AKADEMIA OBRONY NARODOWEJ

Wydział Strategiczno-Obronny

płk mgr inż. Dobrosław MAŃA

RYZYKO W SYSTEMIE BEZPIECZEŃSTWA INFORMACYJNEGO PAŃSTWA W ASPEKCIE STANDARDÓW NATO I UNII EUROPEJSKIEJ

Biblioteka Główna
Akademii Sztuki Wojennej
57161
09-057161-000-0

57161

WARSZAWA 2004

AKADEMIA OBRONY NARODOWEJ

Wydział Strategiczno-Obronny

BIBLIOTEKA GŁÓWNA - ARCHIWUM
Nr ewid. 57161
Akademii Obrony Narodowej

płk mgr inż. Dobrosław MĄKA

RYZYKO W SYSTEMIE BEZPIECZEŃSTWA INFORMACYJNEGO PAŃSTWA W ASPEKCIE STANDARDÓW NATO I UNII EUROPEJSKIEJ

Rozprawa doktorska napisana pod kierunkiem prof. zw. dr. hab. inż. Piotra SIENKIEWICZA

Warszawa 2004

Pamięci Matki pracę tę poświęcam

SPIS TREŚCI

WSTĘP.....*7*

1. Podstawy metodologiczne badań nad bezpieczeństwem informacyjnym...*13*
1.1. Przedmiot badań.....*13*
1.2. Cel badań.....*14*
1.3. Problemy badawcze i hipotezy robocze.....*15*
1.3.1. Problem główny i szczegółowe problemy badawcze.....*15*
1.3.2. Hipotezy robocze.....*18*
1.4. Metody, techniki i narzędzia badawcze.....*21*
1.4.1. Modelowanie procesów pomiaru i doskonalenia parametrów jakościowych bezpieczeństwa informacyjnego z zastosowaniem systemu (zbioru narzędzi) *TQM*.....*26*
1.4.2. Wybór *analizy systemowej* jako metody badawczej.....*29*
1.5. Obszar i organizacja badań.....*36*
1.5.1. Badania wybranych elementów potencjału informacyjnego w oparciu o przebieg konfliktów zbrojnych.....*36*
1.5.2. Dostosowanie narzędzi badawczych do celów badań.....*37*
1.5.3. Analiza możliwości zastosowania narzędzi ewaluacji efektywności informacyjnej do pomiaru ryzyka naruszenia bezpieczeństwa informacji.....*37*
1.5.4. Organizacja badań.....*38*

2. Rola czynnika informacyjnego w bezpieczeństwie państwa.....*41*
2.1. Wykorzystanie metod potęgometrycznych do oceny bezpieczeństwa państwa.....*45*
2.1.1. Modelowanie i pomiar potęgi państw.....*46*
2.1.2. Metody i modele potęgometryczne.....*48*
2.1.3. Miary potęgi państw jako czynnik oceny bezpieczeństwa.....*55*
2.2. Bezpieczeństwo narodowe w ujęciu statycznym i dynamicznym.....*56*
2.2.1. Wymiar bezpieczeństwa narodowego.....*56*
2.2.2. Priorytetowe aspekty bezpieczeństwa narodowego XXI wieku..*60*
2.2.3. Płaszczyzna informacyjna bezpieczeństwa narodowego.....*61*

2.3 Rola czynnika informacyjnego w militarnym obszarze bezpieczeństwa państwa.....*63*
2.3.1. Elementy walki informacyjnej w obszarze działań bojowych.....*63*
2.3.2. Identyfikacja, ocena i kwantyfikacja informacji.....*76*
2.3.3. Kwantyfikacja informacji według *teorii C. E. Shannona*.....*80*
2.3.4. Taksonomia informacyjna w oparciu o sieciocentryczną architekturę systemów informacyjnych pola walki.....*82*
2.3.5. Miary efektywności informacyjnej pola walki.....*89*
2.3.6. Pomiar efektywności informacyjnej w oparciu o doświadczenia operacji *Iraqi Freedom – prawa F. W. Lanchestera*.....*97*
2.3.7. Bezpieczeństwo informacji determinantą dominującej roli czynnika informacyjnego na współczesnym polu walki.....*107*
2.4. Prawno-organizacyjne determinanty bezpieczeństwa informacyjnego.....*111*
2.4.1. Obowiązujące ustawodawstwo w zakresie bezpieczeństwa informacji i ochrony danych.....*112*
2.4.2. Zasady polityki bezpieczeństwa informacyjnego.....*114*
2.4.3. Rola krajowych władz bezpieczeństwa i służb ochrony państwa w zakresie ochrony informacji niejawnych.....*120*
2.4.4. Zarządzanie bezpieczeństwem informacyjnym państwa w obszarze wewnętrznym i w aspekcie międzynarodowym z wykorzystaniem zbioru narzędzi *TQM*.....*127*

3. Standardy NATO i Unii Europejskiej w zakresie bezpieczeństwa informacyjnego.....*135*
3.1. Międzynarodowe standardy i normy bezpieczeństwa informacyjnego.....*136*
3.1.1. Kryteria i procedury bezpieczeństwa informacyjnego.....*136*
3.1.2. Standardy i normy bezpieczeństwa teleinformatycznego.....*137*
3.1.3. Znaczenie wprowadzenia pakietu standardów bezpieczeństwa teleinformatycznego – *Common Criteria*.....*138*
3.1.4. Ewaluacja i certyfikacja w oparciu o *Wspólne Kryteria Oceny Zabezpieczeń Teleinformatycznych*.....*139*
3.2. Stan prawno-organizacyjny ochrony informacji niejawnych NATO.....*152*
3.2.1. Struktura instytucjonalna bezpieczeństwa informacyjnego NATO.....*152*
3.2.2. Dyrektywy, zalecenia i wytyczne NATO w zakresie zapewnienia bezpieczeństwa informacyjnego sojuszu.....*156*
3.2.3. Instytucjonalne formy reagowania na naruszenia bezpieczeństwa informacyjnego - *CIRC - Computer Incidents Response Capabilty*...*160*
3.2.4. Wpływ standardów bezpieczeństwa informacyjnego NATO na rozwiązania narodowe w obszarze legislacyjnym.....*162*

3.3. Standardy Unii Europejskiej w zakresie bezpieczeństwa informacyjnego.....*164*
3.3.1. Programy rozwoju społeczeństwa informacyjnego w dyrektywach Unii Europejskiej.....*166*
3.3.2. Regulacje prawne związane z ochroną kluczowych zasobów informacyjnych Unii Europejskiej.....*170*
3.3.3. Problematyka *cyberprzestępczości* w polityce bezpieczeństwa informacyjnego Unii Europejskiej.....*172*
3.3.4. Elementy wspólnej polityki NATO i Unii Europejskiej w obszarze bezpieczeństwa informacyjnego.....*174*
3.4. Analiza zagrożeń informacyjnych imperatywem wynikającym z uwarunkowań międzynarodowych oraz z dominującej roli informacji w bezpieczeństwie państwa.....*175*

4. Analiza zagrożeń bezpieczeństwa informacyjnego i zarządzanie ryzykiem w systemach informacyjnych.....*179*
4.1. Globalizacja zagrożeń w obszarze bezpieczeństwa informacyjnego.....*186*
4.1.1. Rozwój elektronicznej wymiany informacji w procesie globalizacji.....*187*
4.1.2. Wpływ globalizacji na przestrzeń walki informacyjnej.....*188*
4.1.3. Globalizacja informacyjna jako nośnik zagrożeń bezpieczeństwa.....*190*
4.2. Ewaluacja zagrożeń w zakresie bezpieczeństwa informacyjnego...*191*
4.2.1. Wprowadzenie do *analizy systemowej*.....*195*
4.2.2. Struktura narzędzi ewaluacyjnych.....*196*
4.2.3. Integralność systemu analizy zagrożeń bezpieczeństwa informacyjnego – *analiza identyfikacyjna*.....*197*
4.2.4. Znaczenie stosowania analizy zagrożeń dla procedur zapewniania bezpieczeństwa systemów informacyjnych w sektorze obronności Rzeczypospolitej Polskiej.....*198*
4.2.5. Zakres i struktura zagrożeń bezpieczeństwa informacyjnego – *analiza problemowa*.....*199*
4.2.6. Istota i źródła zagrożeń w systemach teleinformatycznych.....*200*
4.2.7. *Analiza diagnostyczna* stanu bezpieczeństwa informacyjnego państwa.....*230*
4.3. Ryzyko jako wymierna kategoria obszaru analizy zagrożeń bezpieczeństwa informacyjnego.....*231*
4.3.1. Metody szacowania ryzyka w analizach zagrożeń bezpieczeństwa informacyjnego.....*236*
4.3.2. Zarządzanie ryzykiem jako instrument realizacji polityki bezpieczeństwa informacyjnego – *analiza prognostyczna*.....*239*
4.3.3. Stan zaawansowania i rozwoju systemów zarządzania ryzykiem w wybranych państwach NATO i Unii Europejskiej – *analiza porównawcza*.....*262*

5. Model procesu analizy zagrożeń i zarządzania ryzykiem bezpieczeństwa informacyjnego państwa 281
5.1. *Analiza efektywności* stosowania wyselekcjonowanych narzędzi analizy zagrożeń i zarządzania ryzykiem w zakresie bezpieczeństwa informacyjnego – pomiar efektywności z wykorzystaniem wybranych narzędzi badawczych 286
5.2. Modelowanie narzędzi systemowych w procesie analizy zagrożeń i zarządzania ryzykiem informacyjnym 292

6. Zakończenie – wnioski 303

BIBLIOGRAFIA 309
Literatura przedmiotu 309
Dzienniki urzędowe 320
Normy 321

ZAŁĄCZNIKI 323
Załącznik Nr 1 - Tabele taksonomiczne sprzętu walki informacyjnej 323
Załącznik Nr 2 - Modele matematyczne walki informacyjnej 327
Załącznik Nr 3 Elementy symulacji przebiegu działań bojowych z wykorzystaniem równań Lanchestera 327
Załącznik Nr 4 Prezentacja wybranych narzędzi analizy ryzyka 343

SPIS ILUSTRACJI 349
Diagramy 349
Rysunki 350
Tabele 350
Wykresy 351

WSTĘP

„Przepływ i wymiana informacji
staną się naczelnym czynnikiem
wytwórczości i władzy człowieka"
A. Toffler

Naturalne poznanie świata, wcześniej znacznie ograniczone brakiem pełnego dostępu do informacji, w ostatniej dekadzie XX wieku zostało utrudnione przez nadmiar danych o skrajnie zróżnicowanym poziomie istotności. Globalizacja wydobyła i wyostrzyła zjawisko poznawczego synkretyzmu, a rewolucja informacyjna stworzyła *„społeczeństwo wiedzy"*, uruchomiła szczególny relatywizm poznawczy, który zmusza analityków zjawisk zachodzących w przestrzeni wirtualnej do odpowiedzi na pytanie o realność przedmiotu badań. Zaciera się ostra granica podziału odseparowanych dotąd obszarów nauki. W badaniach realizowanych w ramach niniejszej rozprawy, objętej *grantem KBN jako projekt badawczy Nr O T00A 012 23 z dnia 13.11.2002 r.* uznano, że kluczowym zagadnieniem, od którego zaczynają się wszelkie zmiany we współczesnych stosunkach społecznych (w tym wewnątrzpaństwowych i międzynarodowych) jest *rewolucja informacyjna*.

