klas T., Sienkiewicz P., *Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania.* Wyd. Postępu Telekomunikacji, Kraków 1999.

Gogela R., Novàk L., Šefčik A., *Critical Infrastructure Modelling*, [w:] Security and Protection of Information, 2003.

Golka M., *Poczucie zagrożeń i wyzwań cywilizacyjnych*, Wyd. Fundacji Humaniora, Poznań 2000.

Goszczyńska M., Człowiek wobec zagrożeń. Uwarunkowania oceny i akceptacji ryzyka. Wyd. Żak, Warszawa 1999.

Gryz J., Kwećka R., *Współczesny wymiar terroryzmu, przeciwdziałanie zjawisku*, Warszawa 2007.

Haber L. (red.) *Społeczeństwo informacyjne. Wizja czy rzeczywistość*? Tom I" wyd. Uczelniane Wydawnictwa Naukowo – Dydaktyczne, Kraków 2004.

Haber L., *Od robotnika do Internetu – w kierunku społeczeństwa informacyjnego.* AGH, Kraków 2008.

Hołyst B., Terroryzm. LexisNexis, Warszawa 2009.

Howard John D., Longstaff Thomas A., *A Common Language for Komputer Security Incidents*, Sandia National Laboratories, Albuquerque 1998.

Huntington S.P., *Zderzenie cywilizacji.* Wyd. Spectrum, Warszawa 2008.

Janczak J., Świdzikowski G., *Bezpieczeństwo informacji w wojskowym systemie telekomunikacyjnym.* AON, Warszawa 2004.

Jańczak J., Wisz A., *Sieci teleinformatyczne w działaniach sieciocentrycznych. Materiały konferencyjne.* AON, Warszawa 2007.

Jemioło T. (red.) *Cyberteroryzm nowe wyzwania XXI wieku.* Wyd. WSIZiA w Warszawie, WSP w Szczytnie, WB AON, Warszawa 2009.

Jemioło T., Dawidczyk A., *Wprowadzenie do metodologii badań nad bezpieczeństwem.* AON, Warszawa 2007.

Jemioło T., Rajchel K., *Bezpieczeństwo narodowe i zarządzanie kryzysowe w Polsce w XXI wieku – wyzwania i dylematy*, WSIZiA, Warszawa 2008.

Jemioło T.,(kier.) *Modelownie zagrożeń dla bezpieczeństwa informacyjnego państwa. Teoria walki informacyjnej.* AON, Warszawa 2004.

Kaczmarek T.T., Ryzko izarządznie ryzkiem. Ujęcie interdyscyplinarne. Difin, Warszawa 2006.

Kamieński Ł., Technologia i wojna przyszłości. Wokół nuklearnej i informacyjnej rewolucji w sprawach wojskowych. Wyd. UJ, Kraków 2009.

Keus Hans E., *Network Centric Operations. Implications for Allied and Coalition Operations,* Konferencja SMi Conferences on Network Centric Warfare, London, 4-5 October 2000.

Kinasiewicz M. (red.), *Modelowanie procesów walki informacyjnej. Model „Cyberwar"*. AON, Warszawa 2006.

Kolman R., *Poradnik podnoszenia kwalifikacji*, Ofic.Wyd. Branta, Bydgoszcz-Gdańsk 2004.

Komunikat Komisji do Rady, Parlamentu Europejskiego, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów 2005, COM(2005) 229.

Korzyk A., Violino B., *A Forecasting model for internet security attacks*; The Security Facade, Information Week, 21 October 1996.

Kosiński J., *Nigeryjski spam.* Wyższa Szkoła Policji w Szczytnie. Szczytno 2004.

Kotarbiński T., *Elementy teorii poznania, logiki formalnej i metodologii nauk.* Wrocław 1961.

Koziej S., *Strategia bezpieczeństwa i obronności Rzeczypospolitej polskiej po wstąpieniu do NATO.* Skrypt internetowy. www.koziej.pl.

Koziej S., *Współczesne problemy bezpieczeństwa międzynarodowego i narodowego*, Wyd. Biura Badań Strategicznych PWSBiA, Warszawa 2003.

Koziej S., *Współczesne problemy bezpieczeństwa międzynarodowego i narodowego.* Wyd. Biuro Badań Strategicznych PWSzBiA, Warszawa 2009.

Kozielecki J., *Rozwiązywanie problemów*, Warszawa 1969.

Kozioł J. *Podejmowanie decyzji w warunkach ryzyka*, w: Zeszyty Naukowe AON. *Współczesne siły powietrzne - misje, zadania, tendencje rozwoju,* Nr 2(47) Numer specjalny, Warszawa 2002.

Kręcikij J., *Działania sieciocentryczne. Wybrane problemy.* AON, Warszawa 2008.

Krysiński S., Koziełło M. *Rozwój zdolności sieciocentrycznych NATO.* Kwartalnik Bellona Nr 3/2007.

Kwećka R., *Informacja w walce zbrojnej.* AON, Warszawa 2001; *SIŁY specjalne w kontekście współczesnych zagrożeń,* współautor Gryga M., AON, Warszawa 2002.

Kwiatosz J. *Współczesne Poglądy Na Walkę Informacyjną.* Materiały VIII Konferencji Naukowej „*Automatyzacja Dowodzenia*", Jelenia Góra 2000.

Libicki M., Chale P., Sisson M., *Exploring Terrorist Targeting Preeferences*, RAND, 2007.

Lichocki E., *Model systemu zarządzania kryzysowego w warunkach zagrożeń cyberterrorystycznych dla bezpieczeństwa informacyjnego Sił Zbrojnych Rzeczypospolitej Polskiej.* Rozprawa doktorska, AON, 2009.

Liderman K., *Analiza ryzyka i ochrona informacji w systemach komputerowych,* PWN, Warszawa 2008.

Liderman K., *Analiza ryzyka i ochrona informacji w systemach komputerowych.* PWN, Warszawa 2006.

Liderman K., *Bezpieczeństwo teleinformatyczne.* WAT, Warszawa 2001.

Luszniewicz A., Słaby T., *Statystyka z pakietem komputerowym STATISTICA PL. Teoria i zastosowania,* Wyd. C.H.Beck, Warszawa 2001.

Łacheta M., Molski M., *Bezpieczeństwo i audyt systemów informatycznych*, Wyd. Uczelniane WSzG, Bydgoszcz 2009.

Łobocki M., *Metody badań pedagogicznych*, Warszawa 1982.

MacDonald J., Knopman D., Lockwood J.R., Cecchine G., Willis H., *Unexploded Ordnance A Critical Review of Risk Assessment Methods.* RAND Arroyo Center, 2004.

Maddison G.R., *The Naval C4I Way Ahead – A Blueprint for 2010.* Materiały NG/5 NATO, s. 44.

Madej M., (red), *Bezpieczeństwo teleinformatyczne państwa.* PISM, Warszawa 2009

Madej M., *Zagrożenia asymetryczne bezpieczeństwa państw obszaru transatlantyckiego*, PISM, Warszawa 2007.

Manikowski A., Tarapata Z., *Prognozowanie i symulacja rozwoju przedsiębiorstw*, WSE, Warszawa 2002.

Marecki F., Grabara J.K., Nowak J.S., (red.): *Systemy informatyczne. Bankowość i finanse,* WNT, Warszawa 2004.

Mąka D. *Ryzyko w systemie bezpieczeństwa informacyjnego państwa w aspekcie standardów NATO i Unii Europejskiej.* Rozprawa doktorska, AON, Warszawa 2004.

McLuchan M., *Społeczeństwo sieci.* Wyd. Naukowe PWN, Warszawa 2007.

McLuhan M., *Zrozumieć media.* WNT, Warszawa 2004.

Mierczyk Z. (red.), *Nowoczesne technologie systemów uzbrojenia*, WAT, 2008.

Mitnick K., Kimon W., *Sztuka podstępu,* Wydawnictwo Helion, Warszawa 2002.

Moffat J., *Complexity Theory and Network Centric Warfare, Command and Control Research Programme*, US Dept of Defense, Washington, DC, 2003.

Niemiec A., Nowak J.S., Grabara J.K., *Bezpieczeństwo systemów informatycznych.* PTI Oddział Górnośląski, Katowice 2006.

Nowak S.: Metodologia badań socjologicznych, Warszawa 1970.

Nowakowski Z, Szafran H., Szafran R., *Bezpieczeństwo w XXI wieku.* Wyd. RS DRUK, Rzeszów 2009.

Owens W., *The Emerging U. S. System-of-System*, "Strategic Forum", No 63, 1996.

Pankowski T., *Bezpieczeństwo w systemach informatycznych.* Wyd. Naukowe PWN, Warszawa 2001.

Pawłowski J., (red.) Terroryzm we współczesnym świecie. Wyd. MON, Warszawa 2001.

Piątkowski M., *Wpływ technologii informatycznych i telekomunikacyjnych na wzrost gospodarczy i rozwój przedsiębiorstw w krajach posocjalistycznych*. Rozprawa doktorska. WSPiZ im. L.Koźmińskiego, 2004.

Pilch T., Bauman T., *Zasady badań pedagogicznych. Strategie ilościowe i jakościowe*, Wyd. Żak, Warszawa 2001.

Pipkin L., *Bezpieczeństwo informacji*, WNT, Warszawa 2002.

Płaczek J. (red.), *Diagnoza i perspektywy rozwoju infrastruktury technicznej RP z punktu widzenia obronnego*. Kryptonim „Infra". AON, Warszawa 2009.

Posobiec J., *Organizacja dowodzenia w środowisku sieciocentrycznym*. AON, Warszawa 2008.

Radzikowska B., *Metody prognozowania. Zbiór zadań*. WAE, Wrocław 2004.

Rattray G.J., *Wojna strategiczna w cyberprzestrzeni*. Wyd. Wydawnictwo Naukowo – Techniczne". Warszawa 2004.

Sandman P., Responding to Community Outrage: Strategies effective Risk Communication, American Industrial Hyguene Association Fairfax. 1997.

Sienkiewicz P, Swieboda H., *Teoretyczne podstawy walki informacyjnej*. ZN 1(70) AON, Warszawa 2008.

Sienkiewicz P. (red.), *Model wojskowego systemu logistycznego dla NCW i GOW. Koncepcja, model, wymagania i ograniczenia.* AON, Warszawa 2009.

Sienkiewicz P. (red.), *Modelownie procesów walki informacyjnej. „Model cyberwar"*. AON, Warszawa 2006.

Sienkiewicz P., (red.), *Planowanie eksperymentów symulacyjnych i analiza systemów z wykorzystaniem symulacji komputerowej*. AON, Warszawa 2009.

Sienkiewicz P., (red.), Zarządzanie ryzykiem w sytuacjach kryzysowych. AON, Warszawa 2006.

Sienkiewicz P., (red.) *Modelowanie rozwoju globalnego społeczeństwa informacyjnego*. AON, Warszawa 2003.

Sienkiewicz P., *10 wykładów.* AON, Warszawa 2005.

Sienkiewicz P., *Analiza systemowa. Podstawy i zastosowania*, Bellona, Warszawa 1995.

Sienkiewicz P., Bezpieczeństwo i wolność w globalnym społeczeństwie informacyjnym. AGH, Kraków 2007.

Sienkiewicz P., *Ewolucja struktur organizacji.* Zeszyty Naukowe AON Nr 3/2007.

Sienkiewicz P., *Inżynieria systemów kierowania*, PWE, Warszawa 1988.

Sienkiewicz P., *Modelowanie rozwoju globalnego społeczeństwa informacyjnego. Modele rozwoju globalizacji*, AON, Warszawa 2003.

Sienkiewicz P., Swieboda H., *Edukacyjne determinanty rozwoju społeczeństwa informacyjnego*. Zeszyty Naukowe WWSI, Nr 2, Warszawa 2007.

Sienkiewicz P., Świeboda H. *Teoretyczne podstawy walki informacyjnej*. Zeszyty Naukowe AON Nr 1, 2008

Sienkiewicz P., Świeboda H., *Analiza systemowa jakości życia w społeczeństwie informacyjnym*, BOS'06, Warszawa 2006.

Sienkiewicz P., Świeboda H., i in. *Bezpieczeństwo obywateli RP jako czynnik jakości życia.* AON, Warszawa 2009.

Sienkiewicz P., Świeboda H., *Niebezpieczna przestrzeń cybernetyczna*, Transformacje 1-4 (47-50), Wyd. Fundacja Edukacyjna, Transformacje, grudzień 2006.

Sienkiewicz P., Świeboda H., Perspektywy badań systemowych nad bezpieczeństwem. Międzynarodowa konferencja naukowa nt. Bezpieczeństwo wymiar współczesny oraz perspektywy badań. Kraków 2008.

Sienkiewicz P., Świeboda H., Sieci teleinformatyczne jako instrument państwa – walka informacyjna i szpiegostwo elektroniczne. PISM, Warszawa 2009.

Sienkiewicz P., Świeboda H., *Społeczna percepcja zagrożeń bezpieczeństwa obywateli w warunkach globalnego społeczeństwa informacyjnego*. AON, Warszawa 2009.

Sienkiewicz P., Świeboda H., *Wybrane metody naukowych badań nad bezpieczeństwem i obronnością*. AON, Warszawa 2008.

Sienkiewicz P., *Teoria efektywności systemów*. Ossolineum, Wrocław 1987.

Sienkiewicz P., *Wartość informacji w systemach zarządzania organizacja*. AGH, Kraków 2009.

Sienkiewicz P., *Współczesne badania systemowe. Cz.II – teorie, analiza, inżynieria.* Transformacje (w druku).

Sienkiewicz P.,(red.), *Zarządzanie ryzykiem w sytuacjach kryzysowych.* AON, Warszawa 2006.

Simon H.A., *Podejmowanie decyzji kierowniczych.* Nowe nurty. Warszawa 1982.

Siwik (red.), *Od społeczeństwa industrialnego do społeczeństwa informacyjnego.* AGH, Kraków 2007.

Slovic P., *Risk As Analysis and Risk As Feelings.* New Orleans, Louisiana, 2002.

Słownik terminów bezpieczeństwa narodowego, AON, Warszawa 2002.

Soros G., *Nowy paradygmat rynków finansowych*, MT Biznes, Warszawa 2008.

Stabryła A., Zarządzanie projektami ekonomicznymi i organizacyjnymi, PWN, Warszawa 2006.

Stańczyk J., *Współczesne pojmowanie bezpieczeństwa.* Instytut Studiów Politycznych PAN, Warszawa 1996.

Stiglitz J.E., *Ekonomia sektora publicznego*, PWN, Warszawa 2004.

Strategia Bezpieczeństwa Narodowego RP 2007.

Strategia Bezpieczeństwa Narodowego RP, Warszawa 2003.

Szafrański B., i in. Interoperacyjność i bezpieczeństwo systemów informatycznych administracji publicznej. PTI Oddział Górnośląski, Katowiec 2006.

Szewczyk A., *Oblicza ubóstwa w społeczeństwie informacyjnym*, PWN, Warszawa 2006.

Szewczyk A., *Społeczeństwo informacyjne – problemy rozwojowe.* Difin, Warszawa 2007.

Szpyra R., *Cyberterroryzm – poszukiwanie istoty i charakterystyki.* [w:] T. Jemioło, J.Kisielnicki i in. (red.), *Cyberterroryzm nowe wyzwania XXI wieku.* Warszawa 2009.

Szpyra R., *Militarne operacje informacyjne*, AON, Warszawa 2003.

Szpyra R., *Operacje informacyjne państwa w działaniach sił powietrznych*, rozprawa habilitacyjna. AON, Warszawa 2002.

Szynowski R., (red.), *Zarządzanie zasobami osobowymi na rzecz bezpieczeństwa państwa*, Warszawa 2007.

Świeboda H., *Bezpieczeństwo informacyjne dla bezpieczeństwa narodowego*, ZN AON Nr 3(68) Warszawa 2007.

Świeboda H., *Edukacja a jakość życia, materiały konferencyjne.* Zakopane 2007.

Świeboda H., Sienkiewicz P., Lichocki E., *Analiza systemowa zjawiska cyberterroryzmu*, ZN AON, Nr 2(63), Warszawa 2006.

Świeboda H., Sienkiewicz P., Pelc M., *Aspekty logistyczne bezpieczeństwa krytycznej infrastruktury państwa,* ZN AON, Kwartalnik Nr 2(67)B, Warszawa 2007.

Toffler A. *Szok przyszłości.* Wyd. KRUPISZ, 2007.

Toffler *A., Trzecia fala.* PIW, Warszawa 1997.

Toffler A.H., *Wojna i antywojna. Jak przetrwać na progu XXI wieku*, WWL Muza SA, Warszawa 1997.

Tyszka T., *Psychologia ekonomiczna.* vol. 1,2, Warszawa 2004.

Vatis M.A., *Cyber Attacks During the War on Terrorism: A Predictive Analysis, Institute for Security Technology Studies at Dartmouth College,* September 22, 2001.

Verton D., *Black Ice: Niewidzialna groźba cyberterroryzm.* Wydawnictwo Helion, Warszawa 2004.

Waltz E., *Information Warfare. Principles and operations.* Artech Mouse, Boston, London 1998.

Warden J., *The Enemy as System*, 1995.

Wierzbicki A.P. *Badania operacyjne i systemowe w epoce cywilizacji wiedzy.* IBS PAN BOS'08, Warszawa 2008.

Wilson C., *Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress* Updated April 1, 2005.

Wizja Sił Zbrojnych RP 2030. MON, Departament Transformacji, Warszawa, maj 2008.

Wolanin J., Zarys teorii bezpieczeństwa obywateli. Warszawa 2005.

Yourdon E., *Wojna na bity,* WNT, 2004.

Zacher L., (red.), *Filozofowie o technice.* KAW, Warszawa 1986.

Zacher L., *Gry o przeszłe światy.* Komitet prognoz Polska 2000 Plus, PAN, Warszawa 2006.

Zacher L., *Transformacja społeczeństw, od informacji do wiedzy.* C.H.Beck, Warszawa 2007.

Zaczyński W.P., *Statystyka w pracy badawczej nauczyciela.* Wyd. Żak, Warszawa 1997.

Zajas S. (red.), *Nauki wojskowe a nauki o bezpieczeństwie i obronności.* AON, Warszawa 2009.

Zaleśkiewicz T., *Przyjemność czy konieczność. Psychologia spostrzegania i podejmowania ryzyka.* Wyd. GWP, Gdańsk 2005.

Zdrodowski B., Wiśniewski B., (red.), *Kierowanie bezpieczeństwem narodowym.* AON, Warszawa 2008.

Zeliaś A., Pawełek B., Wanat S., *Prognozowanie ekonomiczne. Teoria przykłady, zadania,* PWN, Warszawa 2004.

Zeliaś A., *Teoria prognozy.* PWE, Warszawa1979.

Zeszyty Naukowe AON, Kwartalnik nr 3(68) A, *System dowodzenia w środowisku sieciocentrycznym.* Warszawa 2007.

Zeszyty Naukowe AON. *Współczesne Siły Powietrzne - Misje, Zadania, Tendencje Rozwoju,* Nr 2/47) Numer specjalny, Warszawa 2002.

Zięba R., *Bezpieczeństwo międzynarodowe po zimnej wojnie.* Wyd. Akademickie i Profesjonalne, Warszawa 2008.

Artykuły prasowe, inne

AIRMIC, ALARM, IRM:2002, translation copyright FERMA: 2003.

Broad anti-terrorism package passed by Congress, signed by President, Cybercrime Law Report, Pike & Fisher, Inc., vol.1, no. 16, November 5, 2001.

Communication on the Future of European Regulatory Audiovisual Policy, 2003, COM(2003) 784.

Crime Is Soaring in Cyberspace, New York Times, 27 stycznia 2003.

Cyber Liability & Higher Education, Aon Professional Risk Solutions, White Paper.

Estonian Cyber Security Strategy, MON Estonii.

Exploring Information Superiority, RAND Corporation, SANTA Monica USA, 2004.

Film Piracy, Organized Crime, and Terrorism, RAND. org.

Global Trends 2025: *A Transformed World from the Government Printing Office* (GPO Stock #041-015-00261-9; ISBN 978-0-16-081834-9).

Green Paper on convergence of the telecommunications, media and information technology sectors and the implications for regulation towards an information society approach, 1998, COM(97) 623.

Highlights of GAO-07-368, a report to F. James Sensenbrenner Jr., House of Representatives. INFORMATION SECURITY, FBI Needs to Address Weaknesses in Critical Network. April 2007.

INFORMATION WARFARE: COMBATING THE THREAT IN THE 21ST CENTURY. The Research Departament Air Command and Staff College. March 1997.

Integrator, Nr 5-6/2002.

IP/07/453 roczne sprawozdanie z realizacji inicjatywy i2010.

IT Risk Management, Trends through December 2006, Symantec.

Jak przetrwać katastrofę? Dobry plan ratunkowy, PC Kurier 3/2002.

McAfee Virtual Criminology Report : North American Study into Organized Crime and the Internet.

Measuring Stability and Security in Iraq. September 2008.

Newsweek Polska, nr 08/01/2004.

Report to Congress In accordance with the Department of Defense Appropriations Act 2008.

Rezolucja Parlamentu Europejskiego z dnia 19 lutego 2009 r. w sprawie europejskiej strategii bezpieczeństwa i europejskiej polityki bezpieczeństwa i obrony (2008/2202 (INI));

Rządowy Program Ochrony Cyberprzestrzeni RP na lata 2009-2011 (uchwalony 2009).

SERVING THE ARMY F OR 25 YEARS, Annual Report 2007. ARROYO CENTER, www.rand.org

The National Strategy to Secure Cyberspace Publisher: Morgan James Publishing (February 1, 2003).

The Physical Protection of Critical Infrastructures and Key Assets, *The Vulnerability of the Computerized Society* - Considerations and Proposals' Report by a Swedish Government Committee (ADB och samhällets sårbarhet, övervaganden och forslag, Sårbarhetskommiteé), Stockholm 1979.

Wykorzystanie technologii informacyjno-telekomunikacyjnych w przedsiębiorstwach w 2007r, GUS, Warszawa.

Yoshio Utsumi, Orędzie, Sekretarza Generalnego Międzynarodowego Związku Telekomunikacyjnego (ITU) z okazji Światowego Dnia Telekomunikacji - 17 maja 2006.

Z bankowości elektronicznej korzysta już ponad 11 milionów użytkowników, [w:] „Gazeta Prawna", 16.10.2008.

Artykuły na stronach WWW

Addressing the Nation's Cyber Security Challenges: Reducing Vulnerabilities Requires Strategic Investment and Immediate Action, Testimony of Sami Saydjari Before the House Committee on Homeland Security 25.04.2007, http://homeland.house.gov/SiteDocuments/20070425145307-82503.pdf.

Babik W., Uniwersytet Jagielloński, Kraków 2006, [w:] www.ap.krakow.pl/ptn/ref2006/Babik.pdf.

Cooperative Cyber Defence Centre of Excellence International Status, http://www.ccdcoe.org/38.html

Davis J., *Hackers Take Down the Most Wired Country in Europe*, „Wired Magazine", 15.09.2007, http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all.

Defence Policies '07 in Brief: Estonia, Latvia and Lithuania, "Baltic Security and Defense Review", vol. 10,2008, www.bdcol.ee/files/files/documents/Research/12_%20%20Defence%20Policy.pdf.

Denning D. E., *Cyberterrorism, Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services*, US House of Representatives, 23.05.2000, http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html.

Denning D. E., *Is Cyber Terrorism Coming*?, Prezentacja w Naval Postgraduate School, Center of Terrorism and Irregular Warfare, Monterey, 2.05.2002, http://handle.dtic.mil/100.2/ADA485000.

Estonian approach to Cyber Security: Estonian National Strategy on Cyber Security and Cooperative Cyber Defence Centre of Excellence, Przemówienie ministra obrony Jaaka Aaviksoo na forum OBWE, 4.07.2008, http://www.mod.gov.ee/?op=body&id=494&prn=1.

Gagnon B., *Are We Headed for a "Cyber-9/11*?: "The American Failure in Cyberstrategy", Center for United States Studies of the Raoul Dandurand Chair of Strategic and Diplomatic Studies, Occasional Paper nr 5, Quebec 2004, http://www.dandurand.uqam.ca/download/pdf/articles/cyber911.pdf.

IDS 2007, *A Forecast of Worldwide Information Growth Through* 2010 [w:] www.emc.com/about/destination/digital_universe

Internet World Stats 2008, http://www.internetworldstats.com/europa.htm#pl.

Merkel Calls on China to Respect International Rules, Serwis Internetowy Deutsche Welle z 27.08.2007, http://www.dwworld.de/dw/article/0,2144,2753209,00.html.

Mitliaga V., *Cyber-terrorism: A Call for Governmental Action*?, British and Irish Law, Education and Technology Association 16th Annual Conference, Edynburg, 9-10.04.2001, http://www.bileta.ac.uk/01papers/mitliaga.html.

Nowe NATO rodzi się w Krakowie, „Gazeta Wyborcza", 19.02.2009, http://wyborcza.pl/1,76842,6297288,Nowe_NATO_rodzi_sie_w_Krakowie.html.

Pietrzak A., *Cyberterroryzm, Niezależne Inicjatywa Naukowa Paradygmat*. [w:] http://www.paneuropa.l.pl/index.php3?id=1063721220.

Podolski A., *Europejska współpraca wywiadowcza – brakujące ogniwo europejskiej polityki zagranicznej i bezpieczeństwa*?, Centrum Stosunków Międzynarodowych. www.csm.org.pl

Polska chce walczyć z cyberterroryzmem, Gazeta.pl Gospodarka 20.12.2007, http://gospodarka.gazeta.pl/gospodarka/1,33181,4779921.html.

Rosyjscy hackerzy podbijają Estonię, „Gazeta Wyborcza", 17.05.2007, http://gospodarka.gazeta.pl/technologie/1,81010,4140556.html.

Ryan J., *"iWar": A new threat, its convenience – and our increasing vulnerability*, "NATO Review", Winter 2007, http://www.nato.int/docu/review/2007/issue4/english/analysis2.html.

Shimeall T., Williams P., Dunlevy C., *Countering New Cyber War*, "NATO Review", Winter 2001/2002, http://www.nato.int/docu/rev-pdf/eng/0104-en.pdf, s. 17-18.

The National Strategy to Secure Cyberspace Publisher: Morgan James Publishing (February 1, 2003), [online]:http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf

Wilson C., *Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues*, Congressional Report Service' Report for Congress, 20.03.2007, www.fas.org/sgp/crs/natsec/RL31787.pdf, s.8-9.

World War III. A Cyber War has begun, Raport The Technolytics Institute, September 2007, www.technolytics.com/Cyber_War_Released.pdf.

Zdanowicz Z., *Skracanie dystansu*, dostęp on line: *http://www.gazeta-it.pl/2,15,195,index.html*

Raporty

Raport CERT Polska 2007, http://www.cert.pl/PDF/Raport_CP_2007.

Raport CERT Polska, 1996, http://www.cert.pl/PDF/Raport_CP_1996.

Raport CERT Polska, 1997, http://www.cert.pl/PDF/Raport_CP_1997.

Raport CERT Polska, 1998, http://www.cert.pl/PDF/Raport_CP_1998.
Raport CERT Polska, 1999, http://www.cert.pl/PDF/Raport_CP_1999.
Raport CERT Polska, 2000, http://www.cert.pl/PDF/Raport_CP_2000.
Raport CERT Polska, 2001, http://www.cert.pl/PDF/Raport_CP_2001.
Raport CERT Polska, 2002, http://www.cert.pl/PDF/Raport_CP_2002.
Raport CERT Polska, 2003, http://www.cert.pl/PDF/Raport_CP_2003.
Raport CERT Polska, 2004, http://www.cert.pl/PDF/Raport_CP_2004.
Raport CERT Polska, 2005, http://www.cert.pl/PDF/Raport_CP_2005.
Raport CERT Polska, 2006, http://www.cert.pl/PDF/Raport_CP_2006.
Raport CERT Polska, 2008, http://www.cert.pl/PDF/Raport_CP_2008.
Raport *e-gov* w Polsce, CapGemini 2004, [w:] http://www.pl.capgemini.com/resources/news/2004/.

Strony WWW

http://centrum.bezpieczenstwa.pl/content/blogcategory/0/10/
http://ists.dartmouth.edu
http://ukie.gov.pl
http://www.afcyber.af.mil/
http://www.afit.edu/en/ccr/index.cfm
http://www.cert.org/research/taxonomy_988667.pdf
http://www.cpni.gov.uk/
http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf.
http://www.in4.pl
http://www.internetworldstats.com./
http://www.mod.gov.ee/static/sisu/files/Estonian_Cyber_Security_Strategy.pdf.
http://www.mon.gov.pl
http://www.money.pl
http://www.mswia.gov.pl/strategia/;
http://www.nato.int/docu/review/2007/issue4/polish/analysis2.html
http://www.ndu.edu/inss/research/inss_research.htm
http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/etc/faqs.html
http://www.securtystandard.pl
www.csm.org.pl.
www.mcafee.com.
www.ncirc.nato.int.
www.nitrd.gov.
http://www.foresightenergetyczny.pl/
www.wp.mil.pl/pliki/File/Wizja_SZRP_2030.pdf.
http://www.bbn.gov.pl/dokumenty/SBN_RP.pdf

Ustawy i dokumenty

Ustawa o ochronie danych (Dz.U.1997r., nr133, poz.883).
Ustawa o podpisie elektronicznym (Dz.U. 2001r., nr 130, poz.1450).
Ustawa o prawie autorskim (Dz.U. 1994r., nr 24, poz. 83).
ustawa o świadczeniu usług droga elektroniczną (Dz.U. 2002r., nr144, poz.1204).
Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym. (Dz.U. Nr 89, poz. 590).
Ustawa z dnia 26 kwietnia 2007 r o zarządzaniu kryzysowym Dz.U. Nr 89/2007 r., poz. 590.
Ustawa z dnia 29 grudnia 1992 r. o radiofonii i telewizji (Dz.U. z 1993r., nr 7, poz. 34).
Ustawa z dnia 29 listopada 1990 r. o łączności ze zmianami w 1995r. (Dz.U. 1995r., nr 117, poz.564, tekst jednolity).

Publikacje autorki związane z tematem:

1. *Teoretyczne podstawy walki informacyjnej*. Zeszyty Naukowe AON NR 1(70) 2008, współautor P. Sienkiewicz.
2. *Bezpieczeństwo informacyjne jako czynnik jakości życia.* ZN AON nr 3(68) 2008, s.135, współautor P. Sienkiewicz.
3. *Bezpieczeństwo informacyjne dla bezpieczeństwa narodowego*. ZN AON NR 3(68) 2007.
4. *Aspekty logistyczne bezpieczeństwa krytycznej infrastruktury państwa*, nr 2(67)B 2007, s. 140, współautor P. Sienkiewicz.
5. „Seria Badania systemowe" prof. dr hab. inż. Jakub Gutenbaum (red.), IBS PAN, Warszawa 2008, ISBN 83-894-7520-0 EAN 9788389475206.
    1. *Modele ewaluacji jakości życia w badaniach systemowych* i tom 64/2008, s. 343-351, współautor P. Sienkiewicz.
    2. *Zagrożenia dla bezpieczeństwa logistycznego imprez masowych*, współautorzy: P. Sienkiewicz, P. Górski, M. Pelc.
    3. *Zagrożenia informacyjne bezpieczeństwa narodowego.*
4. *Diagnoza i perspektywa rozwoju systemu łączności w RP w aspekcie zapewnienia potrzeb obronnych.* [w:] *Diagnoza i perspektywy rozwoju infrastruktury technicznej RP z punktu widzenia obronnego* (pod red.) J. Płaczek, 12(2) w tym s.185-218, S 7276, współautor: P. Sienkiewicz, AON, Warszawa 2008.
5. *Standardy normalizacyjne oraz akty prawne w zakresie bezpieczeństwa systemów informatycznych.* [w:] *„Interoperacyjność i wymagania standaryzacyjne NATO"* pod red. B. Zdrodowskiego, 16(1) w tym s.91-133, S/7274, współautor: P. Sienkiewicz, AON, Warszawa 2008.
6. *Metodologia badań nad bezpieczeństwem* [w:] *Wybrane metody naukowych badań nad bezpieczeństwem i obronnością. Studium metodologiczne*, pod red. P. Sienkiewicz, 10(2), S/7229, współautor P. Sienkiewicz, AON, Warszawa 2008.
7. *Metody scenariuszowe* [w:] *Wybrane metody naukowych badań nad bezpieczeństwem i obronnością. Studium metodologiczne*, pod red. P. Sienkiewicz, 10(2), S/7229, AON, Warszawa 2008.
8. *Technologiczne determinanty jakości życia w społeczeństwie informacyjnym*, [w:] *Fenomen Internetu* pod red. A. Szewczyk, E. Krok, 25(1), s.41-49. ISBN 83-60637-23-7; 978-83-60637-23-4, Uniwersytet Szczeciński.
9. *Analiza systemowa jakości życia w warunkach „nowej gospodarki"* [w:] *Przemiany społeczno-ekonomiczne a przedsiębiorczość i innowacyjność przedsiębiorstw w warunkach nowej gospodarki*, (red.) Z. Stachowiak, 16(1), s.15-30 ISBN 83-925315-4-8, Siedlce 2008.
10. *Analiza systemowa polityki bezpieczeństwa wewnętrznego Chińskiej Republiki Ludowej. Uwarunkowania gospodarcze.* [w:] *Ewolucja polityki bezpieczeństwa ChRL* [Chińskiej Republiki Ludowej]: scenariusze zmian i ewaluacja skutków, kier. J. Buczyński, 10(3), S/7312, AON, Warszawa 2008.
11. *Wystarczalność obronna państwa w ujęciu analizy systemowej* [w:] *Zarys ekonomiki bezpieczeństwa.* Współautor P. Sienkiewicz, red. prof. dr hab. Janusz płaczek (w druku) AON, Warszawa 2009.
12. *Prognozowanie zagrożeń dla bezpieczeństwa informacyjnego* [w:] *Współczesny wymiar terroryzmu przeciwdziałanie zjawisku.* AON, Warszawa 2008.
13. *Jakość życia w społeczeństwie informacyjnym*, s.189-207, [w:] Księga Jubileuszowa prof. L.Zachera pt. *Ku przyszłości.* Współautor P. Sienkiewicz ISBN 978-83-60807-93-4 ISBN 978-83-89437-82-2, Wydawnictwa Akademickie i Profesjonalne, Waliz, Warszawa 2008.
14. *Edukacyjne determinanty rozwoju społeczeństwa informacyjnego.* [*ZESZYT NAUKOWY NR 2.* WWSI, Warszawa, 2007], str. 137-161, współautor: Piotr Sienkiewicz

INNE FORMY UPOWSZECHNIENIA WYNIKÓW

2008 rok

X Międzynarodowa Konferencja Naukowa, Badania i Operacyjne i systemowe. nt. Badania i Operacyjne i systemowe BOS'2008. IBS PAN współorganizator AON, Warszawa, wrzesień 2008.

Konferencja AON nt. Kierowanie bezpieczeństwem narodowym, referat nt. *Zarządzanie bezpieczeństwem w organizacji.*

Konferencja Jubileuszowa prof. Zachera, wygłoszenie referatu nt. *Zagrożenia dla demokracji w wizjach społeczeństwa informacyjnego.* (współautor P. Sienkiewicz) WSPiZ Koźmińskiego.

Konferencja Międzynarodowa nt Sieci teleinformatyczne jako instrument państwa – walka informacyjna i szpiegostwo elektroniczne. PISM, Warszawa 2008.

Seminarium nt. Świadczenie na rzecz obrony, referat pt. *Realizacja świadczeń na rzecz obrony przez przedsiębiorstwa infrastruktury krytycznej – wybrane elementy*, AON, 2007.

Międzynarodowa konferencja naukowa nt. Bezpieczeństwo wymiar współczesny oraz perspektywy badań, Krakowska Szkoła Wyższa im. Andrzeja Modrzewskiego, referat pt. *Perspektywy badań systemowych nad bezpieczeństwem.* Kraków, październik 2008.

Uniwersytet Rzeszowski, referat nt. *Technologie informacyjne a jakość życia w społeczeństwie informacyjnym.* Artykuł pod tym samym tytułem publikacja, wrzesień 2008.

Międzynarodowa konferencja naukowo-szkoleniowa: Terrorism and Security of Mass Events, organizator Wojskowy Instytut Medyczny, Waplewo, listopad 2008 referat (współautor P. Sienkiewicz) nt.

1. *Metodhods of the anlysis of the risk of terrorist threats and*
2. *Cyberterrorism as a threat to the security of mass events.*

2009 rok

Konferencja Naukowa, Służby mundurowe w systemie bezpieczeństwa EURO 2012, Sieradz 2009, wygłoszony referat nt Aspekty systemowe zarządzania bezpieczeństwem.

Konferencja naukowa nt. Ryzyko w zarządzaniu kryzysowym. AON, Warszawa, referat: Ryzyko zagrożeń informacyjnych dla bezpieczeństwa narodowego. AON, Warszawa 2009.

Konferencja naukowa, Cyberterroryzm nowe wyzwania XXI wieku. Warszawa 2009.

Konferencja naukowa nt. EUROPA - INTEGRACJA, POLITYKA, BEZPIECZEŃSTWO. Referat :

Bezpieczeństwo europejskiej przestrzeni cybernetycznej. AMW, Gdynia 2009.

Konferencja naukowa, nt. Rynki przesyłu i przetwarzania informacji – stan obecny i perspektywy rozwoju. Referat: Analiza systemowa rozwoju społeczeństwa informacyjnego: wizje i scenariusze, szanse i zagrożenia. USz, Szczecin 2009.