Rozwój technologii informacyjnych i komunikacyjnych spowodował, że przeszliśmy z ery industrialnej w erę postindustrialną, w epokę informacji. Zaczął się kształtować nowy model społeczeństwa informacyjnego. Państwo redefiniuje obecnie swą tradycyjną rolę organizatora życia społecznego, odpowiadając na zmiany jakie w dobie globalizacji niesie większa aktywność podmiotów transnarodowych;

Pojawiła się kategoria infrastruktury krytycznej, której zniszczenie lub uszkodzenie może osłabić bezpieczeństwo państwa, w tym jego zdolności obronne. Główne jej elementy to: systemy kierowania, zarządzania i dowodzenia, telekomunikacja, system energetyczny, system bankowy i finansowy, produkcja, magazynowanie oraz transport surowców strategicznych, ratownictwo oraz ciągłość funkcjonowania władzy i służb publicznych.

Przedmiotem badań staje się bezpieczeństwo informacyjne, tj. nowa dziedzina bezpieczeństwa państwa, łącząca w sobie szereg cząstkowych ujęć, które odnieść należy do narzędzi i procedur ochrony danych, informacji i systemów informacyjnych.

Nowa dziedzina budzi liczne kontrowersje, zaznaczające się już w zróżnicowaniu pojęciowym. Stosowane są określenia:

- bezpieczeństwo informacji — odnoszące się do ochrony danych, poufności danych, informacji niejawnych i informacji strategicznych;
- cyberbezpieczeństwo - rozumiane jako bezpieczeństwo sieci i systemów informacyjnych, nadzór przepływu danych;
- bezpieczeństwo teleinformacyjne - jako pojęcie, określające ochronę zinformatyzowanych działów strategicznych, do których można dotrzeć przy pomocy szeroko pojmowanych połączeń sieciowych.

Podstawą bezpieczeństwa informacyjnego jest przekonanie o konieczności ochrony wszelkich informacji prowadzących do wiedzy, a co za tym idzie – do decyzji. W stosunku do innych dziedzin bezpieczeństwa narodowego bezpieczeństwo informacyjne pozostaje obszarem strategicznym. Zapewnienie bezpieczeństwa systemów i sieci informacyjnych, ich poufność, integralność i nienaruszalność stanowi podstawę wąskiej definicji bezpieczeństwa informacyjnego.

Definicja szeroka traktowałaby bezpieczeństwo informacyjne jako dział bezpieczeństwa, uznający wzrost roli informacji w podtrzymywaniu stabilności systemów politycznych, społecznych, gospodarczych i obronnych współczesnych państw. Bezpieczeństwo informacyjne w szerszym wymiarze obejmuje zabezpieczenie przed atakiem sieciowym i skutkami takiego ataku, który niósłby destrukcję dla funkcjonowania państwa. Strategia bezpieczeństwa informacyjnego jawi się zatem jako zjawisko wielopoziomowej ingerencji państwa w metody i narzędzia ochrony zasobów informacyjnych różnych rodzajów użytkowników.

Definicja bezpieczeństwa informacyjnego oznaczałaby działania legislacyjne i techniczne, ukierunkowane na ochronę:

- zasobów informacyjnych;
- nośników informacji;
- skomputeryzowanych działów gospodarki, a szczególnie infrastruktury krytycznej, czyli tych obszarów, których destrukcja spowodowałaby zagrożenie bezpieczeństwa państwa.

W koncepcjach bezpieczeństwa informacyjnego silnie podkreśla się skalę zagrożeń dla sektora obronności państwa i przemysłu zbrojeniowego.

Zagrożenie bezpieczeństwa narodowego może być przesłanką obniżenia autorytetu państwa, destabilizacja bezpieczeństwa międzynarodowego rodzi nowe zagrożenia, których skrajne oblicze - międzynarodowy terroryzm, obserwujemy w ostatnich latach. Tylko *państwo* może właściwie reagować w sytuacjach kryzysowych, związanych z atakiem na infrastrukturę krytyczną, może wykorzystywać ustawowo powołane instytucje – *służby ochrony państwa* i *krajowe władze bezpieczeństwa*.

Historyczna transformacja ustrojowa Rzeczypospolitej Polskiej i towarzyszące jej istotne zmiany polityczno-gospodarczego oblicza naszego kraju wyraźnie odcisnęły się na realiach nowego ładu europejskiego, stanowiąc element konstruktywnej stabilizacji i stymulator umacniania ponadnarodowych struktur całego kontynentu zarówno w obszarze ekonomiczno-społecznym jak i w sferze szeroko rozumianego bezpieczeństwa. Świadectwem naszej aktywności w urzeczywistnianiu idei zjednoczonej Europy jest integracja z Unią Europejską, a wyrazem spełnienia dążeń do pełnego włączenia się w tworzenie europejskiego systemu bezpieczeństwa jest przystąpienie Polski w 1999 roku do Organizacji Traktatu Północnoatlantyckiego

Jakościowo nowa sytuacja polityczno-wojskowa naszego kraju, stanowiąc czynnik wzmacniający narodowe bezpieczeństwo, implikuje jednocześnie potrzebę współuczestnictwa w konstruowaniu europejskiego systemu obronnego, którego głównym filarem jest Sojusz Północnoatlantycki, jego potencjał wojskowy oraz siły zbrojne państw członkowskich. Polska, przystępując do NATO, spełniła szereg wymogów w poszczególnych obszarach sektora obronności, stanowiących zespół warunków wstępnych i zobowiązała się do kontynuacji procesu integracyjnego, postrzeganego przez sojuszników jako wyznacznik naszej wiarygodności.

Przeobrażenia systemów politycznych, ekonomicznych i obronnych doprowadzają często do zmian doktrynalnych i strukturalnych bez naukowej analizy przemian i dbałości o zachowanie niejednokrotnie cennych, sprawdzonych i utrwalonych elementów świadczących o narodowej tożsamości. Brak takiej analizy sprowadza dążenia reformatorskie do krytyki bieżącego stanu i do prób mechanicznego przeniesienia na grunt krajowy obcych rozwiązań.

Dla przedmiotu niniejszej rozprawy szczególne znaczenie ma wyrażony w aktach legislacyjnych i porozumieniach międzynarodowych obowiązek zapewnienia

bezpieczeństwa wzajemnie przesyłanych, przetwarzanych i gromadzonych informacji. Szczególnym wyzwaniem jest takie dostosowanie narodowych systemów teleinformatycznych, aby sprostały wymogom wynikającym z wprowadzanych przez agendy Unii Europejskiej i organa bezpieczeństwa NATO dyrektyw.

Państwa NATO i kraje Unii Europejskiej nie prowadzą wspólnej polityki bezpieczeństwa informacyjnego, akty prawne w tej dziedzinie mają charakter narodowy. Silnie zróżnicowany obraz rozwiązań w tym zakresie nasuwa pytanie o kierunek działań dostosowawczych w polskim obszarze bezpieczeństwa informacyjnego w perspektywie pełnej integracji. Ujęty do zaprezentowania w rozprawie przegląd systemów i metod analizy zagrożeń, pomiaru i sterowania ryzykiem informacyjnym ma pozwolić na dokonanie wyboru narzędzi i modelowanie procesów analitycznych.

Polityka bezpieczeństwa informacyjnego nie jest obiektem jednoznacznie i niezmiennie ustalonym i zdefiniowanym. Podlega stałej ewolucji, wynikającej głównie z wprowadzania nowych technologii i zmian środowiska w jakim są one osadzane. Pomimo braku jednolitej polityki bezpieczeństwa informacyjnego, w ramach NATO funkcjonują grupy robocze, dostosowujące dyrektywy bezpieczeństwa do nowych potrzeb. Coraz częściej nowe dyrektywy dopuszczają możliwość stosowania rozwiązań komercyjnych dla systemów przetwarzania informacji niejawnych, co potęguje potrzebę stałego dokonywania pomiaru zagrożeń i analizy ryzyka.

W krajowym obszarze bezpieczeństwa informacyjnego brak narzędzi analizy zagrożeń i sterowania ryzykiem utrudnia konstruktywne podejście do modernizacji sprzętu, systemów i sieci przesyłania i przetwarzania informacji oraz spłyca ocenę zasadności wdrażania nowych rozwiązań uniemożliwiając dokonywanie porównań i kalkulacji ilościowo-wartościowych.

W większości państw NATO i Unii Europejskiej wdrożone są do użytku pakiety analizy ryzyka. Elementem ograniczającym ich bezpośrednie zastosowanie w Polsce jest brak wiarygodnych danych (baz danych dot. zagrożeń), wykorzystywanych do obliczenia prawdopodobieństwa wystąpienia danego zagrożenia. Programy te nie mają również odniesienia do obowiązujących w Polsce aktów prawnych, norm i

standardów, co utrudnia wskazanie odpowiednich środków i metod ochrony, wymaganych przez narodową legislację.

Powyższe względy implikują zasadność wypracowania modelu procesów analizy zagrożeń i zarządzania ryzykiem, uwzględniających metody odnoszące się do krajowych uwarunkowań.

Przedstawiona rozprawa ma na celu próbę uzupełnienia tej luki w procedurach zapewniania bezpieczeństwa informacyjnego Rzeczypospolitej Polskiej.