Spis tabel

Rozdział 1

Tabela 1-1. Różnice między ujęciem systemowym a ujęciem tradycyjnym 26
Tabela 1-2. Etapy realizacji badań 31

Rozdział 2

Tabela 2-1. Zagrożenia dla bezpieczeństwa 36
Tabela 2-2. Profile napastników w cyberprzestrzeni 42
Tabela 2-3. Kryteria klasyfikacji zagrożeń 43
Tabela 2-4. Klasyczna klasyfikacja zagrożeń 44
Tabela 2-5. Podział zagrożeń wg kryterium pochodzenia i losowości 45
Tabela 2-6. Macierz współzależności sektorów infrastruktury krytycznej państwa 53
Tabela 2-7. Typologia destrukcyjnych działań na obiekty informacyjne 58
Tabela 2-8. Klasyfikacja sprawców i ich działań 58
Tabela 2-9. Przykłady ataków uznanych za cyberterrorystyczne 60
Tabela 2-10. Oczekiwane skutki walki informacyjnej 64
Tabela 2-11. Inicjatywy UE w zakresie bezpieczeństwa informacyjnego 70
Tabela 2-12. Zagrożenia społeczeństwa w różnych obszarach działalności 76
Tabela 2-13. Choroby informacyjne 78
Tabela 2-14. Istota bezpieczeństwa narodowego i informacyjnego 82

Rozdział 3

Tabela 3-1. Ogólna liczba incydentów w latach 1966-2008 104
Tabela 3-2. Wartości błędów dla okresu kontrolnego przy α=0,1 107
Tabela 3-3. Zestawienie błędów dla okresu kontrolnego i wyznaczone prognozy 109
Tabela 3-4. Zestawienie wyników prognoz oraz ich błędów ex post dla zagrożenia „ogólna liczba incydentów" 110
Tabela 3-5. Dane zarejestrowane CERT Spam 111
Tabela 3-6. Zestawienie zbiorcze wyników błędów dla podzbioru kontrolnego, prognoz i ich błędów dla zagrożenia „wielkość zarejestrowanego spamu" 111
Tabela 3-7. Porównanie metod prognozowania dla zarejestrowanych wielkości spamu 113
Tabela 3-8. Wartości zarejestrowane zagrożenia „robak sieciowy" przez CERT na przestrzeni lat 1993-2008 114
Tabela 3-9. Błędy dla okresu kontrolnego i dla prognoz wygasłych dla zagrożenia „robak sieciowy" 116
Tabela 3-10. Wartości błędów dla okresu kontrolnego dla zagrożenia „robak sieciowy" przy α=0,9 i β=0,15 (Holt) 116
Tabela 3-11. Porównanie metod prognozowania dla „robaka sieciowego" 118
Tabela 3-12. Zestawiane danych, stałych wygładzania, prognoz i ich błędów dla zagrożenia „zarejestrowane ataki dobowe" 119
Tabela 3-13. Zestawienie danych dla zagrożenia „unikalne skanowania", analiz oraz prognoz 120
Tabela 3-14. Szereg czasowy zagrożenia „zarejestrowane alarmy w 2008 roku" 121
Tabela 3-15. Prognozy oraz błędy wyznaczone z wykorzystaniem modeli średniej ruchomej 122
Tabela 3-16. Wyznaczone prognozy według modelu Browna przy różnych stałych wygładzania dla zagrożenia „zarejestrowane alarmy w 2008 roku" 122
Tabela 3-17. Zestawienie dla zagrożenia „symulowane dane" 123
Tabela 3-18. Zbiorcze zestawienie wyników analiz dla zagrożenia „symulowane dane" 125
Tabela 3-19. Zestawienie analiz dla zagrożenia „symulowane dane 2" 126
Tabela 3-20. Raport wstępnego przetworzenia danych (robaki sieciowe) 131
Tabela 3-21. Wyniki analizy poprawności danych oraz wstępnego przetworzenia (robaki sieciowe) ... 132
Tabela 3-22. Raport uczenia sieci dla zagrożenia „robaki sieciowe" 133
Tabela 3-23. Zestawienie błędów uczonej sieci robaki sieciowe 133
Tabela 3-24. Raport statystyk dla zagrożeń: „robak sieciowy", koń trojański, „spam" 135
Tabela 3-25. Zestawienie prognoz dla zagrożeń: „spam", robaki sieciowe", „koń trojański" 137

Tabela 3-26. Zalety i wady sieci neuronowych 137
Tabela 3-27. Kryteria oceny w postrzeganiu ryzyka 139
Tabela 3-28. Analiza systemowa determinant niepewności i ryzyka 140
Tabela 3-29. Charakterystyka próby 145
Tabela 3-30. Zagrożenia bezpieczeństwa narodowego w obszarze informacyjnym 148
Tabela 3-31. Osobiste niepokoje - procentowy rozkład odpowiedzi 148
Tabela 3-32. Modalna 151
Tabela 3-33. Modalna dla social engineering 155
Tabela 3-34. Wyznaczanie prawdopodobieństwa w oparciu o częstość występowania zagrożenia 156
Tabela 3-35. Miejsce Polski w rankingu zagrożeń 157
Tabela 3-36. Postawy wobec przyszłości w technice pisania scenariuszy 158
Tabela 3-37. Kombinacje scenariuszy 160
Tabela 3-38. Typologia scenariuszy 160
Tabela 3-39. Charakterystyka scenariuszy 161
Tabela 3-40. Etapy konstruowania scenariusza 162
Tabela 3-41. Typologia ataków 164
Tabela 3-42. Syntetyczny scenariusz II 169
Tabela 3-43. Zagrożenia dla KIP 171
Tabela 3-44. Scenariusz IV 172
Tabela 3-45. Przykładowy ogólny scenariusz zagrożeń na szczeblu państwa 174
Tabela 3-46. Scenariusz możliwych prawdopodobnych zagrożeń dla dziadziny telekomunikacji 175
Tabela 3-47. Scenariusz możliwych i prawdopodobnych zagrożeń dla energetyki 176
Tabela 3-48. Scenariusze dla systemów na różnych stopniach zarządzania administracyjnego przewidzianych dla dziedziny transportu 176
Tabela 3-49. Scenariusz dla dziedziny komunikacji z podaniem podatności wg. Skali 1-6 178
Tabela 3-50. Scenariusz z wyróżnieniem form ataku dla infrastruktury komunikacyjnej 180
Tabela 3-51. Scenariusz z podaniem form ataku dla obszaru administracji 181
Tabela 3-52. Zestawienie rang dla scenariuszy 183
Tabela 3-53. Delficka metoda analizy ryzyka 185
Tabela 3-54. Zbiorcze zestawienie charakterystyki modeli prognostycznych 192

Rozdział 4

Tabela 4-1. Identyfikacja obszarów ryzyka oraz możliwych zagrożeń 200
Tabela 4-2. Opis zidentyfikowanego ryzyka 200
Tabela 4-3. Macierz predefiniowanych wartości zasobów 201
Tabela 4-4. Metoda porządkowania zagrożeń 202
Tabela 4-5. Metoda wyznania częstości zagrożeń 202
Tabela 4-6. Metoda wyznaczania szacunkowej wielkości potencjalnych strat 202
Tabela 4-7. Mapa ryzyka 203
Tabela 4-8. Ocena prawdopodobieństwa wystąpienia ryzyka 203
Tabela 4-9. Przykładowa ocena skutków wystąpienia ryzyka 204
Tabela 4-10. Szacowanie poziomu ryzyka 204
Tabela 4-11. Procedura probabilistycznej analizy ryzyka zagrożeń informacyjnych dla bezpieczeństwa organizacji/instytucji 205
Tabela 4-12. Określenie głównych konsekwencji zagrożeń dla informacyjnego bezpieczeństwa organizacji (instytucji) 205
Tabela 4-13. Rangowanie ryzyka 205
Tabela 4-14. Czas, koszt, zakres działania 205
Tabela 4-15. Przykład kategorii prawdopodobieństwa i szkód dla cyberataków 206
Tabela 4-16. Przykład analizy 206
Tabela 4-17. Wyznaczenie macierzy poziomu ryzyka 207
Tabela 4-18. Podział ról i odpowiedzialności w procesie zabezpieczania cyberprzestrzeni 210
Tabela 4-19. Wpływ zagrożeń informacyjnych na stabilność funkcjonowania pastwa 220

Spis rysunków

Rozdział 1

Rysunek 1-1. Zakres badań nad bezpieczeństwem w ramach europejskiego programu badań nad bezpieczeństwem realizowanych przez Polską Platformę Bezpieczeństwa Wewnętrznego 13
Rysunek 1-2. Przestrzeń zagrożeń militarnych w społeczeństwie informacyjnym 14
Rysunek 1-3. Przestrzeń zagrożeń bezpieczeństwa narodowego w społeczeństwie informacyjnym 14
Rysunek 1-4. Ogólny model przedmiotu (obiektu) badań i jego konkretyzacja 19
Rysunek 1-5. Metody badań nad bezpieczeństwem (konfliktami, zagrożeniami) politycznym 27
Rysunek 1-6. Analiza systemowa sytuacji problemowej 29
Rysunek 1-7. Ogólny model procesu badań naukowych 30
Rysunek 1-8. Ogólny model procesu badań naukowych nad bezpieczeństwem informacyjnym RP..... 30
Rysunek 1-9. Typologia metod i technik badań naukowych 32

Rozdział 2

Rysunek 2-1. Rozwój technologii informacyjnych (informatycznych) 38
Rysunek 2-2. Technologie informacyjne i ich wpływ na koncepcje walki informacyjnej w XX wieku ... 39
Rysunek 2-3. Ogólna typologia zagrożeń bezpieczeństwa systemów informacyjnych 41
Rysunek 2-4. Klasyfikacja ze względu na przyczyny zagrożeń 44
Rysunek 2-5. Zagrożenia systemów informacyjnych 46
Rysunek 2-6. Taksonomia zagrożeń: podstawowe grupy złośliwego oprogramowania oraz ich wzajemne powiązania 47
Rysunek 2-7. Istota zagrożeń informacyjnych 49
Rysunek 2-8. Obszary informacyjnie wrażliwe, newralgiczne w systemie bezpieczeństwa państwa 50
Rysunek 2-9. Strefy współzależności systemów informatycznych i teleinformatycznych 52
Rysunek 2-10. Hierarchia zagrożeń informacyjnych i ich skutków 55
Rysunek 2-11. Model „cyberataku" na obiekty teleinformatyczne 56
Rysunek 2-12. Konceptualizacja NCW 67
Rysunek 2-13. Multidyscyplinarny aspekt badań nad bezpieczeństwem 69
Rysunek 2-14. Obszary personalnego bezpieczeństwa informacyjnego 73
Rysunek 2-15. Obszary zagrożeń bezpieczeństwa obywateli 75
Rysunek 2-16. Interakcje między potrzebami społecznymi a techniką 79
Rysunek 2-17. Poziomy bezpieczeństwa wpływające na jakość życia 79
Rysunek 2-18. Procentowy rozkład odpowiedzi 80
Rysunek 2-19. Obszary bezpieczeństwa informacyjnego 84
Rysunek 2-20. Zagrożenia informacyjne w kontekście KIP 85

Rozdział 3

Rysunek 3-1. Predykcja, prognozy i scenariusze 93
Rysunek 3-2. Proces wyznaczania prognozy 98
Rysunek 3-3. Proces prognozowania 100
Rysunek 3-4. Liczba incydentów w latach 1996-2008 104
Rysunek 3-5. Dane rzeczywiste teoretyczne i prognoza przy k=2 dla zagrożenia „ogólna liczba incydentów" 105
Rysunek 3-6. Dane rzeczywiste, teoretyczne i prognoza przy k=3 dla zagrożenia „ogólna liczba incydentów" 105
Rysunek 3-7. Prognoza z zastosowaniem modelu prostego wygładzania wykładniczego przy α=0,1 dla zagrożenia „ogólna liczba incydentów" 106

Rysunek 3-8. Rzeczywiste realizacje oraz wartości teoretyczne i prognozy przy różnych stałych wygładzania dla zagrożenia „ogólna liczba incydentów" 107
Rysunek 3-9. Wartości empiryczne, wartości teoretyczne oraz prognoza przyrostu liczby incydentów... 109
Rysunek 3-10. Wielkość zarejestrowanego spamu w latach 1993-2008 111
Rysunek 3-11. Opis trendu za pomocą wielomianu kwadratowego zagrożenia „wielkość zarejestrowanego spamu" 111
Rysunek 3-12. Prognoza przy empirycznie wyznaczonych alfa i beta dla zagrożenia „wielkość zarejestrowanego spamu" 112
Rysunek 3-13. Wartości bieżące dla zagrożenia „wielkość zarejestrowanego spamu" oraz prognoza dla k=2 i k=3 112
Rysunek 3-14. Wartości rzeczywiste oraz prognozowane dla zagrożenia „wielkość zarejestrowanego spamu" przy różnych wielkościach alfa 113
Rysunek 3-15. Zarejestrowane incydenty „robak sieciowy" 114
Rysunek 3-16. Wartość bieżąca i prognozowana dla zagrożenia „robak sieciowy", przy k=2 114
Rysunek 3-17. Wartość prognozy dla zagrożenia „robak sieciowy" przy k=3 115
Rysunek 3-18. Wartość prognozy dla zagrożenia „robak sieciowy" przy k=6 115
Rysunek 3-19. Szereg prognozowany przy alfa=0,9 dla zagrożenia „robak sieciowy" 116
Rysunek 3-20. Wartości historyczne, teoretyczne i prognoza dla zagrożenia „robak sieciowy" 117
Rysunek 3-21. Prognozy „robaka sieciowego" przy alfa=1 i beta=0 117
Rysunek 3-22. Wartości teoretyczne oraz prognozy dla zagrożenia „zarejestrowane ataki dobowe" 120
Rysunek 3-23. Wartości rzeczywiste, teoretyczne oraz prognoza dla zagrożenia „unikalne skanowania" . 121
Rysunek 3-24. Wykres zagrożenia „zarejestrowane alarmy w 2008 roku" 121
Rysunek 3-25. Zarejestrowane dane z 2008 roku oraz wygładzone stałą wygładzania k=2 i k=3 122
Rysunek 3-26. Prognozowanie z wykorzystaniem modelu Browna przy różnych wielkościach alfa dla zagrożenia dla zagrożenia „zarejestrowane alarmy w 2008 roku" 123
Rysunek 3-27. Zagrożenia „symulowane dane" jako rzeczywiste dane o występowaniu incydentów 124
Rysunek 3-28. Wyznaczone wartości teoretyczne i prognoza dla zagrożenia „symulowane dane" 124
Rysunek 3-29. Wartości szeregu czasowego zagrożenia „symulowane dane 2" 125
Rysunek 3-30. Wartości rzeczywiste jako zarejestrowane dla zagrożenia „symulowane dane 2" i teoretyczne oraz prognoza 125
Rysunek 3-31. Porównanie schematu biologicznego neuronu z siecią neuronową 127
Rysunek 3-32. Schemat procesu prognozowania za pomocą sztucznej sieci neuronowej 129
Rysunek 3-33. Menu programu Forecaster XL 130
Rysunek 3-34. Menu programu tworzenie sieci 131
Rysunek 3-35. Menu programu, trenowanie sieci 131
Rysunek 3-36. Wykres średniego błędu kwadratowego trenowanej sieci robaki sieciowe (Training Error Graph) 133
Rysunek 3-37. Klasyczna hierarchia potrzeb według Maslowa 141
Rysunek 3-38. Schemat procesu badawczego 142
Rysunek 3-39. Procentowy rozkład odpowiedzi wydatki na bezpieczeństwo 149
Rysunek 3-40. Procentowa analiza odpowiedzi o wyrażenie zgody na ograniczenia 149
Rysunek 3-41. Analiza procentowa odpowiedzi o instytucje, które najbardziej narażone są na ataki 150
Rysunek 3-42. Rozkład procentowy postrzeganie zagrożeń informatycznych cz. 1 151
Rysunek 3-43. Rozkład zagrożeń informatycznych cz. II 152
Rysunek 3-44. Rozkład zagrożeń informatycznych cz. III 153
Rysunek 3-45. Rozkład zagrożeń informatycznych cz. IV 154
Rysunek 3-46. Rozkład zagrożeń informatycznych cz. V 155

Rysunek 3-47. Scenariusze rozwoju otoczenia 162
Rysunek 3-48. Lejek scenariusza 162
Rysunek 3-49. Mapa Warszawy 172
Rysunek 3-50. Mapa okolicy Stadionu Narodowego 172
Rysunek 3-51. Hipotetyczny scenariusz ataku na łącze sieci telekomunikacyjnej 173
Rysunek 3-52. Proces gromadzenia oraz analizy danych o zagrożeniach informacyjnych za pomocą techniki delfickiej 187

Rozdział 4

Rysunek 4-1. Równowaga między zagrożeniami a zabezpieczeniami 194
Rysunek 4-2. Model oceny ryzyka w sytuacjach kryzysowych 195
Rysunek 4-3. Prawdopodobieństwo jako funkcja niepowodzeń i wielkości straty 196
Rysunek 4-4. Podstawowe elementy procesu zarządzania ryzykiem 197
Rysunek 4-5. Zależności między elementami bezpieczeństwa i zagrożeń w kontekście zarządzania ryzykiem 199
Rysunek 4-6. Zależności między elementami bezpieczeństwa i zagrożeń w kontekście zarządzania ryzykiem..... 207
Rysunek 4-7. Płaszczyzny bezpieczeństwa informacyjnego..... 209
Rysunek 4-8. Proces projektowania systemu bezpieczeństwa 211
Rysunek 4-9. System zarządzania bezpieczeństwem RP 212
Rysunek 4-10. Struktura systemu monitorowania zagrożeń bezpieczeństwa informacyjnego RP 213
Rysunek 4-11. System prognozowania zagrożeń 213
Rysunek 4-12. Schemat identyfikacji zasobów systemu informacyjnego 214
Rysunek 4-13. Makroalgorytm identyfikacji sytuacji zagrożeń , ... 215
Rysunek 4-14. Model analizy prognostycznej bezpieczeństwa informacyjnego 215
Rysunek 4-15. Model procesu zarządzania bezpieczeństwem informacyjnym (z wykorzystaniem metody wielowymiarowej ryzyka zagrożeń informacyjnych 216
Rysunek 4-16. Schemat polityki bezpieczeństwa informacyjnego 217

Streszczenie

Słowa kluczowe: bezpieczeństwo, zagrożenia informacyjne, analiza systemowa, zarządzanie bezpieczeństwem informacyjny, model, ryzyko,

Praca poświęcona jest aktualnej problematyce bezpieczeństwa informacyjnego oraz jego wpływowi na bezpieczeństwo narodowe. W rozdziale metodologicznym zaprezentowano proces badań oparty na analizie systemowej jako metametodzie. Pierwsza część rozprawy ma charakter opisowy i poświęcona jest współczesnym zagrożeniom informacyjnym: ich istocie, źródłom i przyczynom. Dokonano analizy identyfikacyjnej podstawowych źródeł zagrożeń informacyjnych, ich: rodzaj (typ), częstość, przewidywane skutki dla wybranych obiektów krytycznej infrastruktury państwa (KIP) – o istotnym znaczeniu dla bezpieczeństwa narodowego. Obiekty zagrożeń opisano za pomocą takich charakterystyk, jak: podatność (wrażliwość) na zagrożenia, wartość, straty (potencjalne, dopuszczalne, graniczne). Szczególną uwagę poświęcono zagrożeniom cyberterrorystycznym, ze względu na specyficzny charakter (wagę) jako elementu kształtującego oblicze współczesnego terroryzmu.

Analiza identyfikacyjna zagrożeń pozwoliła na przyjęcie ogólnej metodyki ewaluacji (analizy i oceny) ryzyka zagrożeń informacyjnych dla bezpieczeństwa narodowego uwzględniający dwa podstawowe aspekty:

a) ilościowy: ryzyko jako funkcja intensywności zagrożeń, podatności na zagrożenia, oczekiwanych skutków dla obiektu;

b) jakościowy: ryzyko jako funkcja ryzyka obliczeniowego i społecznego wzburzenia, przy czym jako „społeczne wzburzenie" określono uogólniony wskaźnik społecznej percepcji zagrożeń informacyjnych (ryzyka informacyjnego).

W części eksperymentalnej zawarto wyniki z przeprowadzonych badań nad wykorzystaniem metod ilościowych i jakościowych w prognozowaniu zagrożeń informacyjnych. Opracowano ogólną metodykę prognozowania zagrożeń informacyjnych wykorzystującą doświadczenia w dziedzinie technik heurystycznych (scenariusze, „burza mózgów", Delphi), a także możliwości zastosowania sztucznych sieci neuronowych oraz symulacji komputerowej. Zakładając istnienie bazy danych empirycznych (źródło: zasoby Internetu oraz CERT) określono szeregi czasowe, co pozwoliło na zastosowanie standardowych technik analitycznych (np. metody wygładzania Holta, Wintersa). Prognozowanie zagrożenia w postaci szeregów czasowych, oparto na założeniu o probabilistycznym charakterze rozpatrywanych zjawisk, czyli założono występowanie czynników losowych (o znanym lub nie rozkładzie prawdopodobieństwa). Metody jakościowe (sondaż, scenariusze) zastosowano dla wyrażenia ogólnego wskaźnika społecznej percepcji zagrożeń informacyjnych oraz dla sytuacji trudnych typu incydentalnego do prognozowania.

Zaproponowano model zarządzania bezpieczeństwem informacyjnym wykorzystując następujące założenia:

a) metodyka ewaluacji ryzyka stanowi podstawę dla konstruowania procedur analityczno-ocenowych w systemie zarządzania ryzykiem;

b) metodyka identyfikacji zagrożeń stanowi podstawę dla opracowania metodyki prognozowania zagrożeń, której przeznaczeniem jest wspomaganie procedur decyzyjnych w systemie zarządzania bezpieczeństwem informacyjnym.

System zarządzania bezpieczeństwem informacyjnym traktowany jest jako jeden z istotnych podsystemów systemu zarządzania bezpieczeństwem państwa (krytycznej infrastruktury państwa). Opracowano w rozprawie ogólne modele tych systemów, które są wyrazem przyjętej w rozprawie metodologii badań nad zagrożeniami informacyjnymi dla bezpieczeństwa narodowego. Ze względu na złożony, niepewny i dynamiczny charakter badanych zjawisk wykorzystano ogólne zasady metodyki badań systemowych, a w szczególności posłużono się analizą systemową.

INFORMATION THREATS OF NATIONAL SECURITY OF REPUBLIC POLAND

Summary

keywords: *security, information threats, systemic analysis, managing information security, model, risk;*

This dissertation is devoted to the current information security problems and influence they impose on the national security. The overall research process which is based on the comprehensive analysis as the metamethod is presented in the methodological chapter.

The first part of the dissertation has a descriptive character and is devoted to the description of contemporary information threats, their essence, sources and causes. This is where the identification analysis of basic sources of the information threats - their kinds, frequency, predicted effects on the chosen objects of the critical infrastructure - was pursued. The objects vulnerable to threats are characterized with the such indicators as: susceptibility (sensitivity) to threats, value, losses (potential, acceptable, border). Special attention was given to the cyberterrorist threats because of their exceptional character (weight) as the element shaping the face of contemporary terrorism.

The identification analysis allowed for assuming the general evaluation methodology (analysis and estimation) of the information threats to the national security risk which considers two basic aspects:

a) quantitative: risk as the threat intensification function, susceptibility to threats, expected effects to the objects;

b) qualitative: risk as a function of the analytical risk and the social ferment, where the social ferment is considered as the generalized indicator of the social perception to the information threats (information risk).

The experimental part of the dissertation comprises of the results from the conducted research on using the quantitative and qualitative methods for forecasting the information threats.

The general information threats forecasting methodology that has been hereby elaborated, built on experience from the heuristic techniques (scenarios, brainstorming, Delphi) as well as the capability of using artificial neuron networks and computer simulation. Assuming the existence of the empirical data base (sources, internet, CERT) the detailed time series were defined what allowed for using standard analytical techniques (e.g. Holt's Linear Exponential Smoothing, Winters method). Threat forecasting in the form of time series was based on the assumption concerning the probabale character of the considered occurrences, thus the existence of random factors was assumed (of known or not probability expansion). Qualitative methods (sounding, scenarios) were imposed on expressing the general indicator of the social perception to the information threats and to the complex situations of the incidental type.

The information security management model was proposed while using the following assumptions:

a) risk evaluation methodology constitutes a basis for construction of the analytical-evaluating procedures which work in the risk management system;
b) threats identification methodology constitutes a basis for construction of the threats forecasting methodology the destiny of which is to support the decision procedures in the information security management system.

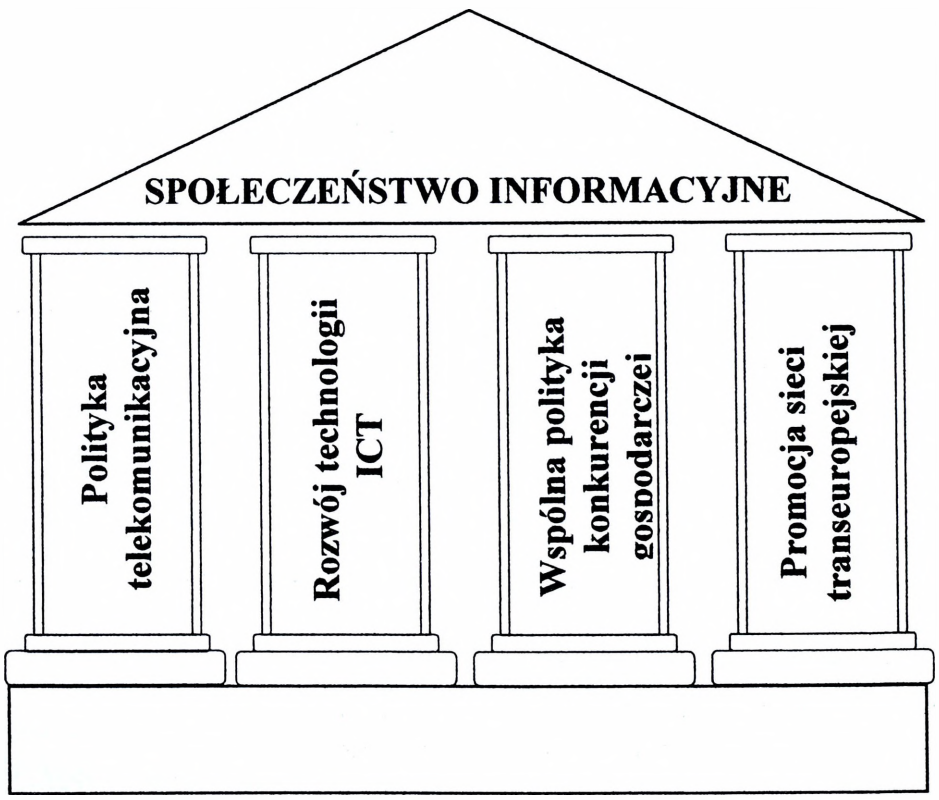
The information security management system is treated as one of the crucial subsystems of the state security management system (national critical infrastructure). In this dissertation the general models of such systems have been elaborated and they are the expression of the methodology concerning research of information threats to the national security. Due to the fact that the phenomena examined are characterized with high level of complexity, uncertainty and dynamics, the general comprehensive research methodology was utilized, with special regard to the comprehensive analysis.

Tabela ZI-1. Programy UE wspierające budowę społeczeństwa informacyjnego

Rok			Programy/zalecenia/cele	
Programy badawczo-rozwojowe w zakresie technologii ICT	1984	Programy badawczo-rozwojowe	ESPRIT	Stymulacja rozwoju technologii informacyjnych
	1986	Programy telematyczne	DRIVE - transport AIM - zdrowie DELTA – zdalne szkolenie RACE – zaawansowane technologie komunikacyjne	
	Spójna polityka budowy społeczeństwa informacyjnego			
	1993	Biała Księga Komisji: *Wzrost konkurencyjności i zatrudnienie: wyzwania i kierunki wejścia w XXI wiek*	Problematyka białej księgi koncentrowała się przede wszystkim na kwestiach ekonomicznych i konieczności liberalizacji gospodarki europejskiej, w tym sektorów informacyjnych	
	1994	Raport Bangemanna Zaprezentowany na Szczycie Europy na wyspie Korfu	– masowe udostępnienie użytkownikom sieci cyfrowych, mobilnych oraz szerokopasmowych, – rozpowszechnienie podstawowych usług typu poczty elektronicznej i transferu plików w sieci Internet, – wprowadzenie wybranych aplikacji, charakteryzujących się funkcjami demonstracyjnymi ułatwiającymi ich szeroką popularyzację.	
	1994	4 Program Ramowy badań i rozwoju na lata 1994-1998	Inkorporacja programów z lat 80-tych	
		Komunikat Komisji: *Droga do Europy ku społeczeństwu informacyjnemu. Plan działania*		
	1995	Powołanie *Information Society Form*		
	1996	Komunikat Komisji UE: *Społeczeństwo informacyjne od Korfu do Dublina – nowo wyłaniające się priorytety*		
	1997	Budowa europejskiego społeczeństwa informacyjnego dla wszystkich		
		Zielona Księga: *Konwergencja telekomunikacji, mediów i technologii informacyjnych*		
	1998	Nowy cykl programów badań i rozwoju	5 Program Ramowy na lata 1998-2002	
	1999	Zielona Księga: *Publiczny sektor informacji: kluczowy zasób Europy* e-Europa społeczeństwo		

	informacyjne dla wszystkich		
2000	Strategia lizbońska e-Europa. Plan działania	– tańszy, szybszy i bezpieczny Internet; – inwestycje w ludzi i umiejętności; – stymulacja użytkowania Internetu.	
2002	e-Europa 2002	– działania zapewniające powszechność szerokopasmowego dostępu i bezpiecznej infrastruktury informatycznej, usługi, aplikacje i zawartością obejmujące sieciowe usługi publiczne i „e-biznes".	6 program ramowy badań i rozwoju technologicznego
2003	e-Europa 2005	– dzielenie się wiedzą podczas realizacji projektów, tzw. dobra praktyka Technologia szerokopasmowa, Bezpieczeństwo, e-Rząd, e-Zdrowie, e-Nauka, e-Biznes	
2005	Plan Działań i2010	– transformacja krajów Unii Europejskiej w silne i konkurencyjne społeczeństwa oparte na wiedzy	

Źródło: opracowanie własne

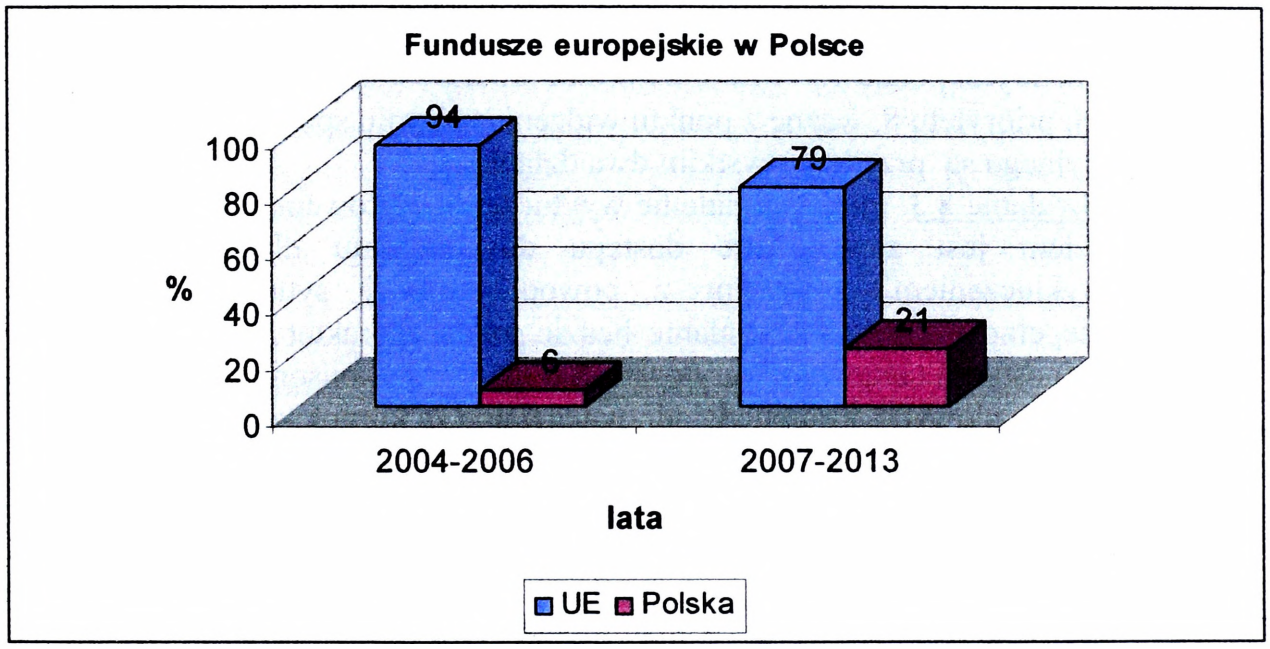


Rysunek ZI-1. Filary społeczeństwa informacyjnego
Źródło: Information Society Policy – An Overview and History.European Commission, Brussels 2001.

Od 1994 roku Polska jest członkiem Unii Europejskiej, na mocy traktatu akcesyjnego podpisanego 16 kwietnia 1993 roku. Zdecydowany wzrost przyznawanych funduszy nastąpił w latach 2004-2006 (400 %) (tabela i rys). Zmianie uległa również struktura budżetu. Wydatki na programy społeczeństwo informacyjne w latach 2007-13 będzie stanowiły 2 500 mln Euro co daje ok. 7,91 % budżetu.

Tabela ZI-2. Wielkość budżetów przyznawanych dla Polski

Budżet w latach 2004-2006	Budżet w latach 2007-2013
Europejska 2004-2006 -213,0 mld euro Polska 2004-2006 – 12,8 mld euro	ok. 67,3 mld euro będzie pochodziło z budżetu UE, ok.11,86 mld euro z krajowych środków publicznych ok. 6,4 mld euro zostanie zaangażowanych ze strony podmiotów prywatnych.



Rysunek ZI-2 Fundusze europejskie dostępne w Polsce
Źródło: opracowanie własne na podstawie: www.eficom.pl

Perspektywa finansowa 2007-2013 – szansa na rozwój społeczeństwa informacyjnego

Projekty związane z szeroko pojętym rozwojem społeczeństwa informacyjnego finansowane są w ramach:

- Programu Operacyjnego Innowacyjna Gospodarka.
- Szesnastu Regionalnych Programów Operacyjnych.
- Programu Operacyjnego Rozwój Polski Wschodniej.

Z środków korzystają między innymi. administracja centralna i lokalna, szkolnictwo, służba zdrowia, służby mundurowe i przedsiębiorstwa dofinansowując np.:

Program Operacyjny Innowacyjna Gospodarka a rozwój społeczeństwa informacyjnego

Program Operacyjny Innowacyjna Gospodarka (PO IG) ma na celu rozwój polskiej gospodarki w oparciu o innowacyjne przedsiębiorstwa poprzez wspieranie szeroko rozumianej innowacyjności i projektów o dużym znaczeniu dla gospodarki. Jednym z celów POIG jest także wzrost wykorzystania technologii informacyjnych i komunikacyjnych w gospodarce. Realizację tego celu przewiduje się przede wszystkim poprzez wdrożenie dwóch priorytetów:

- **Priorytet 7**. „Społeczeństwo informacyjne – budowa elektronicznej administracji", którego alokacja: 788 milionów Euro, dystrybuowana będzie wyłącznie poprzez tzw. projekty kluczowe. Są to projekty strategiczne dla polskiej gospodarki, których wdrożenie bez środków unijnych z pewnością byłoby utrudnione. Do takich projektów należą m.in. Polska ID karta: pl.ID i e-PUAP2 (oba projekty Ministerstwa Spraw Wewnętrznych i Administracji), czy projekt Informatyzacji wydziałów ksiąg wieczystych (projekt Ministerstwa Sprawiedliwości.
- **Priorytet 8.** „Społeczeństwo informacyjne – zwiększanie innowacyjności gospodarki", którego celem jest stymulowanie rozwoju gospodarki elektronicznej poprzez wspieranie tworzenia nowych, innowacyjnych e-usług, innowacyjnych rozwiązań elektronicznego biznesu, zmniejszenie technologicznych, ekonomicznych i mentalnych barier wykorzystania e-usług w społeczeństwie oraz zapewnienie obywatelom dostępu do Internetu szerokopasmowego. Na realizację tego priorytetu przeznaczone jest ponad 1,2 miliona Euro ze środków funduszy strukturalnych
- W ramach priorytetu 8, ważne z punktu widzenia rozwoju społeczeństwa informacyjnego są przede wszystkim dwa działania:
  - Działanie 8.3. Przeciwdziałanie wykluczeniu cyfrowemu – eInclusion, którego celem jest zapewnienie dostępu do Internetu dla osób zagrożonych wykluczeniem cyfrowym z powodu trudnej sytuacji materialnej lub niepełnosprawności. Działanie będzie miało charakter dotacji przekazywanej jednostkom samorządu terytorialnego (JST) lub konsorcjom JST i organizacji pozarządowych, które będą odpowiedzialne za kompleksową realizację działań związanych z udzieleniem wsparcia uprawnionym gospodarstwom domowym na terenie gminy. Dotacja będzie przyznana m.in. całkowite lub częściowe pokrycie kosztów dostępu do Internetu, pokrycie kosztów dostarczenia, instalacji oraz serwisowania sprzętu komputerowego i/lub niezbędnego oprogramowania, zakup usługi przeprowadzenia szkoleń z zakresu obsługi komputera oraz korzystania z Internetu dla użytkowników końcowych projektu.
  - Działanie 8.4. Zapewnienie dostępu do Internetu na etapie ostatniej mili, którego celem jest stworzenie możliwości bezpośredniego dostarczania usługi szerokopasmowego dostępu do Internetu na etapie tzw. ostatniej mili dla grupy docelowej (dostarczanie Internetu bezpośrednio do użytkownika) poprzez wsparcie mikro-, małych i średnich przedsiębiorców zamierzających dostarczać tę usługę na obszarach, na których prowadzenie tej działalności na zasadach rynkowych jest nieopłacalne finansowo. Przedsiębiorcy będą mogli otrzymać dofinansowanie na np. projekty polegające na dofinansowaniu budowy i utrzymaniu dedykowanej infrastruktury teleinformatycznej stworzonej pomiędzy najbliższym lub najbardziej efektywnym punktem dystrybucji Internetu a grupą lub grupami docelowymi. Na obszarze gminy może być realizowany więcej niż 1 projekt tego typu. Minimalna wartość wsparcia to 30 tys. PLN.