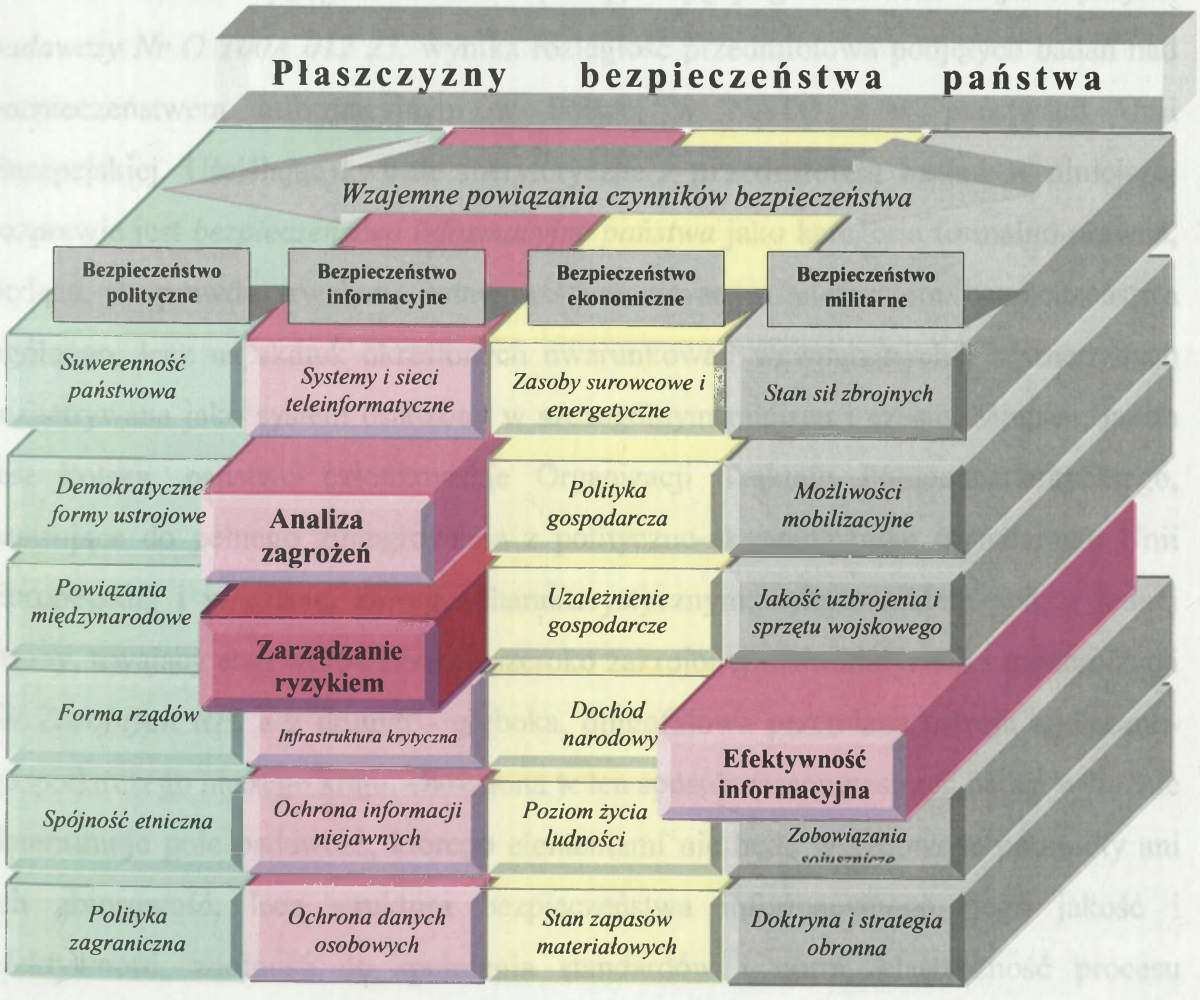


Diagram 1: ***Obszar przedmiotowy rozprawy***
Źródło: opracowanie własne

Rozdział 1

1. Podstawy metodologiczne badań nad bezpieczeństwem informacyjnym

„Niepokój naszej epoki jest w dużej mierze wynikiem tego, że próbujemy wykonywać dzisiejszą pracę za pomocą wczorajszych zarządzeń i z wczorajszymi pomysłami"
Marshall Mc Luhan

1.1. Przedmiot badań

Z szeroko ujętego tematu rozprawy, objętej grantem KBN jako *projekt badawczy Nr O T00A 012 23,* wynika rozległość przedmiotowa podjętych badań nad bezpieczeństwem informacyjnym w Polsce, w NATO i w państwach Unii Europejskiej. Uściślając kwestie merytoryczne - **przedmiotem badań** w niniejszej rozprawie jest *bezpieczeństwo informacyjne państwa* jako kategoria formalno-prawna, będąca co prawda trwałym, ustawowo umocowanym elementem bezpieczeństwa ogólnego, lecz na skutek określonych uwarunkowań wewnętrznych i zewnętrznych rozpatrywana jako system osadzony w szczególnym miejscu i czasie. Miejscu, jakim jest Polska, państwo członkowskie Organizacji Traktatu Północnoatlantyckiego, aspirujące do pełnego zintegrowania z polityczno-ekonomicznym organizmem Unii Europejskiej i w czasie, którego charakterystycznym wyznacznikiem jest, z jednej strony, trwający etap wprowadzania szeroko zakrojonej restrukturyzacji i modernizacji *Sił Zbrojnych RP*, a z drugiej - głęboka, długofalowa przemiana ustroju społeczno-gospodarczego naszego kraju. Określona w ten sposób czasoprzestrzeń badań wyraźnie determinuje pole badawcze, którego elementami nie będą wytypowane podmioty ani ich zbiorowość, lecz struktura bezpieczeństwa informacyjnego, jego jakość i efektywność, zdolność do spełnienia standardów i norm, elastyczność procesu kreowania polityki bezpieczeństwa i późniejszego doskonalenia jej wdrażania oraz możliwość jej dostosowania do wymogów współpracy międzynarodowej. Tłem tego pola badawczego, elementem postrzeganym jako zespół czynników warunkujących właściwą interpretację zależności pomiędzy zróżnicowanymi kryteriami przyjętymi do

badań będzie korelacja między miarą efektywności informacji i sposobem jej zabezpieczania oraz wpływ funkcjonalny wybranych cech bezpieczeństwa informacyjnego w NATO i w Unii Europejskiej na kształt pożądanych zmian w tym zakresie w warunkach narodowych. Implikuje to przyjęcie *przedmiotu badań* w niniejszej rozprawie: ***wpływ znaczenia informacji na konieczność wprowadzenia rozwiązań w zakresie analizy zagrożeń i zarządzania ryzykiem w obszarze polskiej polityki bezpieczeństwa informacyjnego z uwzględnieniem doświadczeń NATO i Unii Europejskiej.***

1.2. Cel badań

Zgodnie z charakterem i ogólnie przyjętą procedurą przedsięwzięć badawczych przyjęto w pracy dwa podstawowe cele badawcze :

- poznawczy;
- utylitarny.

Celem poznawczym pracy jest wykazanie braku efektywnych rozwiązań w zakresie analizy zagrożeń bezpieczeństwa informacyjnego państwa i narzędzi zarządzania ryzykiem informacyjnym w dynamicznie zmieniającej się sytuacji polityczno-wojskowej i ekonomiczno-społecznej, a także analiza przyczyn takiego stanu rzeczy w powiązaniu z prognozą ewentualnych negatywnych skutków zachowawczej polityki bezpieczeństwa informacyjnego. Rozprawa ma ponadto na celu porównawcze scharakteryzowanie systemów bezpieczeństwa informacyjnego w NATO i w państwach Unii Europejskiej z wykazaniem cech wspólnych i rozbieżnych, analizą rozwiązań korzystnych i możliwych do zastosowania na gruncie krajowym z jednoczesnym uwypukleniem cech sprzyjających zachowaniu tożsamości narodowej w procesach integracyjnych.

Celem utylitarnym jest wskazanie kierunków i sposobów kreowania i wdrażania polityki bezpieczeństwa informacyjnego państwa z wykorzystaniem najlepszych doświadczeń NATO i państw członkowskich Unii Europejskiej w tym zakresie, przy jednoczesnej optymalizacji środków pozyskiwanych zarówno ze źródeł wewnętrznych (własne uregulowania legislacyjne i wytwarzane narzędzia analityczne), jak i zewnętrznych (wzorce sojusznicze i opracowania zagraniczne) oraz próba

przedstawienia optymalnego modelu bezpieczeństwa informacyjnego państwa z uwypukleniem narzędzi analizy zagrożeń i pomiaru ryzyka. Niniejsza rozprawa ma również wykazać zasadność stosowania wobec obszaru bezpieczeństwa informacyjnego państwa (jako określonego systemu) nowoczesnych narzędzi pomiaru i ciągłego doskonalenia jakości, których zbiór znany jest pod pojęciem ***TQM*** *(Total Quality Management - Kompleksowe Zarządzanie Jakością)*[1]. Stosowanie systemu *TQM* w procesach kontroli i zarządzania ma bowiem tę zaletę, że pozwala na płynne doskonalenie podmiotu poddanego oddziaływaniu tych narzędzi, eliminując konieczność dokonywania okresowych, dogłębnych i kapitałochłonnych reform. Podsumowując, praca ma więc na celu nie tylko wykazanie konieczności, wskazanie zakresu i kierunków modernizacji metod zapewnienia bezpieczeństwa informacyjnego, lecz także uzasadnienie potrzeby stałego stosowania narzędzi pomiaru i doskonalenia jakości tego obszaru bezpieczeństwa państwa.

Tak określone cele ogólne pracy stanowią podstawę do sformułowania szczegółowych problemów badawczych, które wyznaczać będą przedmiot analiz empirycznych, przyjętych metod i narzędzi badawczych, ocen jakości bezpieczeństwa informacyjnego państwa oraz wysuwanych propozycji zmian modelowych.

1.3. Problemy badawcze i hipotezy robocze

1.3.1. Problem główny i szczegółowe problemy badawcze

Problem badawczy wynika z zadanej sytuacji problemowej i stanowi ogólnie sformułowane pytanie (z reguły złożone), na które nie mamy gotowej odpowiedzi. W zależności od stopnia złożoności sytuacji problemowej pytanie (pytania) mogą mieć charakter *rozstrzygnięcia* lub charakter *dopełnienia*[2]. Pytania o charakterze dopełnieniowym (zawierające elementy, mające wiele alternatywnych rozwiązań) winny być sprowadzone (*zbinaryzowane*) do pytań rozstrzygnięcia (dających wybór tylko do dwóch przeciwstawnych odpowiedzi).

[1] *Omówione szerzej w podrozdziale* 2.4.4
[2] K. Ajdukiewicz. *Logika pragmatyczna.* PWN. Warszawa 1965 s. 15

C. Doskonalenie zasad **planowania przedsięwzięć bezpieczeństwa** informacyjnego;
D. Realizacja **celów bezpieczeństwa informacyjnego** z typowaniem podmiotów badawczych, wdrożeniowych i realizacyjno-eksploatacyjnych.
E. Dostosowywanie **standardów bezpieczeństwa informacyjnego** do obowiązujących kryteriów międzynarodowych.
F. Zintensyfikowanie stosowania **programów wdrożeniowych** w zakresie bezpieczeństwa informacyjnego państwa jako element przystosowania do nowej sytuacji w **wymiarze sojuszniczym i europejskim.**
G. Stosowanie metod **pomiaru i doskonalenia jakości** bezpieczeństwa informacyjnego z zastosowaniem zbioru narzędzi ***TQM.***

Przedstawione powyżej problemy i szczegółowe kwestie badawcze nie wyczerpują wszystkich zagadnień, które należy podjąć realizując projektowany temat badań. Konieczne jest ich dalsze rozwijanie w kolejnych etapach postępowania badawczego, a także podjęcie badań ewaluacyjnych, aby dać pełniejsze odpowiedzi na tak postawione problemy.

1.3.2. Hipotezy robocze

Na podstawie własnych doświadczeń z działalności związanej z procesem przystąpienia Rzeczypospolitej Polskiej do Organizacji Traktatu Północnoatlantyckiego, aktywności zawodowej w obszarze bezpieczeństwa teleinformatycznego a także w wyniku dokonania analizy systemów bezpieczeństwa informacyjnego państw NATO i Unii Europejskiej - po zapoznaniu się z literaturą przedmiotu i z wynikami dotychczas prowadzonych badań, z wykorzystaniem kontaktów bezpośrednich z przedstawicielami agend NATO i reprezentantami narodowymi w *Podkomitecie Bezpieczeństwa NATO* – autor przyjął w rozprawie następujące hipotezy robocze:

1. **Hipotezy dotyczące słabych stron polskiego systemu bezpieczeństwa informacyjnego:**

   HIPOTEZA 1: W polskim **systemie bezpieczeństwa informacyjnego,** pomimo wprowadzanych zmian legislacyjnych, strukturalnych, organizacyjnych i technicznych - nadal występują liczne niedociągnięcia, braki w świadomości i wyszkoleniu osób funkcyjnych, ma miejsce opóźnienie we wprowadzaniu wspólnych sojuszniczych i unijnych zasad, zawartych w dokumentach o roboczej nazwie *Common Criteria*;

   HIPOTEZA 2: Duża liczba stwierdzonych **naruszeń bezpieczeństwa** informacyjnego świadczy o braku lub o niskiej efektywności narzędzi analizy zagrożeń oraz mechanizmów ich wprowadzania;

   HIPOTEZA 3: Ze względu na trwający proces ujednolicania **norm i standardów narodowych** oraz wzajemnego dostosowania legislacyjnej podbudowy bezpieczeństwa informacyjnego NATO i Unii Europejskiej - **utrudniona jest współpraca międzynarodowa** i wymiana informacji podlegających ochronie, a udział w programach wdrożeniowych nie jest w pełni efektywny.

2. **Hipotezy dotyczące możliwości wdrożenia narzędzi wspomagających politykę bezpieczeństwa informacyjnego państwa:**

   HIPOTEZA 1: Przy zastosowaniu nowoczesnych metod i narzędzi **pomiaru, analizy** i **poprawy jakości** bezpieczeństwa informacyjnego oraz przy wykorzystaniu szansy **rozszerzenia profilu kształcenia i szkolenia** z powyższej problematyki - występuje możliwość zapewnienia bezpieczeństwa informacyjnego państwa.

   HIPOTEZA 2: Wskazanie i zastosowanie wybranych i przeanalizowanych rozwiązań stosowanych w NATO i w państwach Unii Europejskiej przy jednoczesnym korelowaniu **prognozowania rozwoju** narzędzi przetwarzania informacji z procesami **zapewniania jej bezpieczeństwa** stanowi przesłankę interoperacyjnego związania narodowego systemu bezpieczeństwa informacyjnego z sojuszniczym i unijnym.

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

   HIPOTEZA 1: Upowszechnienie nowoczesnych **metod i narzędzi** pomiaru i analizy zagrożeń bezpieczeństwa informacyjnego przy jednoczesnym właściwym doborze treści, form i środków kształcenia i szkolenia będzie stanowić warunek zapewnienia bezpieczeństwa informacyjnego państwa.

HIPOTEZA 2: Realizacja zasady uzyskiwania przewagi informacyjnej (dominacji) przy pełnym wykorzystywaniu własnych, sojuszniczych i europejskich **narzędzi bezpieczeństwa informacyjnego** doprowadzi do właściwego sprzężenia wysiłku osób odpowiedzialnych za efektywność informacyjną i organów uprawnionych do kreowania polityki bezpieczeństwa informacyjnego i sprawowania nad nim funkcjonalnego nadzoru.

HIPOTEZA 3: Optymalne dostosowanie **standardów bezpieczeństwa informacyjnego** z wprowadzeniem nowatorskich metod pomiaru i doskonalenia jakości z zastosowaniem zbioru narzędzi ***TQM*** wraz z wykorzystaniem wybranych wzorców z systemów bezpieczeństwa informacyjnego NATO i państw Unii Europejskiej przy zachowaniu elementów narodowej tożsamości pozwoli na płynne przystosowanie polityki bezpieczeństwa informacyjnego państwa do nowej sytuacji w **wymiarze europejskim i transatlantyckim**.

W wyniku zdefiniowania w ***Rozdziale 1.1*** przedmiotu badań i zinterpretowaniu charakteru zależności pomiędzy zagadnieniami określonymi jako szczegółowe problemy badawcze, można wyróżnić następujące zmienne:

- ***zmienne zależne:*** wartość informacji pola walki, jakość narzędzi analiz i pomiarów bezpieczeństwa informacyjnego, jakość programów i metod nauczania i szkolenia w zakresie bezpieczeństwa informacyjnego, nakłady na bezpieczeństwo informacyjne;
- ***zmienne niezależne:*** stan prawny w zakresie bezpieczeństwa informacyjnego, narodowe normy i kryteria bezpieczeństwa, elementy wzorcowe NATO i państw Unii Europejskiej, dostosowanie standardów bezpieczeństwa do wymogów NATO i UE;
- ***zmienne pośredniczące:*** metody analizy zagrożeń i zarządzania ryzykiem, problematyka certyfikacji i akredytacji, zapewnienie elastyczności rozwiązań wobec wymogów współczesnych operacji informacyjnych.

Doboru i zakwalifikowania zmiennych dokonano kierując się zasadą stosowalności i skuteczności w zadanej sytuacji problemowej, zgodnie z metodologią określającą, że: *„przez zmienne niezależne rozumie się pewne czynniki powodujące określone zmiany w innych czynnikach (zmiennych), a przez zmienne zależne - czynniki, podlegające wyraźnym wpływom ze strony zmiennych niezależnych"*[3].

[3] M. Łobocki. *Metody badań pedagogicznych.* PWN. Warszawa 1978 s. 74

Charakter zależności między wymienionymi zmiennymi nie jest jednolity, gdyż np. wskaźniki ze zbioru zmiennych niezależnych, jakie będą brane pod uwagę w badaniach, jako mające wpływ na zmienne zależne, jedynie z uproszczonego założenia mają charakter stały. Aby właściwie uchwycić, zobrazować i wykazać współzależności między określonymi zmiennymi należy zastosować odpowiednią metodę, za pomocą której nie tylko można będzie zweryfikować postawione hipotezy, ale również rozwiązać problem badawczy. Ze względu na złożony charakter problemu badawczego, należy zastosować metodę umożliwiającą tzw. ***weryfikację projektującą***, tzn. taką, która wywoła spełnienie warunków założonych w hipotezie, a w związku z występowaniem zależności o charakterze złożonym, weryfikacja ta powinna mieć charakter analityczny, syntetyczny i globalny. Taką weryfikację może zapewnić ***analiza systemowa*** jako metoda zawierająca wszystkie wymienione elementy weryfikacyjne. Głębsze uzasadnienie jej wyboru, jej opis oraz sposób osadzenia w zbiorze narzędzi pomiaru i doskonalenia jakości systemów - przedstawiono w ***Rozdziale 4.2.1.***

1.4. Metody, techniki i narzędzia badawcze

Według T. Nowackiego, twórcy pedagogiki pracy określa się *metodę* jako *„sposób wykonania działania, charakteryzujący się szczególnym doborem i układem elementów składowych, przy czym jest to sposób uprzednio przemyślany i zaplanowany, a jednocześnie nadający się do powtórzenia w sytuacjach takich samych lub zbliżonych"*[4]. Wyodrębnia on takie metody, jak: obserwację, badanie wytworów pracy, zbieranie opinii, diagnozowanie.

Sprawdzoną metodą badawczą jest ***ewaluacja***, tj. systematyczne badanie wartości, zalet lub słabości przyjętego projektu. Jest to analiza, a następnie zastosowanie profesjonalnych instrumentów oceny różnorodnych działań i programów społecznych leżących poza bezpośrednim naciskiem scentralizowanych i zazwyczaj wysoce upolitycznionych ośrodków władzy, co staje się wielkim wyzwaniem współczesnych strategii zarządzania, ale także elementem stymulującym rozwój,

efektywność, a przede wszystkim jakość owych działań. Dotyczy to niemal wszystkich sfer naszego życia na przełomie wieków. Uwaga ta w szczególny sposób dotyczy bezpieczeństwa informacyjnego. Od chwili przystąpienia Rzeczypospolitej Polskiej do NATO bezpieczeństwo informacyjne podlega ciągłemu procesowi doskonalenia, nie tylko w sferze programowej i instytucjonalnej, ale w równej mierze pod względem wyposażenia w techniki analizy i oceny rzeczywistych jego efektów, widzianych przy tym znacznie szerzej, niż przez pryzmat rutynowych wskaźników standardowej sprawozdawczości. Dlatego ewaluacja w procesach zapewniania bezpieczeństwa informacji, a także w pomiarze jej wartości, stoi przed zadaniem szczególnym, opisuje bowiem „*efekty*", które nie zawsze są mierzalne, jako że dotyczą nie tylko przyrostu wiedzy, ale także zmian osobowości, postaw i stylu pracy człowieka.

Według P. Sienkiewicza, autora licznych prac z zakresu teorii zarządzania i analizy systemowej *„metoda jest to procedura postępowania, która umożliwia nam w danych warunkach posługiwanie się posiadanymi narzędziami w celu poznania prawdy, poznania obiektywnej rzeczywistości oraz przekształcenia jej zgodnie z przyjętym celem działania*"[5]. *Metoda* jest więc umiejętnością wyboru takiego postępowania w określonej sytuacji problemowej, która umożliwia osiąganie pożądanego celu. *Metodologia*, jako teoria *metody*, powstała pod wpływem rozwoju nauki jako wyraz zaspokojenia potrzeby ogólnej problematyki *metody*, jej stosunku do innych dziedzin.

Kierując się przytoczonymi wyżej definicjami *metody*, dostrzegając w pełni złożoność problematyki, jaką stanowi sfera bezpieczeństwa informacyjnego w Polsce, zastosowano w niniejszej pracy nowoczesną *metodę badawczą*, stanowiącą jednocześnie zbiór technik analitycznych i procedur - ***analizę systemową.***

Niesprawne i sztywne struktury organizacyjne systemu bezpieczeństwa informacyjnego państwa oraz brak bezpośrednich i efektywnych więzi tego systemu ze źródłami informacji to jedna z głównych barier rozwoju. W warunkach polskich jest to jeden z wielu czynników hamujących przebieg transformacji systemowej,

[4] T. Nowacki. *Metodologia Pedagogiki Pracy*. WSiP. Warszawa. 1978. s. 53 - 59
[5] P. Sienkiewicz. *Analiza systemowa. Podstawy i zastosowania*. Bellona 1994 s. 35

utrudniających zapewnienie interoperacyjności z sojusznikami i organami NATO oraz proces integracji w ramach Unii Europejskiej i przyśpieszenie przemian zmierzających do ogólnej racjonalizacji działania.