Regionalne Programy Operacyjne (RPO) na lata 2007-2013 wskazują cele i priorytety rozwoju, jakie województwa będą realizowały w nadchodzącym okresie programowania. Przykładowe przedsięwzięcia wspierane w zakresie budowy społeczeństwa informacyjnego w 16 RPO dotyczą takich zagadnień, jak:

- Budowa szkieletowych lokalnych i regionalnych sieci szerokopasmowych łączonych z siecią szerokopasmową na poziomie centralnym,
- Publiczne Punkty Dostępu do Internetu,
- Platformy elektroniczne na poziomie regionalnym i lokalnym,
- E-usługi publiczne o wymiarze regionalnym i lokalnym (w tym e-zdrowie, e-praca, e-edukacja), e-usługi w administracji publicznej - elektroniczny obieg dokumentów, e-usługi świadczone na rzecz przedsiębiorstw,
- Wsparcie wdrażania ICT w przedsiębiorstwach oraz zapewnienie szerokiego dostępu i wykorzystania technik ICT dla MŚP,
- Geograficzne Systemy Informacji Przestrzenne dla poziomu regionalnego i lokalnego.

Na inwestycje w zakresie budowy społeczeństwa informacyjnego w ramach 16 RPO przeznaczone będzie ok. 1,28 mln euro, co stanowi 7,7% całej alokacji EFRR.

Program Operacyjny Rozwój Polski Wschodniej - Specjalna szansa dla Polski Wschodniej -

Najbiedniejsze polskie regiony - lubelskie, podkarpackie, podlaskie, świętokrzyskie i warmińsko-mazurskie, są w Unii Europejskiej objęte szczególnymi prawami. Stąd też stworzono w Polsce specjalny program, wyłącznie dla pięciu województw Polski Wschodniej, w ramach którego zostanie sfinansowana z funduszy strukturalnych również infrastruktura społeczeństwa informacyjnego.

Działanie II.1 Sieć szerokopasmowa Polski Wschodniej przewiduje dofinansowanie budowy ponadregionalnej sieci szerokopasmowej składającej się z 5 regionalnych sieci szkieletowych województw Polski Wschodniej oraz dofinansowanie szkoleń mieszkańców Polski Wschodniej zagrożonych „wykluczeniem cyfrowym". Podstawowym celem projektu jest zapewnienie do 2013 roku dostępu do usług szerokopasmowych dla 90 % gospodarstw domowych i 100% instytucji publicznych i przedsiębiorców w 5 województwach Polski Wschodniej. Wartość planowanego projektu to ok. 300 milionów Euro, z czego około 45 milionów Euro pochodzić będzie z budżetów samorządów.

Tabela ZI-3. Fundusze na ICT w Polsce w perspektywie finansowej 2007-2013

Programy Regionalne			
Województwo	**Budowa społeczeństwa informacyjnego (w mln EUR)**	**Środki na Technologie Informatyczne i Komunikacyjne oraz budowę sieci szerokopasmowych (w mln EUR)**	**Udział %**
dolnośląskie	120,1	46,8	38,97
kujawsko-pomorskie	57,1	19	33,27
lubelskie	72,4	18,8	25,97
lubuskie	37,3	16,5	44,24
łódzkie	70,4	28,2	40,06
małopolskie	75	30	40,00
mazowieckie	205,1	149,2	72,75
opolskie	25,6	13,7	53,52
podkarpackie	94,8	8,2	8,65
podlaskie	50,9	25,5	50,10
pomorskie	40,3	24,2	60,05
śląskie	200,9	95	47,29
świętokrzyskie	29	10,9	37,59
warmińsko-mazurskie	62,2	19,3	31,03
wielkopolskie	102,6	42,2	41,13
zachodniopomorskie	42	30	71,43
Łącznie w programach regionalnych:	**1285,7**	**577,5**	**44,92**
Programy Krajowe			
Program Operacyjny Innowacyjna Gospodarka (POIG)	2204	200	9,07
Program Operacyjny Rozwój Polski Wschodniej (PORPW)	300	300	100
Łącznie w programach krajowych:	**2504**	**500**	**19,97**
Fundusze na budowę sieci szerokopasmowej oraz społeczeństwo informacyjne (łącznie z programów regionalnych i krajowych)	**3789,7**	**1077,5**	**28,43**

Źródło: WWW.eficom.pl

PROGRAM DLA BEZPIECZEŃSTWA NA LATA 2007-2013

Decyzja Rady z dnia 12 lutego 2007 r. ustanawiająca na lata 2007–2013, jako część ogólnego programu w sprawie bezpieczeństwa i ochrony wolności, szczegółowy program "Zapobieganie, gotowość i zarządzanie skutkami terroryzmu i innymi rodzajami ryzyka dla bezpieczeństwa" (2007/124/WE, Euratom)

W ramach tego programu UE będzie się starała dążyć do synergii, spójności i komplementarności tego programu z innymi instrumentami unijnymi i wspólnotowymi, programem ramowym w dziedzinie badań, rozwoju technologicznego i działań demonstracyjnych, Funduszem Solidarności Unii Europejskiej oraz instrumentem finansowym ochrony ludności.

Jedną z form finansowania są dotacje przyznawane w następstwie zaproszeń do składania wniosków. Wsparcie może przyjąć także formę zamówienia publicznego.
Komisja przyjmuje roczne programy prac określające cele szczegółowe, priorytety tematyczne, opis środków towarzyszących.

Programy szczegółowe:

Zapobieganie oraz zarządzanie skutkami aktów terroryzmu i innych rodzajów ryzyka
Program obejmuje okres od 1 stycznia 2007 r. do 31 grudnia 2013 r.

Program ten ma przyczynić się do wsparcia wysiłków państw członkowskich mających na celu zapobieganie, przygotowanie i ochronę ludzi i infrastruktury krytycznej przed ryzykiem związanym z atakami terrorystycznymi, a także zapewnienia ochrony w obszarach: zarządzanie kryzysowe, środowisko, zdrowie publiczne, transport, badania i rozwój technologiczny.

Celami szczegółowymi są:

– ochrona ludności i infrastruktury krytycznej, w szczególności poprzez:

a) stymulowanie, promowanie i wspieranie ocen ryzyka dotyczących infrastruktury krytycznej w celu modernizacji systemów bezpieczeństwa;
b) stymulowanie, promowanie i wspieranie opracowywania metodologii ochrony infrastruktury krytycznej, w szczególności metodologii w zakresie oceny ryzyka;
c) promowanie i wspieranie korzystania z tych samych środków operacyjnych mających na celu poprawę bezpieczeństwa w zakresie transgranicznych łańcuchów dostaw, pod warunkiem że zasady konkurencji na rynku wewnętrznym nie zostaną zakłócone;
d) promowanie i wspieranie rozwoju standardów bezpieczeństwa oraz wymiany know-how i doświadczeń w zakresie ochrony ludności i infrastruktury krytycznej;
e) promowanie i wspieranie koordynacji i współpracy na skalę wspólnotową w zakresie ochrony infrastruktury krytycznej.

– zarządzanie skutkami aktów terroryzmu:

a) stymulowanie, promowanie i wspieranie wymiany know-how i doświadczeń w celu ustanowienia najlepszych praktyk;
b) promowanie wspólnych ćwiczeń i praktycznych scenariuszy obejmujących komponenty dotyczące ochrony i bezpieczeństwa w celu zwiększenia koordynacji i współpracy między stosownymi uczestnikami na szczeblu europejskim.

Wsparcie finansowe będzie udzielane do projektów:

- o wymiarze europejskim zainicjowane przez Komisję
- ponadnarodowych, w których muszą uczestniczyć partnerzy z co najmniej 2 państw członkowskich
- krajowe w państwach członkowskich, które: przygotowują projekty ponadnarodowe lub działania wspólnotowe („środki przygotowawcze"), uzupełniają projekty ponadnarodowe lub działania wspólnotowe („środki uzupełniające"), przyczyniają się do rozwoju innowacyjnych metod lub technologii, których wyniki można wykorzystać w działaniach na poziomie wspólnotowym, lub rozwijają takie metody lub technologie w celu przekazania ich innym państwom członkowskim lub innemu krajowi przystępującemu lub kandydującemu.

Dostęp do programu przeznaczony jest dla organów i organizacji posiadających osobowość prawną z siedzibą w państwach członkowskich. Organy i organizacje nastawione na osiąganie zysku będą miały dostęp do dotacji wyłącznie w powiązaniu z organizacjami non-profit lub organizacjami państwowymi.

Zapobieganie i walka z przestępczością

Decyzja Rady z dnia 12 lutego 2007 r. ustanawiająca na lata 2007–2013, jako część ogólnego programu w sprawie bezpieczeństwa i ochrony wolności, szczegółowy program "Zapobieganie i walka z przestępczością" (2007/125/WSiSW)

Program obejmuje okres od 1 stycznia 2007 r. do 31 grudnia 2013 r.
Program przyczynia się do wzmocnienia poziomu bezpieczeństwa obywateli przez zapobieganie i zwalczanie przestępczości (dotyczy to przestępczości zorganizowanej, terroryzmu, handlu ludźmi i przestępstw przeciwko dzieciom, nielegalnego handlu narkotykami i nielegalnego handlu bronią, korupcją i nadużyć finansowych. Ma objąć cztery główne tematy: zapobieganie przestępczości i kryminologia, ściganie przestępstw, ochrona i wsparcie dla świadków, ochrona ofiar.

Celami szczegółowymi są:

a) stymulowanie, promowanie i rozwój horyzontalnych metod i narzędzi niezbędnych do strategicznych działań związanych z zapobieganiem i zwalczaniem przestępczości oraz gwarantowaniem bezpieczeństwa i porządku publicznego,
b) promowanie i rozwój koordynacji, współpracy i wzajemnego zrozumienia między organami ścigania, innymi organami krajowymi i odpowiednimi organami Unii w odniesieniu do priorytetów zidentyfikowanych przez Radę,
c) promowanie i rozwój najlepszych praktyk w dziedzinie ochrony i wsparcia dla świadków; i
d) promowanie i rozwój najlepszych praktyk w dziedzinie ochrony ofiar przestępstw.

Wsparcie finansowe będzie udzielane do projektów:

- o wymiarze europejskim zainicjowane oraz zarządzane przez Komisję
- ponadnarodowych, w których muszą uczestniczyć partnerzy z co najmniej 2 państw członkowskich
- krajowe w państwach członkowskich, które: przygotowują projekty ponadnarodowe lub działania wspólnotowe („środki przygotowawcze"), uzupełniają projekty ponadnarodowe lub działania wspólnotowe („środki uzupełniające"), przyczyniają się

do rozwoju innowacyjnych metod lub technologii, których wyniki można wykorzystać w działaniach na poziomie wspólnotowym, lub rozwijają takie metody lub technologie w celu przekazania ich innym państwom członkowskim lub innemu krajowi przystępującemu lub kandydującemu

- dotacje operacyjne dla organizacji pozarządowych nienastawionych na osiąganie zysku i realizujących cele niniejszego programu na poziomie europejskim

Wsparcie finansowe będzie udzielane na działania: poprawiające współpracę i koordynację operacyjną, z zakresu analizy, monitorowania i oceny, rozwój i transfer technologii i metodologii, szkolenia, wymianę pracowników i ekspertów, związane z podnoszeniem świadomości i rozpowszechnianiem informacji.

Dostęp do programu przeznaczony jest dla organów ścigania, innych publicznych lub prywatnych podmiotów, uczestników działań i instytucji, w tym organów lokalnych, regionalnych i krajowych, partnerów społecznych, szkół wyższych, urzędów statystycznych, organizacji pozarządowych, partnerstw publiczno-prywatnych i odpowiednich organów międzynarodowych. A także dla organów i organizacji posiadających osobowość prawną z siedzibą w państwach członkowskich.

PRZEGLĄD DEFINICJI WALKI INFORMACYJNEJ I DZIAŁAŃ (OPERACJI) INFORMACYJNYCH

WALKA INFORMACYJNA
Walka informacyjna to działania informacyjne prowadzone w czasie kryzysu lub konfliktu dla osiągnięcia pożądanych celów w relacjach z przeciwnikiem lub wsparcia działań prowadzących do tych celów. *Joint Doctrine for Information Operations, Joint PUB 3-13, Joint Chiefs of Staff, Washington 1998.*
Walka informacyjna to działania informacyjne prowadzone dla obrony własnej informacji i systemów informacyjnych lub prowadzone dla atakowania i wywarcia wpływu na informację lub systemy informacyjne przeciwnika. Ta walka jest prowadzona głównie w czasie kryzysu lub konfliktu. Jednak defensywny komponent tej walki, podobnie jak obrana powietrzna, jest prowadzony w całym spektrum działań militarnych, od pokoju do wojny. *AFDD 2-5 Information Operations. USAF.*
Walka informacyjna to działania podejmowane dla osiągnięcia przewagi informacyjnej przez wpływanie na informacje przeciwnika, jego zależne od informacji procesy, informacyjne systemy i sieci komputerowe przy jednoczesnej obronie własnej informacji, zależnych od informacji procesów, informacyjnych systemów i sieci komputerowych. *DOD & Joint Staff – CJCSI 3210.01, [w:] FM 100-6 Information Operations, Headquarters, Departament of the Army,* 1996, *s.2-2.*
Walka informacyjna to działania mające na celu wzbranianie przeciwnikowi dostępu do informacji i jej funkcji lub ich eksploatację, degradację bądź niszczenie; ochrona sieci przeciw takim działaniom oraz eksploatowanie własnych militarnych funkcji informacyjnych. S. Widnall, R. Fogleman, *Cornerstones of Information Warfare, Headquarters, Departament of the Air Force, Washington 1995.*
Walka informacyjna jest elektronicznym konfliktem, w którym informacja jest strategicznym dobrem wartym podboju lub destrukcji. W. Schwartau, *Information Warfare. Cyberterroryzm: Protecting Your Personal Sekurity In the Electronic Age, Thunder, Mouth Press 1996, s.28-32.*
Walka informacyjna to działania podejmowane dla osiągnięcia przewagi informacyjnej, prowadzone w ramach wspierania narodowej strategii militarnej. Działania te mają na celu wpływanie na informację i systemy informacyjne przeciwnika przy wpływaniu i obronie własnej informacji i jej systemów. E. Paige, [za:] *G. Ivefors, Information Warfare. Defeat the enemy before battle – a warfare revolution in teh 21st century?; http://www.kla.liu.eci~guniv/infowar/* 26.01.2001.
Walka informacyjna w najogólniejszym sensie jest użyciem informacji dla osiągnięcia naszych narodowych celów. Podobnie jak dyplomacja, ekonomiczna rywalizacja czy użycie sił zbrojnych, informacja sama w sobie jest kluczowym czynnikiem narodowej potęgi. Ponadto, co jeszcze ważniejsze, informacja staje się głównym narodowym zasobem, który wspiera dyplomację, ekonomiczną rywalizację oraz przemoc militarną. Walka informacyjna w tym sensie może być postrzegana jako konflikt między państwami lub narodami prowadzony częściowo przez globalnie połączoną infrastrukturę informacyjną i komunikacyjną J. Arquilla, D. Ronfeldt, *Cyberwar is Coming,* [w:] *Comparative Strtegy* 12-1993, s. 41-65 [za:] G. Stein, *Information Warfare,* [w:] A.D. Campen, D.H. Deart, R.T. Goodden, *Cyberwar: Securtity, Strategy, and Conflict in the information Age, AFCEA International Press,* Fairfax 1996, s.175.

Walka informacyjna jest formą konfliktu, w którym bezpośrednie atakowanie systemów informacyjnych jest środkiem atakowania wiedzy i przekonań przeciwnika. Walka informacyjna może być prowadzona jako komponent kompleksowej wrogiej działalności – w postaci wojny sieciowej (*netwar*) lub cyberwojny (*cyberwar*) – lub może przybrać formę walki samodzielnej R. Szafrański, *Cyberwar: A Theory of Information Warfare: Preparing For 2020,* [w:] A. D. Campen, D.H. Deart, R.T. Goodden, *Cyberwar: Security, Strategy, and Conflikt in the International Press,* Fairfax 1996, s.233.
Walka informacyjna jest przygotowaniem do użycia lub użyciem fizycznej lub cyfrowej broni dla dezorganizacji lub niszczenia informacji lub systemów informacyjnych w celu degradowania lub przerwania wykonywania funkcji, które zależą od informacji lub informacyjnych systemów R.J. Knecht, *Thoughts About Information Warfare,* [w:] A.D. Campen, D.H. Deart, R.T. Goodden, *Cyberwar: Securty, Strategy, and Conflict in the Information Age, AFCEA International Press,* Fairfax 1996, s.165.
Walka informacyjna jest konfliktem, w którym informacja jest jednocześnie zasobem, obiektem ataku i bronią. Walka informacyjna obejmuje także fizyczną destrukcję infrastruktury, która wykorzystywana jest przez przeciwnika do działań operacyjnych R. Stark, *Future Warfare: Information Superiority through Info War,* Southwest Missouri State University *http://www.smsu.edu*
Walka informacyjna jako samodzielna technika prowadzenia wojny nie istniej. W zamian istnieje kilka oddzielnych form walki informacyjnej, z których każda pretenduje do bycia ogólniejsza koncepcją. Obecnie wyróżnić można siedem form walki informacyjnej – konfliktu, który zawiera ochronę, manipulację, degradację lub uniemożliwianie dostępu do informacji. Formami tymi są: walka o przewagę w dowodzeniu, walka bazująca na wiedzy, walka elektroniczna, walka psychologiczna, walka hackerska, ekonomiczna walka informacyjna i cyberwalka. M. Libijki, *What is Information Warfare? NDU,* Washington 1995, s. x.
Walka informacyjna to działania kooperacji negatywnej wzajemnej, w których cel destrukcyjnego oddziaływania skoncentrowany jest na systemach informacyjno-sterujących przeciwnych sobie stron. Przedmiotem walki informacyjnej jest system informacyjno-sterujący. L. Ciborowski, *Walka informacyjna,* Toruń 1999.
Walką informacyjną *(information warfare, infowar)* nazywamy całokształt działań ofensywnych i defensywnych koniecznych do uzyskania przewagi informacyjnej nad przeciwnikiem i osiągnięcia zamierzonych celów militarnych (politycznych). Istotą tak rozumianej walki jest: (1) zniszczenie (lub degradacja wartości) zasobów informacyjnych przeciwnika oraz stosowanych przez niego systemów informacyjnych; (2) zapewnienie bezpieczeństwa własnych zasobów informacyjnych i wykorzystywanych systemów informacyjnych. P. Sienkiewicz, *Współczesne koncepcje walki informacyjnej, [w]* R. Szpyra, *Informacyjny wymiar współczesnych działań powietrznych. Materiały z sympozjum naukowego,* Warszawa 2002.
Walka informacyjna to zorganizowana w formie przemocy aktywność zewnętrzna państwa prowadząca do osiągnięcia określonych celów politycznych, skierowana na niszczenie lub modyfikowanie systemów informacyjnego komunikowania przeciwnika lub przepływającej przez nie informacji oraz aktywność zapewniająca ochronę własnych systemów informacyjnego komunikowania i przesyłanej informacji przed podobnym działaniem przeciwnika. Militarna walka informacyjna to zorganizowana w formie przemocy militarna aktywność zewnętrzna państwa prowadząca do osiągnięcia określonych celów politycznych, skierowana na niszczenie lub modyfikowanie systemów informacyjnego komunikowania przeciwnika lub przepływającej przez nie informacji oraz aktywność zapewniająca ochronę własnych systemów informacyjnego komunikowania i przesyłanej informacji przed podobnym działaniem przeciwnika. R. Szpyra, *Operacje informacyjne państwa w działaniach sił powietrznych. Rozprawa habilitacyjna,* Warszawa 2002.

DZIAŁANIA (OPERACJE) INFORMACYJNE
Działania informacyjne to akcje podjęte dla wpływania na informacje i systemy informacyjne przeciwnika przy jednoczesnej ochronie własnej informacji i systemów informacyjnych. *Joint Doctrine for Information Operations. Joint PUB 3-13, Joint Chiefs of Staff,* Washington 1998.
Działania informacyjne to ciągłe działania militarne w militarnym środowisku informacyjnym, które uaktywniają, wzmacniają i chronią zdolności własnych sił do gromadzenia, przetwarzania i działania na informacji dla osiągnięcia (korzyści) przewagi w pełnym spektrum działań militarnych. Działania informacyjne zawierają interakcje z globalnym środowiskiem informacyjnym i eksploatację informacji przeciwnika lub uniemożliwienie mu dostępu do informacji i zdolności podejmowania decyzji. *FM 100-6 Information Operations, Headquarters, Department of the Army, 1996, s.2-3.*
Działania informacyjne obejmują przedsięwzięcia podejmowane dla zdobycia, wykorzystania, obrony lub ataku na informuję lub systemy informacyjne i łączą zarówno aspekt informacji w walce, jak i walkę informacyjną. Działania te prowadzone są przez wszystkie fazy operacji i w całym zakresie działań militarnych. *AFDD 2-5 Information Operations, USAF.*
Działania informacyjne to przedsięwzięcia podjęte w celu wywarcia wpływu na decydentów w ramach wsparcia politycznych i militarnych celów poprzez oddziaływanie na informacje innych, ich procesy informacyjne oraz systemy dowodzenia, kontroli, łączności i informacyjne, przy wykorzystaniu i ochronie własnej informacji i systemów informacyjnych. *MC 422 – NATO Information Operations Policy.*
Działania informacyjne to działania podjęte dla wpływania na decydentów w ramach wspierania procesu osiągania celów politycznych i militarnych, mające charakter wpływania na informacje, procesy informacyjne, systemy dowodzenia i kontroli oraz systemy komunikacyjno-informacyjne (CIS) przy eksploatowaniu i ochronie własnej informacji i systemów informacyjnych. *Allied Joint Doctrine AJP -01 NATO,* Wydanie 1999.
Działania informacyjne są zorganizowanymi działaniami określonego systemu socjotechnicznego o charakterze ofensywnym lub defensywnym, których celem jest degradacja wartości zasobów informacyjnych przeciwnika i ochrona wartości własnych zasobów informacyjnych. Zasoby informacyjne obejmują informacje pozyskiwane, przesyłane, przetwarzane i przechowywane za pomocą systemów informacyjnych (informatycznych), telekomunikacyjnych i masowego komunikowania, które posiadają istotna wartość z punktu widzenia bezpieczeństwa państwa i jego instytucji (organizacji). P. Sienkiewicz, *Teoria systemów bezpieczeństwa. Część I i II.* AON, Warszawa 2003.
Działania informacyjne państwa rozumiane będą jako zorganizowana aktywność państwa prowadząca do osiągnięcia określonych celów politycznych, skierowana na zewnętrzne i wewnętrzne systemy informacyjnego komunikowania lub przepływającą przez nie informację. Militarne działania informacyjne to zorganizowana aktywność militarna państwa prowadząca do osiągnięcia określonych celów politycznych, skierowana na zewnętrzne i wewnętrzne systemy informacyjnego komunikowania lub przepływającą przez nie informację. R. Szpyra, *Operacje informacyjne państwa w działaniach sił powietrznych. Rozprawa habilitacyjna,* Warszawa 2002.

Wyniki badań empirycznych prognozowania zagrożeń z wykorzystaniem sieci neuronowej w postaci aplikacji Excel'a Alyuda Forecaster XL

SESJA 1 (przykład 1)

Tabela Z-IV-1. Zbiór wejściowy: szereg czasowy zawierający sumę incydentów w poszczególnych miesiącach 1997r. z ich prognozą

		incydenty
	incydenty	
sty-97	241	241,52331
lut-97	238	233,48121
mar-97	260	260,36117
kwi-97	275	275,04212
maj-97	248	237,50528
cze-97	256	256,4114
lip-97	230	230,53772
sie-97	199	199,38482
wrz-97	245	245,50511
paź-97	257	244,6822
lis-97	236	246,34261
gru-97	224	245,15941

Tabela Z-IV-2. Raport analizy danych oraz ich wstępnego przetworzenia dla zagrożenia „incydenty 1 1997r.

Data Analysis and Preprocessing Report

Generated by Alyuda Forecaster XL - 2009-07-17 at 10:37:30

Input range: book - _97-incydenty.xls; sheet - Arkusz1; range - B2:C14; columns - 2; rows - 13.

Target range: in the last column of input range.

Summary

2 columns and 12 rows analysed.

2 columns and 12 rows are accepted for neural network training.

The following columns recognized as categorical:

(encoded to 12 columns).

The following columns recognized as numeric:

incydenty.

Data analysis and preprocessing successfully completed.

Analysis Details

Input	Target	LEGEND	
	incydenty		
categorical	numeric		Input values
1997-01-01	241		
1997-02-01	238		Target values
1997-03-01	260		
1997-04-01	275		Removed rows and columns
1997-05-01	248		
1997-06-01	256		Missing values
1997-07-01	230		
1997-08-01	199		Outliers
1997-09-01	245		
1997-10-01	257		
1997-11-01	236		
1997-12-01	224		

Tabela Z–IV-3. Wstępne przetworzenie danych dla zagrożenia „incydenty 1 1997r. (c.d.)

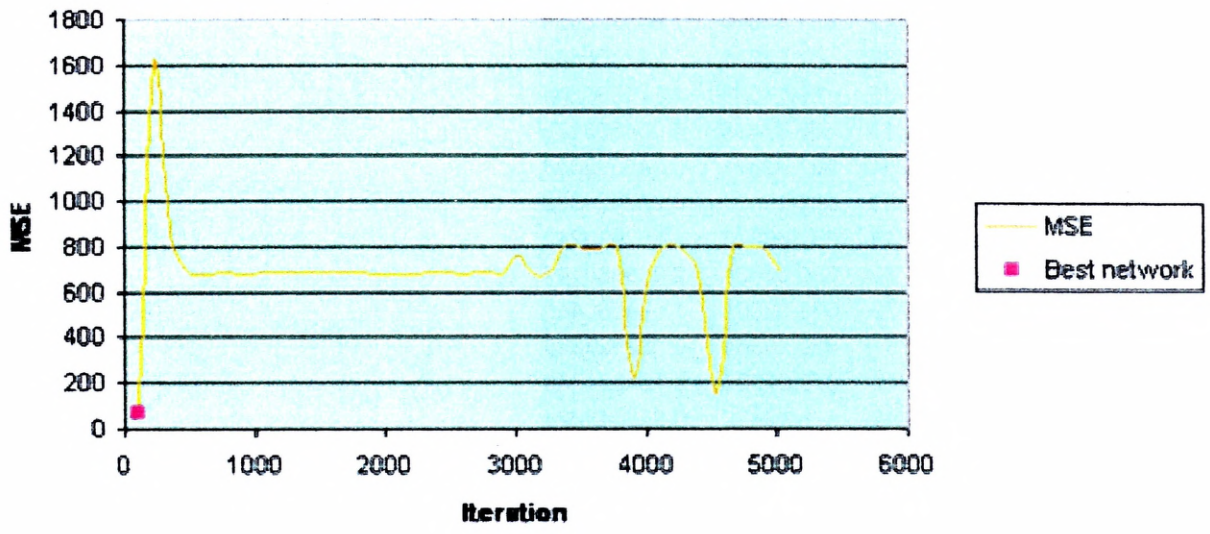
Preprocessing Details

Input												Target
												incydenty
[c]: 1997-01-01	[c]: 1997-02-01	[c]: 1997-03-01	[c]: 1997-04-01	[c]: 1997-05-01	[c]: 1997-06-01	[c]: 1997-07-01	[c]: 1997-08-01	[c]: 1997-09-01	[c]: 1997-10-01	[c]: 1997-11-01	[c]: 1997-12-01	[n]
min:n/a	min:n/a	min:n/a	min:n/a	min:n/a	min:n/a	min:n/a	min:n/a	min:n/a	min:n/a	min:n/a	min:n/a	min: 199
max:n/a	max:n/a	max:n/a	max:n/a	max:n/a	max:n/a	max:n/a	max:n/a	max:n/a	max:n/a	max:n/a	max:n/a	max: 275
0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	0,0421053
-0,4	0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	0,0105263
-0,4	-0,4	0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	0,2421053
-0,4	-0,4	-0,4	0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	0,4
-0,4	-0,4	-0,4	-0,4	0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	0,1157895
-0,4	-0,4	-0,4	-0,4	-0,4	0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	0,2
-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,073684
-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	0,4	-0,4	-0,4	-0,4	-0,4	-0,4
-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	0,4	-0,4	-0,4	-0,4	0,0842105
-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	0,4	-0,4	-0,4	0,2105263
-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	0,4	-0,4	-0,010526
-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	0,4	-0,136842

Przygotowanie danych (warstwy wejściowej) do trenowania sieci, w modelu wielomianowej sieci polega na zapisie danych w kolumnach

Tabela Z-IV-4. Raport z treningu sieci dla zagrożenia „incydenty 1 1997r.

Summary	
	Problem type: regression
	STOP TRAINING CONDITIONS
	Training stops automatically.
	Training stop reason: maximum number of iterations was achieved.
	TRAINING RESULTS
	Iterations trained: 5031
	The best network was restored.



Rysunek Z-IV-1. Wykres błędu MSE sieci w trakcie treningu (*Training Error Graph*)

Tabela Z-IV-5. Przykładowe zestawienie błędów otrzymanych podczas treningu sieci dla zagrożenia „incydenty 1 1997r.

Training Error Table

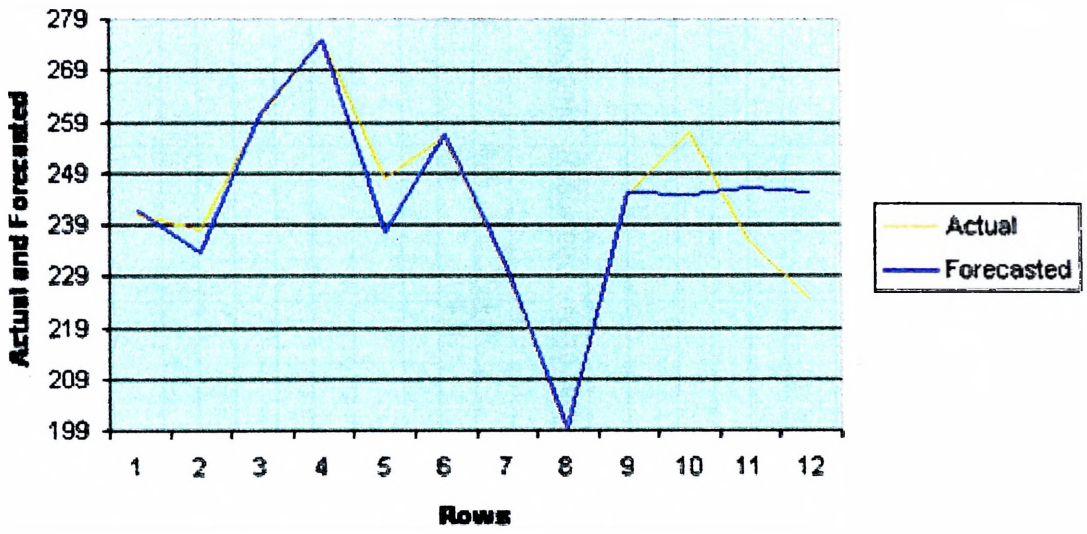
Iteration No.	AE	AE improv.	MSE	MSE improv.
[best] - 101	4,4557267	0	71,322804	0
229	36,780113	-32,324387	1607,7719	-1536,449132
355	21,750141	15,0299723	871,41199	736,3599435
481	16,002951	5,74719007	694,09698	177,3150146
607	14,033966	1,96898533	677,13334	16,96363634
733	15,723594	-1,6896279	689,37841	-12,24507345
859	15,100272	0,62332172	681,53019	7,848228828
989	14,336477	0,76379484	677,7561	3,77408864
1119	16,43925	-2,1027735	692,4589	-14,70280544
1245	15,675169	0,7640813	686,37435	6,084553175
1371	15,307497	0,36767254	687,22391	-0,849562683
1497	15,499379	-0,1918823	688,18634	-0,962424332
1623	15,478302	0,02107645	687,66023	0,52610242
1749	15,94088	-0,4625778	690,62621	-2,965980147
1881	14,630803	1,31007739	678,88061	11,74560466
2007	14,795192	-0,1643891	679,26354	-0,382928628
2133	14,77723	0,01796212	679,07927	0,184271758
2259	14,352273	0,42495646	678,42422	0,655045024
2385	15,173977	-0,8217032	686,62964	-8,205417519
2511	15,23485	-0,0608732	686,90565	-0,276011608
2637	14,343174	0,89167542	677,84767	9,057982653
2763	15,341085	-0,9979106	687,47964	-9,631977267
2889	14,288733	1,05235224	677,55128	9,928365439
3015	17,175912	-2,8871796	759,19519	-81,643913
3141	14,019064	3,15684807	677,11341	82,08178396
3267	15,185344	-1,1662798	686,5775	-9,464095473
3393	17,321811	-2,1364668	804,27622	-117,6987141
3519	15,582184	1,73962679	791,87285	12,40337057
3645	15,557826	0,02435841	791,63623	0,236615977
3771	16,979968	-1,4221421	803,33506	-11,6988267
3897	9,5483474	7,43162026	218,23264	585,1024133
4023	15,597707	-6,0493595	688,0849	-469,8522562
4149	16,317242	-0,7195353	794,21478	-106,1298742
4275	15,56093	0,7563122	791,70842	2,50635701
4401	15,414621	0,14630881	686,66931	105,039106
4527	6,1270336	9,28758768	153,62197	533,0473371
4653	16,609333	-10,4823	801,36752	-647,745546
4779	16,49377	0,11556303	795,68381	5,683707199
4905	15,214441	1,27932894	791,11908	4,564732366
5031	15,232506	-0,0180647	686,84738	104,2717058

Tabela Z-IV-6. Informacja o wybranej sieci (dla założonych parametrów) dla zagrożenia „incydenty 1 1997r.

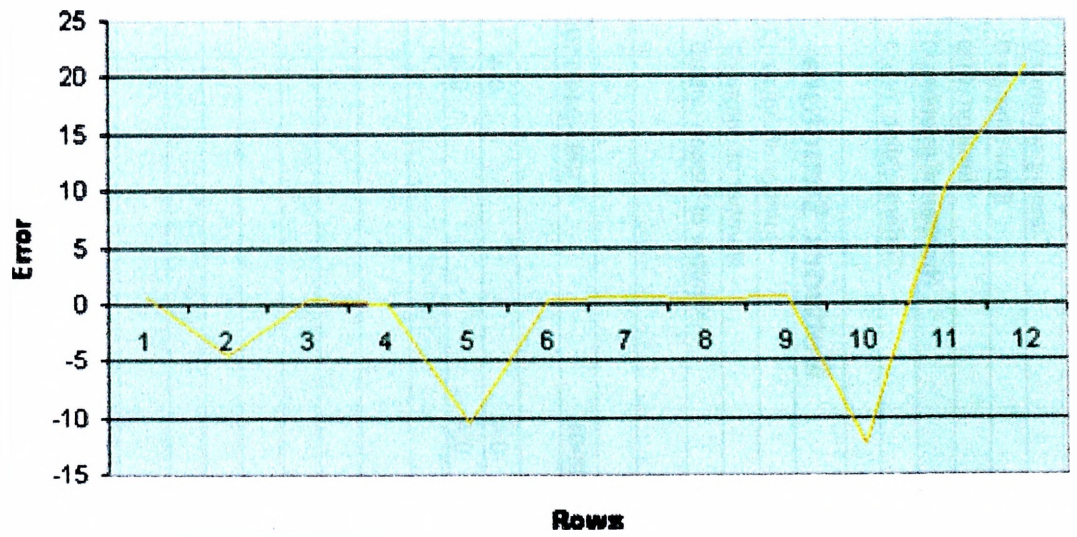
Neural Network Information													
Generated by Alyuda Forecaster XL - 2009-07-17 at 10:37:31													
			Training parameters										
			Stopping condition:	0									
			Training set error:	0									
			Error change:	0									
			Iteration No:	0									
			Number of iterations:	0									
			Generalization loss:	0									
			Network Structure										
			Number of inputs:	12									
			Number of outputs:	1									
			Number of hidden units:	0									
Input data types													
Types	1												
1997-01-01	1997-02-01	1997-03-01	1997-04-01	1997-05-01	1997-06-01	1997-07-01	1997-08-01	1997-09-01	1997-10-01	1997-11-01	1997-12-01		
Intervals	12												
MIN	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	
MAX	0,4	0,4	0,4	0,4	0,4	0,4	0,4	0,4	0,4	0,4	0,4	0,4	
Output data types													
Types	1												
#NUM#													
Intervals	1												
MIN	199												
MAX	275												
Weights													
Outputs													
1	13												
0,1239146	-0,1324847	-0,5568163	0,974849	2,3814232	-0,3446824	0,7137298	-0,7135193	-3,062533	0,0812381	0,0366307	0,1269314	0,0624656	

Tabela Z-IV-7. Raport zbiorczy statystyk dla danych empirycznych i uzyskanych w czasie testowania sieci dla zagrożenia „incydenty 1 1997r.