Złożoność sfery bezpieczeństwa informacyjnego państwa wymaga ***podejścia*** i ***działań systemowych***. Według J. Koniecznego *„zrozumieć współczesny świat może tylko ten, kto rozumie systemy w nim występujące. Otaczający nas świat jest bowiem pełen systemów, wśród których wypadło nam żyć i działać. Rządzą się one swoistymi, obiektywnymi prawami, które człowiek współczesny musi poznać, aby być świadomym podmiotem działania w tym świecie systemów. Widzenie i myślenie systemowe stało się dzisiaj nie tylko modną rozrywką, lecz także życiową koniecznością. Muszą dziś zgłębić systemowe prawa planiści i projektanci, producenci, badacze i nauczyciele, czyli uczestnicy złożonych działań realizowanych w złożonych realnych systemach"*[6].

Zalety analizy systemowej jako metody badań przedstawił przekonywująco A.K. Koźmiński, pisząc o teorii organizacji, iż:

1. *Analiza systemowa, traktując organizację jako **system** sprzyja podejmowaniu decyzji z całościowego punktu widzenia, przeciwdziałając tym samym tendencjom do suboptymalizacji, czyli traktowania poszczególnych części jako „samych dla siebie" i usprawniania ich ze szkodą dla funkcjonowania całości.*

2. *Analiza systemowa stwarza dogodną płaszczyznę współpracy między ekspertami reprezentującymi różne dziedziny wiedzy, rozwijające się dotąd w izolacji od siebie, oraz między interdyscyplinarnymi zespołami ekspertów, a kierownictwem organizacji.*

3. *Analiza systemowa stwarza szansę rozwiązywania na naukowych podstawach zasadniczych dla funkcjonowania organizacji problemów słabo ustrukturalizowanych, które dotąd rozwiązywano opierając się jedynie na intuicji, doświadczeniu, wyczuciu itp.*

4. *Analiza systemowa pozwala na syntezę elementów tak różnych, jak intuicja, wyczucie, opis wywodzący się z nauk społecznych i badania operacyjne. Stwarza ona szansę przezwyciężenia sprzeczności między kwantyfikowanymi i niekwantyfikowanymi metodami i procedurami podejmowania decyzji.*

5. *Dzięki zastosowaniu badań operacyjnych wszędzie tam, gdzie to możliwe, analiza systemowa czyni procedury decyzyjne bardziej precyzyjnymi, obiektywnymi i sprawdzalnymi. Równocześnie jednak nie zawiera w sobie*

[6] J. Konieczny. *Inżynieria systemów działania.* WNT. Warszawa 1983. s. 11

postulatu stosowania wyłącznie metod kwantyfikowanych, pozwalając uświadomić granice ich stosowania i tym samym zapobiec ogromnym nieraz kosztom pomyłek, wynikających z nadmiernych uproszczeń...[7].

Rozwiązywanie sytuacji problemowych wymaga więc działań i metod systemowych. Tworzenie, rozwijanie i doskonalenie tych metod to zadanie współczesnych badań systemowych. Już Arystoteles stwierdził, że *„całość to więcej niż suma poszczególnych części"*. Tą całością, będącą przedmiotem badań jest ***SYSTEM***, w podjętej pracy - system bezpieczeństwa informacyjnego państwa.

Według P. Sienkiewicza *„**systemem** określa się każdy złożony obiekt wyróżniony w badanej rzeczywistości, stanowiący całość tworzoną przez zbiór obiektów elementarnych i powiązań między nimi"*[8]. Wśród metod stosowanych w badaniach systemowych, których celem jest zaspokojenie zidentyfikowanych wcześniej potrzeb i rozwiązanie szczególnych sytuacji problemowych, na czoło wysuwa się ***analiza systemowa.***

Analiza systemowa jest :

- zbiorem metod i technik analitycznych, ocenowych i decyzyjnych, służących racjonalnemu rozwiązywaniu systemowych sytuacji decyzyjnych;
- badaniem wspomagającym działania osób odpowiedzialnych za decyzje lub linie postępowania w warunkach niepewności i ryzyka[9].

Do podstawowych zalet analizy systemowej należy zaliczyć takie cechy, jak: wprowadzenie znacznej dozy obiektywizmu do procesu, który jest w znacznej mierze subiektywny, uwzględnienie szerszego kontekstu do badań obiektu, a także uwzględnienie czynnika niepewności i ryzyka. Ponadto analiza systemowa pozwala skoncentrować uwagę na skutkach działania, dzięki czemu może sprzyjać ujawnieniu nieprzewidzianych następstw analizowanego działania. Niepodważalną zaletą metody jest niejako zmuszenie uczestników rozwiązywania problemu do jednolitej i systematycznej oceny i racjonalnego porównywania wariantów systemów. Powiązanie metod analizy systemowej z nowoczesnym **zbiorem narzędzi** pomiaru i poprawy jakości ***TQM*** (*Total Quality Management - Kompleksowe Zarządzanie Jakością)* pozwala nie tylko na wnikliwą analizę problemu badawczego, ale również na **ciągłe**

[7] A.K. Koźmiński. *Analiza systemowa organizacji.* WP. Warszawa 1976 s. 41
[8] P. Sienkiewicz. *Analiza systemowa. Podstawy i zastosowania.* Bellona 1994

doskonalenie jakości wypracowanego modelu, w przypadku niniejszej rozprawy - systemu bezpieczeństwa informacyjnego państwa.

W klasycznym (według Instytutu *RAND*[10]) ujęciu analizy systemowej przyjmuje się następujący schemat postępowania:

1. Analiza problemu:
   a) jaki problem ma być rozwiązany i co jest celem jego rozwiązania?;
   b) jak działa obecny system i jakie niedostatki (braki) występują w jego działaniu?;
   c) jakie wymagania i ograniczenia są istotne dla systemu?
2. Analiza funkcji:
   a) jakie funkcje powinien spełniać system?;
   b) określenie istotnych czynników, od których zależy pełnienie poszczególnych funkcji;
   c) określenie zależności między istotnymi czynnikami.
3. Opracowanie wariantów - alternatywnych rozwiązań systemu.
4. Identyfikacja systemów konkurencyjnych dla danego (analizowanego) systemu.
5. Opracowanie modelu ocenowego systemu (kryteria oceny, zależności, charakterystyki wpływu otoczenia).
6. Opracowanie dodatkowych rozwiązań alternatywnych dla systemu.

Celem wypracowania najbardziej efektywnego kierunku doskonalenia bezpieczeństwa informacyjnego - należy zastosować metodę, która w praktyce sprowadza się do wykorzystania zbioru procedur analitycznych. Procedury analityczne ukierunkowane na rozwiązanie systemowych sytuacji decyzyjnych są oparte na zadanych wstępnie warunkach, narzędziach weryfikacji i możliwie pełnym banku danych. Jednym z kryteriów klasyfikacji analizy systemowej jest kryterium ilościowo-jakościowe. Z kolei według kryterium rodzaju wyniku analizy wyróżnia się analizę: problemową, identyfikacyjną, diagnostyczną, prognostyczną, efektywności i decyzyjną.

Uzasadnienie wyboru analizy systemowej jako metody analitycznej i doboru technik badawczych przedstawiono w ***Rozdziale 4.2.1.***

---

[9] *Ibidem*

[10] *RAND Corporation. 1700, Main Street, Santa Monica CA USA* - Instytut zajmujący się od 1948 r. studiami strategicznymi i inżynierią systemów

1.4.1. Modelowanie procesów pomiaru i doskonalenia parametrów jakościowych bezpieczeństwa informacyjnego z zastosowaniem systemu (zbioru narzędzi) TQM

Tradycyjne systemy zarządzania i kontroli wszelkich obiektów (systemów), ograniczające się do sterowania procesami szeroko pojętej produkcji (ukierunkowanej działalności) niejako „*od wewnątrz*", spełniają swoje zadania jedynie do momentu wyczerpania się własnego potencjału doskonalenia jakości danego obiektu (systemu). Ujawnia się wówczas niedostosowanie obiektu (systemu) do zmieniających się warunków zewnętrznych, skutkujące mniej lub bardziej dolegliwym „*kryzysem*" w jego funkcjonowaniu. Narastanie tego kryzysu wyzwala określone, zewnętrzne „*siły reformatorskie*", które, z reguły kosztem wstrzymania lub co najmniej wyhamowania procesów produkcyjnych, dokonują głębokich, kapitałochłonnych przeobrażeń danego obiektu (systemu), po czym następuje okres weryfikacji przyjętych założeń, najczęściej również kosztowny i połączony ze stratami, wynikającymi z konieczności realizacji przedsięwzięć korekcyjnych, prowadzących czasem nawet do podważenia założeń reformatorskich i wypracowania kolejnych. W powszechnie znanej opinii obiekt (system) jakim jest bezpieczeństwo informacyjne również nie ustrzegł się w ostatnich latach procesów o tym charakterze.

W ostatnich latach intensyfikacja światowych badań nad funkcjonowaniem systemów doprowadziła jednak do wypracowania procedur, które mogą przyczynić się do wyeliminowania lub przynajmniej ograniczenia negatywnych zjawisk w procesach sterowania, zarządzania i kontroli, nie wyłączając sektora bezpieczeństwa państwa, w tym bezpieczeństwa informacyjnego.

Dążenie do ciągłej poprawy jakości stanowiło punkt wyjścia dla twórców systemu ***Kompleksowego Zarządzania Jakością - TQM*** (*Total Quality Management*), sformułowanego i rozwiniętego przez zespół amerykańskich naukowców na bazie filozofii *naukowej organizacji pracy* F.W. Taylora

„*Kompleksowe Zarządzanie Jakością - TQM jest metaforą do procesu i związanego z nim systemu zarządzania podlegających ciągłym zmianom i stworzonych zarówno dla spełnienia ogólnokulturowej misji oraz dla praktyki gospodarczej i*

wszelkich innych przedsięwzięć, sprowadzaną praktycznie do podążania za ciągłą poprawą uzyskiwanej jakości wytwarzanych wyrobów czy też świadczonych usług"[11].

TQM jest rygorystycznym, wyspecjalizowanym procesem, zaprojektowanym w celu sprostania wyzwaniom bieżącej praktyki mającym na celu doskonalenie umiejętności jak najrzetelniejszego spełniania oczekiwań i wymagań klientów. Zasada realizacji ciągłej poprawy jakości implikuje działania, których głównym celem jest doskonałość wyrobów czy też usług (np. informacyjnych).