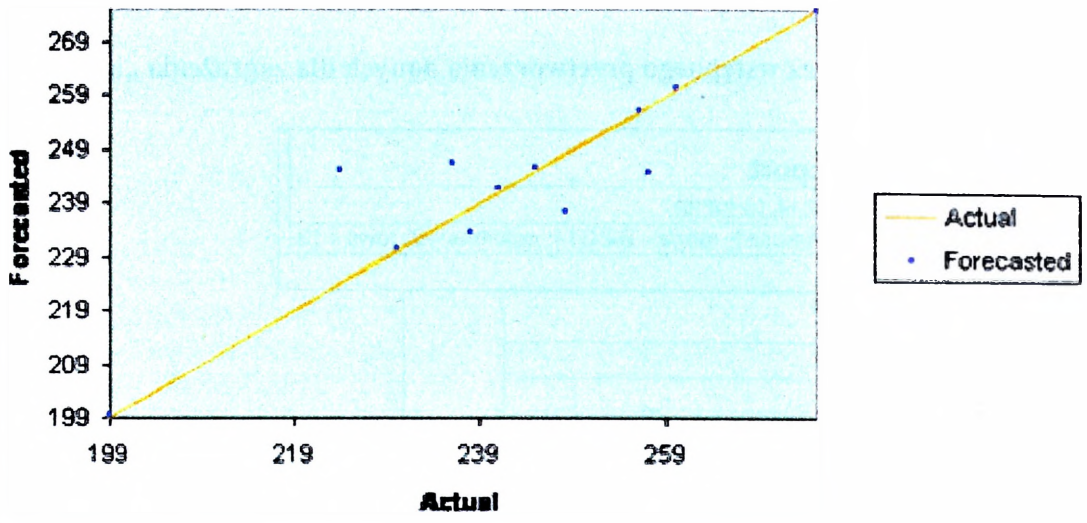
Summary					
	Training set	Test set			
# of rows:	10	2			
CCR:	n/a	n/a			
Average AE:	4,6585466	7,5067518			
Average MSE:	70,768601	65,279266			
Tolerance type:	Relative	Relative			
Tolerance:	10%	30%			
# of Good forecasts:	10 (100%)	2 (100%)			
# of Bad forecasts:	0 (0%)	0 (0%)			
RSquared: 0,8026					
Correlation: 0,8972					



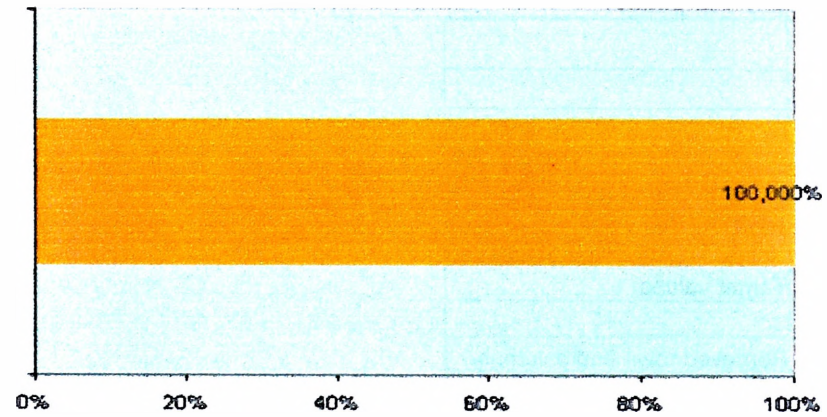
Rysunek Z-IV-2. Wykres danych empirycznych i prognozy dla zagrożenia „incydenty 1 1997r. (*Actual vs. Forecast (by Rows)*)



Rysunek Z-IV-3. Wykres odchyleń błędów (*Deviation Graph*) dla zagrożenia „incydenty 1 1997r.



Rysunek Z-IV-4. Punktowy wykres rozrzutu prognozy dla zagrożenia „incydenty 1 1997r. (*Actual vs. Forecast (Scatter Plot)*)



Rysunek Z-IV-5. Wykres analizy poprawności danych wejściowych dla zagrożenia „incydenty 1 1997r. (*Input Importance*)

Tabela Z-IV-8. Zestawienie: danych empirycznych, prognozy, błędów dla zagrożenia „incydenty 1 1997r.

Actual vs. Forecasted Table

Input	Target	Output			
	incydenty	Forecast	Abs. Error	Rel. Error	Estimate
1997-01-01	241	241,52331	0,523308	0,22%	Good
1997-02-01	238	233,48121	-4,5187854	1,90%	Good
1997-03-01	260	260,36117	0,3611715	0,14%	Good
1997-04-01	275	275,04212	0,0421174	0,02%	Good
1997-05-01	248	237,50528	-10,494718	4,23%	Good
1997-06-01	256	256,4114	0,4113997	0,16%	Good
1997-07-01	230	230,53772	0,5377191	0,23%	Good
1997-08-01	199	199,38482	0,3848245	0,19%	Good
1997-09-01	245	245,50511	0,5051069	0,21%	Good
1997-10-01	257	244,6822	-12,317802	4,79%	Good
1997-11-01	236	246,34261	10,342611	4,38%	Good
1997-12-01	224	245,15941	21,159407	9,45%	Good

Sesja 1 (przykład 2)

Tabela Z-IV-9. Raport analizy danych oraz wstępnego przetworzenia danych dla zagrożenia „incydenty 1 1997r.

Data Analysis and Preprocessing Report

Generated by Alyuda Forecaster XL - 2008-07-17 at 10:38:38

Input range: book - _97-incydenty1.xls; sheet - Arkusz1; range - B2:C14; columns - 2; rows - 13.

Target range: in the last column of input range.

Summary

2 columns and 12 rows analysed.

2 columns and 12 rows are accepted for neural network training.

The following columns recognized as categorical:

data(encoded to 12 columns).

The following columns recognized as numeric:

incydenty.

Data analysis and preprocessing successfully completed.

Analysis Details

Input	Target	LEGEND
data	incydenty	
categorical	numeric	Input values
1997-01-01	241	
1997-02-01	238	Target values
1997-03-01	260	
1997-04-01	275	Removed rows and columns
1997-05-01	248	
1997-06-01	256	Missing values
1997-07-01	230	
1997-08-01	199	Outliers
1997-09-01	245	
1997-10-01	257	
1997-11-01	236	
1997-12-01	224	

Tabela Z-IV-10. Wstępne przetworzenie danych, dla zagrożenia „incydenty 1 1997r. ciąg dalszy

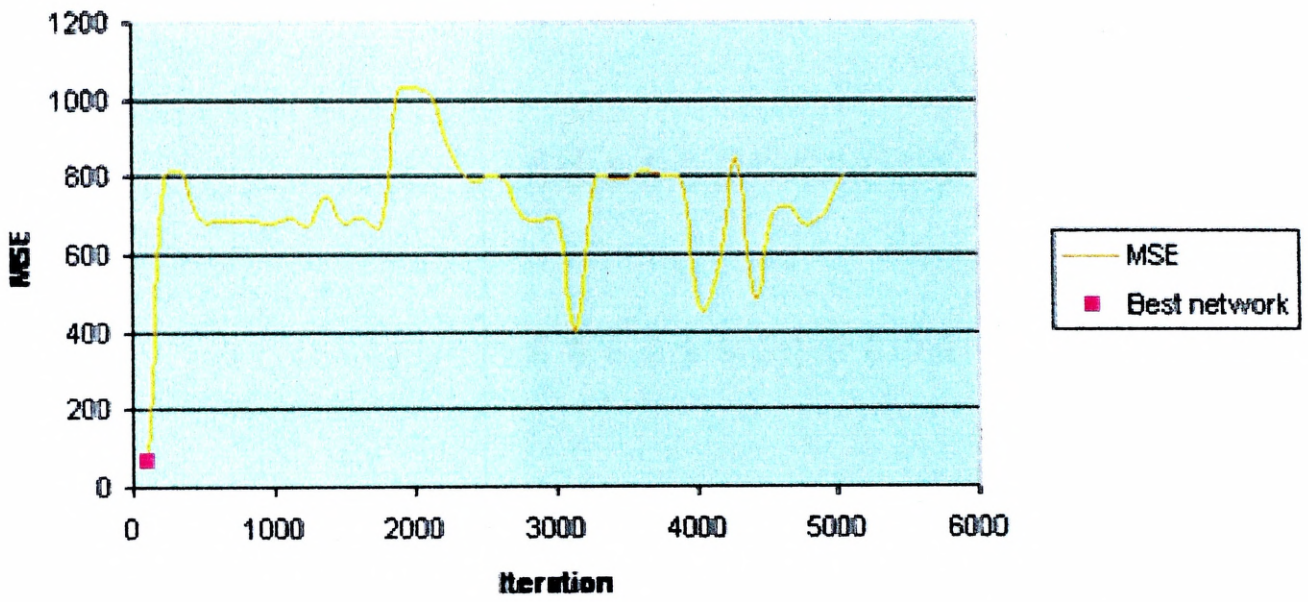
Preprocessing Details

Input												Target
data												incydenty
[c]: 1997-01-01	[c]: 1997-02-01	[c]: 1997-03-01	[c]: 1997-04-01	[c]: 1997-05-01	[c]: 1997-06-01	[c]: 1997-07-01	[c]: 1997-08-01	[c]: 1997-09-01	[c]: 1997-10-01	[c]: 1997-11-01	[c]: 1997-12-01	[n]
min:n/a	min:n/a	min:n/a	min:n/a	min:n/a	min:n/a	min:n/a	min:n/a	min:n/a	min:n/a	min:n/a	min:n/a	min: 199
max:n/a	max:n/a	max:n/a	max:n/a	max:n/a	max:n/a	max:n/a	max:n/a	max:n/a	max:n/a	max:n/a	max:n/a	max: 275
0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	0,0421053
-0,4	0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	0,0105263
-0,4	-0,4	0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	0,2421053
-0,4	-0,4	-0,4	0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	0,4
-0,4	-0,4	-0,4	-0,4	0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	0,1157895
-0,4	-0,4	-0,4	-0,4	-0,4	0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	0,2
-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,073684
-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	0,4	-0,4	-0,4	-0,4	-0,4	-0,4
-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	0,4	-0,4	-0,4	-0,4	0,0842105
-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	0,4	-0,4	-0,4	0,2105263
-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	0,4	-0,4	-0,010526
-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	0,4	-0,136842

Tabela Z-IV-11. Raport uczenia sieci dla zagrożenia „incydenty 1 1997r.

Training Report
Generated by Alyuda Forecaster XL - 2008-07-17 at 10:38:38
Input range: book - _97-incydenty1.xls; sheet - Arkusz1; range - B2:C14; columns - 2; rows - 13.
Target range: in the last column of input range.

Summary
Problem type: regression
STOP TRAINING CONDITIONS
Training stops automatically.
Training stop reason: maximum number of iterations was achieved.
TRAINING RESULTS
Iterations trained: 5039
The best network was restored.



Rysunek Z-IV-6. Wykres błędu średniokwadratowego dla uczącej się sieci dla zagrożenia „incydenty 1 1997r.

Tabela Z-IV-12. Przykładowe zestawienie tabelaryczne błędów dla uczącej się sieci dla zagrożenia „incydenty 1 1997r.

Training Error Table

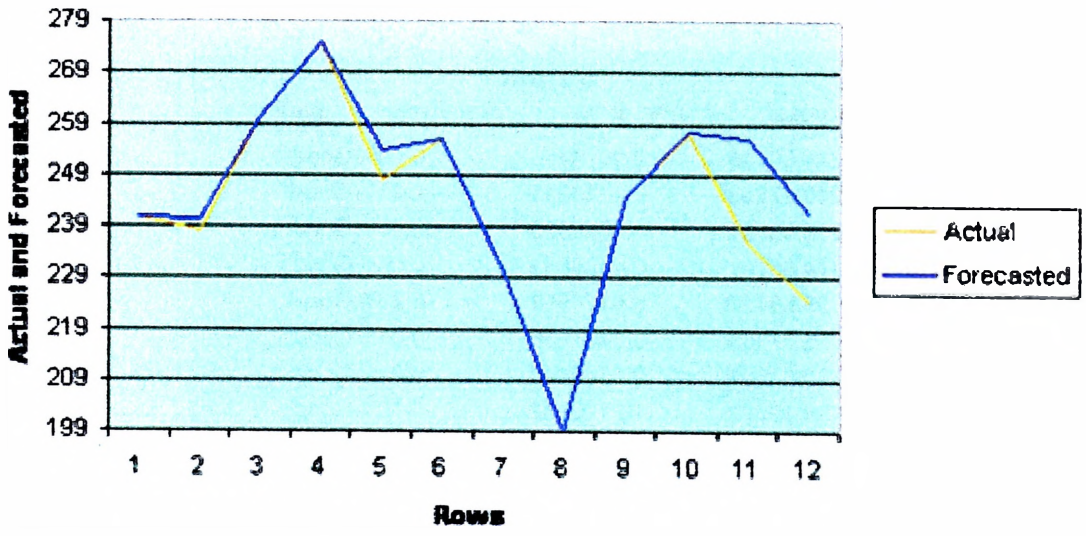
Iteration No.	AE	AE improv.	MSE	MSE improv.
[best] - 101	3,8066597	0	69,143145	0
227	22,134086	-18,327426	792,34871	-723,2055671
353	22,354042	-0,2199564	815,44132	-23,09260511
479	16,060629	6,29341305	695,70415	119,7371644
605	15,099852	0,96077699	686,51781	9,186338262
738	16,052968	-0,9531155	690,77861	-4,260799274
873	15,472505	0,58046302	687,76582	3,0127968
999	14,357897	1,11460759	677,57599	10,18983091
1125	16,391491	-2,0335936	692,18955	-14,613568
1251	14,109875	2,28161521	677,36749	14,82206592
1377	18,480481	-4,3706057	751,38338	-74,01589104
1503	14,749651	3,73082983	679,17352	72,20985751
1629	16,464647	-1,7149954	693,5501	-14,37658214
1763	14,018742	2,44590465	677,13162	16,4184794
1889	20,043413	-6,0246706	1018,6692	-341,5375351
2015	20,892759	-0,8493462	1030,3502	-11,68103346
2141	18,255247	2,63751219	1002,8477	27,50249319
2267	21,259017	-3,0037701	862,22111	140,6265925
2393	15,498635	5,76038177	787,51315	74,70796005
2519	17,193871	-1,6952359	804,77777	-17,2646206
2645	15,190141	2,00373011	791,13331	13,64445862
2771	16,448344	-1,2582036	696,78146	94,35184777
2897	15,344717	1,10362792	686,98872	9,792736276
3023	16,004598	-0,6598811	690,12669	-3,13796286
3149	11,097174	4,90742405	395,14388	294,9828041
3275	16,422696	-5,3255228	792,7404	-397,5965129
3401	16,048155	0,37454139	793,34396	-0,603562525
3527	16,107674	-0,0595195	794,28094	-0,936977029
3653	18,860217	-2,7525421	818,74664	-24,4657002
3779	16,946029	1,91418743	800,55589	18,19074733
3905	15,327019	1,61901007	791,2217	9,334189797
4031	13,645307	1,68171215	456,03095	335,1907477
4157	10,725117	2,92019038	574,95276	-118,9218112
4283	20,704983	-9,9798661	847,28671	-272,3339481
4409	12,191938	8,51304426	487,38392	359,9027902
4535	17,075823	-4,8838846	697,09261	-209,7086914
4661	17,437851	-0,362028	719,00501	-21,91240283
4787	14,032544	3,40530694	677,16202	41,84299406
4913	15,990895	-1,9583514	703,77905	-26,61703209
5039	15,805118	0,18577745	807,71987	-103,9408214

Tabela Z-IV-13. Zestawienie danych dla wyuczonej sieci dla zagrożenia „incydenty 1 1997r.

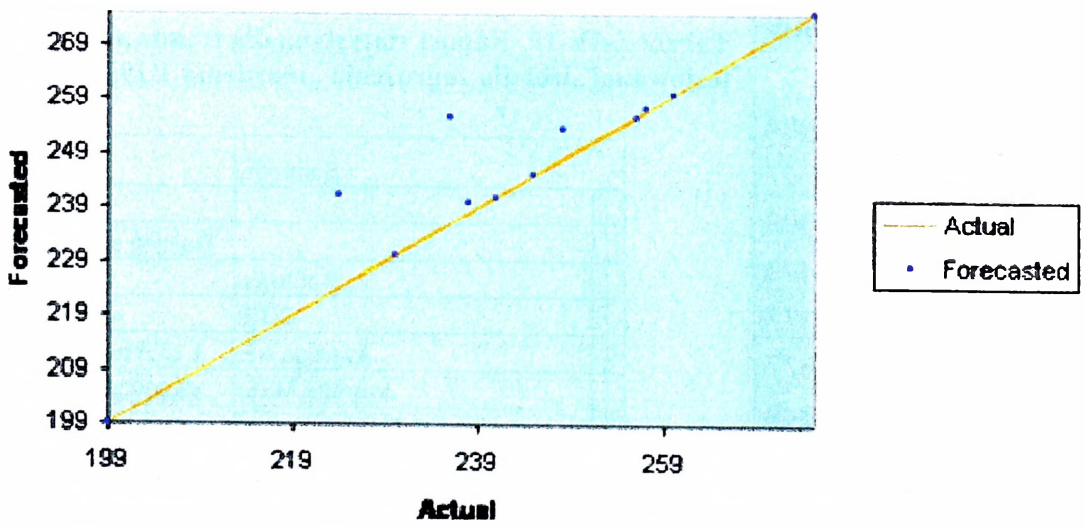
Neural Network Information												
Generated by Alyuda Forecaster XL - 2008-07-17 at 10:38:39												
			Training parameters									
			Stopping condition:	0								
			Training set error:	0								
			Error change:	0								
			Iteration No:	0								
			Number of iterations:	0								
			Generalization loss:	0								
			Network Structure									
			Number of inputs:	12								
			Number of outputs:	1								
			Number of hidden units:	0								
Input data types												
Types	1											
1997-01-01	1997-02-01	1997-03-01	1997-04-01	1997-05-01	1997-06-01	1997-07-01	1997-08-01	1997-09-01	1997-10-01	1997-11-01	1997-12-01	
Intervals	12											
MIN	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4
MAX	0,4	0,4	0,4	0,4	0,4	0,4	0,4	0,4	0,4	0,4	0,4	0,4
Output data types												
Types	1											
#NUM#												
Intervals	1											
MIN	199											
MAX	275											
Weights												
Outputs												
1	13											
0,6985069	-0,2301145	-0,274311	0,8772349	2,2842295	0,4713362	0,6159481	-0,8110424	-3,1597086	-0,0163448	0,7160566	0,6098494	-0,2199366

Tabela Z-IV-14. Zestawienie dla wytrenowanej i przetestowanej sieci dla zagrożenia „incydenty 1 1997r.

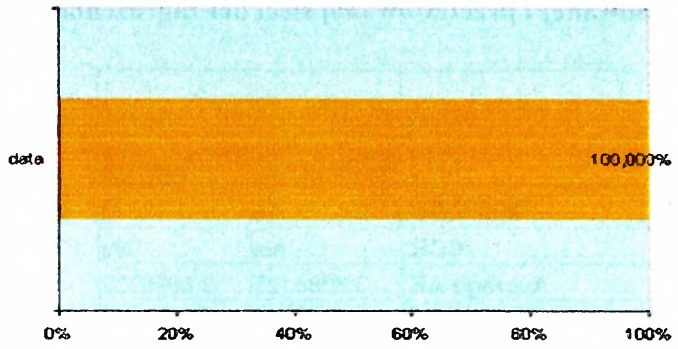
Summary		
	Training set	Test set
# of rows:	10	2
CCR:	n/a	n/a
Average AE:	3,8061125	3,8926132
Average MSE:	69,124837	18,111119
Tolerance type:	Relative	Relative
Tolerance:	10%	30%
# of Good forecasts:	10 (100%)	2 (100%)
# of Bad forecasts:	0 (0%)	0 (0%)
RSquared: 0,8287		
Correlation: 0,9328		



Rysunek Z-IV-7. Wykres danych empirycznych i prognozy dla zagrożenia „incydenty 1 1997r. (*Actual vs. Forecast (by Rows)*)



Rysunek Z-IV-8. Punktowy wykres rozrzutu prognozy **dla zagrożenia „incydenty 1 1997r. (*Actual vs. Forecast (Scatter Plot)*)**



Rysunek Z-IV-9. Wykres analizy poprawności danych wejściowych dla zagrożenia „incydenty 1 1997r. (*Input Importance*)

Tabela Z-IV-15. Dane empiryczne, prognozowane oraz średni błąd bezwzględny i rzeczywisty dla zagrożenia „incyenty 1 1997r.

Actual vs. Forecasted Table

Input	Target	Output			
data	incydenty	Forecast	Abs. Error	Rel. Error	Estimate
1997-01-01	241	241,00745	0,0074456	0,00%	Good
1997-02-01	238	240,17253	2,1725311	0,91%	Good
1997-03-01	260	259,96501	-0,0349883	0,01%	Good
1997-04-01	275	274,85701	-0,1429862	0,05%	Good
1997-05-01	248	253,6127	5,6126952	2,26%	Good
1997-06-01	256	255,97383	-0,0261656	0,01%	Good
1997-07-01	230	230,03004	0,0300448	0,01%	Good
1997-08-01	199	199,19573	0,195732	0,10%	Good
1997-09-01	245	245,00162	0,0016162	0,00%	Good
1997-10-01	257	257,54641	0,5464107	0,21%	Good
1997-11-01	236	255,87635	19,876354	8,42%	Good
1997-12-01	224	241,19938	17,199382	7,68%	Good

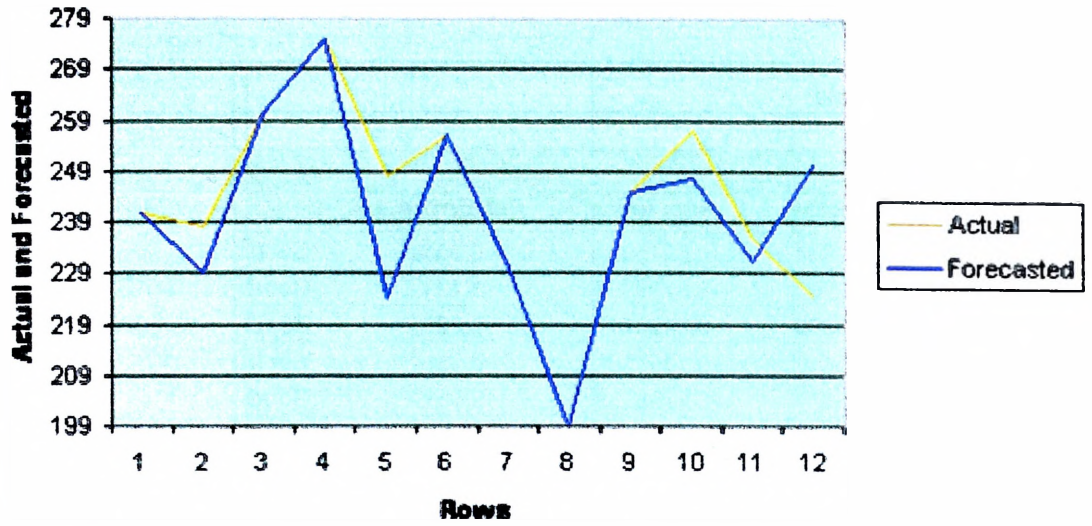
Sesja 1 (przykład 3)

Tabela Z-IV-16. Dane wprowadzające i prognozowane dla zagrożenia „incydenty 1 1997r.

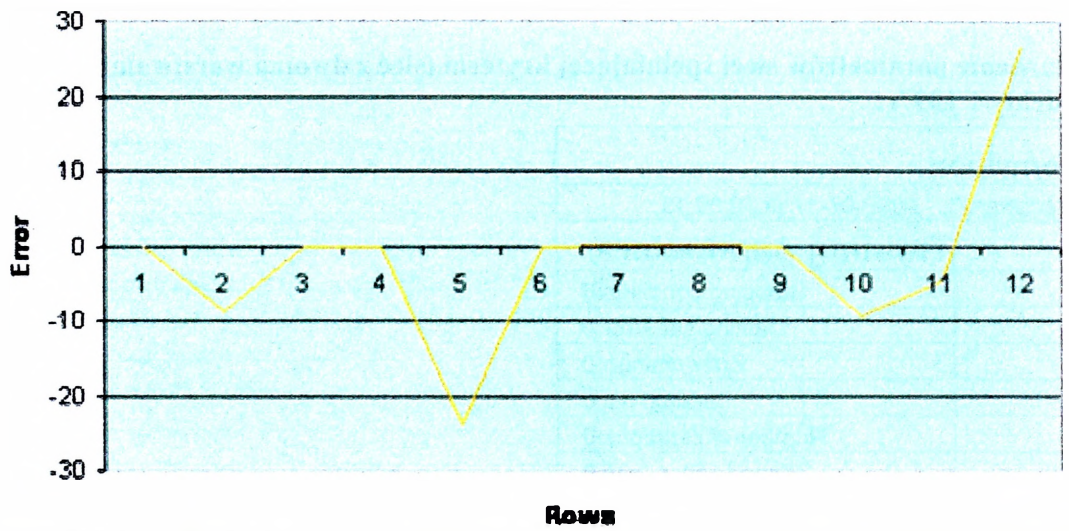
		incydenty
	incydenty	
sty-97	241	240,9984
lut-97	238	229,12707
mar-97	260	259,95603
kwi-97	275	274,85449
maj-97	248	224,23177
cze-97	256	255,96677
lip-97	230	230,01849
sie-97	199	199,19185
wrz-97	245	244,99095
paź-97	257	247,63113
lis-97	236	231,28609
gru-97	224	250,81316
sty-98	223	223,42312

Tabela Z-IV-17. Raport statystyka dla trenowanej i testowanej sieci dla zagrożenia „incydenty 1 1997r.

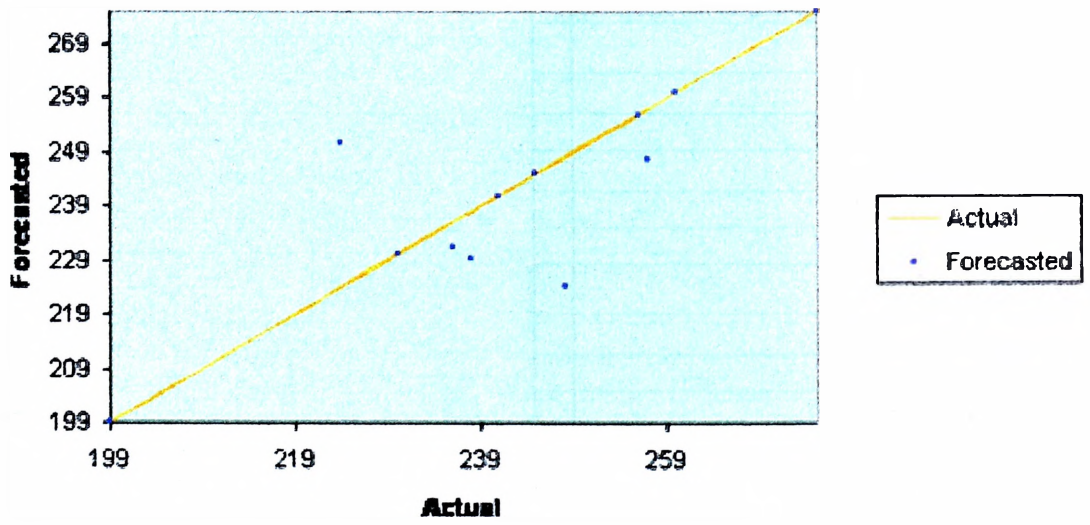
Summary		
	Training set	Test set
# of rows:	10	2
CCR:	n/a	n/a
Average AE:	4,1339641	16,320582
Average MSE:	82,900364	321,8289
Tolerance type:	Relative	Relative
Tolerance:	10%	30%
# of Good forecasts:	9 (90%)	2 (100%)
# of Bad forecasts:	1 (10%)	0 (0%)
RSquared: 0,6532		
Correlation: 0,8310		



Rysunek Z-IV-10. Wykres danych empirycznych i prognozy dla zagrożenia „incydenty 1 1997r. (*Actual vs. Forecast (by Rows)*)



Rysunek Z-IV-11 Wykres odchyleń błędów dla zagrożenia „incydenty 1 1997r. (*Deviation Graph*)



Rysunek Z-IV-12. Punktowy wykres rozrzutu prognozy dla zagrożenia „incydenty 1 1997r. (*Actual vs. Forecast (Scatter Plot)*)

Tabela Z-IV-18. Zestawienie danych empirycznych, prognozowanych oraz błędów prognozy dla zagrożenia „incydenty 1 1997r.

Actual vs. Forecasted Table					
Input	Target	Output			
	incydenty	Forecast	Abs. Error	Rel. Error	Estimate
1997-01-01	241	240,9984	-0,0015991	0,00%	Good
1997-02-01	238	229,12707	-8,8729306	3,73%	Good
1997-03-01	260	259,95603	-0,0439717	0,02%	Good
1997-04-01	275	274,85449	-0,1455101	0,05%	Good
1997-05-01	248	224,23177	-23,768233	9,58%	Good
1997-06-01	256	255,96677	-0,0332271	0,01%	Good
1997-07-01	230	230,01849	0,0184871	0,01%	Good
1997-08-01	199	199,19185	0,191855	0,10%	Good
1997-09-01	245	244,99095	-0,0090511	0,00%	Good
1997-10-01	257	247,63113	-9,3688727	3,65%	Good
1997-11-01	236	231,28609	-4,7139087	2,00%	Good
1997-12-01	224	250,81316	26,813159	11,97%	Bad

Tabela Z-IV-19. Zestawienie parametrów sieci spełniającej kryteria (sieć z dwoma warstwami ukrytymi) dla zagrożenia „incydenty 1 1997r.

Neural Network Information				
Generated by Alyuda Forecaster XL - 2009-07-17 at 10:39:18				
			Training parameters	
			Stopping condition:	0
			Training set error:	0
			Error change:	0
			Iteration No:	0
			Number of iterations:	0
			Generalization loss:	0
			Network Structure	
			Number of inputs:	1
			Number of outputs:	1
			Number of hidden units:	2
Input data types				
Types	1			
#NUM#				
Intervals	1			
MIN	1996			
MAX	2008			
Output data types				
Types	1			
#NUM#				
Intervals	1			
MIN	50			
MAX	2516			
Weights				
Outputs				
1	4			
-0,1714808	-2,7949834	2,5041896	2,2922459	
Hidden				
2	3			
10,631653	174,69502	0		
-13,362618	119,8264	-12,572717		

Tabela Z-IV-20. Raport z analizy danych i wstępnego ich przetworzenia dla zagrożenia „incydenty 1 1997r. (*Data Analysis and Preprocessing Report*)

Summary

2 columns and 13 rows analysed.

2 columns and 13 rows are accepted for neural network training.

The following columns recognized as numeric:

lata ,

liczba incydentów.

Data analysis and preprocessing successfully completed.

Analysis Details

Input	Target
lata	liczba incydentów
numeric	numeric
1996	50
1997	75
1998	100
1999	105
2000	126
2001	741
2002	1013
2003	1196
2004	1222
2005	2516
2006	2427
2007	2108
2008	1796

LEGEND

Input values

Target values

Removed rows and columns

Missing values

Outliers

Preprocessing Details

Input	Target
lata	liczba incydentów
[n]	[n]
min: 1996	min: 50
max: 2008	max: 2516
-0,4	-0,4
-0,333333	-0,3918897
-0,266667	-0,3837794
-0,2	-0,38215734
-0,133333	-0,375344688
-0,066667	-0,175831306
0	-0,087591241
0,0666667	-0,028223844
0,1333333	-0,019789132
0,2	0,4
0,2666667	0,371127332
0,3333333	0,267639903
0,4	0,166423358

Tabela Z-IV-21. Raport zbiorczy statystyk dla danych empirycznych trenowanej sieci dla zagrożenia „incydenty 1 1997r.