W dotychczasowych procesach doskonalenia jakości pracy (informacji) dominuje kontrola produktu końcowego, a nie zjawiska zachodzące w trakcie procesu. System *TQM* zmienia tę zasadę – proces wymiany informacji nie może być traktowany jako zbiór docelowych, liniowych, następujących po sobie odcinków komunikacji jednostronnej, lecz jako proces spiralny, wzorowany na *spirali postępu Jurana* czy *układzie cyklicznym Deminga* (nazywanym w niektórych źródłach *wykresem Guilbert'a*) - ***Diagram Nr 15 s. 131.***

W odróżnieniu od międzynarodowych norm jakości *ISO 9000*, które są standardem - *TQM* jest zbiorem narzędzi nacechowanym określoną strategią postępowania. Wdrażanie *TQM* w obszarze bezpieczeństwa należy uwzględnić przy wprowadzaniu *Systemu Zapewnienia Jakości ISO 9000*, uznawanego w 73 krajach świata (odpowiednik polski *PN-EN 29000*), stanowiącego niejako szkielet koncepcji *TQM*. Wdrożenie norm *ISO* w polityce bezpieczeństwa informacyjnego państwa zapewni:

- włączenie wszystkich zaangażowanych w proces przetwarzania informacji do pracy nad poprawą jakości tego procesu i zapewnieniu mu bezpiecznego środowiska;
- ustalenie jednoznacznych, precyzyjnych kryteriów i miar;
- ustalenie standardów postępowania.

Rdzeniem i jednocześnie siłą zbioru narzędzi *TQM* jest wzajemne powiązanie dwóch głównych celów jego zastosowania: pomiaru jakości (efektywności) działań i doskonalenie systemu, którego parametry podlegają pomiarowi. Narzędzia stosowane

[11] M. Piotrowski. *Totalne Zarządzanie Jakością,*. ITE-EiP. Radom-Warszawa 1997, s. 153

w procesach wspomaganych przez *TQM* pozwalają na realizację obydwu celów. Do narzędzi tych należą:

1. Grupa główna - 7 narzędzi tradycyjnych (*Seven Tools*):

- ***szczegółowa sieć działań*** - schemat kolejnych etapów przebiegu procesu z zestawieniem działań niezbędnych do osiągnięcia głównego celu, działań wspomagających i działań pomocniczych;
- ***diagram Ishikawy*** - schemat przyczynowo-skutkowy typu „rybi szkielet", pozwalający na identyfikację czynników określających przyczyny wywołujące skutki, np. niepowodzenia;
- ***zasada Pareto 80/20*** - wykres pozwalający na rozpoznanie czynników mających najistotniejszy wpływ na przebieg procesu („źródłem 80% problemów w procesie jest 20% czynników mających wpływ na jego przebieg");
- ***wykres rozrzutu*** - analiza zależności między dwiema zmiennymi celem określenia ich związku przyczynowo-skutkowego;
- ***cykl Deminga*** - zamknięty obieg procesowy: planowanie - wykonanie - badania - działanie, przydatny w procesie ciągłego doskonalenia;
- ***histogram*** - wykres słupkowy obrazujący rozkład dwóch danych z możliwością określenia prawidłowości przebiegu procesu;
- ***formularz kontroli statystycznej*** - graficzne przedstawienie przebiegu i zmienności trwającego procesu z kontrolą ewentualnego przekraczania określonych limitów.

2. Grupa narzędzi *pomiaru jakości*:

- ***schemat pokrewieństw*** - porządkowanie danych poprzez grupowanie czynników, między którymi istnieje naturalny związek;
- ***pole sił*** - zobrazowanie i rozdzielenie czynników wspomagających proces oraz przeszkód na drodze jego realizacji;
- ***schemat wpływów*** - macierz pomiaru siły oddziaływania czynników mających wpływ na przebieg procesu;
- ***lista kontrolna*** - rejestrator informacji o przedsięwzięciach mających wpływ na powodzenie procesu;
- ***koło decyzji*** - schemat znany również pod nazwą „*diagram rozchodzących się efektów*", dający możliwość przewidywania i analizowania skutków podjętych decyzji.

Zastosowanie kryteriów *Kompleksowego Zarządzania Jakością TQM* w polityce bezpieczeństwa informacyjnego państwa obok wymiernych korzyści polegających na ciągłym pomiarze i doskonaleniu jakości pozwoliłoby na odwrócenie dotychczasowej hierarchii procesu informacyjnego w kierunku upodmiotowienia samej informacji jako najważniejszego ogniwa systemu. Wprowadzeniu *TQM* będącego zbiorem narzędzi, procedurą, a nie normą, powinno towarzyszyć wdrożenie *Systemu Zapewnienia Jakości ISO 9000* (*PN-EN 29000*), jako międzynarodowego standardu jakości. Jest to niezbędne ze względu na konieczność porządkowania problemów zarządzania, będącego jednym z czynników warunkujących jakość bezpieczeństwa państwa, w tym bezpieczeństwa informacyjnego.

Według M. Piotrowskiego do czynników warunkujących wprowadzanie systemu *TQM* należą:

- efektywne przewodnictwo;
- prowadzenie **analizy systemowej**;
- zdolność rozwiązywania problemów;
- prowadzenie działalności szkoleniowo-treningowych;
- prowadzenie poradnictwa;
- łatwość nawiązywania i utrzymywania kontaktów międzyludzkich;
- zdolność do tworzenia zespołów i kierowania nimi[12].

Zastosowanie systemu *TQM* i wybranych jego narzędzi pozwala na zdefiniowanie i ocenę procesów zachodzących w obszarze bezpieczeństwa informacyjnego państwa. W ***Rozdziale 241*** wykorzystano system *TQM* w omawianym procesie zarządzania bezpieczeństwem informacyjnym przez organa ustawowo powołane do tego zadania.

1.4.2. Wybór analizy systemowej jako metody badawczej

Główny problem badawczy niniejszej rozprawy polega na wykazaniu potrzeby, określeniu możliwości i kierunków oraz wskazaniu zakresu i sposobu doskonalenia systemu bezpieczeństwa informacyjnego celem efektywnego włączenia go w trwający

proces transformacji państwa z jednoczesnym nadaniem cech sprzyjających integracji z Unią Europejską.

Analizując zadanie należy stwierdzić, że ogólnie system bezpieczeństwa informacyjnego istnieje, znana jest jego struktura i zachowanie (reguły działania); poszukuje się takich parametrów na wejściu, dla których zachowanie systemu jest najkorzystniejsze w sensie przyjętego kryterium.

Uzasadnienie wyboru analizy systemowej

Analiza systemowa ma na celu określenie pożądanego działania lub linii postępowania przez rozpoznanie i rozważenie dostępnych wariantów oraz porównanie przewidywanych ich, bliższych i dalszych, skutków.

Analiza systemowa - podstawowe etapy :

- zbadanie celów działania (akcji lub linii postępowania);
- zbadanie możliwych sposobów osiągnięcia zamierzonych celów z uwzględnieniem nowych alternatywnych rozwiązań;
- ocena pozytywnych i negatywnych, bliższych i dalszych skutków każdego z możliwych wariantów działania uwzględniająca niepewność przyszłości i ryzyko;
- analiza porównawcza wariantów działania według różnych kryteriów efektywności i przedstawienie wyników w sposób umożliwiający wybór - decyzję.

Rozwiązywanie problemów systemowych poprzez realizację procedur przekształcających w funkcji czasu przedstawia następujący diagram:

[12] *Ibidem*, s.178

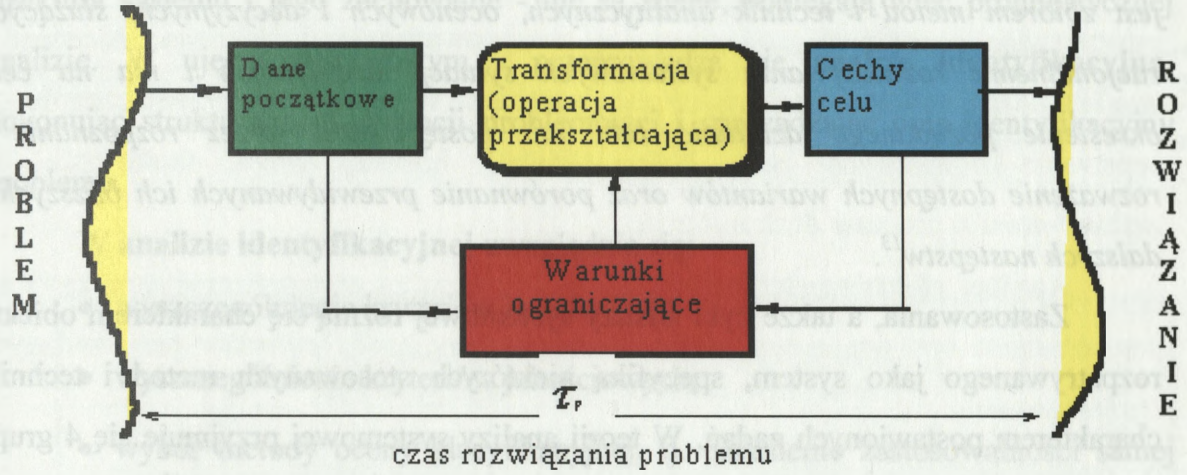


Diagram 2: Schemat rozwiązywania problemów systemowych

Źródło: P. Sienkiewicz. *Analiza systemowa. Podstawy i zastosowania*. Bellona 1994

Dany jest system początkowy, należy określić taki system końcowy, który spełnia ustalone wymagania (*cele, ograniczenia...)*. Mamy tu do czynienia z zadaniami optymalizacyjnymi, czyli z poszukiwaniem systemu optymalnego w sensie przyjętego kryterium i dla danych ograniczeń. Określony w ten sposób system końcowy może służyć za wzorzec, do którego porównuje się inne warianty systemu, lub jako wariant rekomendowany przez analityka systemów. Często system optymalny jest trudny do praktycznej realizacji, powstaje bowiem w wyidealizowanych raczej warunkach. Wtedy - w rezultacie kompromisu między systemem początkowym, ale niezadowalającym z określonego punktu widzenia, a systemem optymalnym, lecz trudnym do wdrożenia - przyjmuje się system zalecany. Spełnia on warunki wynikające ze studium stosowalności.

Definiując analizę systemową jako uporządkowany zbiór procedur (technik) analityczno-ocenowych wspomagających rozwiązywanie systemowych sytuacji decyzyjnych w warunkach niepewności i ryzyka - przyjmuje się klasyczny schemat analizy systemowej - wypełniając treścią poszczególne jego elementy i definiując zadanie: *dokonać optymalizacji wyboru metody doskonalenia bezpieczeństwa informacyjnego Rzeczypospolitej Polskiej w funkcji członkostwa w NATO i w Unii Europejskiej.*

***Analiza systemowa** przyjęta jako metoda badawcza przedmiotowego materiału jest zbiorem metod i technik analitycznych, ocenowych i decyzyjnych, służących racjonalnemu rozwiązywaniu systemowych sytuacji decyzyjnych i ma na celu określenie pożądanego działania lub linii postępowania przez rozpoznanie i rozważenie dostępnych wariantów oraz porównanie przewidywanych ich bliższych i dalszych następstw*[13].