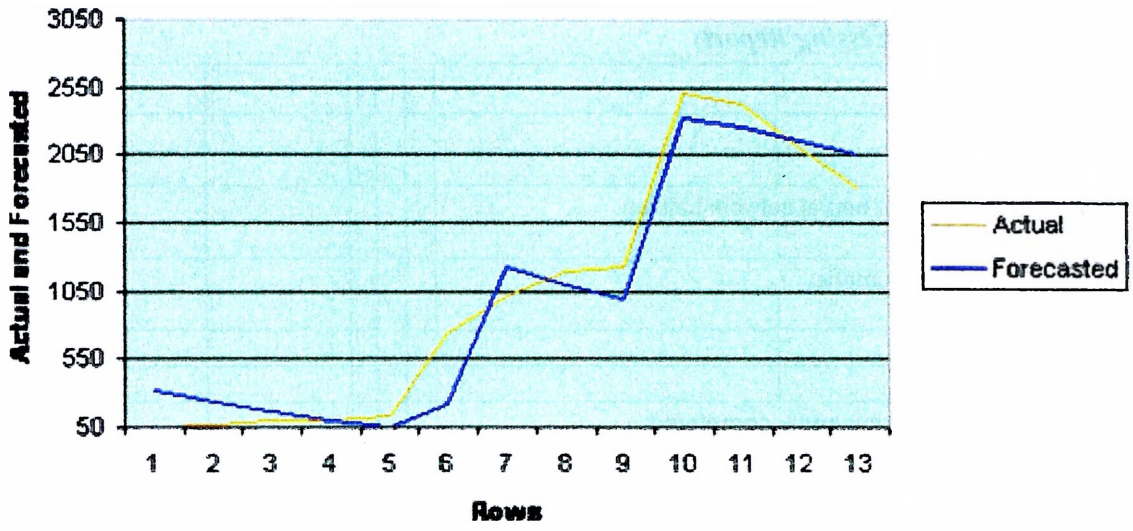
Summary

	Training set	Test set
# of rows:	11	2
CCR:	n/a	n/a
Average AE:	151,12693	349,16137
Average MSE:	30829,418	154598,36
Tolerance type:	Relative	Relative
Tolerance:	10%	30%
# of Good forecasts:	5 (45%)	0 (0%)
# of Bad forecasts:	6 (55%)	2 (100%)

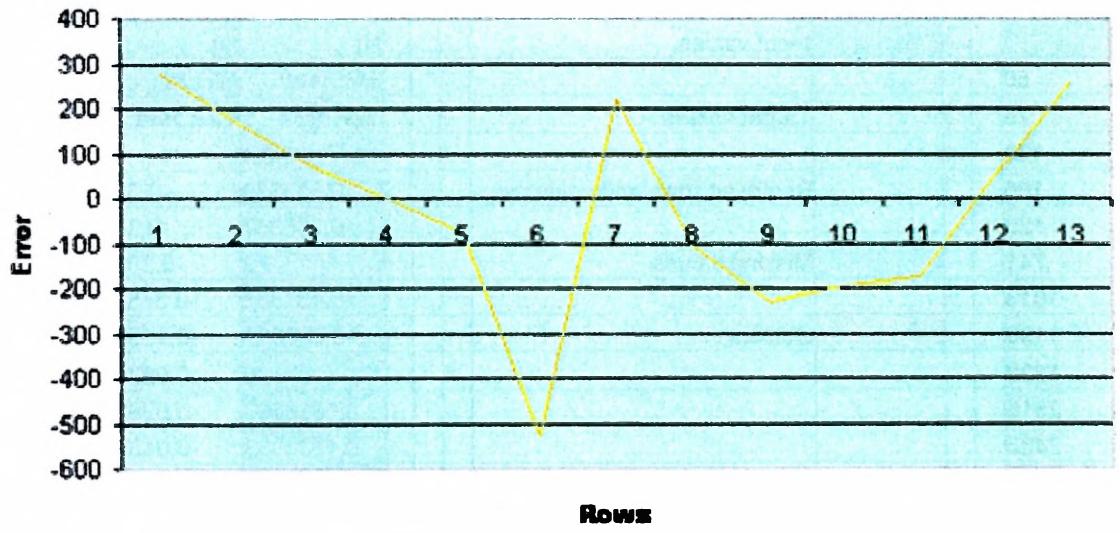
RSquared: 0,9381

Correlation: 0,9688

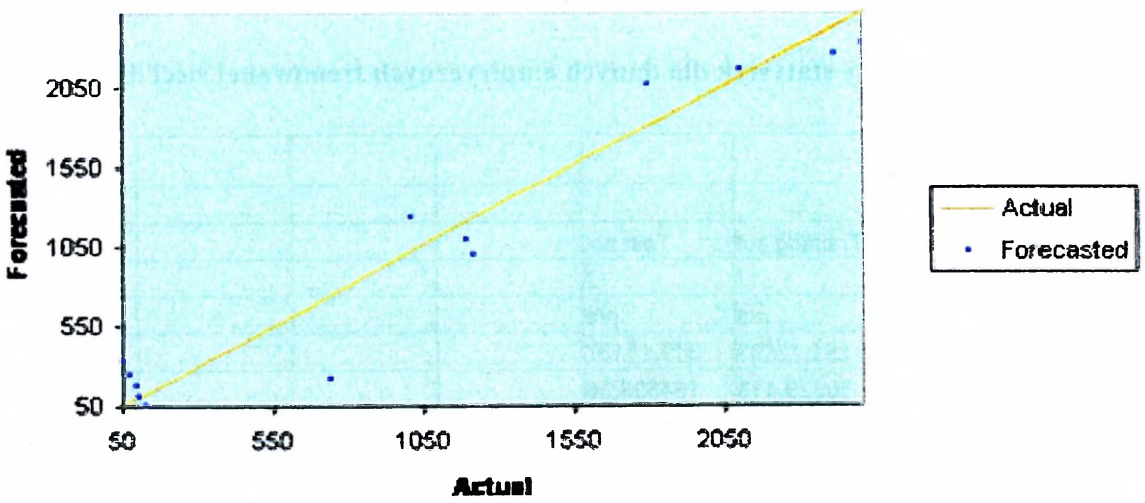
Dobre dopasowanie danych (korelacja 0,9688), ale tylko 45% stanowią dobre prognozy



Rysunek Z-IV-13.Wykres danych empirycznych i prognozy dla zagrożenia „incydenty 1 1997r. (*Actual vs. Forecast (by Rows)*)



Rysunek Z-IV-14. Wykres odchyleń błędów dla zagrożenia „incydenty 1 1997r. (Deviation Graph)



Rysunek Z-IV-15. Punktowy wykres rozrzutu prognozy dla zagrożenia „incydenty 1 1997r. (*Actual vs. Forecast (Scatter Plot)*)

Sesja 2 (przykład 1)

Tabela Z-IV-22. Zestawienie danych empirycznych i prognoz oraz błędów prognozowania dla zagrożenia liczba incydentów w latach 1996 – 2008

Actual vs. Forecasted Table

Input lata	Target liczba incydentów	Forecast	Abs. Error	Rel. Error	Output Estimate
1996	50	326,62132	276,62132	553,24%	Bad
1997	75	243,37229	168,37229	224,50%	Bad
1998	100	169,94124	69,941239	69,94%	Bad
1999	**105**	**105,74352**	**0,7435189**	0,71%	Good
2000	126	50,055055	-75,944945	60,27%	Bad
2001	741	211,04954	-529,95046	71,52%	Bad
2002	1013	1232,4887	219,48871	21,67%	Bad
2003	1196	1089,9592	-106,04079	8,87%	Good
2004	1222	992,63736	-229,36264	18,77%	Bad
2005	2516	2322,4204	-193,57957	7,69%	Good
2006	2427	2253,3205	-173,67953	7,16%	Good
2007	2108	2161,5282	53,52821	2,54%	Good
2008	1796	2059,4658	263,46577	14,67%	Bad

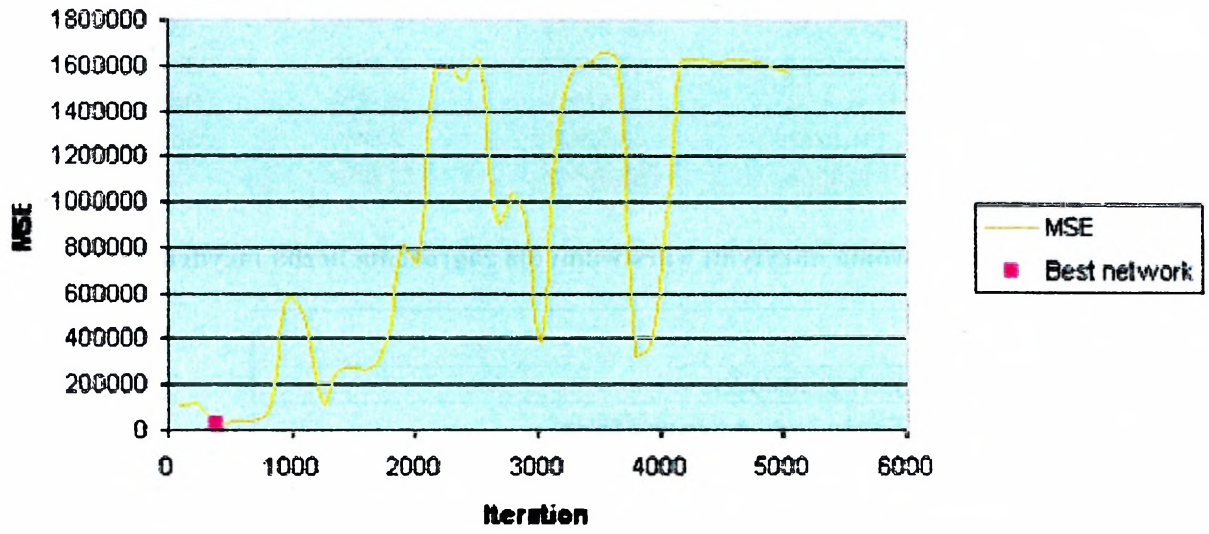
Tabela Z-IV-23. Raport dla sieci z dwoma ukrytymi warstwami dla zagrożenia liczba incydentów w latach 1996 – 2008

Neural Network Information					
Generated by Alyuda Forecaster XL - 2008-07-17 at 10:40:55					
			Training parameters		
			Stopping condition:	0	
			Training set error:	0	
			Error change:	0	
			Iteration No:	0	
			Number of iterations:	0	
			Generalization loss:	0	
			Network Structure		
			Number of inputs:	1	
			Number of outputs:	1	
			Number of hidden units:	2	
Input data types					
Types	1				
#NUM#					
Intervals	1				
MIN	1996				
MAX	2009				
Output data types					
Types	1				
#NUM#					
Intervals	1				
MIN	50				
MAX	2516				
Weights					
Outputs					
1	4				
-0,2522691	-3,692139	2,6275939	-2,5147554		
Hidden					
2	3				

11,237086	129,20649	0		
7,4605207	-97,012317	8,1350904		

Tabela Z-IV-24. Podsumowanie treningu sieci dla zagrożenia liczba incydentów w latach 1996 – 2008

Summary	
	Problem type: regression
	STOP TRAINING CONDITIONS
	Training stops automatically.
	Training stop reason: **maximum number of** iterations was achieved.
	TRAINING RESULTS
	Iterations trained: **5061**
	The best network was restored.



Rysunek Z-IV-16. Wykres błędu MSE uczącej się sieci dla zagrożenia liczba incydentów w latach 1996 – 2008 (*Training Error Graph*)

Tabela Z-IV-25. Zestawienie błędów w trakcie uczenia sieci dla zagrożenia liczba incydentów w latach 1996 – 2008

Training Error Table				
Iteration No.	AE	AE improv.	MSE	MSE improv.
101	**259,16776**	**0**	**115750,86**	**0**
237	253,92161	5,24614676	107965,02	7785,833973
[best] - 385	154,78096	99,1406534	31909,176	76055,84609
513	117,97512	36,8058431	35503,095	-3593,919522
660	96,176637	21,7984787	39822,893	-4319,797991
822	252,04104	-155,8644	88605,106	-48782,21325
948	415,78555	-163,74451	569209,89	-480604,7857
1107	363,31486	52,4706855	503057,19	66152,70086
1242	249,53996	113,774903	119655,2	383401,9913
1368	218,4766	31,0633592	252392,94	-132737,739
1494	268,99513	-50,518532	270416,76	-18023,82365
1634	390,25392	-121,25879	277352,24	-6935,475549
1767	319,09976	71,1541641	380568,38	-103216,1466
1896	449,90252	-130,80276	811792,44	-431224,0578
2034	417,17977	32,7227489	733731,49	78060,95576
2160	697,07448	-279,89471	1564671	-830939,5627

2286	726,91572	-29,841238	1588010,9	-23339,88506
2412	678,02333	48,8923882	1541103,4	46907,50419
2538	720,73974	-42,716408	1630280,3	-89176,84203
2664	458,99182	261,747924	924409,34	705870,9311
2790	526,44439	-67,452572	1045258,6	-120849,2574
2916	492,74997	33,6944196	912261,05	132997,55
3042	336,29938	156,450588	394040,19	518220,8619
3168	648,87722	-312,57784	1307794,1	-913753,9537
3294	686,61224	-37,735017	1574013,1	-266218,9123
3423	673,5321	13,0801425	1612161	-38147,97101
3549	795,22561	-121,69352	1660456,2	-48295,22152
3675	656,94425	138,281366	1613063,1	47393,13914
3801	382,45664	274,487604	337622,84	1275440,269
3927	461,63497	-79,178328	369125,61	-31502,76861
4053	439,06804	22,5669293	922455,91	-553330,3065
4179	672,72735	-233,6593	1612484,5	-690028,6165
4305	709,20428	-36,47693	1623888,5	-11403,93086
4431	667,55688	41,6474022	1613672,2	10216,22574
4557	713,0896	-45,532724	1624387,2	-10714,96557
4683	720,06014	-6,9705395	1628174,4	-3787,179435
4809	699,09558	20,9645551	1621338,2	6836,137011
4935	732,00745	-32,911862	1588859,4	32478,86275
5061	664,98745	67,0199989	1565026,3	23833,04838

Tabela Z-IV-26. Zestawienie analizy danych i ich wstępnego przetworzenia dla zagrożenia liczba incydentów w latach 1996 – 2008

Summary

2 columns and 14 rows analysed.

2 columns and 14 rows are accepted for neural network training.

The following columns recognized as numeric:

lata ,

liczba incydentów.

1 values recognized as missing.

Data analysis and preprocessing successfully completed.

Analysis Details

Input	Target
lata	liczba incydentów
numeric	numeric
1996	50
1997	75
1998	100
1999	105
2000	126
2001	741
2002	1013
2003	1196
2004	1222
2005	2516
2006	2427
2007	2108
2008	1796
2009	

LEGEND

Input values

Target values

Removed rows and columns

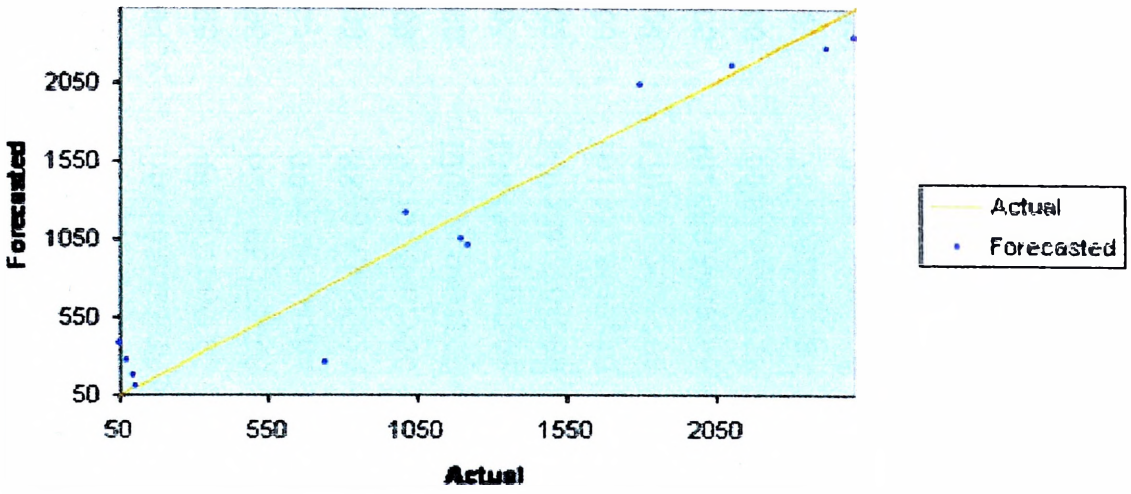
Missing values

Outliers

Preprocessing Details

Input	Target
lata	liczba incydentów
[n]	[n]
min: 1996	min: 50
max: 2009	max: 2516
-0,4	-0,4
-0,338462	-0,3918897
-0,276923	-0,3837794
-0,215385	-0,38215734
-0,153846	-0,375344688
-0,092308	-0,175831306
-0,030769	-0,087591241
0,0307692	-0,028223844
0,0923077	-0,019789132
0,1538462	0,4
0,2153846	0,371127332
0,2769231	0,267639903

| | | |



Rysunek Z-IV-19. Wykres danych empirycznych i mapa odchyleń prognozy dla zagrożenia liczba incydentów w latach 1996 – 2008 ***(Actual vs. Forecast (Scatter Plot))***

Tabela Z-IV-28. Dane empiryczne i prognoza oraz błędy prognozy dla zagrożenia liczba incydentów w latach 1996 – 2008

Actual vs. Forecasted Table

Input	Target				Output
lata	liczba incydentów	Forecast	Abs. Error	Rel. Error	Estimate
1996	50	378,06652	328,06652	656,13%	Bad
1997	75	270,94067	195,94067	261,25%	Bad
1998	100	178,62881	78,628814	78,63%	Bad
1999	105	100,15944	-4,8405569	4,61%	Good
2000	126	34,349053	-91,650947	72,74%	Bad
2001	741	257,51738	-483,48262	65,25%	Bad
2002	1013	1218,238	205,238	20,26%	Bad
2003	1196	1046,7806	-149,2194	12,48%	Bad
2004	1222	1009,735	-212,26504	17,37%	Bad
2005	2516	2335,6713	-180,32871	7,17%	Good
2006	2427	2272,6289	-154,37107	6,36%	Good
2007	2108	2162,2517	54,251656	2,57%	Good
2008	1796	2036,5352	240,53523	13,39%	Bad
2009					

Sieć przetrenowana.

Sesja 3 (przykład 1)

Tabela Z-IV-29. Dane empiryczne i prognozowane dla zagrożenia „robak sieciowy"

lata	robak sieciowy	robak sieciowy
1993	10	36,13374855
1994	36	45,0533379
1995	44	54,73365882
1996	62	65,196046
1997	79	76,45304304
1998	88	88,50665923
1999	95	101,3467235
2000	120	114,9494508
2001	138	129,2761502
2002	149	144,2701089
2003	161	159,8513518
2004	170	181,3626263
2005	462	460,8449258
2006	55	57,53282153
2007	78	16,62072591
2008	24	21,19882726
2009	28,63362	28,63361673

Tabela Z-IV-30. Wstępne przetwarzanie danych dla zagrożenia „robak sieciowy"

Analysis Details

Input	Target
lata	robak sieciowy
numeric	numeric
1993	10
1994	36
1995	44
1996	62
1997	79
1998	88
1999	95
2000	120
2001	138
2002	149
2003	161
2004	170
2005	462
2006	55
2007	78
2008	24
2009	

LEGEND

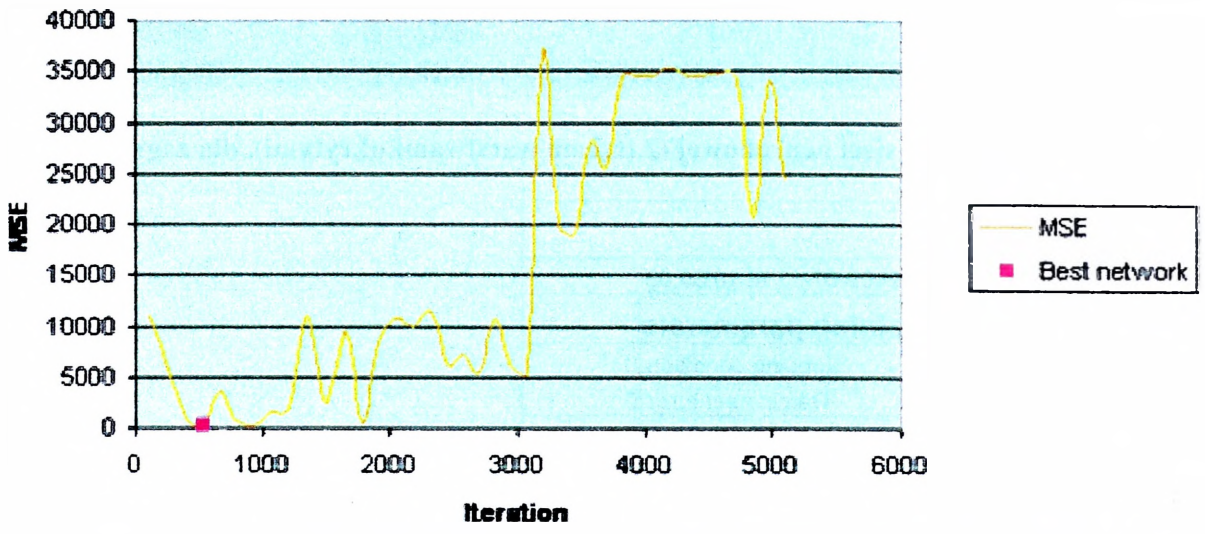
- Input values
- Target values
- Removed rows and columns
- Missing values
- Outliers

Preprocessing Details

Input	Target
lata	robak sieciowy
[n]	[n]
min: 1993	min: 10
max: 2009	max: 462
-0,4	-0,4
-0,35	-0,353982301
-0,3	-0,339823009
-0,25	-0,307964602
-0,2	-0,277876106
-0,15	-0,261946903
-0,1	-0,249557522
-0,05	-0,205309735
0	-0,173451327
0,05	-0,153982301
0,1	-0,132743363
0,15	-0,116814159
0,2	0,4
0,25	-0,320353982
0,3	-0,279646018
0,35	-0,375221239
0,4	-0,417699115

Tabela Z-IV-31. Raport uczenia sieci dla zagrożenia „robak sieciowy"

Summary								
	Problem type: regression							
	STOP TRAINING CONDITIONS							
	Training stops automatically.							
	Training stop reason: **maximum number** of iterations was achieved.							
	TRAINING RESULTS							
	Iterations trained: 5**094**							
	The best network was restored.							



Rysunek Z-IV-20.Wykres błędów MSE dla uczącej się sieci dla zagrożenia „robak sieciowy"

Tabela Z-IV-32. Zestawienie błędów trenowania sieci dla zagrożenia „robak sieciowy"

Training Error Table

Iteration No.	AE	AE improv.	MSE	MSE improv.
101	65,379593	0	11049,78	0
263	51,**810614**	**13,5689789**	**5098,8135**	**5950,966332**
406	**13,484101**	38,326513	576,35555	4522,457962
[best] - 532	8,7628434	4,72125793	318,69344	257,6621164
669	49,013189	-40,250345	3651,8648	-3333,171368
799	19,592336	29,4208525	583,65807	3068,206738
939	12,282632	7,30970368	337,04798	246,6100826
1083	29,104259	-16,821626	1498,4497	-1161,401761
1211	35,109907	-6,0056487	1863,3406	-364,890828
1340	48,03461	-12,924702	11021,605	-9158,264105
1490	32,565489	15,4691208	2486,6103	8534,994349
1650	63,513138	-30,947649	9408,9565	-6922,346144
1776	12,895457	50,6176813	512,13448	8896,821993
1910	70,289982	-57,394526	8301,75	-7789,615554
2053	43,033106	27,2568767	10777,423	-2475,672576
2181	81,434665	-38,40156	9891,3067	886,1159095
2315	100,896	-19,461334	11545,55	-1654,243166
2441	52,47818	48,4178193	6180,4462	5365,103676
2567	59,351153	-6,8729728	7289,3474	-1108,901207
2695	37,241639	22,1095141	5415,823	1873,524376
2821	84,916043	-47,674405	10715,117	-5299,293859
2947	45,044544	39,8714995	6085,7342	4629,382694
3073	36,489993	8,55455035	5414,1239	671,6102907
3199	125,12722	-88,637227	37130,314	-31716,19025
3325	77,74052	47,3867004	19945,095	17185,21879

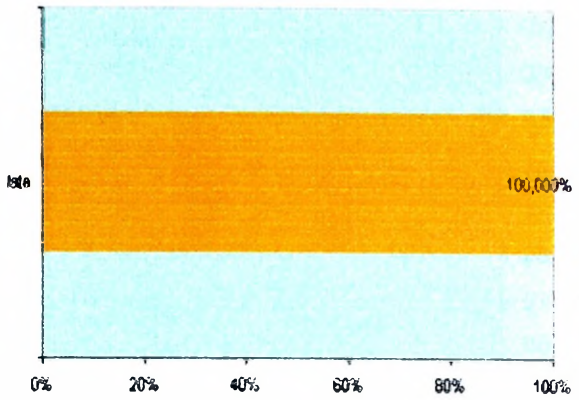
3451	63,928261		13,812259	19015,97	929,1251317
3577	126,65046		-62,722194	28171,1	-9155,129851
3703	86,081416		40,5690392	25726,254	2444,846308
3829	88,773129		-2,6917136	34299,398	-8573,144658
3955	94,511468		-5,7383389	34570,123	-270,7245182
4081	95,269865		-0,7583966	34697,131	-127,0083262
4207	102,63815		-7,3682845	35249,428	-552,2967673
4333	97,680975		4,95717463	34612,977	636,4512505
4459	96,133488		1,54748702	34613,558	-0,581442447
4585	98,693058		-2,5595703	34801,281	-187,723002
4716	88,991754		9,70130452	34297,64	503,6417104
4842	75,048286		13,9434675	20658,672	13638,96705
4968	87,224987		-12,176701	34269,278	-13610,60561
5094	103,37884		-16,153858	24213,895	10055,38328

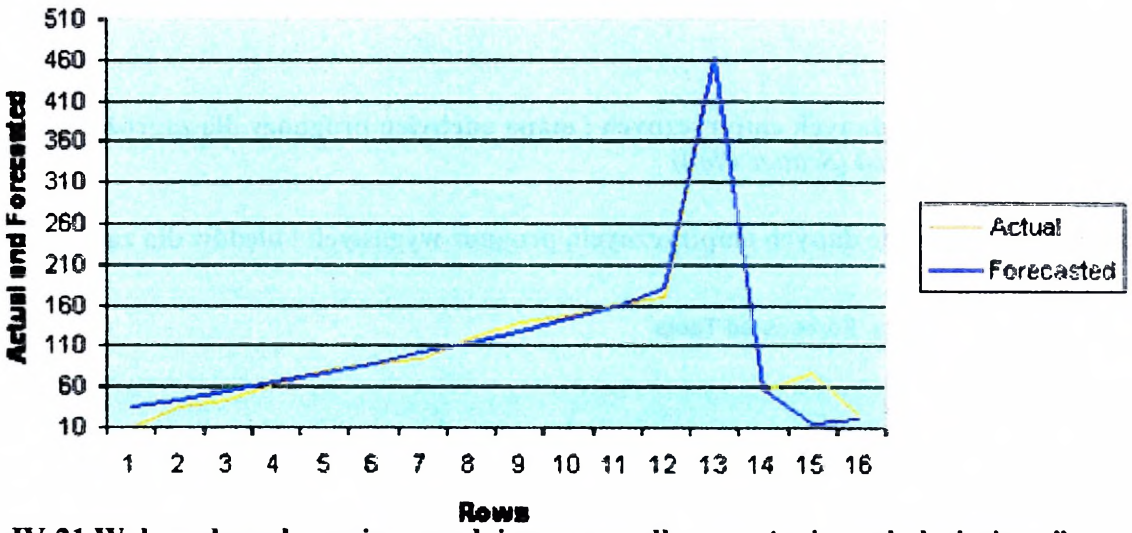
Tabela Z-IV-33. Dane wybranej sieci neuronowej (z trzema warstwami ukrytymi), dla zagrożenia robak sieciowy

Neural Network Information				
Generated by Alyuda Forecaster XL - 2009-07-17 at 10:35:03				
			Training parameters	
			Stopping condition:	0
			Training set error:	0
			Error change:	0
			Iteration No:	0
			Number of iterations:	0
			Generalization loss:	0
			Network Structure	
			Number of inputs:	1
			Number of outputs:	1
			Number of hidden units:	3
Input data types				
Types	1			
#NUM#				
Intervals	1			
MIN	1993			
MAX	2009			
Output data types				
Types	1			
#NUM#				
Intervals	1			
MIN	10			
MAX	462			
Weights				
Outputs				
1	5			
-1,8196197	2,4233596	-3,0172202	2,87378	1,9059158
Hidden				
3	4			
-14,429282	62,143228	0	0	
1,5070482	85,653336	36,925157	0	
-1,3268902	-1,4792102	-48,036358	-2,8051814	

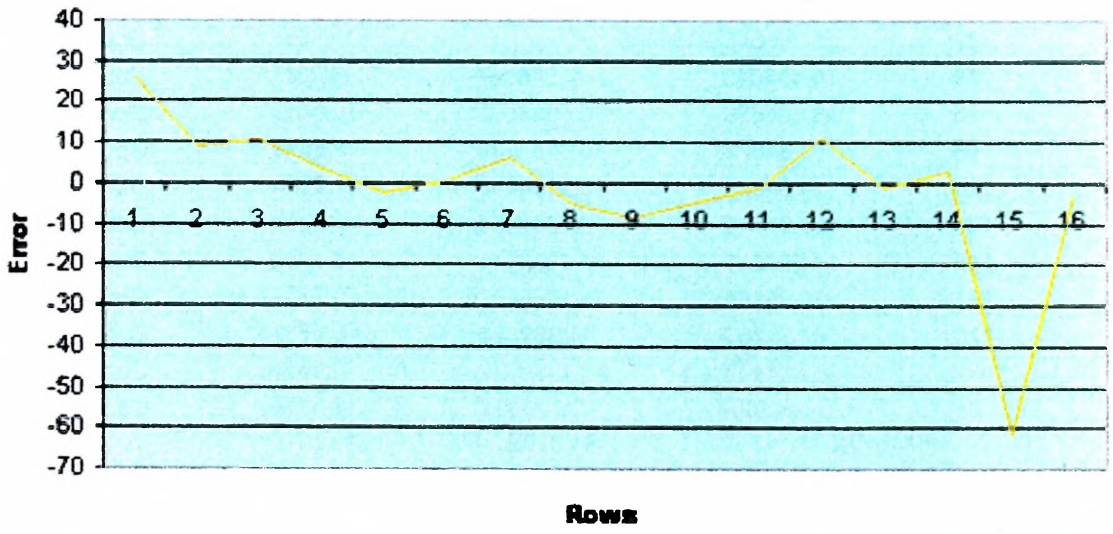
Tabela Z-IV-34. Zestawienie statystyk dla wyuczonej i sieci testowanej – ocena poprawności danych dla zagrożenia „robak sieciowy"

Summary		
	Training set	Test set
# of rows:	13	3
CCR:	n/a	n/a
Average AE:	8,7836082	14,40471
Average MSE:	318,18052	279,48838
Tolerance type:	Relative	Relative
Tolerance:	10%	30%
# of Good forecasts:	10 (77%)	2 (67%)
# of Bad forecasts:	3 (23%)	1 (33%)
RSquared: 0,9703		
Correlation: 0,9852		

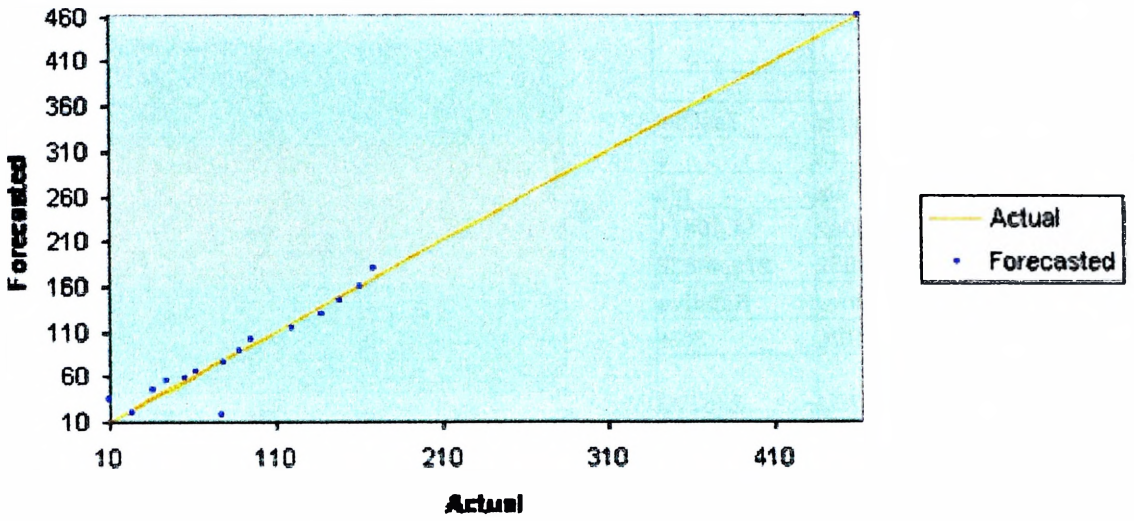




Rysunek Z-IV-21.Wykres danych empirycznych i prognozy dla zagrożenia „robak sieciowy"



Rysunek Z-IV-22. Wykres odchyleń dla zagrożenia robak sieciowy (*Deviation Graph*)



Rysunek Z-IV-23. Wykres danych empirycznych i mapa odchyleń prognozy dla zagrożenia „robak sieciowy" (*Actual vs. Forecast (Scatter Plot)*)

Tabela Z-IV-35. Zestawienie danych empirycznych, prognoz wygasłych i błędów dla zagrożenia robak sieciowy

Actual vs. Forecasted Table

Input	Target	Output			
lata	robak sieciowy	Forecast	Abs. Error	Rel. Error	Estimate
1993	10	36,133749	26,133749	261,34%	Bad
1994	36	45,053338	9,0533379	25,15%	Bad
1995	44	54,733659	10,733659	24,39%	Good
1996	62	65,196046	3,196046	5,15%	Good
1997	79	76,453043	-2,546957	3,22%	Good
1998	88	88,506659	0,5066592	0,58%	Good
1999	95	101,34672	6,3467235	6,68%	Good
2000	120	114,94945	-5,0505492	4,21%	Good
2001	138	129,27615	-8,7238498	6,32%	Good
2002	149	144,27011	-4,7298911	3,17%	Good
2003	161	159,85135	-1,1486482	0,71%	Good
2004	170	181,36263	11,362626	6,68%	Good
2005	462	460,84493	-1,1550742	0,25%	Good
2006	55	57,532822	2,5328215	4,61%	Good
2007	78	16,620726	-61,379274	78,69%	Bad
2008	24	21,198827	-2,8011727	11,67%	Bad
2009					

Sesja 3 (trzy warstwy ukryte)

Tabela Z-IV-36. Dane dla zagrożenia „robak sieciowy" i prognoza na 2009

lata	robak sieciowy	robak sieciowy
1993	10	27,38251904
1994	36	36,60220341
1995	44	46,75393769
1996	62	57,87719624
1997	79	69,9995765
1998	88	83,13362598
1999	95	97,27372784
2000	120	112,3932867
2001	138	128,4421078
2002	149	145,3403919
2003	161	162,9188116
2004	170	185,9897627
2005	462	459,9662913
2006	55	54,89872242
2007	78	20,44132117
2008	24	25,13676544
2009	33,86128	33,86127909

Tabela Z-IV-37. Wstępne przetwarzanie danych dla zagrożenia „robak sieciowy"

Summary
2 columns and 17 rows analysed.
2 columns and 17 rows are accepted for neural network training.
The following columns recognized as numeric:
lata,
robak sieciowy.
1 values recognized as missing.
Data analysis and preprocessing successfully completed.

Tabela Z-IV-38. Wstępne przetwarzanie danych ciąg dalszy raportu dla zagrożenia „robak sieciowy"

Analysis Details

Input	Target
lata	robak sieciowy
numeric	numeric
1993	10
1994	36
1995	44
1996	62
1997	79
1998	88
1999	95
2000	120
2001	138
2002	149
2003	161
2004	170
2005	462
2006	55
2007	78
2008	24
2009	

LEGEND

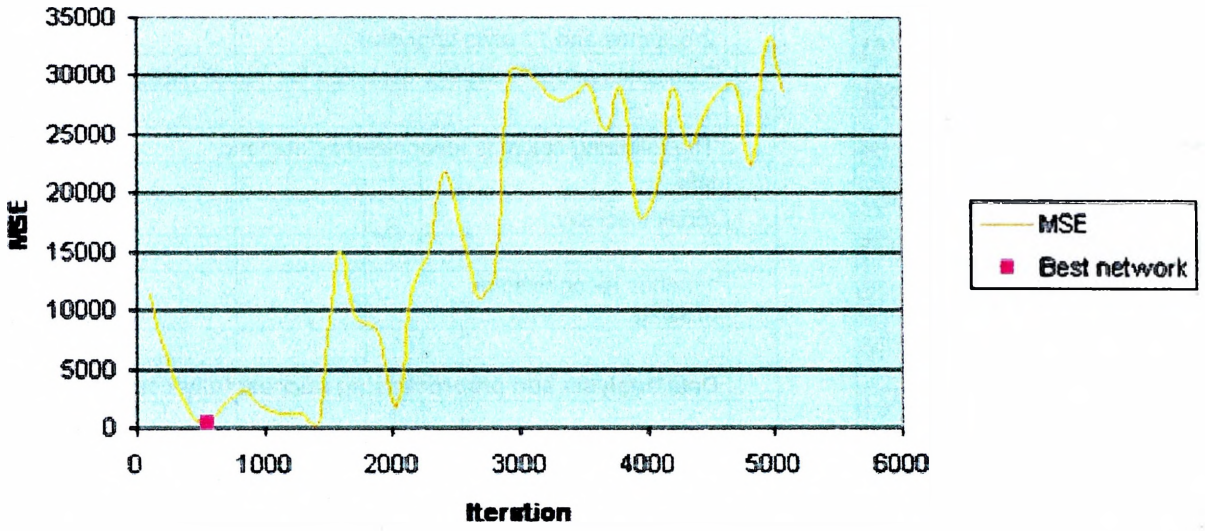
- Input values
- Target values
- Removed rows and columns
- Missing values
- Outliers

Preprocessing Details

Input	Target
lata	robak sieciowy
[n]	[n]
min: 1993	min: 10
max: 2009	max: 462
-0,4	-0,4
-0,35	-0,353982301
-0,3	-0,339823009
-0,25	-0,307964602
-0,2	-0,277876106
-0,15	-0,261946903
-0,1	-0,249557522
-0,05	-0,205309735
0	-0,173451327
0,05	-0,153982301
0,1	-0,132743363
0,15	-0,116814159
0,2	0,4
0,25	-0,320353982
0,3	-0,279646018
0,35	-0,375221239
0,4	-0,417699115

Tabela Z-IV-39. Podsumowanie trenowania sieci dla zagrożenia „robak sieciowy"

Summary								
	Problem type: regression							
	STOP TRAINING CONDITIONS							
	Training stops automatically.							
	Training stop reason: **maximum number of** iterations was achieved.							
	TRAINING RESULTS							
	Iterations trained: 5084							
	The best network was restored.							



Rysunek Z-IV-24. Wykres błędów MSE trenowanej sieci dla zagrożenia „robak sieciowy

Tabela Z-IV-40. Zestawienie błędów w kolejnych iteracjach podczas treningu sieci dla zagrożenia „robak sieciowy"

Training Error Table				
Iteration No.	AE	AE improv.	MSE	MSE improv.
101	67,715573	0	11344,924	0
269	51,889312	**15,8262608**	**5009,7225**	**6335,201527**
433	**19,751526**	32,1377853	972,92688	4036,795639
[best] - 559	9,734045	10,0174815	314,11341	658,8134721
699	30,281765	-20,54772	2130,4377	-1816,324311
841	45,475843	-15,194078	3190,9585	-1060,520784
973	29,462325	16,0135178	1703,6354	1487,323117
1131	20,354671	9,10765443	1270,7516	432,883806
1287	19,353376	1,00129503	1228,9678	41,78377571
1418	15,104283	4,24909243	362,90163	866,0661767
1573	80,388873	-65,28459	14727,691	-14364,78906
1709	48,225089	32,1637842	9401,6627	5326,027979
1885	48,1545	0,07058872	8087,5848	1314,077949
2026	28,368925	19,7855753	1823,5539	6264,03087
2158	95,994176	-67,62525	11925,781	-10102,22671
2284	56,864441	39,1297345	14669,869	-2744,088224
2416	68,372022	-11,507581	21753,384	-7083,515201
2542	69,567358	-1,1953357	16271,312	5482,071997
2668	64,609177	4,95818091	11051,394	5219,918114
2794	53,214281	11,3948959	13223,44	-2172,046075
2920	95,745928	-42,531647	30263,95	-17040,50996
3046	103,0144	-7,2684769	30412,649	-148,698967
3175	81,062858	21,9515463	29004,632	1408,017013
3301	106,4614	-25,398542	27889,126	1115,505825

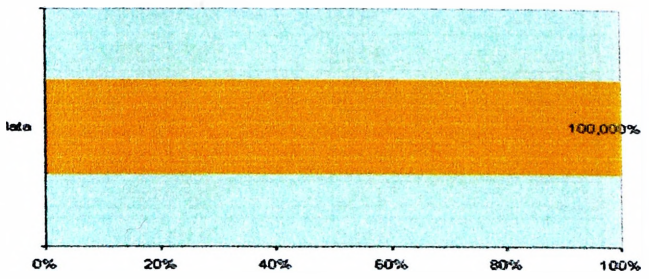
3427	78,22415	28,2372499	28403,062	-513,9357239	
3553	82,804325	-4,5801746	29180,621	-777,5596314	
3679	91,161206	-8,3568811	25332,884	3847,737328	
3813	76,726637	14,4345689	28910,18	-3577,29565	
3942	97,13295	-20,406313	18047,064	10863,11527	
4069	72,037336	25,0956142	20416,828	-2369,763729	
4195	84,373808	-12,336472	28876,742	-8459,913582	
4321	71,717291	12,6565174	24057,197	4819,544421	
4454	105,23305	-33,515759	26530,628	-2473,430469	
4580	79,013537	26,2195123	28781,552	-2250,924352	
4706	83,76706	-4,7535227	29140,422	-358,869524	
4832	75,348986	8,41807379	22473,426	6666,995465	
4958	122,03739	-46,688404	33177,958	-10704,53185	
5084	76,290319	45,7470712	28587,894	4590,063867	

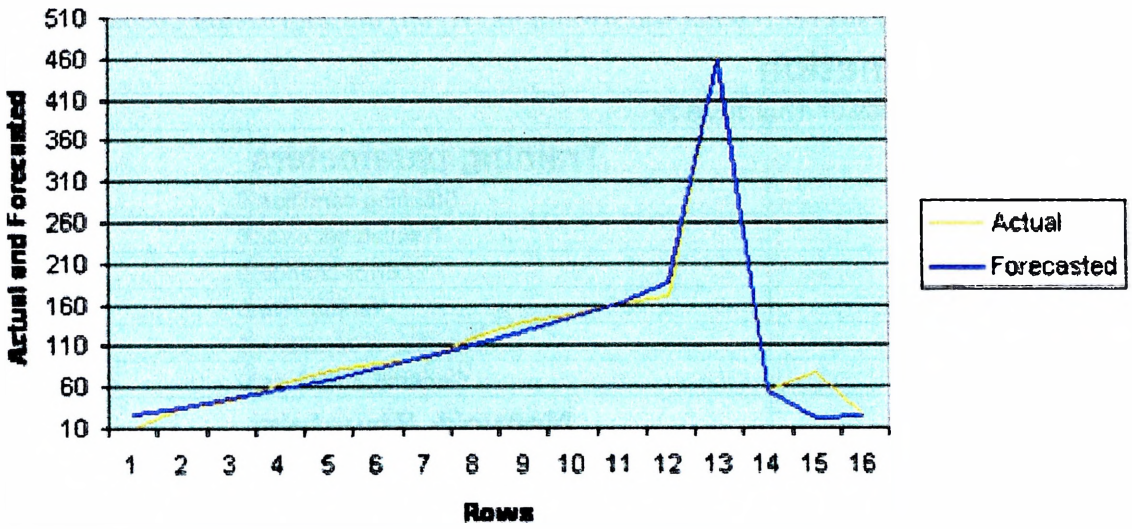
Tabela Z-IV-41. Dane o wybranej sieci (z trzema warstwami ukrytymi) dla zagrożenia „robak sieciowy”

Neural Network Information					
Generated by Alyuda Forecaster XL - 2009-07-17 at 10:46:29					
			Training parameters		
			Stopping condition:	0	
			Training set error:	0	
			Error change:	0	
			Iteration No:	0	
			Number of iterations:	0	
			Generalization loss:	0	
			Network Structure		
			Number of inputs:	1	
			Number of outputs:	1	
			Number of hidden units:	3	
Input data types					
Types	1				
#NUM#					
Intervals	1				
MIN	1993				
MAX	2009				
Output data types					
Types	1				
#NUM#					
Intervals	1				
MIN	10				
MAX	462				
Weights					
Outputs					
1	5				
-1,8456637	2,7309256	-1,9489726	2,6367418	2,775423	
Hidden					
3	4				
-13,318474	55,708139	0	0		
-3,73753	109,04776	33,686428	0		
-3,5880175	-11,874983	-53,091285	-0,9415821		

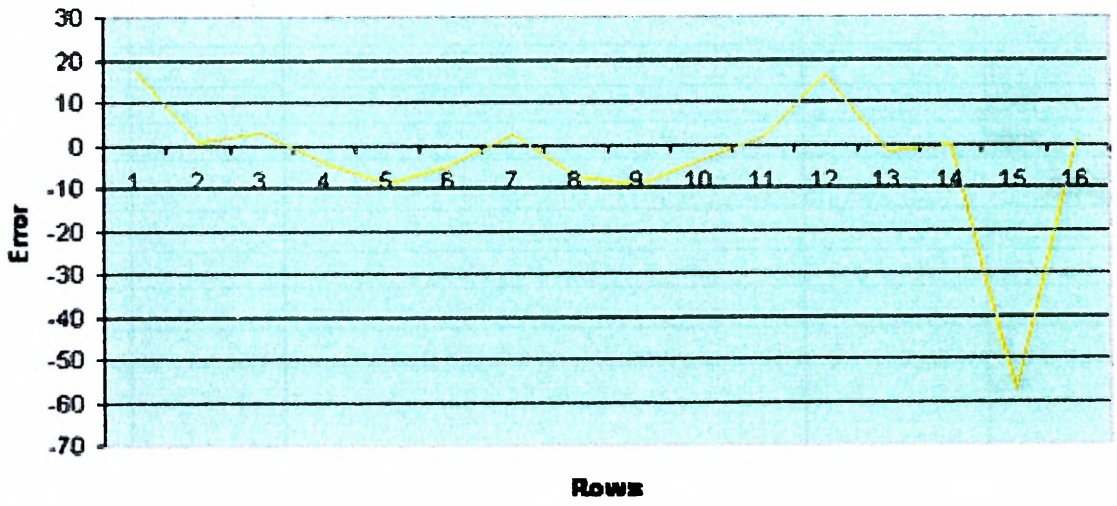
Tabela Z-IV-42. Zestawienie statystyk dla wyuczonej i przetestowanej sieci – wykres poprawności danych dla zagrożenia „robak sieciowy

Summary		
	Training set	Test set
# of rows:	13	3
CCR:	n/a	n/a
Average AE:	9,7336245	4,6760297
Average MSE:	314,12278	**31,253878**
Tolerance type:	Relative	**Relative**
Tolerance:	10%	30%
# of Good forecasts:	11 (85%)	3 (100%)
# of Bad forecasts:	2 (15%)	0 (0%)
RSquared: 0,9751		
Correlation: 0,9884		

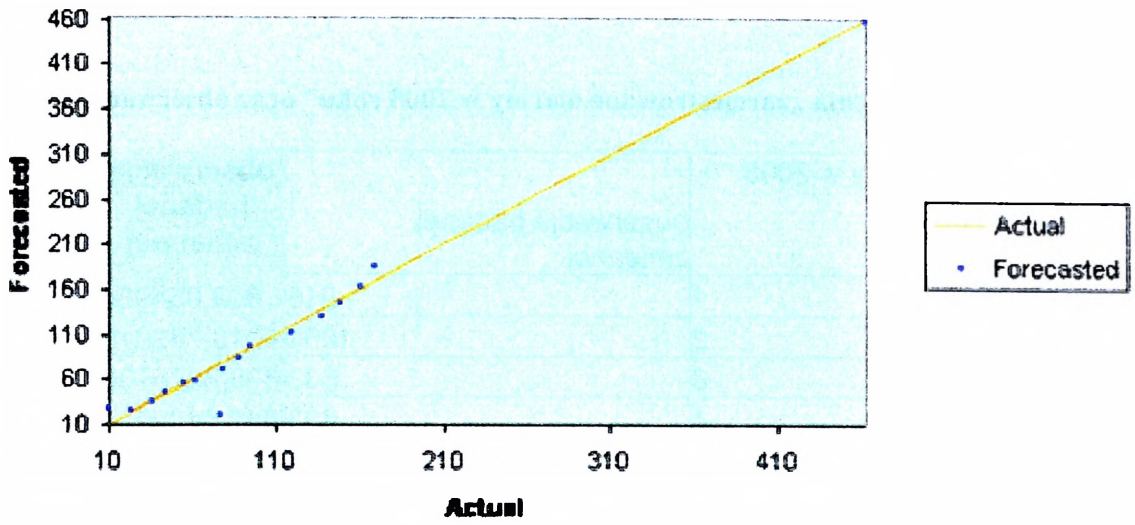




Rysunek Z-IV-25. Wykres danych empirycznych oraz prognozowanych dla zagrożenia „robak sieciowy"



Rysunek Z-IV-26. Wykres odchyleń dla zagrożenia „robak sieciowy (*Deviation Graph*)



Rysunek Z-IV-27. Wykres danych empirycznych i mapa odchyleń prognozy dla zagrożenia „robak sieciowy" (*Actual vs. Forecast (Scatter Plot)*)

Tabela Z-IV-43. Zestawienie prognoz i błędów wyuczonej sieci dla zagrożenia „robak sieciowy"

Actual vs. Forecasted Table

Input	Target	Output			
lata	robak sieciowy	Forecast	Abs. Error	Rel. Error	Estimate
1993	10	27,382519	17,382519	173,83%	Bad
1994	36	36,602203	0,6022034	1,67%	Good
1995	44	46,753938	2,7539377	6,26%	Good
1996	62	57,877196	-4,1228038	6,65%	Good
1997	79	69,999577	-9,0004235	11,39%	Good
1998	88	83,133626	-4,866374	5,53%	Good
1999	95	97,273728	2,2737278	2,39%	Good
2000	120	112,39329	-7,6067133	6,34%	Good
2001	138	128,44211	-9,5578922	6,93%	Good
2002	149	145,34039	-3,6596081	2,46%	Good
2003	161	162,91881	1,9188116	1,19%	Good
2004	170	185,98976	15,989763	9,41%	Good
2005	462	459,96629	-2,0337087	0,44%	Good
2006	55	54,898722	-0,1012776	0,18%	Good
2007	78	20,441321	-57,558679	73,79%	Bad
2008	24	25,136765	1,1367654	4,74%	Good
2009					

Sesja 4

Tabela Z-IV-44. Dane dla zagrożenia „zarejestrowane alarmy w 2008 roku" oraz obserwacje zmiennej w procesie uczenia sieci

wszystkie zarejestrowane alarmy w 2008 roku	obserwacje badanej zmiennej	**obserwacje badanej zmiennej**
1	916	802,054936
2	1061	1018,732915
3	633	635,3276706
4	893	848,8424674
5	798	799,2583978
6	786	906,8919774
7	947	947,9067778
8	846	878,7979661
9	671	672,9685348
10	755	755,8943289
11	1098	1098,249631
12	1931	1928,026455
1/2009	1967,98215	1964,40964

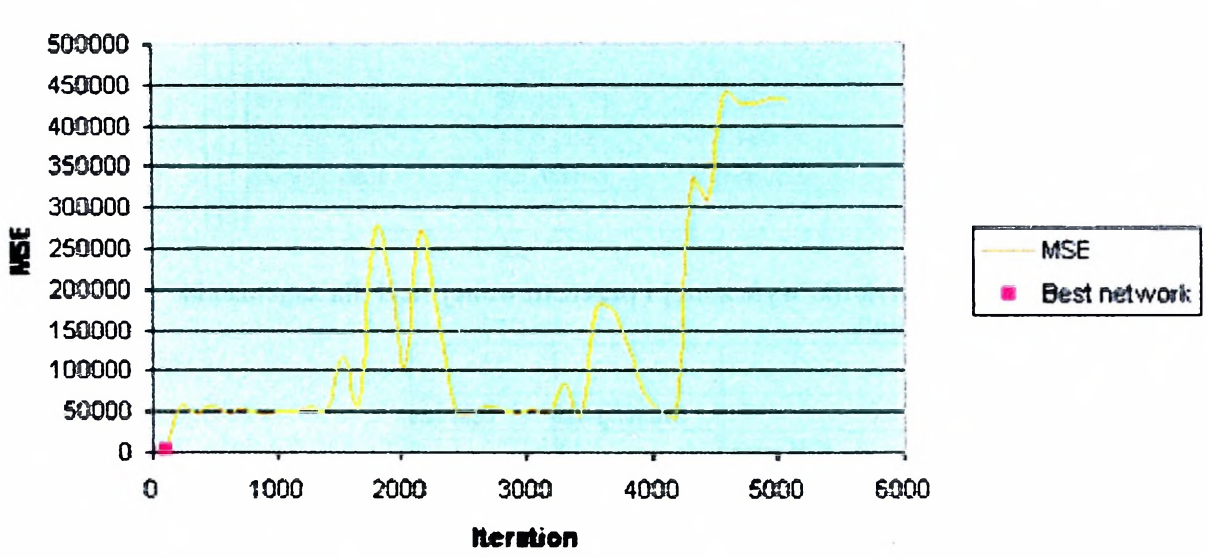
Tabela Z-IV-45. Zestawienie informacji o wytrenowanej sieci neuronowej dla zagrożenia „zarejestrowane alarmy w roku 2008"

Neural Network Information													
Generated by Alyuda Forecaster XL - 2008-07-17 at 10:41:36													
			Training parameters										
			Stopping condition:	0									
			Training set error:	0									
			Error change:	0									
			Iteration No:	0									
			Number of iterations:	0									
			Generalization loss:	0									
			Network Structure										
			Number of inputs:	13									
			Number of outputs:	1									
			Number of hidden units:	0									
Input data types													
Types	1												
1	2	3	4	5	6	7	8	9	10	11	12	sty-09	
Intervals	13												
MIN	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4	-0,4
MAX	0,4	0,4	0,4	0,4	0,4	0,4	0,4	0,4	0,4	0,4	0,4	0,4	0,4
Output data types													
Types	1												

#NUM#													
Intervals	1												
MIN	633												
MAX	1967,9821												
Weights													
Outputs													
1	14												
0,1455246	-0,5778099	0,2661533	1,5824097	0,3701463	0,5908795	0,1358841	0,0177991	0,2464866	1,2995471	0,8051143	0,5265874	3,5893691	3,8619422

Tabela Z-IV-46. Zestawienie dla trenowanej sieci dla zagrożenia „zarejestrowane alarmy w 2008 roku"

Summary	
Problem type: regression	
STOP TRAINING CONDITIONS	
Training stops automatically.	
Training stop reason: maximum number of iterations was achieved.	
TRAINING RESULTS	
Iterations trained: 5079	
The best network was restored.	



Rysunek Z-IV-28. Wykres błędu MSE dla trenowanej sieci dla zagrożenia „zarejestrowane alarmy w 2008 roku"

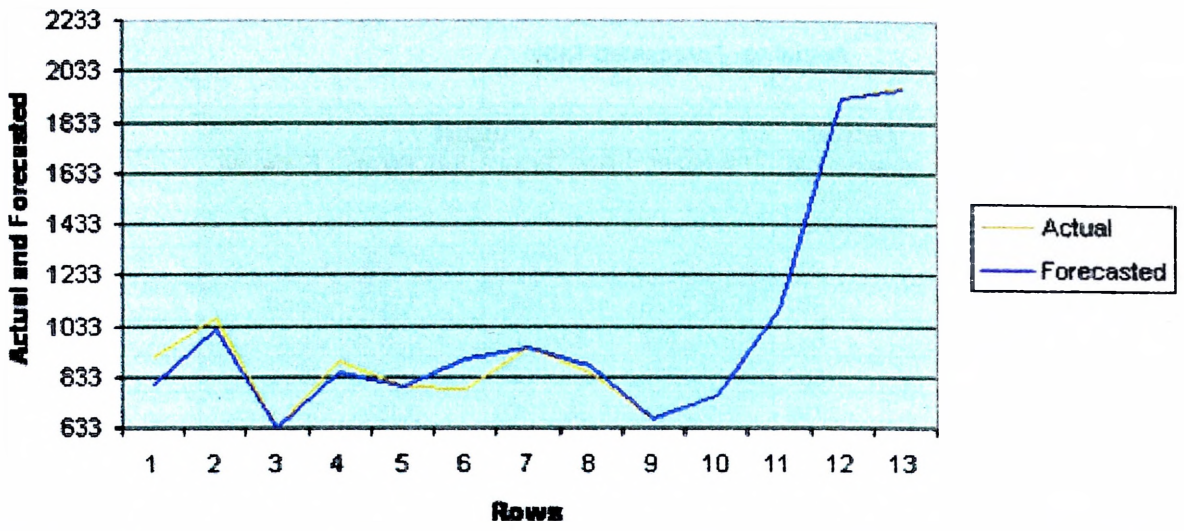
Tabela Z-IV-47. Zestawienie błędów uczonej sieci dla zagrożenia „zarejestrowane alarmy w 2008 roku"

Training Error Table				
Iteration No.	**AE**	**AE improv.**	**MSE**	**MSE improv.**
[best] - 101	**18,514815**	**0**	**1463,224**	**0**
227	165,54866	-147,03384	55431,772	-53968,5479
353	134,98059	30,5680635	48896,355	6535,416735
479	157,86766	-22,887067	54845,099	-5948,743902
605	121,13311	36,7345469	48225,854	6619,245366
736	172,8788	-51,745686	52895,881	-4670,027084
862	154,56259	18,3162086	48755,747	4140,133614

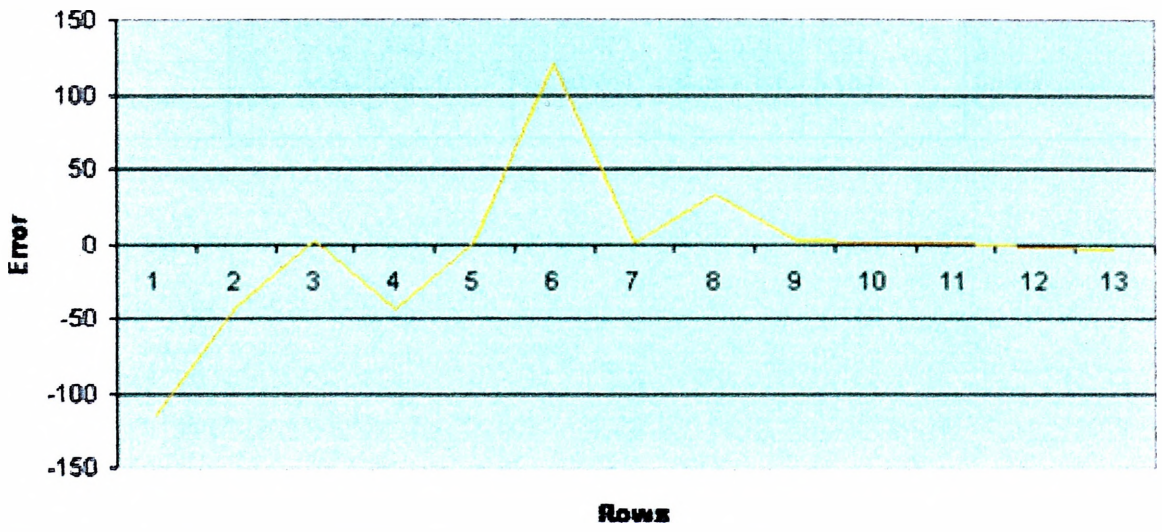
1023	150,9571	3,60549094	51553,207	-2797,459492
1155	137,58648	13,3706168	50592,276	960,9304874
1281	165,23538	-27,648893	57064,808	-6472,532139
1407	149,85193	15,3834505	52415,216	4649,592059
1533	201,76699	-51,915067	117930,22	-65515,00597
1660	135,61409	66,1528989	60894,645	57035,57746
1786	301,91695	-166,30286	273429,51	-212534,8693
1912	254,91506	47,0018967	211100,88	62328,63251
2038	189,10192	65,8131379	103813,51	107287,3747
2164	323,08879	-133,98687	272806,15	-168992,645
2290	210,3905	112,69829	177218,3	95587,85179
2424	154,03281	56,3576907	52753,328	124464,9719
2550	127,54811	26,4847079	48329,587	4423,741162
2676	171,79883	-44,250725	55581,255	-7251,667961
2802	154,97009	16,8287378	52989,826	2591,429082
2928	129,7996	25,1704966	48608,644	4381,181575
3054	161,7427	-31,943108	52738,034	-4129,38959
3180	126,16173	35,5809761	48367,342	4370,692222
3306	270,52596	-144,36424	83647,796	-35280,45391
3432	125,16338	145,362581	48302,757	35345,03838
3567	245,12934	-119,96596	179147,44	-130844,6872
3693	257,02686	-11,897519	173246,44	5901,005101
3819	178,09272	78,9341339	127254,42	45992,0224
3945	170,26177	7,83095651	70305,836	56948,58127
4071	141,22904	29,0327284	49313,117	20992,71864
4197	122,65145	18,5775935	45664,214	3648,903533
4323	400,89856	-278,24711	335661,2	-289996,9844
4449	278,67154	122,22702	309089,16	26572,03553
4575	411,96493	-133,2934	439267,98	-130178,8134
4701	350,62395	61,3409823	426439,7	12828,27689
4827	356,06698	-5,4430268	426832,56	-392,8650106
4953	392,10105	-36,034074	432528,54	-5695,976753
5079	370,04464	22,056414	428436,61	4091,929529

Tabela Z-IV-48. Zestawienie statystyk dla wyuczonej i przetestowanej sieci dla zagrożenia „zarejestrowane alarmy w 2008 roku"

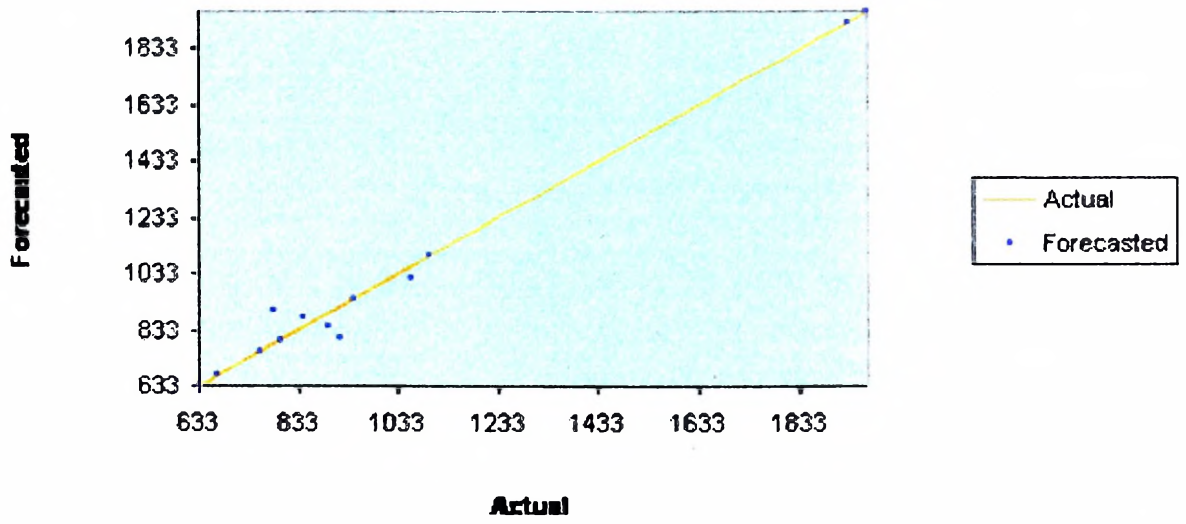
Sumary			
		Training set	Test set
	# of rows:	11	2
	CCR:	n/a	n/a
	Average AE:	18,641087	81,579531
	Average MSE:	1458,4762	8200,6883
	Tolerance type:	Relative	Relative
	Tolerance:	10%	30%
	# of Good forecasts:	10 (91%)	2 (100%)
	# of Bad forecasts:	1 (9%)	0 (0%)
RSquared: 0,9855			
Correlation: 0,9928			



Rysunek Z-IV-29. wykres dla danych empirycznych i prognoza dla zagrożenia „zarejestrowane alarmy w 2008 roku"



Rysunek Z-IV-30. Wykres odchyleń danych empirycznych dla zagrożenia „zarejestrowane alarmy w 2008 roku"



Rysunek Z-IV-31. Wykres danych empirycznych i mapa odchyleń prognozy dla zagrożenia „zarejestrowane alarmy w 2008 roku" (*Actual vs. Forecast (Scatter Plot)*)

Tabela.Z-IV-49. Zestawienie prognoz oraz błędów prognozowania dla wyuczonej sieci

Actual vs. Forecasted Table					
Input	**Target**	**Output**			
wszystkie zarejestrowane alarmy w 2008 roku	**obserwacje badanej zmiennej**	**Forecast**	**Abs. Error**	**Rel. Error**	**Estimate**
1	916	802,05494	-113,94506	12,44%	Bad
2	1061	1018,7329	-42,267085	3,98%	Good
3	633	635,32767	2,3276706	0,37%	Good
4	893	848,84247	-44,157533	4,94%	Good
5	798	799,2584	1,2583978	0,16%	Good
6	786	906,89198	120,89198	15,38%	Good
7	947	947,90678	0,9067778	0,10%	Good
8	846	878,79797	32,797966	3,88%	Good
9	671	672,96853	1,9685348	0,29%	Good
10	755	755,89433	0,8943289	0,12%	Good
11	1098	1098,2496	0,2496307	0,02%	Good
12	1931	1928,0265	-2,9735452	0,15%	Good
sty-09	1967,0	1964,4096	-3,5725096	0,18%	Good

TAKSONOMIA ZAGROŻEŃ

Funkcjonują również klasyfikacje, których zadaniem jest ułatwienie standaryzacji zagrożeń w celu ujednolicenia polityk bezpieczeństwa oraz umożliwienia porównywalności prowadzonych w różnych ośrodkach statystyk. Do niedawna statystykę zagrożeń oraz incydentów naruszających bezpieczeństwo systemów prowadzono w wielu ośrodkach na świecie, w Europie i w Polsce bez ujednolicenia klasyfikacji. Stwarzało to trudności w komparatystyce zagrożeń oraz jednoznacznej ich interpretacji.

Od kilku lat funkcjonują jednolite, międzynarodowe kryteria „*Common Language*" [1], stosowne przez CERT (*Computer Emergency Response Team*)[2] poszczególnych krajów w tym między innymi od 2001 przez polski oddział CERT. Od tego też roku stosuje się klasyfikację w rejestrowaniu incydentów naruszeń bezpieczeństwa teleinformatycznego przy czym wyróżnia się dwa typy ataków: (1) odnotowanych naruszeń bezpieczeństwa teleinformatycznego, (2) odnotowanych ataków w ujęciu zaatakowanych komputerów. Pierwsza grupa ataków obejmuje także próby włamań (naruszeń) bezpieczeństwa, druga tylko przypadki ataków zrealizowanych.

Od 2002 roku do statystyk CERT wprowadzono, ściśle wg. *Common Landuage*, cechy charakteryzujące zdarzenia: działanie (*action*), intruza oraz cel (*target*) jaki zaatakował (tabela ZV-1).

Tabela ZV-1. Klasyfikacja według CERT

	Klasyfikacja	**Charakterystyka**
Klasyfikacja CERT	Skanowanie	przegląd adresów sieciowych oraz portów sieciowych
	Atak na system operacyjny	ogół ataków na systemy operacyjne w celu przejęcia kontroli nad nimi
	Spamming	rozsyłanie niechcianej poczty elektronicznej
	Atak na serwer (WWW, DNS, inne...)	odmowa serwisu – unieruchomienie usługi
	Atak na system poczty	
	Social engineering	psychologia społeczna ukierunkowana na zdobywanie informacji o atakowanym systemie od osób pracujących z tym systemem

[1] Kryteria klasyfikacyjne wg. John'a D. Howarda'a i Thomas'a A. Longstaff'a

[2] Zespół osób powołany w ramach instytucji lub organizacji, którego zadaniem jest reagowanie na zdarzenia naruszające bezpieczeństwo sieci oraz prowadzenie działalności informacyjno-zapobiegawczej Organizacją zrzeszającą wszystkie lokalne zespoły CERT jest FIRST (Forum of Incident Response and Security Teams). W Polsce zespół CERT działa od 1996 roku (do 2000 r. jako oddział »NASK); od lutego 1997 należy do FIRST (Organizacją zrzeszającą wszystkie lokalne zespoły CERT jest FIRST (Forum of Incident Response and Security Teams).

	Nielegalne oprogramowanie	dystrybucja nielegalnego oprogramowania
	Rozpowszechnianie nielegalnych i obraźliwych treści	
	Inne	pozostałe, niemieszczące się w pozostałych kategoriach

Źródło: opracowanie własne na podstawie Raportów CERT

Tabela ZV-2. Klasyfikacja według „*Common Langueage*"

Incydent						
	Atak					
			Zdarzenie			
Napastnicy	**Narzędzia**	**Podatność na zagrożenia**	**działanie**	**obiekt**	**Nieuprawnione rezultaty**	**Założenia**
Hakerzy Nowicjusze, black Hat, Grey Hat, White Hat, Hacktivist	Fizyczny atak	Wadliwie zaprojektowany system	próbkowanie	finansowy	Powiększenie dostępu	Pokonać, przestraszyć
Terroryści państwowi, niepaństwowi	Programy nieznany agent	Błędy w konfiguracji systemu i urządzeń sieciowych	skanowanie	działanie	Ujawnienie informacji	Zyski polityczne
Napastnicy wewnętrzni	Dystrybucja oprogramowania	Niewłaściwie skonfigurowany system operacyjny	przepełnienie	dane	Fałszowanie informacji	Zyski finansowe
Profesjonalni i kryminaliści			uwierzytelnianie	komponent	Nieuprawniona zmiana informacji	Zniszczenie
			ominięcie			
			podszywanie się			
Wandale			czytanie	komputer	Kradzież źródeł	
Woyeurs			kopiowanie	sieć		
			kradzież	Internet		
			modyfikowanie			
			kasowanie			

Źródło: na podstawie: Common Language

Wyróżnienie grupy intruzów pozwala zidentyfikować i scharakteryzować napastników (tabela ZV-3.)

Tabela ZV- 3. Klasyfikacja sprawców i ich działań.

Sprawcy	**Działania**
Hakerzy	Czytanie i/lub Modyfikacja zasobów obiektu
Szpiedzy	Kradzież i kopiowanie danych w celu przekazania ich do określonego adresata
Terroryści	Modyfikacja zasobów w celu destrukcji lub wywołania efektu propagandowego.
Nieuczciwi pracownicy	Kradzież i/lub kopiowanie danych w celu udostępnienia ich konkurencji lub kompromitacji firmy z powodów osobistych
Profesjonalni przestępcy	Kradzieże i kopiowanie zasobów systemu, a także ich kasowanie i modyfikowanie w celu uzyskania korzyści majątkowej
Wandale	Bezmyślne kasowanie danych i/lub ich modyfikacja
Voyeur	Czytanie danych, czytanie i/lub kopiowanie z powodów emocjonalnych

Źródło: P.Sienkiewicz, H.Świeboda, *Analiza systemowa zjawiska cyberterroryzmu.* ZN AON.

W ramach projektu „*The European CSIRT Network – eCSIRT.net*" wypracowano zmodyfikowaną typologię ataków i jest ona obecnie z powodzeniem stosowana a obejmuje następujące typy i podtypy incydentów (tabela):

Tabela ZV-4. Typologia ataków wg. *The European CSIRT Network – eCSIRT.net*

Lp.	**Typy ataków**	**Podtyp incydentu**
1	Obraźliwe i nielegalne treści:	– spam – dyskredytacja, obrażanie – pornografia dziecięca, przemoc
2	Złośliwe (destrukcyjne) oprogramowanie	– wirusy – robaki sieciowe, – konie trojańskie, – oprogramowanie szpiegowskie, – dialery.
3	Gromadzenie informacji:	– skanowanie – podsłuch – inżynieria społeczna
4	Próby włamań:	– wykorzystanie znanych luk systemowych – próby nieuprawnionego logowania – wykorzystanie nieznanych luk systemowych
5	Włamania:	– włamania na konto uprzywilejowane – włamania na konto zwykłe – włamanie do aplikacji
6	Dostępność zasobów	– atak Dos – rozproszony Dos – Sabotaż komputerowy

7	Bezpieczeństwo informacji	– nieuprawniony dostęp do informacji – nieuprawniona zmiana informacji
8	oszustwa komputerowe	– nieuprawnione wykorzystywanie zasobów – naruszenie praw autorskich – kradzież tożsamości, podszycie się

Źródło: The European CSIRT Network – eCSIRT.net

Oczywiście funkcjonują klasyfikacje podobne, które również są oparte na kryteriach „*Common Language*" jak chociażby systematyka przyjęta w Wielkiej Brytanii i Holandii (tab. 6).

Tabela ZV-5. Klasyfikacja empiryczna wspólna według JANET Cert Anglia i CERT-NL Holandia

Klasyfikacja empiryczna, wspólna (wg JANET CERT Anglia i CERT-NL Holandia)	1. *Abusive mail*	poczta elektroniczna zawierająca obraźliwe treści;
	2. *Denial of Service*	unieruchomienie usługi;
	3. LAN *Sniffing*	podsłuchiwanie transmisji w sieci;
	4. *Probe*	sondowanie atakowanego systemu, np. poprzez skanowanie;
	5. *Root compromise*	uzyskanie uprawnień super użytkownika
	6. Spam	rozsyłanie niechcianej poczty elektronicznej;
	7. Trojan	Trojańskie konie
	8. *Unauthorized use*	nieuprawnione użycie;
	9. Virus	wirusy komputerowe;
	10. *Warez*	rozpowszechnianie nielegalnego oprogramowania.

Źródło:

Wśród wyróżnionych typów ataków występują (tabela ZV-6.):

Tabela ZV-6. Typy ataków

Typ ataków	**Odnotowane źródła ataków**	**Źródła zgłoszeń incydentów**
Próba włamania do systemów	Ośrodki edukacyjne	Użytkownik krajowy
Włamanie do hosta	Dostarczyciele usług internetowych ISP (*Internet Service Provider*)	Użytkownik zagraniczny
Skanowanie hosta	Firmy	CERT lub inna instytucja ds. bezpieczeństwa
Skanowanie sieci	Inne	
Ataki DoS	Nieustalone	
Ataki na serwer WWW (podmiana strony)		

Mail bombing
Skanowanie firewalli
Inne (nielegalne oprogramowanie, social engeenering)

Źródło: opracowanie własne

Charakterystyka typów zagrożeń najczęściej stosowanych podczas ataków

A. Atak siłowy – zgadywanie (łamanie) haseł

Pierwszą metodą jaką zwykle stosują hakerzy jest zgadywanie haseł chroniących dostęp do serwera. W tym celu używa się specjalnych programów do łamania haseł (tzw. crack), które zawierają w sobie całe słowniki w różnych językach. Programy te automatycznie podstawiają kolejne słowa podczas próby dostępu do systemu, aż do skutku. Zwracając uwagę na fakt, że zwykle hasła są proste (najczęściej jest to imię użytkownika konta lub jego inicjały), zadanie w wielu wypadkach nie jest trudne. Często zdarza się, że pewne ważne konta w ogóle nie są chronione hasłami.

B. Podszywanie się lub maskarada

Włamywacze komputerowi stosują często zabieg zwany podszywaniem się lub maskaradą (IP-spoofing, ARP-spoofing, Mail-spoofing i inne). Po zdobyciu odpowiednich informacji o sieci atakujący może podszyć się pod jeden z komputerów, któremu serwer „ufa" (poprzez podanie jego numeru IP jako swojego) i dostać się na niego. Np. atakujący może wysłać dane ze sfałszowanym adresem poczty elektronicznej, które zostaną przez serwer przyjęte. W tych danych może być ukryty np. „koń trojański" – polecenie, które uruchomi program przeszukujący dysk serwera, odnajdzie plik z kontami i hasłami użytkowników i wyśle zawarte w nim dane zwrotnym mailem do fałszywego nadawcy.

Tak samo można przeprowadzić tzw. Web-spoofing, gdzie atakujący podszywa się pod adres serwera WWW, z którego atakowany serwer ściąga informacje. Atakujący przejmuje prośbę o przesłanie żądanej strony WWW od atakowanego i przekazuje do prawdziwego adresata. Po otrzymaniu tej strony odpowiednio do swych zamiarów i potrzeb modyfikuje lub podmienia ją i przekazuje do odbiorcy. W ten sposób może stale wprowadzać w błąd np. jakąś firmę grającą na giełdzie podając fałszywe wyniki notowań akcji i w konsekwencji – doprowadzić ją do poważnych trudności albo nawet bankructwa.

Podszycie się pod legalnego użytkownika systemu informatycznego umożliwia napastnikowi:

- bezpośredni, nieautoryzowany dostęp do chronionych danych firmy, instytucji lub korporacji;

– dalszą penetrację systemu i – w następnej kolejności – pojawienie się kolejnych zagrożeń.

Największe niebezpieczeństwo podszywania się stanowi fakt, że znacznie opóźnione jest wykrycie samego ataku, co istotnie utrudnia wykrycie i identyfikację napastnika. Wynika to z faktu, że podszywający się jest identyfikowany jako „swój", a zatem w systemie nie zauważa się, że pojawił się ktoś „nieznany".