Zastosowania, a także cykl analizy systemowej różnią się charakterem obiektu rozpatrywanego jako system, specyfiką niektórych stosowanych metod i technik, charakterem postawionych zadań. W teorii analizy systemowej przyjmuje się 4 grupy (klasy) *sytuacji systemowej*[14]:

I. System istnieje, znana jest jego struktura i zachowanie (reguły działania); poszukuje się takich parametrów na wejściu, dla których zachowanie systemu będzie najkorzystniejsze w sensie przyjętego kryterium.

II. System istnieje, znana jest jego struktura; na podstawie struktury należy określić jego prawdopodobne (pożądane) zachowanie.

III. System istnieje, ale nie jest znana jego struktura ani jego zachowanie; należy określić prawdopodobne zachowanie i na tej podstawie wnioskować o strukturze systemu, a następnie określić warunki istnienia struktury pożądanej.

IV. System dotychczas nie istnieje, jednak ma być zbudowany i należy zaprojektować taką jego strukturę, aby system z określonym prawdopodobieństwem wykazywał pożądane zachowanie (funkcjonowanie).

Dla powyższych sytuacji charakterystyczne są zadania identyfikacji systemu (parametrów, reguł, struktury) oraz optymalizacja struktury i funkcjonowania systemu. W przypadku zastosowania analizy systemowej do oceny przystosowania bezpieczeństwa informacyjnego do wymogów interoperacyjności z NATO i do pełnej integracji z Unią Europejską oraz wypracowania modelu polityki bezpieczeństwa informacyjnego państwa - znajduje zastosowanie **grupa III,** bowiem system bezpieczeństwa informacyjnego istnieje i funkcjonuje, podlega przeobrażeniom wynikającym z zabiegów reformatorskich, ze względu jednak na brak pełnej wiedzy o

[13] P. Sienkiewicz. *Analiza systemowa. Podstawy i zastosowania.* Warszawa. Bellona 1994.
[14] *Ibidem*

wpływie *Ustawy o Ochronie Informacji Niejawnych* z 1999 roku na jego jakość - struktura systemu i jego zachowanie - nie są znane, podlegają więc prognostycznej analizie. W ujęciu systemowym - przeprowadza się **analizę identyfikacyjną,** dokonując strukturalizacji sytuacji problemowej i sporządzając opis identyfikacyjny problemu.

W **analizie identyfikacyjnej** uwzględnia się:

- wyszczególnienie kryteriów ilościowych;
- wyszczególnienie kryteriów jakościowych;
- wybór metody oceny klasyfikacyjnej, tj. określenie zastosowalności samej analizy systemowej.

Nawiązując do treści zadania przeprowadza się **analizę problemową,** zmierzającą do określenia i rozważenia czynników wpływających na stan systemu:

- zbadanie celów działania (akcji lub linii postępowania);
- zbadanie możliwych sposobów osiągnięcia zamierzonych celów;\
- określenie czynników wpływających na stan systemu.

Celem **analizy diagnostycznej** jest :

- określenie zbioru cech i zbioru stanów systemu;
- określenie zasad wyboru metody transformacji;
- określenie kryteriów jakościowych wyboru.

Określenie zbioru cech i zbioru stanów przyjętego systemu optymalizacji pozwala na określenie zadawalającego lub niezadowalającego stanu systemu, co jest właściwym celem analizy diagnostycznej. Wynik pozwala określić przyjętą metodę oceny jako wiarygodną. Potwierdzeniem powyższego poprzez wypełnienie analizy diagnostycznej konkretną treścią jest opis przebiegu procesu na założonych warunkach.

Na **analizę prognostyczną** składa się :

- określenie zbioru alternatywnych opisów przyszłości systemu;
- analiza uwarunkowań osiągania stanów przyszłych;
- określenie założeń programu rozwoju systemu.

Biorąc pod uwagę złożoność i niejednorodność problematyki bezpieczeństwa informacyjnego państwa - celowym jest przeprowadzenie dodatkowej procedury - **analizy porównawczej**, mającej na celu wskazanie występujących w poszczególnych państwach pożądanych cech bezpieczeństwa informacyjnego, możliwych do zastosowania w procesie doskonalenia.

Analiza efektywności polega na realizacji zadań optymalizacyjnych, czyli na poszukiwaniu systemu optymalnego w sensie przyjętych kryteriów przy zadanych ograniczeniach.

Na **analizę decyzyjną** składają się następujące przedsięwzięcia :

- określenie sytuacji decyzyjnej;
- analiza sytuacji decyzyjnej;
- określenie funkcji użyteczności na zbiorach działań i modelach;
- poszukiwanie możliwości realizacji wariantu - model systemu.

Podsumowaniem procesu analitycznego w analizie systemowej jest **decyzja wyboru** pomiędzy wariantami rozwiązania zadania. W analizie decyzyjnej - po zdefiniowaniu możliwych wariantów należy znaleźć odpowiedź na pytanie: *czy wykonalność wariantu jest zadowalająca ?*

W celu odpowiedzi na to pytanie należy ocenić możliwość realizacji każdego wariantu poprzez porównanie z założonymi kryteriami i ograniczeniami. Wynikiem powyższego jest kolejna eliminacja wariantów niedopuszczalnych i niemożliwych do realizacji, a w jej wyniku - wybór wariantu i ostateczna decyzja - wynik rozwiązania postawionego zadania.

Strukturę analizy systemowej w zakresie rozpatrywanego obiektu - systemu bezpieczeństwa informacyjnego państwa przedstawia schemat:

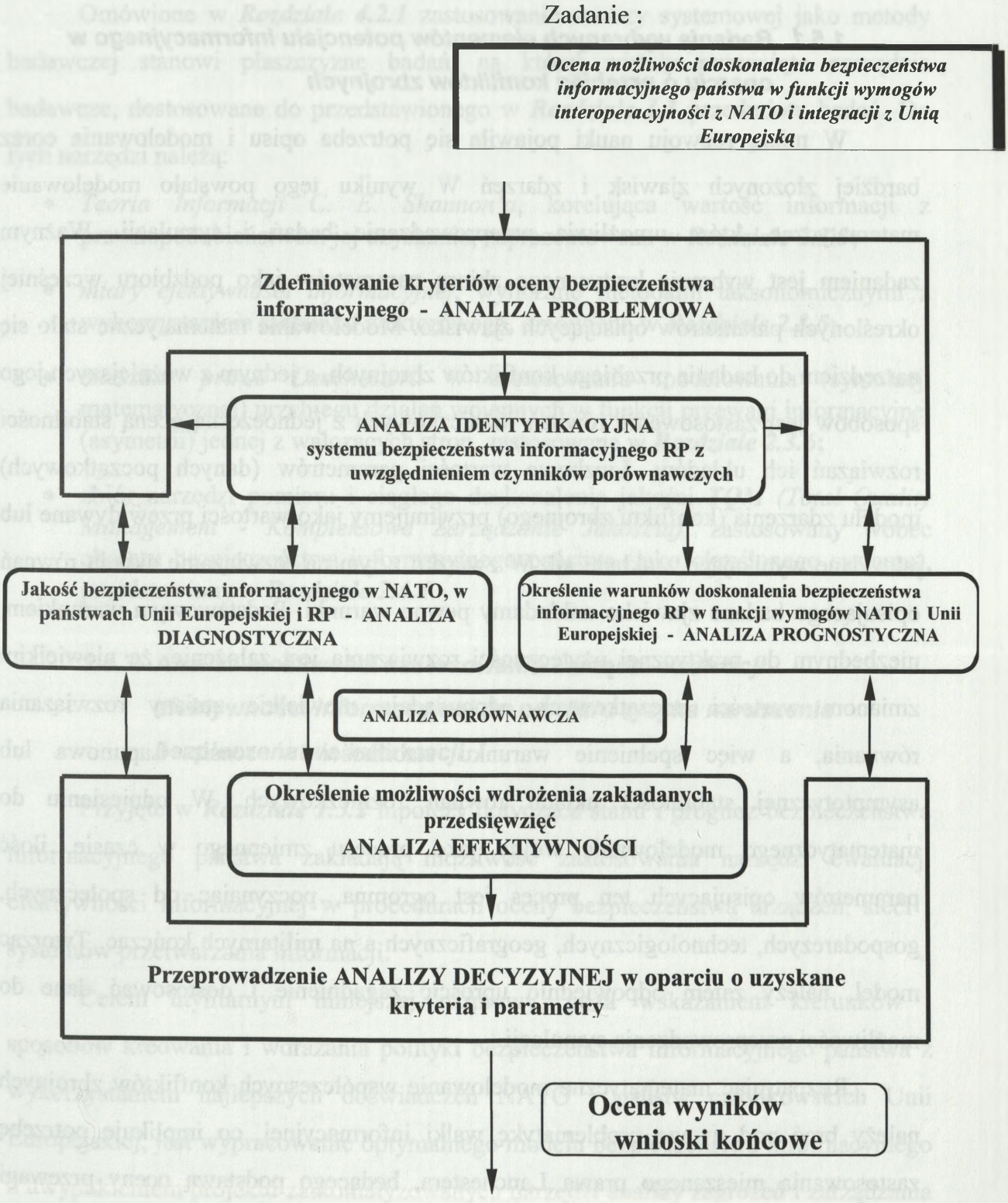


Diagram 3: ***Analiza systemowa bezpieczeństwa informacyjnego – procedury***

Źródło: P. Sienkiewicz. *Analiza systemowa. Podstawy i zastosowania.* Bellona 1994

1.5. Obszar i organizacja badań

1.5.1. Badania wybranych elementów potencjału informacyjnego w oparciu o przebieg konfliktów zbrojnych

W miarę rozwoju nauki pojawiła się potrzeba opisu i modelowania coraz bardziej złożonych zjawisk i zdarzeń W wyniku tego powstało modelowanie matematyczne, które umożliwia przeprowadzenie badań i symulacji. Ważnym zadaniem jest wybranie krytycznego zbioru parametrów jako podzbioru wcześniej określonych parametrów opisujących zjawisko. Modelowanie matematyczne stało się narzędziem do badania przebiegu konfliktów zbrojnych, a jednym z ważniejszych jego sposobów jest zastosowanie równań różniczkowych z jednoczesną oceną stabilności rozwiązań ich układów. Liczbowe wartości parametrów (danych początkowych) modelu zdarzenia (konfliktu zbrojnego) przyjmujemy jako wartości przewidywane lub jako dane wynikające z układu sił. W związku z tym na rozwiązanie układu równań opisującego badane zjawisko nakładamy pewne warunki. Podstawowym warunkiem, niezbędnym do praktycznej użyteczności rozwiązania jest założenie, że niewielkim zmianom wartości początkowych odpowiadają niewielkie zmiany rozwiązania równania, a więc spełnienie warunku stabilności w sensie Lapunowa lub asymptotycznej stabilności układu równań różniczkowych. W odniesieniu do matematycznego modelowania wojny jako procesu zmiennego w czasie, ilość parametrów opisujących ten proces jest ogromna, poczynając od społecznych, gospodarczych, technologicznych, geograficznych a na militarnych kończąc. Tworząc model, należy zatem odpowiednio uprościć zagadnienie i dostosować dane do możliwości przeprowadzenia symulacji.