Tabela ZV-7. Rodzaje podszywania się

Rodzaj	**Scenariusz**	**Jak to możliwe?**	**Zapobieganie**
e-mail	Wysłanie podrobionego e-maila z fałszywym wierszem „od:" do serwera SMTP	Brak uwierzytelniania w SMTP	Sprawdzać źródłowy adres IP komunikatu lub używać podpisów cyfrowych
Przekaźnik poczty anonimowej	Napastnik wysyła e-mail z konta na przekaźniku poczty anonimowej	Brak uwierzytelniania w SMTP	Używać podpisów cyfrowych
login	Wykorzystanie czyjejś nazwy użytkownika i hasła do dostania się do hosta	Brak ostrożności przy hasłach	Chronić hasła lub używać silnego uwierzytelniania
rutownie	Wysłanie podrobionych pakietów RIP lub ICMP do routera lub pakietu w trybie source router do hosta	Brak uwierzytelniania w protokołach RIP, przekierownie ICMP, trybie source routed	Nie używać tych protokołów w komunikacji z niezaufanymi sieciami
partner	Wysłanie podrobionego e-maila do Internie z prośbą o zmianę nazwy domeny internetowej lub podmianę adresu IP	Internie nie stosuje pełnego uwierzytelniania, chyba że żąda tego klient	Zapewnić uwierzytelnianie zmian domeny w InterNIC
Spoofing DNS	Wysłanie nieproszonej odpowiedzi z podrobioną nazwa domeny i adresem do serwera DNS ofiary	Brak uwierzytelniania w DNS	Używać zmodyfikowanego DNS, który nie buforuje wpisów
Adres IP	Wysłanie pakietu z podrobionym IP do „ufającego" hosta	Adres źródłowy rzadko sprawdzany	Zablokować dostęp z zewnątrz przez zaufane wewnętrzne adresy
Przejęcie kontroli nad sesja	Napastnik wstawia podrobione pakiety do zestawionej sesji, przykładowe narzędzia :HUNT i Juggernaut	Uwierzytelnianie już było	Szyfrować sesje
Spoofing WWW	Napastnik sporządza kopię całej strony internetowej, ruch przechodzi przez komputer napastnika, co pozwala mu śledzić	W ataku „man –in-the-middle" napastnik przepisuje wszystkie adresy URL ze strony internetowej, tak, że	Wyłączyć obsługę JavaScript zwrócić uwagę, by w przeglądarce była wyświetlana linia

	działania ofiary, przechowywać hasła i numery kont	kierują one ofiarę na serwer napastnika	adresu, kontrolować wyświetlany adres URL

Źródło: www.symantec.pl

C. Podsłuchiwanie (Sniffing)

Podsłuch elektroniczny często jest uznawany za najbardziej niebezpieczne zagrożenie występujące w sieciach informatycznych. Większość informacji, np. w sieci internetowej jest przekazywana otwartym tekstem, a bywa, że nawet nie są szyfrowane informacje poufne i tajne. Atakujący może zatem zastosować monitoring ruchu w danej sieci i przechwycić interesującą transmisję pomiędzy poszczególnymi maszynami.

Jednym ze sposobów podsłuchu jest przechwyt elektromagnetyczny. Przechwyt niejawnej informacji następuje poprzez szerokopasmowe superczułe odbiorniki radiowe, umożliwiające odbiór sygnałów emitowanych w postaci fal radiowych przez niektóre elementy systemów informatycznych. Celem podsłuchu najczęściej nie jest bezpośredni dostęp do transmitowanych danych. Przechwycenie transmisji pozwala zdobyć np. hasło użytkownika w momencie jego logowania się do serwera, aby następnie podszyć się pod niego i zdobyć dostęp do wybranego komputera w sieci. Innym celem podsłuchu może być identyfikacja topologii sieci, poprzez analizę informacji sterującej, zawartej w przechwyconych (podsłuchanych) pakietach. Znajomość topologii sieci jest bowiem elementem podstawowego rozeznania przed podjęciem dalszych ataków, prowadzących do celu zamierzonego hakera.

D. Szukanie dziur, tylne drzwi (back door)

Sprawdzanie istnienia luk bezpieczeństwa w systemie jest podstawowym kierunkiem ataku każdego włamywacza. Luki te związane są z błędami w oprogramowaniu lub z błędną konfiguracją systemu (niektóre usługi dają wtedy możliwość bezpośredniego wejścia do systemu). Atakujący posługuje się zwykle podczas takiego ataku specjalnymi skanerami podatności – złożonymi programami sprawdzającymi wybrany system na okoliczność istnienia takich luk. Najbardziej znanym, chociaż aktualnie już mocno przestarzałym takim skanerem jest program SATAN, napisany specjalnie dla administratorów systemów komputerowych, aby mogli oni sprawdzać poziom bezpieczeństwa swych serwerów.
Zaprojektowane jako cenne narzędzie użytkowe skierowane przeciwko działalności hakerów, programy tego typu stały się bronią w rękach włamywaczy komputerowych.

E. Odmowa świadczenia usług (Denial of Service)

Często samo włamanie do sieci nie jest tak groźne, jak jego destabilizacja. Grupa ataków określana mianem Denial of Service (DoS) daje sposobność atakującym do wyłączania na serwerze sieci różnych usług, takich jak np. poczta elektroniczna czy WWW. Atak polega na wysyłaniu dostatecznie dużych strumieni informacji, które powodują przeładowanie (całkowite zapełnienie, „zatkanie") pamięci serwera, a w konsekwencji jego destabilizację. Jednym z najbardziej znanych ataków tego typu jest tzw. SYNflood attack. Polega on na wysyłaniu dużej ilości pakietów inicjujących połączenie dla wybranej usługi (np. poczta, FTP). Serwer nie nadąża z realizacją tych połączeń i blokuje dostęp do danej usługi. W ten sposób hakerzy wielokrotnie już paraliżowali działanie poczty elektronicznej na serwerach dostawców Internetu.

Inne znane i stosowane typy ataku prowadzące do blokowania usług to broadcast storm oraz smurf attack.

Pierwszy z tych ataków prowadzi do tzw. zalewania komunikatami, co wymusza oddawanie zasobów serwera do obsługi komunikatów, a to w konsekwencji prowadzi do jego nadmiernego obciążenia, a nawet zablokowania. Atak polega na odpowiednim spreparowaniu komunikatów sieciowych, powodujących ich lawinowe powielanie.

Drugi z ataków, smurf attack, często wykorzystywany w intersieci, polega na wysyłaniu pakietów ICMP ECHO ze sfałszowanym adresem nadawcy (fałszywym adresem jest, oczywiście, atakowany). Wszystkie komputery w tej sieci odpowiadają pakietami ICMP ECHO REPLAY na adres ofiary.

Bardzo poważnym zagrożeniem, wykorzystującym wiele komputerów w skoordynownym ataku mającym na celu wyczerpanie przepustowości rutera i zasobów stosu sieciowego, a w rezultacie zerwanie łączności jest Atak Distributed Denial of Sernice (DDos). Prowadzi to do stworzenia sieci komputerów do ataku Dos prze włamanie się do tych komputerów, zdobycie uprawnień root, zapewnienie zdalnej kontroli i zainstalowanie oprogramowania służącego do ataku. W kolejnym kroku nasteruje wysłanie do wszystkich przejętych komputerów pakietów z instrukcjami o typie ataku, czasie jego trwania i adresie celu. Następuje wysyłanie pakietów (z fałszywymi adresami źródłowymi) do ofiary przez siec komputerów DDos.

Tabela ZV-8. Charakterystyka ataków Denial of Service

Atak	Dysk	Pasmo	Wewnętrzna struktura danych lub przepełnienie bufora	Cykl CPU lub załamanie	Opis
Przesyłanie dużych plików przez FTP	X				Wypełnia dysk danymi-śmieciami
Spowodowanie wpisu obszernych komunikatów o błędach do dziennika	X		X	X	Przepełnia dysk lub bufor
SYN Flood			X		Zamyka port na krótki czas
Teardrop			X	X	Wykorzystuje nachodzące na siebie fragmenty pakietów IP
Smurf		X			Przekierowuje broadcast, jako źródło podaje adres IP ofiary
Snork		X			Wysyła fałszywy komunikat o błędzie do portu 135 w NT
Bomba UDP		X		X	Fałszywy pakiet pomiędzy portami echo i chargen
Atak OOB			X	X	Użycie podrobionych wartości istotnych wskaźników danych
Ping od Death			X	X	Przepełnienie bufora datogramami IP
Flood Ping				X	Zalewa sieć
WinNuke		X	X	X	Wysyła śmieci do portu 139 w NT
land			X	X	Podaje jako źródło adres ofiary
Bomby e-mailowe, spam	X			X	Zapycha serwer/bramkę pocztową lub skrzynkę użytkownika

Źródło: www. symantec.pl

F. Inżynieria Społeczna (Social Engineering)

Inżynieria społeczna polega na tym, że zanim haker dokona właściwego ataku na wybraną sieć, często przeprowadza specjalny wywiad na temat wybranej organizacji, firmy lub korporacji, np. zdobywa różnymi sposobami informacje na temat zatrudnionych, konfiguracji sieci, zasobów systemu, haseł użytkowników itp. Często wykorzystuje element zaskoczenia, np. dzwoniąc do administratora sieci i podając się za ustawionego wyżej

w hierarchii pracownika prosi o zmianę hasła na swoim koncie albo podając się za osobę upoważnioną, prosi jakiegoś pracownika o przesłanie w sieci określonego raportu pod fałszywy adres.[3]

Wśród stosownych metod socjotechnicznych możemy wyróżnić kilkanaście sposobów (tabela ZV-8):

Tabela ZV-9. Metody socjotechniczne

Lp	Typ ataku	Charakterystyka
1	Atak z fałszywa ankietą	Obietnica wygrania wycieczki do egzotycznych krajów lub innej nagrody, łatwego zysku po udzieleniu odpowiedzi na kilka pytań
2	Atak z podszywaniem się	Podawanie się za osobę uprawniona i żądanie informacji, wykorzystanie fałszywego identyfikatora, ubioru służb porządkowych
3	Atak nieustający	Ciągłe nękanie ofiary poczuciem winy, onieśmielanie i inne negatywne oddziaływania, by zdobyć informacje
4	Atak z podpuszczeniem	Wypowiadanie kłamstw i niedorzeczności, by zdobyć informacje w odpowiedzi
5	Atak na ignoranta	Nakłonienie kogoś, by wyjaśnił, zaprzeczył lub uzupełnił „pseudowiedzę" napastnika
6	Atak z przynętą	Wykorzystanie atrakcyjności seksualnej w celu zdobycia informacji lub dostępu
7	Atak przez łapówkę	Użycie zwykłego przekupstwa
8	Atak z Help Desk	Podszycie się pod obecnego lub nowego użytkownika potrzebującego pomocy, by zdobyć dostęp do sieci lub sewera
9	Atak z wmieszaniem się w tłum	Spotkania i imprezy firmowe SA znakomitym miejscem zdobycia informacji i dostępu. Wmieszanie się w grupę pracowników i udawanie jednego z nich.
10	Atak brutalny	Z użyciem siły, zastraszenie , grożenie bronią , szantaż
11	Atak prze obserwację	Rejestrowanie aktywności i działań ludzi w czasie, dostaw towarów itp.

Źródło: www.symantec.pl

[3]A. Barczak, T.Sydoruk *„Bezpieczeństwo systemów informatycznych zarządzania"*, Dom Wydawniczy "Bellona", Warszawa 2003, s.43-48.

Tabela ZV-10. Zanotowane incydenty.

Typ incydentu	Charakterystyka	2003	2004	2005	2006	2007	2008
1. Obraźliwe i nielegalne treści		**4,8%** 1	**11,5%** 0	**11,2 0**	**36,6**	**25,81**	
Spam	Elektroniczne wiadomości rozsyłane bez zgody adresata. Adresat nie oczekuje na wiadomość.	48	130	275	857	531	466
Dyskredytacja, obrażanie	Materiały rozpowszechniane drogą elektroniczną o treści obraźliwej lub niezgodnej z prawdą.	2	3	8	21	10	
Pornografia dziecięca, przemoc	Pornografia i przemoc.	6	7	0	8	3	
2. Złośliwe oprogramowanie		**6,7%** 0	**13,5%** 3	**23,6**	**14**	**13,99**	
Wirus	Ciąg instrukcji napisany w celu spowodowania szkód w systemach komputerowych, dołączający się w sposób utajony do programów i przenoszący się wraz z ich kopiami na inny komputer.	32	57	11	28	16	3
Robak sieciowy	Program, który mnoży się w sposób nie kontrolowany w sieci komputerowej.	41	89	462	55	78	24
Koń trojański	Program, który nadużywa zaufania użytkownika wykonując bez jego wiedzy dodatkowe, szkodliwe czynności.	7	16	117	191	105	104
Oprogramowanie szpiegowskie	Program zbierający dane o użytkowniku bez jego zgody a często nawet wiedzy.	0	0	0	3	7	
Dialer	Prosty program łączący użytkownika Internetu ze stronami tematycznymi, zdolny do samodzielnego kopiowania się oraz wpisywania w rejestr.	0	0	3	0	3	

Typ incydentu	Charakterystyka	2003	2004	2005	2006	2007	2008
3. Gromadzenie informacji		**81,5%** 0	**54,7%** 1	**51,9 0**	**27,4**	**24,72**	**26,84**
Skanowanie	Polega na wysyłaniu przez osobę nieupoważnioną określonych zapytań do skanowanych komputerów po to, by uzyskać informacje umożliwiające włamanie.	976	659	1292	658	511	466
Podsłuch	Sniffing, jedna z technik przechwytywania danych, trudna do wykrycia.	0	0	6	2	0	8
Inżynieria społeczna	Zdolność do uzyskiwania informacji o kimś lub umiejętność spowodowania, aby określona osoba zrobiła to, czego się od niej oczekuje. Wykorzystywana przy atakach w sieci.	0	9	7	5	9	8
4. Próby włamań		**0,4%** 2	**2,5%** 3	**4,6 0**	**3,7**	**4,65**	**5,40**
Wykorzystanie znanych luk systemowych	Luki i niedopracowania systemu wykorzystane są do uzyskania dostępu do komputera czy danych ofiary.	1	6	18	28	60	24
Próby nieuprawnionego logowania	Użycie niewłaściwego identyfikatora i/lub hasła po to, by uzyskać dostęp do zabezpieczonych usług lub zasobów.	1	21	99	62	36	62
Wykorzystanie nieznanych luk systemowych	Wykorzystanie luk systemowych bez wiedzy o ich istnieniu, przypadkowa ingerencja.	1	1	0	0	1	0
5. Włamania		**1,6%** 11	**2,4%** 7	**0,7 0**	**0,6**	**1,61**	**4,51**
Włamanie na konto uprzywilejowane	Ingerencja, wejście, znalezienie drogi dostępu do obszarów danych, informacji nieprzeznaczonych dla danego użytkownika. Obejście zabezpieczeń systemowych czy złamanie hasła blokującego dostęp.	6	16	9	3	10	6
Włamanie na konto zwykłe		2	3	7	**8**	19	16

Typ incydentu	Charakterystyka	2003	2004	2005	2006	2007	2008
Włamanie do aplikacji		0	3	2	1	4	57
6. Dostępność zasobów		**1,7%** 0	**6,3%** 0	**1,2** **0**	**1,7**	**1,90**	**1,45**
Atak blokujący serwis (DoS)	Atakiem DoS/DDoS określamy sytuację, w której zamierzone działanie osoby niepowołanej powoduje, że określone usługi stają się niedostępne bądź dostęp do nich jest utrudniony. Do takich nieprawidłowych działań należy chociażby wysyłanie dużej ilości przesyłek pocztowych na czyjeś konto e-mail czy zasypywanie mnogością pytań danego serwera www.	10	15	13	20	**8**	4
Rozproszony atak blokujący serwis (DDoS)		10	62	14	19	32	22
Sabotaż komputerowy	Sabotaż sprzętu komputerowego i oprogramowania mający na celu naruszenie integralności danych.	0	0	1	1	0	0
7. Bezpieczeństwo informacji		**1,3%** 0	**0,3%** 0	**0,1** **0**	**0,2**	**0,52**	**0,39**
Nieuprawniony dostęp do informacji	Skorzystanie z zabronionego, nieuprawnionego dostępu do informacji.	16	2	2	3	4	5
Nieuprawniona zmiana informacji	Wprowadzenie zmian w danych, do których nie ma się dostępu.	0	2	1	2	4	1
8. Oszustwa komputerowe		**1,8%** 0	**8,4%** 0	**5,5**	**14,8**	**26,42**	**40,70**
Nieuprawnione wykorzystanie zasobów	Wykorzystanie danych lub informacji zdobytych w sposób nielegalny lub wykorzystanie danych, których rozpowszechnianie jest niedozwolone.	15	44	26	23	14	3

Typ incydentu	Charakterystyka	2003	2004	2005	2006	2007	2008
Naruszenie praw autorskich	Podszywanie się pod autora, nielegalne rozpowszechnianie i kopiowanie materiałów.	4	29	31	23	135	316
Kradzież tożsamości, podszycie się	Podawanie się, przedstawianie za inną osobę, która nie wyraża na to zgody czy komputer w celu uzyskania dostępu do danych.	2	30	79	304	403	400
9. Inne	Inne incydenty, które nie zostały wyodrębnione w tabeli.	**0,2%** 2	**0,3%** 4	**1,2** **31**	**0,9** **21**	**0,38** **8**	**0,56** **10**

Źródło: opracowanie własne na podstawie danych CERT.

Tak skonstruowana klasyfikacja odzwierciedla charakter coraz bardziej złożonych typów ataków. Śledząc przebieg zmian możemy wyróżnić pewne trendy szczególnie poddając obserwacji dane liczbowe i jakościowe charakterystyki zagrożeń.

TYPOWE PRZYKŁADY ZDARZEN Z GRY WOJENNEJ RAND
„The Day After…in Cyberspace"

Lp.	Numer zdarzenia	Typ ataku	Kategoria broni	Atakowany ośrodek strategiczny
3.	Przerwa w zasilaniu w energię elektryczną	Bomba logiczna	Obezwładniająca	Podstawy systemu
4.	Wyłączenie Publicznej Sieci Telekomunikacyjnej w stanach Karolina/Oregon	Pulapka (*trap door*)	Obezwładniająca	Podstawy systemu
5.	Ft. Lewis Mass Diallng Attack	Przeciążenia informacyjne (*info overload*)	Obezwładniająca	Mechanizm obronny
6.	Wybuch w rafinerii ARAMCO	Bomba logiczna	Obezwładniająca	Podstawy systemu
8.	Katastrofa szybkiego pociągu pasażerskiego	Bomba logiczna	Obezwładniająca	Infrastruktura
9.	Oświadczenie Ambasadora Iranu	Rozmowy	Przejmująca zarządzanie	Przywódcy
11.	Raport CNN „*Financial Targets*" (Cele finansowe)	Perswazja	Przejmująca zarządzanie	Ludność
12.	Publikacja prasowa: Konsorcjum na rzecz pokoju planetarnego (*Consortim for planetarny Peace* – CPP)	Slogany	Przejmująca zarządzanie	Ludność
14.	Przekłamania na wykazie tymczasowej dyslokacji sił	Wirus	Obezwładniająca	Mechanizm obronny
15.	Niesprawność bankomatu	Bomba logiczna	Obezwładniająca	Podstawy systemu
16.	Sprawozdanie CNN z tajnego posiedzenia rządu	Perswazja	Przejmująca zarządzanie	Ludność
18.	Demonstracje CPP	Slogany	Przejmująca zarządzanie	Przywódcy
19.	Katastrofa samolotu pasażerskiego	Bomba logiczna	Obezwładniająca	Infrastruktura
20.	Przejęcie Saudi News	Spamming	Przejmująca zarządzanie	Ludność
21.	Niesprawność Saudyjskiej PSN (Publicznej Sieci Telekomunikacyjnej)	Bomba logiczna	Obezwładniająca	Podstawy systemu
22.	Saudyjska TV zapowiada wspaniały wyczyn	Dezinformacja	Przejmująca zarządzanie	Ludność
23.	Atak w ramach Wojny Informacyjnej (*Information Warfare Attack*) przeciwko bazom amerykańskim	Próby wielokanałowe	Obezwładniająca	Mechanizm obronny
24.	Konferencja informacyjna CPP	Spór	Przejmująca zarządzanie	Ludność
25.	Niesprawność wspólnej stacji radiolokacyjnej obserwacji okrężnej oraz obserwacji atakowanego celu	Worm - Mikrob	Obezwładniająca	Mechanizm obronny
26.	Wyłączenie telefonów w D.C. / Baltimore	Bomba logiczna	Obezwładniająca	Podstawy systemu
27.	Fluktuacja na Giełdzie w Chicago	Bomba logiczna	Obezwładniająca	Podstawy systemu
28.	Przejęcie wiadomości	*Spooling*	Przejmująca zarządzanie	Ludność

CHARAKTERYSTYKA ZŁOŚLIWEGO OPROGRAMOWANIA[1]

Wirus – program lub fragment wrogiego wykonalnego kodu, który dołącza się, nadpisuje lub zamienia inny program w celu reprodukcji samego siebie bez zgody użytkownika. Ze względu na różne rodzaje infekcji wirusy dzielą się na:

- wirusy gnieżdżące się w sektorze rozruchowym twardego dysku (ang. *boot sector viruses*),
- wirusy pasożytnicze (ang. *parasitic viruses*),
- wirusy wieloczęściowe (ang. *multi-partite viruses*),
- wirusy towarzyszące (ang. *companion viruses*),
- makro wirusy (ang. *macro viruses*).

Robaki – wirusy rozmnażające się tylko przez sieć. Nie potrzebują programu „żywiciela" tak jak typowe wirusy. Często powielają się pocztą elektroniczną.

Wabbit – program rezydentny nie powielający się przez sieć. Wynikiem jego działania jest jedna określona operacja np. powielanie tego samego pliku aż do wyczerpania zasobów pamięci komputera.

Trojan – nie rozmnaża się jak wirus, ale jego działanie jest równie szkodliwe. Ukrywa się pod nazwą lub w części pliku, który użytkownikowi wydaje się pomocny. Oprócz właściwego działania pliku zgodnego z jego nazwą, trojan wykonuje operacje w tle szkodliwe dla użytkownika np. otwiera port komputera, przez który może być dokonany atak włamywacza (hackera).

Backdoor – przejmuje kontrolę nad zainfekowanym komputerem umożliwiając wykonanie na nim czynności administracyjnych łącznie z usuwaniem i zapisem danych. Podobnie jak trojan, backdoor podszywa się pod pliki i programy, z których często korzysta użytkownik. Umożliwia intruzom administrowanie systemem operacyjnym poprzez Internet. Wykonuje wtedy zadania wbrew wiedzy i woli ofiary.

Programy szpiegujące – oprogramowanie zbierające informacje o osobie fizycznej lub prawnej bez jej zgody, takie jak informacje o odwiedzanych witrynach, hasła dostępowe itp. Występuje często jako dodatkowe i ukryte komponenty większego programu, odporne na usuwanie i ingerencję użytkownika. Programy szpiegujące mogą wykonywać działania bez wiedzy użytkownika - zmieniać wpisy do rejestru systemu operacyjnego i ustawienia użytkownika. Program szpiegujący może pobierać i uruchamiać pliki pobrane z sieci.

scumware (ang. scum – piana; szumowiny, męty) – żargonowe, zbiorcze określenie oprogramowania, które wykonuje w komputerze niepożądane przez użytkownika czynności.

stealware/parasiteware - służące do okradania kont internetowych,

adware - oprogramowanie wyświetlające reklamy,

Hijacker Browser Helper Object - dodatki do przeglądarek, wykonujące operacje bez wiedzy użytkownika.

Exploit – kod umożliwiający bezpośrednie włamanie do komputera ofiary, do dokonania zmian lub przejęcia kontroli wykorzystuje się lukę w oprogramowaniu zainstalowanym na atakowanym komputerze. Exploity mogą być użyte w atakowaniu stron internetowych,

---

[1] Opracowano na podstawie WWW.wikipedia.pl

których silniki oparte są na językach skryptowych (zmiana treści lub przejęcie kontroli administracyjnej), systemy operacyjne (serwery i końcówki klienckie) lub aplikacje (pakiety biurowe, przeglądarki internetowe lub inne oprogramowanie).

Rootkit – jedno z najniebezpieczniejszych narzędzi hackerskich. Ogólna zasada działania opiera się na maskowaniu obecności pewnych uruchomionych programów lub procesów systemowych (z reguły służących hackerowi do administrowania zaatakowanym systemem). Rootkit zostaje wkompilowany (w wypadku zainfekowanej instalacji) lub wstrzyknięty w istotne procedury systemowe, z reguły jest trudny do wykrycia z racji tego, że nie występuje jako osobna aplikacja. Zainstalowanie rootkita jest najczęściej ostatnim krokiem po włamaniu do systemu, w którym prowadzona będzie ukryta kradzież danych lub infiltracja.

Keylogger – występuje w dwóch postaciach: programowej i sprzętowej. Odczytuje i zapisuje wszystkie naciśnięcia klawiszy użytkownika. Dzięki temu adresy, kody, cenne informacje mogą dostać się w niepowołane ręce. Pierwsze programowe keyloggery były widoczne w środowisku operacyjnym użytkownika. Teraz coraz częściej są procesami niewidocznymi dla administratora.

Dialery – programy łączące się z siecią przez inny numer dostępowy niż wybrany przez użytkownika, najczęściej są to numery o początku 0-700 lub numery zagraniczne. Dialery szkodzą tylko posiadaczom modemów telefonicznych analogowych i cyfrowych ISDN, występują głównie na stronach o tematyce erotycznej.

Mniej szkodliwe złośliwe oprogramowanie to:

– fałszywe alarmy dotyczące rzekomo nowych i groźnych wirusów (ang. false positives); fałszywy alarm to także rzekome wykrycie zainfekowanego pliku, które powodują programy antywirusowe z najwyższym poziomem analizy heurystycznej.

– żarty komputerowe, robione najczęściej nieświadomym początkującym użytkownikom komputerów.

TYPOLOGIA SCENARIUSZY

<table>
<tr><th colspan="2">Cechy główne scenariusza</th><th colspan="3">Podział scenariuszy ze względu na cechy szczegółowe</th></tr>
<tr><td rowspan="6">CEL</td><td>Normatywność</td><td>Scenariusze opisowe, badające możliwe warianty przyszłości, określane również jako scenariusze odniesienia lub nieinterwencyjne</td><td colspan="2">Scenariusze normatywne, najczęściej stosowane obecnie, opisujące prawdopodobne lub pożądane wizje przyszłości, określane jako scenariusze strategiczne, polityczne, interwencyjne</td></tr>
<tr><td>Punkt obserwacji</td><td>Scenariusze eksploracyjne lub forecastingowe, przyjmujące za punkt wyjścia teraźniejszość, kładące nacisk bardziej na wartości poznawcze niż wspieranie podejmowania konkretnych decyzji</td><td colspan="2">Scenariusze backcastingowe za punk wyjściowy przyjmują stan przyszłości i opisują ścieżki osiągnięcia tego stanu, są wiec z natury scenariuszami normatywnymi</td></tr>
<tr><td>Przedmiot badan</td><td>Scenariusze problemowe, za przedmiot badan przyjmują najczęściej problemy społeczne, jak na przykład przyszłość telewizji, przestępczość</td><td>Scenariusze badające obszar, za przedmiot badan przyjmują określony obszar: kraj, region, miasto</td><td>Scenariusze instytucjonalne, za przedmiot badan przyjmują obszary zainteresowania instytucji, grup instytucji lub sektora</td></tr>
<tr><td>Skala czasowa</td><td colspan="2">Scenariusze o perspektywie długoterminowej: powyżej 25 lat</td><td>Scenariusze o perspektywie krótkoterminowej: 3-10 lat</td></tr>
<tr><td>Przestrzeń</td><td colspan="3">W tym zakresie wyróżnia się scenariusze globalne, międzynarodowe, narodowe, regionalne i lokalne oraz łączące informacje właściwe dla kilku z wyżej wymienionych rodzajów.</td></tr>
<tr><td rowspan="4">SPOSÓB REALIZACJI</td><td>Rodzaj danych</td><td colspan="2">Scenariusze jakościowe, maja najczęściej charakter narracyjny i znajdują zastosowanie w analizie złożonych sytuacji o dużym stopniu niepewności i przy braku dostępu do odpowiednich danych ilościowych; na przykład dane na temat wartości humanitarnych, emocji i zachowań</td><td>Scenariusze ilościowe, często stosujące matematyczne modele komputerowe, znajdują zastosowanie w opracowywaniu prognoz dla sektora energetycznego, technologicznego, w makroekonomii i prognoz środowiskowych</td></tr>
<tr><td></td><td colspan="3">Połączenie danych jakościowych i ilościowych w scenariuszach wpływa na zwiększenie spójności i wiarygodności scenariuszy: informacje o charakterze jakościowym ułatwiają przekaz informacji zawartych w scenariuszach opartych na danych ilościowych, natomiast scenariusze typowo jakościowe zyskują większą wiarygodność i spójność poprzez ilościowe opracowanie danych. Połączenie takie stanowi jednak duże wyzwanie metodologiczne.</td></tr>
<tr><td>Sposób gromadzenia danych</td><td colspan="2">Przez uczestnictwo – w oparciu o udział ekspertów oraz w coraz większym stopniu poprzez spotkania robocze uczestników projektu</td><td>Poprzez badania teoretyczne obejmujące na przykład analizy na podstawie symulacji komputerowych, przegląd danych literaturowych</td></tr>
<tr><td></td><td colspan="3"></td></tr>
</table>

	Rodzaj warunków instytucjonalnych	Warunki instytucjonalne opisują dostępne zasoby dla tworzenia scenariuszy, relacje międzyludzkie, polityczne aspekty analiz i mogą być otwarte lub ograniczone. Przykładem może być narzucenie przez władze wprowadzenia scenariusza normatywnego, opartego na aktualnej strategii do zestawu przeprowadzonych scenariuszy opisowych, czego efektem było ograniczenie poznawczego charakteru przeprowadzonych badan.	
ZAWARTOSC SCENARIUSZY	Czas	rozwojowy lub łańcuchowy, opisujący rozwój zdarzeń prowadzących do osiągnięcia danego stanu w przyszłości	migawkowy, opisujący stan końcowy bez analizy procesu prowadzącego do jego osiągnięcia
	Rodzaj zmiennych	heterogeniczne, obejmujące zróżnicowane dane na przykład: demograficzne, na temat ekonomicznej integracji i liberalizacji, nierówności społecznych, kultury konsumenckiej, biotechnologii, technologii informatycznych, degradacji środowiska, decentralizacji politycznej	homogeniczne, obejmujące dane o podobnym charakterze, na przykład: na temat pracowników, pracodawców, rynku pracy
	Rodzaj dynamiki	kontrastowe lub peryferyjne, obejmujące zdarzenia mało prawdopodobne i ekstremalne	trendów, ekstrapolujące aktualne trendy
	Poziom odchyleń	alternatywne, opisujące znacznie różniące się miedzy sobą opcje przyszłości i mające na celu podniesienie poziomu świadomości i zrozumienia nowych lub niepewnych zjawisk, poszerzenie horyzontów myślowych	konwencjonalne, stanowiące ekstrapolacje obecnych trendów, nie uwzględniające nieoczekiwanych zdarzeń mogących je zaburzyć, stanowiące narzędzie raczej dostosowywania obecnej strategii niż budowania nowej
	Poziom integracji	scenariusze o wysokim poziomie integracji, łączące w przejrzysty sposób interdyscyplinarne zmienne i dynamiki na przestrzeni skali czasowej i przestrzennej oraz na tle odnośnych obszarów społecznych, ekonomicznych, środowiskowych i instytucjonalnych, ukazujące duży stopień zależności i oddziaływań pomiędzy zmiennymi i dynamika	scenariusze o niskim poziomie integracji, nie ukazujące oddziaływań pomiędzy prezentowanymi różnymi obszarami

Załącznik IX

ANKIETA

Szanowny Panie! Szanowna Pani
Zwracamy się do Pana(i) z uprzejmą prośbą o wypełnienie poniższej ankiety. Pan(i) wypowiedzi i dane zostaną wykorzystane ***jedynie w celach naukowych****. Zapewniamy Panu(i) całkowitą anonimowość. Zachęcamy także do jak najszczerszego wyrażania swojej opinii w poniższym kwestionariuszu, także, jeśli wykracza ona poza treść przedstawionych pytań.*

Część A. Ocena skutków rozwoju społeczeństwa informacyjnego
Proszę wstawić znak x w rubryce, dla którego zjawiska przewiduje pan(i) tendencję wzrostową lub malejącą.

Nr	*XYZ*	*Wzrośnie*	*Zmaleje*	*Trudno powiedzieć*
1	*Stabilność struktur społecznych*			
2	*rozwarstwienie społeczne*			
3	*Rola narodowego dziedzictwa kulturowego*			
4	*Znaczenie wartości uniwersalnych*			
5	*Alienacja grup społecznych i jednostek*			
6	*Religijność*			
7	*Rola więzi towarzyskich i przyjacielskich*			
8	*Rywalizacja między ludźmi*			
9	*Gotowość do współpracy z innymi*			
10	*Globalna solidarność społeczna*			
11	*Regionalna (europejska) solidarność społeczna*			
12	*Rola powszechnych, standardowych usług publicznych*			
13	*Znaczenie wartości konsumpcyjnych*			
14	*Hedonizm*			
15	*Chaos informacyjny*			
16	*Świadomość społeczna istoty zachodzących przemian*			
17	*Racjonalizacja postaw i zachowań społecznych*			
18	*Przedsiębiorczość jednostek*			
19	*Zróżnicowanie stylów życia*			
20	*Ilość czasu poświęcanego na pracę*			
21	*Rola pracy w kształtowaniu drogi życiowej*			
22	*Satysfakcja z wykonywanej pracy*			
23	*Rola rodziny w życiu społecznym*			
24	*Waga konfliktów międzypokoleniowych*			
25	*Rola opieki społecznej*			
26	*Zagrożenie chorobami cywilizacyjnymi*			
27	*Stopień harmonizacji celów społecznych i gospodarczych*			
28	*Bezrobocie strukturalne*			
29	*Stabilność gospodarcza w skali globalnej*			
30	*Rozwarstwienie gospodarki światowej*			
31	*Ryzyko działalności gospodarczej*			
32	*Rola państwa w gospodarce*			
33	*Skuteczność mechanizmów rynkowych*			
34	*Rola konkurencji i innowacyjności w gospodarce*			
35	*Ochrona prywatności*			
36	*Ochrona praw ludzkich i obywatelskich*			
37	*Humanizacja pracy*			
38	*Podmiotowość pracujących*			
39	*Ochrona własności intelektualnej*			
40	*Ograniczenia i kontrola obiegu informacji*			
41	*Uniformizacja kształcenia*			
42	*Wartość utylitarne wykształcenia*			
43	*Rola wychowawcza szkoły*			
44	*Rola kulturotwórcza uczelni wyższych*			
45	*Zainteresowanie obywateli sprawami politycznymi*			
46	*Udział obywateli w działalności społecznej*			
47	*Rola demokracji bezpośredniej*			
48	*Rola stanowiąca i kontrolna państwa*			
49	*Rola kulturotwórcza mediów masowych*			
50	*Wpływ mediów na postawy i zachowania*			

Część B: Ocena zagrożeń dla bezpieczeństwa narodowego RP
Uwaga: proszę przydzielić punkty – liczbę od: 0,1,2,3,4,5
0- brak zagrożenia lub zagrożenie pomijalne
5 – wysoki stopień zagrożenia
Listę zagrożeń można uzupełnić o własną propozycję

Zagrożenie	**Ocena wpływu**
Terroryzm (typu islamskiego)	
Zderzenie cywilizacji	
Proliferacja broni masowego rażenia	
Cyberterroryzm (infoterroryzm)	
Konflikt na Bliskim Wschodzie	
Polityka Rosji	
Polityka Chin	
Polityka USA	
Globalny kryzys energetyczny	
Konflikt na Dalekim Wschodzie	
Kryzys klimatyczny (ocieplenie globalne, dziura ozonowa)	
Wewnętrzne niepokoje społeczne	
Niestabilność wewnętrznej sytuacji politycznej	
Niestabilna sytuacja w bliskim otoczeniu RP	

Część C. Ocena zagrożeń dla bezpieczeństwa osobistego obywateli RP
Uwaga: proszę przydzielić punkty – liczbę od: 0,1,2,3,4,5
1- brak zagrożenia lub zagrożenie pomijalne
5 – wysoki stopień zagrożenia
Listę zagrożeń można uzupełnić o własną propozycję

Zagrożenia	**ocena**
Przestępczość pospolita (rozboje, kradzieże)	
Choroba własna	
Choroba bliskich	
Wypadki drogowe (komunikacyjne)	
Katastrofy budowlane	
Zjawiska atmosferyczne (powodzie, susze)	
Skażenia chemiczne i radiacyjne	
Przestępstwa bankowe	
Demonstracje, zamieszki, niepokoje społeczne	
Przerwy w dostawie prądu, gazu, wody	
Awarie telekomunikacyjne	
Awarie Internetu	
Przestępstwa teleinformatyczne	
Ograniczenia wolności osobistej	
Cenzura informacji (kontrola zasobów informacyjnych)	
Manipulacje informacjami w mediach	
Bezrobocie	
Lobbing (w pracy)	
Pornografia (dostęp w Internecie)	
Naruszenie praw człowieka i podstawowych wolności	
Uprzedzenia kulturowe i religijne oraz dyskryminacja mniejszości narodowych	
Dyskryminacja płci	
Obcy przybysze (emigranci)	
Wzrost roli religii	

Część D. Ocena skutków rozwoju technologii informatycznych w aspekcie bezpieczeństwa narodowego RP

Uwaga: proszę przydzielić punkty – liczbę od: 0,1,2,3,4,5

2- brak zagrożenia lub zagrożenie pomijalne

5 – wysoki stopień zagrożenia

Listę zagrożeń można uzupełnić o własną propozycję

Zagrożenia	**ocena**
Cyberteroryzm (infoteroryzm)	
Zakłócenia krytycznej infrastruktury państwa	
Hackerstwo	
Przechwytywanie danych	
Oszustwa bankowe	

Jak często przejawia się pana(i) refleksyjność nad tematami zagrożeń:

Można uzupełnić o własne zagrożenia.

Zastanawiam się nad zagrożeniami:	Bardzo często	Dość często	Czasami, rzadko	Raczej nie	wcale
Personalnymi					
Swojego otoczenia					
Kraju					
świata					

Jak Pan(i) ocenia obecną sytuacji na świecie? W porównaniu z sytuacją sprzed 10 lat, obecnie jest:

1. Lepiej, spokojniej ☐
2. Tak jak było ☐
3. Gorzej, bardziej niespokojnie ☐
4. Trudno powiedzieć ☐

Czy istnieją obecnie konflikty, które mogą, zdaniem Pana(i), zagrozić pokojowi na świecie?

1. Istnieją ☐
2. Nie istnieją ☐
3. Trudno powiedzieć ☐

W jakim stopniu prowadzona polityka rządu w naszym kraju jest powodem pana(i) obaw i niepokoju?

1. W bardzo dużym ☐
2. W dużym ☐
3. W niewielkim ☐
4. W żadnym ☐
5. Trudno powiedzieć ☐

Część F : Pytania metrykalne

Płeć:

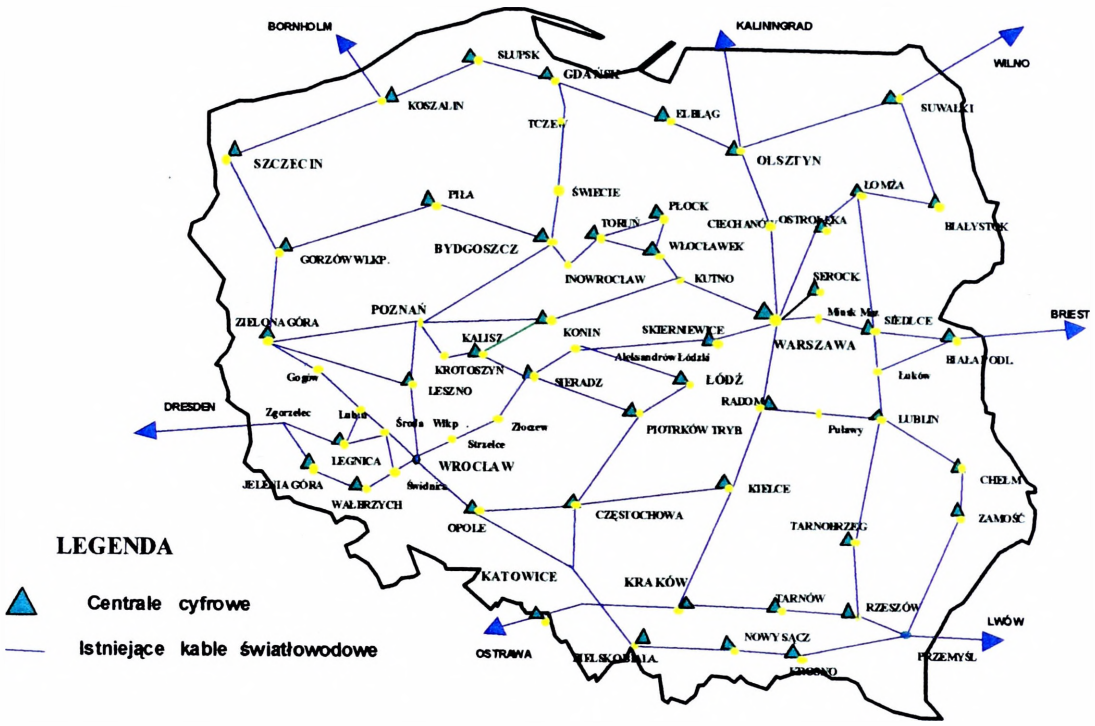
kobieta	
mężczyzna	

Wiek:	- 20	20-30	30-40	40-

Rodzaj studiów:

Ekonomiczne	Techniczne	menadżerskie	wojskowe

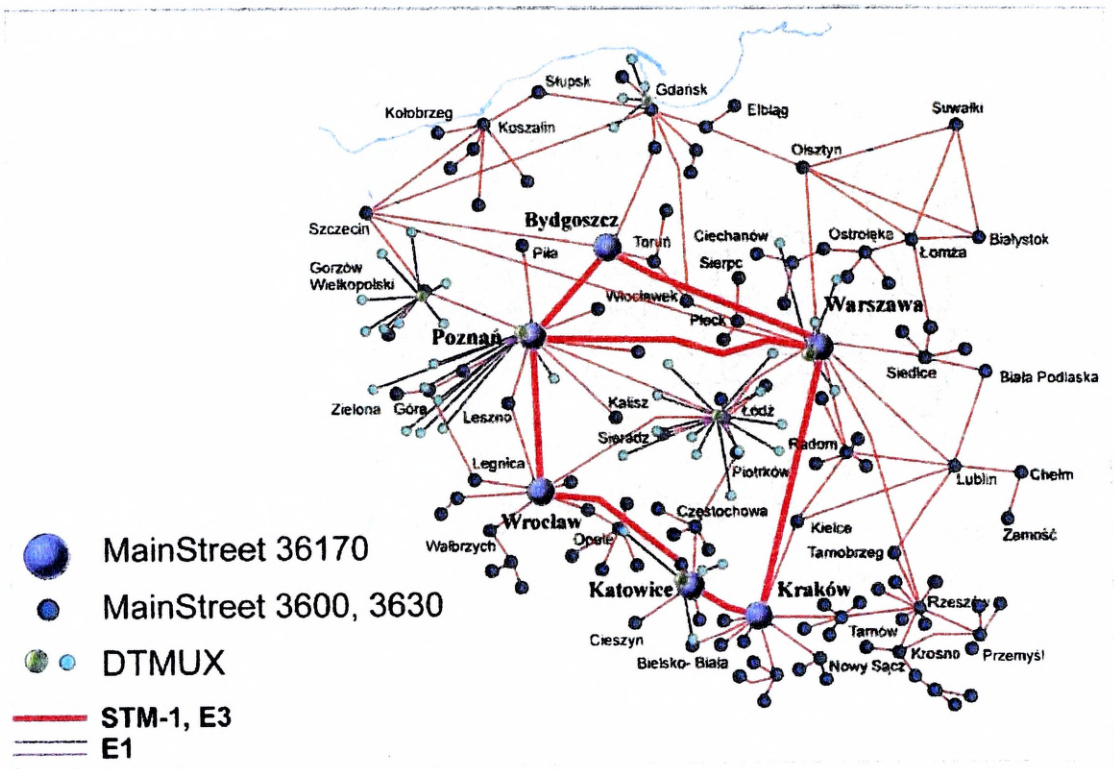
WYBRANE PRZYKŁADY SIECI TELEKOMUNIKACYJNYCH FUNKCJONUJĄCYCH I ROZWIJANYCH SIĘ W POLSCE



Rysunek ZX-1. Sieć światłowodowa TP S.A. (PDH[1]).
Źródło: Materiały Zarządu Łączności i Informatyki

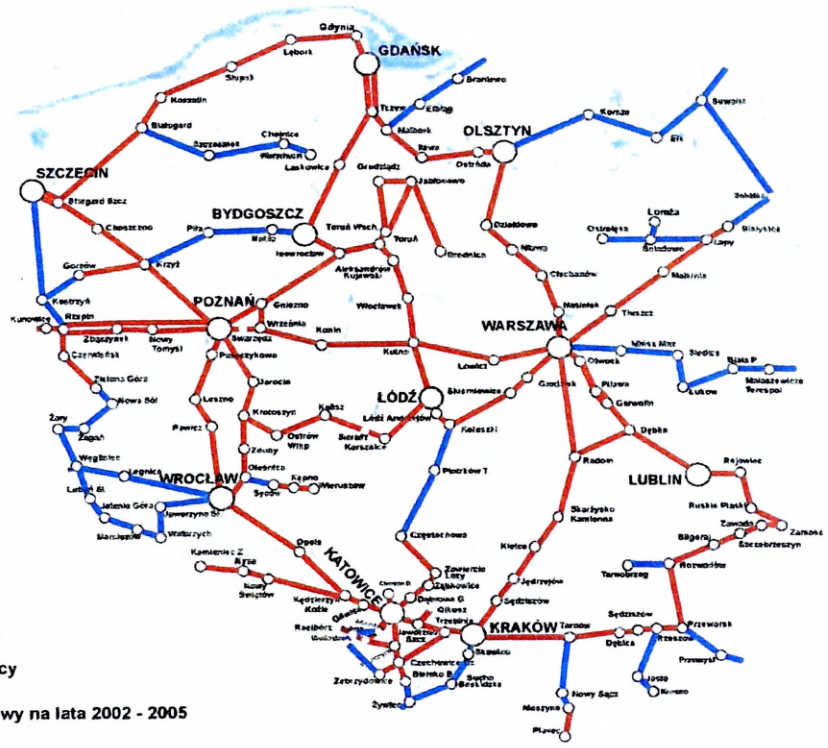
Rysunek ZX-2. Sieć światłowodowa TP S.A. (SDH2)
Źródło: Materiały Zarządu Łączności i Informatyki

[1] Ang. Plesiochronous Digital Hierarchy – plezjochroniczna hierarchia cyfrowa.
[2] Ang. Synchronous Digital Hierarchy – synchroniczna hierarchia cyfrowa.



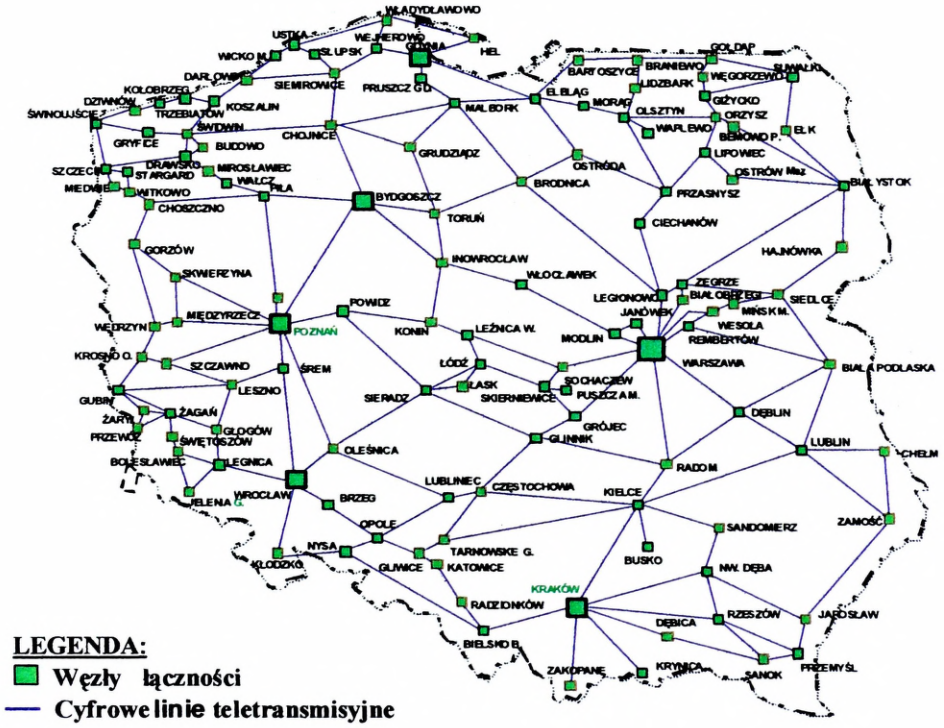
Rysunek ZX-3. Sieć cyfrowych łączy dzierżawionych
Źródło: Materiały firmowe TP S.A.

Rysunek ZX-4. Sieć światłowodowa TEL-ENERGO.
Źródło: Materiały Zarządu Łączności i Informatyki.



Rysunek ZX-5. Sieć POLPAK

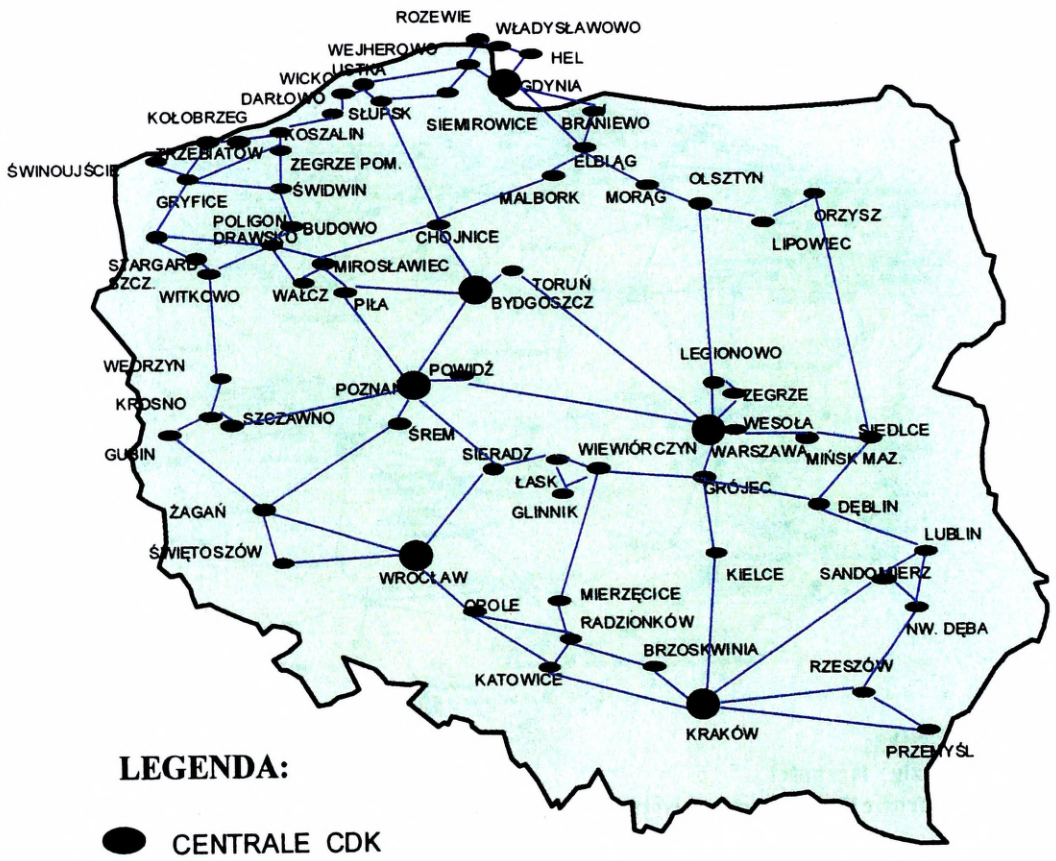
Źródło: tpsa.pl



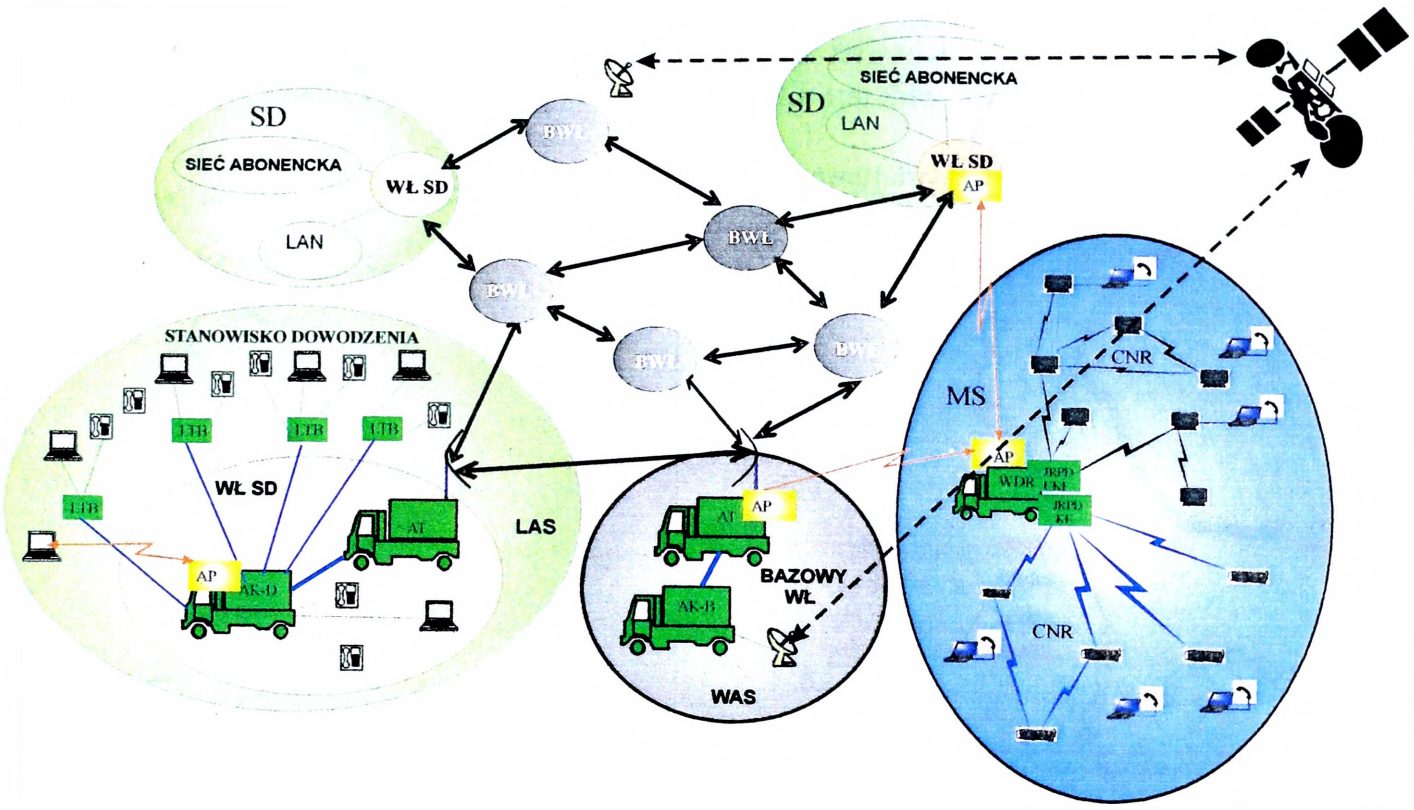
Rysunek ZX-6. Docelowa sieć telekomunikacyjna SZ RP.

Źródło: Materiały Zarządu Łączności i Informatyki.

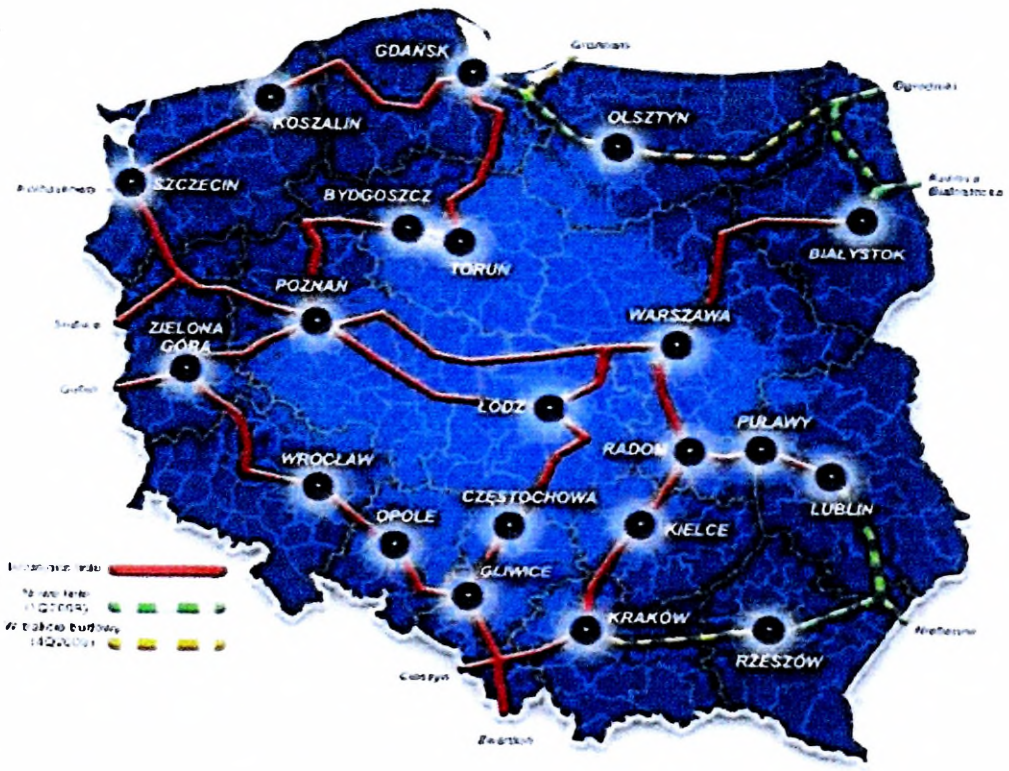
Rysunek ZX-7. Perspektywiczny plan rozmieszczenia EACT.
Źródło: Materiały Zarządu Łączności i Informatyki.



Rysunek ZX-8. Perspektywiczny plan rozmieszczenia central CDK.
Źródło: Materiały Zarządu Łączności i Informatyki.



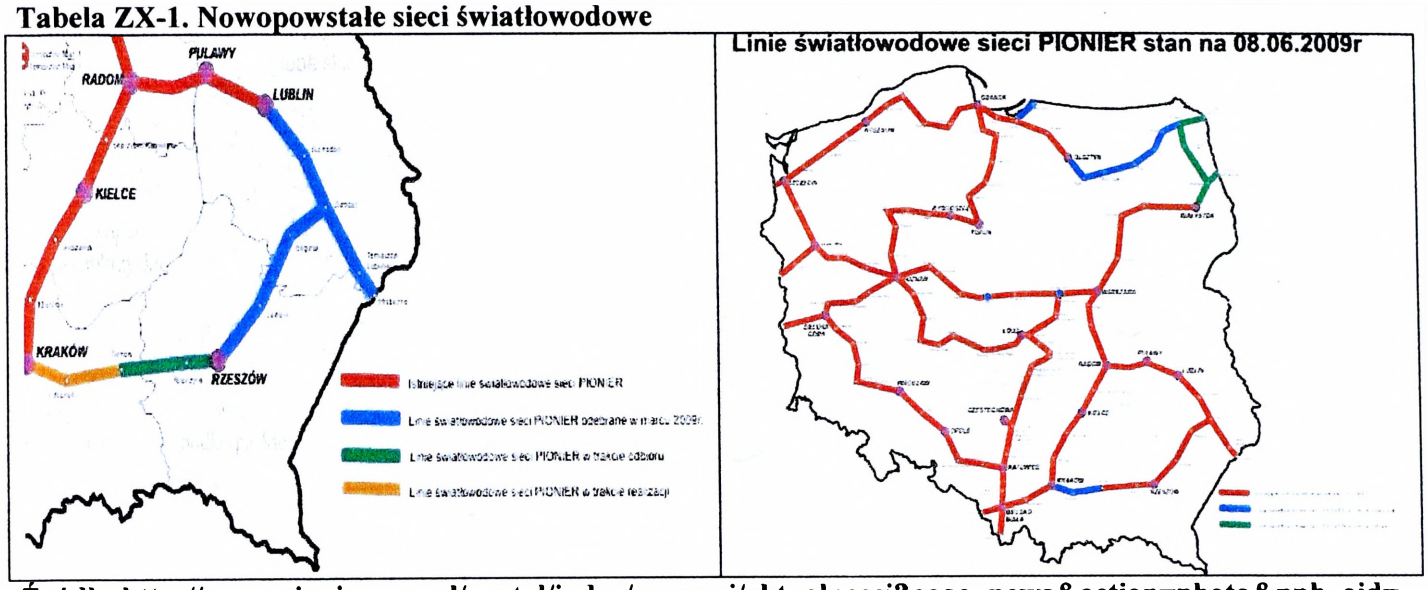
Rysunek ZX-9. Architektura systemu KROKUS
Źródło: Wojskowy Instytut Łączności



Rysunek ZX-10. Infrastruktura światłowodowa sieci PIONIER
Źródło:http://www.pionier.gov.pl/portal/index/nowosci/aktualnosci?page=news&action=photo&pph_oid=1220

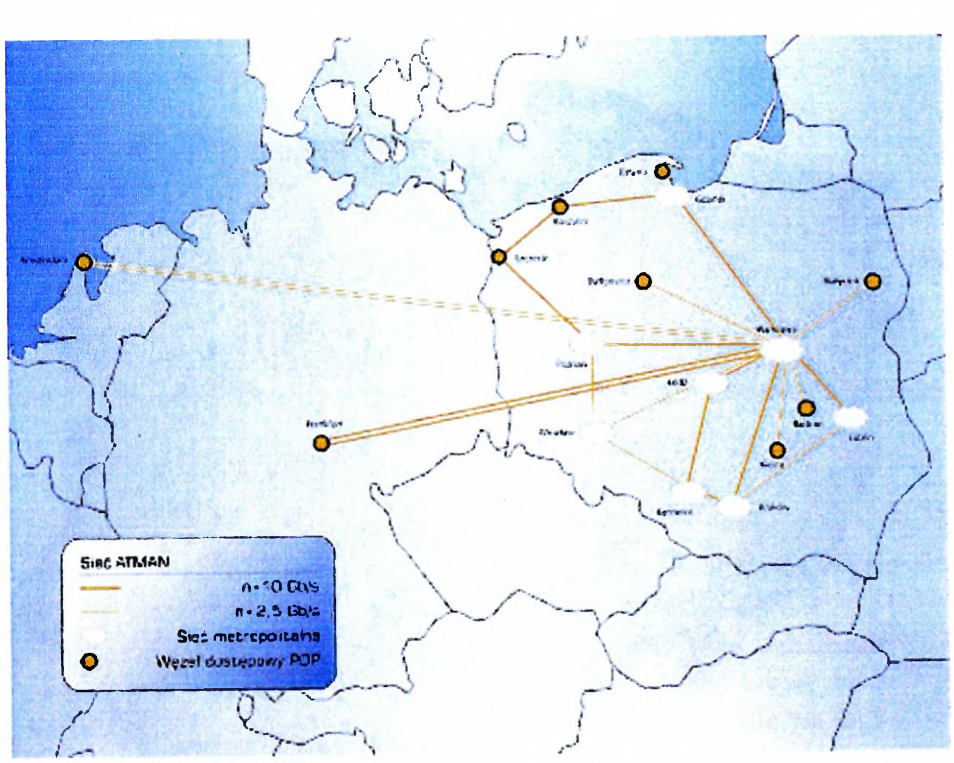
Sieć PIONIER powstała w ramach programu Ministerstwa Nauki i Szkolnictwa Wyższego (wcześniej m.in. Komitet Badań Naukowych), którego celem było dostarczenie nowoczesnej infrastruktury i aplikacji dla środowiska naukowego w Polsce.

Tabela ZX-1. Nowopowstałe sieci światłowodowe



Źródło:http://www.pionier.gov.pl/portal/index/nowosci/aktualnosci?page=news&action=photo&pph_oid=1220

Krajowa sieć ATMAN to węzły telekomunikacyjne w kilkudziesięciu miastach oraz ponad 4500 km łączy o przepustowości od 1 Gb/s do n×10 Gb/s w głównych relacjach. Sieć jest stale rozbudowywana i modernizowana, tak by zaspokoić stale rosnące potrzeby użytkowników, aplikacji biznesowych i serwisów internetowych.

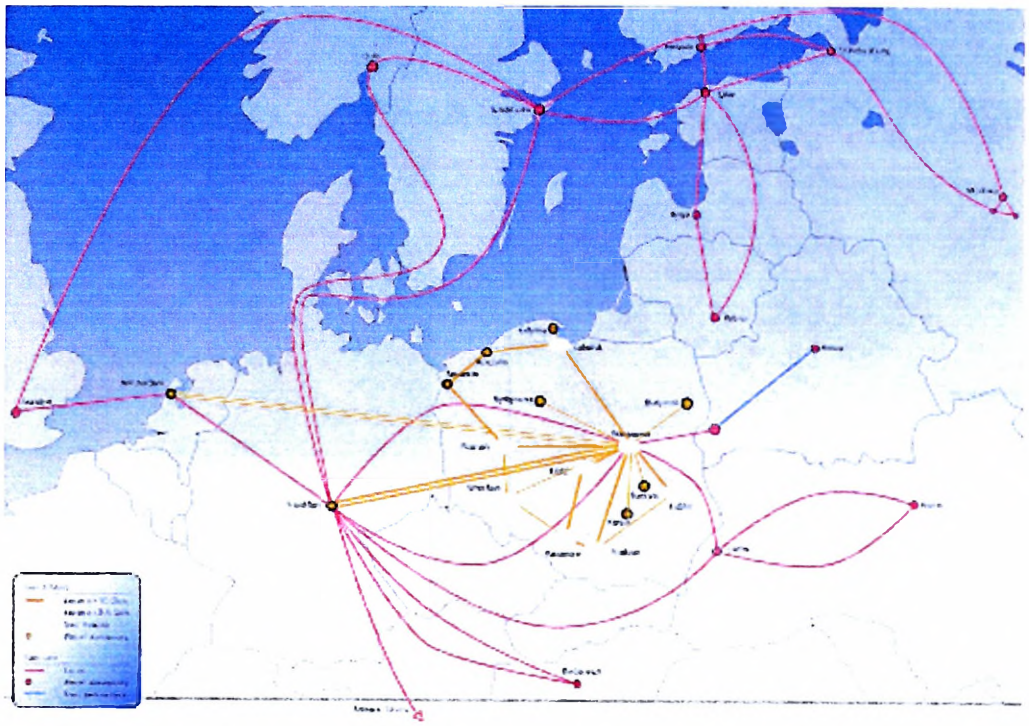


Rysunek ZX-11. Sieć krajowa ATMAN
Źródło: cms.atm.com.pl

Europejska sieć Linx

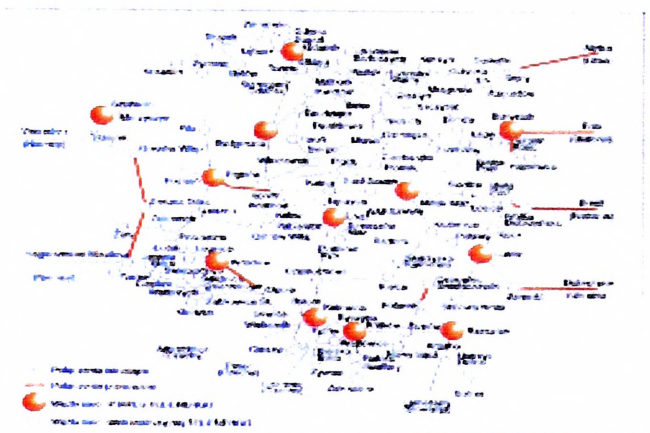
ATM S.A. jest udziałowcem europejskiego operatora Linxtelecom, którego sieć rozciąga się od Skandynawii do Zakaukazia i od Europy Zachodniej do krajów bałtyckich,

Ukrainy i Rosji. Współpraca z Linksem pozwala na świadczenie usług telekomunikacyjnych (w tym kolokacji) nie tylko na terenie kraju, ale całej Europy.

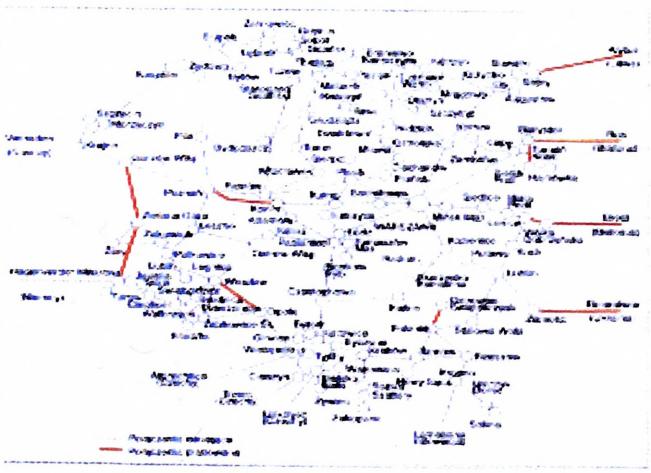


Rysunek ZX-12. Sieć ATMAN – połączenia poza krajowe
Źródło: cms.atm.com.pl

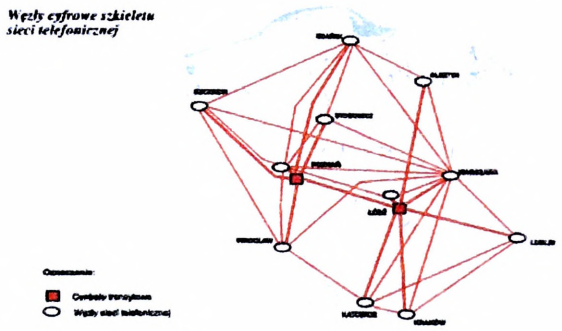
Tabela ZX-2. Przykłady dostępnych sieci w Polsce



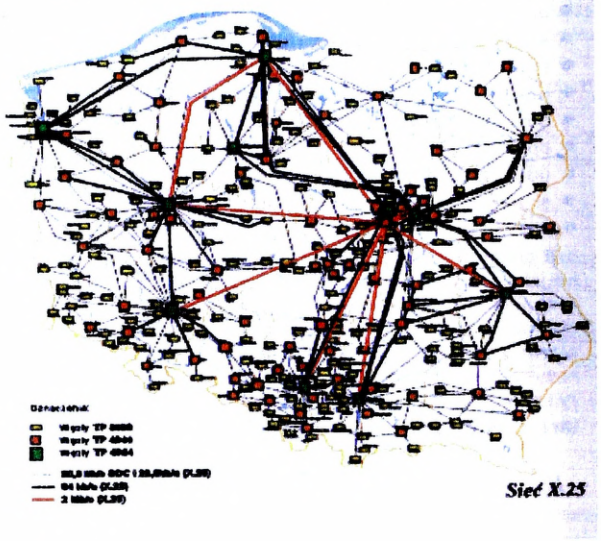
Sieć transmisji danych IP MPLS

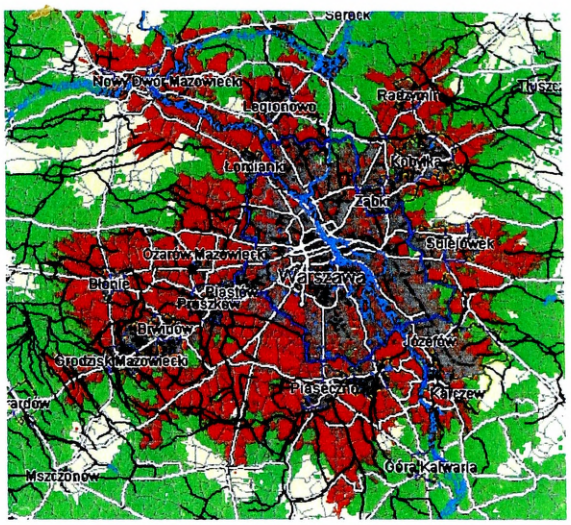


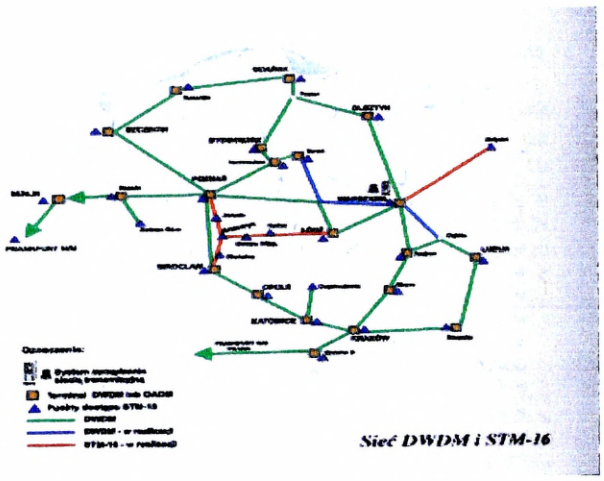
Sieć teletransmisyjna TEL-ENERGO SA

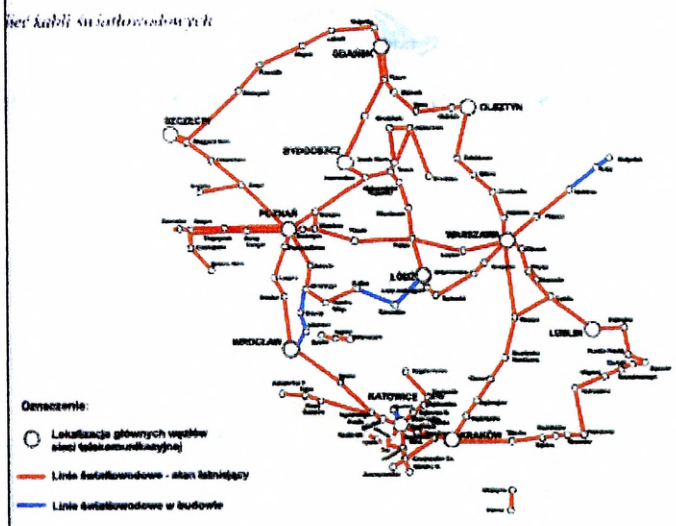


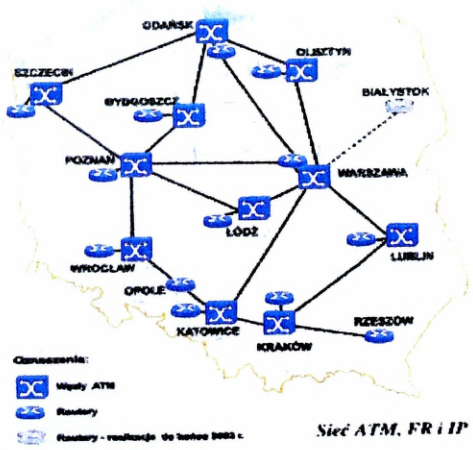
Sieć teletransmisyjna











Uwaga: wszystkie dane można uzyskać przy pomocy Internetu.

BIBLIOTEKA GŁÓWNA - ARCHIWUM
Nr ewid. 75499
Akademii Obrony Narodowej

S/7594