Rozpatrując matematyczne modelowanie współczesnych konfliktów zbrojnych należy brać pod uwagę problematykę walki informacyjnej, co implikuje potrzebę zastosowania mieszanego prawa Lanchestera, będącego podstawą oceny przewagi informacyjnej jednej ze stron. Rozwinięcie matematycznego modelu przebiegu konfliktu zbrojnego z uwzględnieniem przewagi (dominacji) informacyjnej zawarto w ***Rozdziale 2.3.6*** w oparciu o operację *Iraqi Freedom*.

1.5.2. Dostosowanie narzędzi badawczych do celów badań

Omówione w ***Rozdziale 4.2.1*** zastosowanie analizy systemowej jako metody badawczej stanowi płaszczyznę badań, na której zostały rozwinięte narzędzia badawcze, dostosowane do przedstawionego w ***Rozdziale 1.1*** przedmiotu badań. Do tych narzędzi należą:

- *Teoria Informacji C. E. Shannon'a*, korelująca wartość informacji z prawdopodobieństwem jej uzyskania, zaprezentowana w ***Rozdziale 2.3.3***;
- *miary efektywności informacyjnej*, wyliczane metodami taksonomicznymi z wykorzystaniem rachunku wektorowego, omówione w ***Rozdziale 2.3.5***;
- *mieszane prawo Lanchestera* w zastosowaniu modelowania (symulacji matematycznej) przebiegu działań wojennych w funkcji przewagi informacyjnej (asymetrii) jednej z walczących stron, zastosowane w ***Rozdziale 2.3.6***;
- zbiór narzędzi pomiaru i ciągłego doskonalenia jakości ***TQM*** *(Total Quality Management - Kompleksowe Zarządzanie Jakością),* zastosowany wobec obszaru bezpieczeństwa informacyjnego państwa (jako określonego systemu), przedstawiony w ***Rozdziale 2.4.4***.

1.5.3. Analiza możliwości zastosowania narzędzi ewaluacji efektywności informacyjnej do pomiaru ryzyka naruszenia bezpieczeństwa informacji

Przyjęte w ***Rozdziale 1.3.2*** hipotezy dotyczące stanu i prognoz bezpieczeństwa informacyjnego państwa zakładają możliwość zastosowania narzędzi ewaluacji efektywności informacyjnej w procedurach oceny bezpieczeństwa urządzeń, sieci i systemów przetwarzania informacji.

Celem utylitarnym niniejszej rozprawy, poza wskazaniem kierunków i sposobów kreowania i wdrażania polityki bezpieczeństwa informacyjnego państwa z wykorzystaniem najlepszych doświadczeń NATO i państw członkowskich Unii Europejskiej, jest wypracowanie optymalnego modelu bezpieczeństwa informacyjnego z uwypukleniem projektu zautomatyzowanych narzędzi analizy zagrożeń i zarządzania ryzykiem.

Zakładając właściwą efektywność przyjętych narzędzi badawczych do pomiaru wartości informacji – zamiarem niniejszej rozprawy jest wykazanie możliwości ich

zastosowania w projektowanym modelu dostosowawczym narodowego systemu analizy ryzyka w zakresie bezpieczeństwa informacyjnego państwa. Szczególnie przydatne w tym zakresie będą taksonomiczne metody pomiaru z narzędziem, jakim jest rachunek wektorowy, oparty o wypracowanie wzorca bezpieczeństwa i dokonywanie obliczeń *miar podobieństw* i *miar dystansów* w poszczególnych kategoriach z wykorzystaniem cech obiektu, podzielonych na *stymulanty* i *destymulanty* efektywnościowe obiektu badań.

1.5.4. Organizacja badań

Dla celów niniejszej rozprawy przyjęto trójetapową organizację badań.

Pierwszy etap poświęcono badaniom wstępnym, które służyły weryfikacji problemów, narzędzi, i metod badawczych.

Drugi etap objął badania podstawowe, podczas których dokonano opisu stanu bezpieczeństwa informacyjnego w Polsce, jego powiązań z miarami efektywności informacji pola walki oraz ukazano mechanizmy pomiaru zagrożeń i zapewnienia bezpieczeństwa informacyjnego w NATO i w państwach Unii Europejskiej. Etap ten poza funkcją opisowo-charakteryzującą objął również, zgodnie z teorią organizacji badań, elementy podejścia pozytywnego - uwypuklenie dodatnich i świadczących o narodowej tożsamości cech polskiego systemu bezpieczeństwa informacyjnego.

Trzeci etap poświęcono wielofunkcyjnej analizie systemowej z organizacyjnym ujęciem wg tzw. *programu negatywnego*, tj. ukierunkowanego na eliminację stwierdzonych mankamentów przedmiotu badań oraz zaproponowaniu modelu procesu analizy zagrożeń i zarządzania ryzykiem informacyjnym, uwzględniającego wskazane w wyniku analizy wymogi obszaru badań.

Badania empiryczne przeprowadzone w latach 2001-2003 i zakres działań analitycznych realizowanych przez autora rozprawy bazowały na:

- doświadczeniu nabytym w czasie pracy w obszarze bezpieczeństwa informacyjnego;
- zaangażowaniu w proces przygotowań do integracji z NATO w zakresie dostosowania do wymogów sojuszniczych;
- studiowaniu przedmiotowej literatury krajowej i zagranicznej;

- kontaktach i konsultacjach z osobami funkcyjnymi *krajowych władz bezpieczeństwa* i *służb ochrony państwa*;
- kontaktach zagranicznych bezpośrednich :
  - udział w pracach *Podkomitetu SC4 NATO* - bezpieczeństwo. teleinformatyczne;
  - udział w pracach wyspecjalizowanych grup roboczych NATO;
  - uczestnictwo w krajowych i zagranicznych konferencjach i sympozjach związanych z bezpieczeństwem informacyjnym;
- prowadzeniu w okresie ostatnich 3 lat zajęć dydaktycznych na *Zaocznych Podyplomowych Studiach Bezpieczeństwa Informacyjnego* w Akademii Obrony Narodowej;
- kontaktach korespondencyjnych, w wyniku których uzyskano liczne materiały krajowe i zagraniczne obejmujące problematykę bezpieczeństwa informacyjnego:
- wykorzystaniu zasobów bibliotecznych krajowych i zagranicznych ośrodków naukowych i badawczych;
- wykorzystaniu publicznych sieci komputerowych.

Terenem badań jest ogólnie rozumiany obszar bezpieczeństwa informacyjnego w Polsce, w NATO i Unii Europejskiej bez przywiązania do określonej jednostki organizacyjnej, co wynika z uniwersalnego charakteru problemu badawczego.

Zakłada się, że w rezultacie przeprowadzonej pracy badawczej zostanie wykazana potrzeba wdrożenia zbioru narzędzi pomiaru jakości i doskonalenia bezpieczeństwa informacyjnego państwa, zostanie wypracowany model systemu analizy zagrożeń i zarządzania ryzykiem w tym obszarze, a w wyniku postępowania analitycznego i odwzorowania graficznego z uwzględnieniem wybranych wzorców międzynarodowych, przedstawiona zostanie prognoza jego zastosowania z jednoczesnym potwierdzeniem koncepcji stałego stosowania nowoczesnego zbioru narzędzi pomiaru i doskonalenia jakości - *TQM*. Tym samym zostaną osiągnięte cele badań: poznawczy i utylitarny. Realizacja ich będzie możliwa przy zastosowaniu niekonwencjonalnych metod i narzędzi badawczych (analizy systemowej i procedur zarządzania jakością *TQM*).

Wyniki badań i analiz odzwierciedlone są w kolejnych rozdziałach niniejszej rozprawy.

Rozdział 2

2. Rola czynnika informacyjnego w bezpieczeństwie państwa

W dobie dynamicznego rozwoju systemów przepływu informacji równie szybko zmieniają się sposoby rozumienia terminów, dochodzi do zróżnicowanego posługiwania się nimi, czy mieszania ze sobą pojęć pozornie tylko tożsamych. Przyczyną tych nieporozumień może być chociażby wieloznaczność, podobieństwo fonetyczne czy morfologiczne wyrazów (jak ma to miejsce w przypadku *bezpieczeństwa państwa* i *bezpieczeństwa narodowego*). Dlatego na początku warto doprecyzować poszczególne pojęcia.

Słownik Języka Polskiego definiuje **bezpieczeństwo** jako *stan niezagrożenia, spokoju, pewności*[1]. Potoczne rozumienie charakteryzuje bezpieczeństwo jako *stan, w którym nie istnieje żadne zagrożenie*[2].

Inaczej pojęcie bezpieczeństwa interpretuje się w środowisku wojskowym S. Koziej, który uważa, że „*w sensie najogólniejszym* [bezpieczeństwo] to *zdolność przeciwstawiania się wszelkiego rodzaju zagrożeniom*[3]. Mamy więc w tej definicji do czynienia z „elementem aktywnym" bezpieczeństwa w porównaniu z wcześniejszymi „pasywnymi" definicjami zaczerpniętymi z powszechnej a zatem nieprofesjonalnej intuicji językowej.

Według J. Czaputowicza, na skutek gwałtownych przewartościowań geostrategicznych w ostatnim dwudziestoleciu znaczenie terminu „bezpieczeństwo" uległo rozszerzeniu a nawet częściowemu przesunięciu[4]. Zmodyfikowane w erze powszechnej globalizacji pojęcie bezpieczeństwa ma propagować model rozwoju współczesnego świata, którego celem jest tworzenie ponadnarodowych organizmów polityczno-gospodarczych. Specjaliści od bezpieczeństwa nie ukrywają, że tego typu model na dzień dzisiejszy niesie ze sobą więcej zagrożeń niż ewentualnych korzyści.

---

[1] *Słownik Języka Polskiego PWN*, Tom I, Warszawa 1978, s. 147.
[2] *Inny Słownik Języka Polskiego PWN*, Tom I, Warszawa 2000, s. 84.
[3] S. Koziej. *Koncepcja wspólnego bezpieczeństwa w Europie a obronność Polski*; [w]: *Wystarczalność Obronna*, Warszawa 1996, s. 18.
[4] J. Czaputowicz, *System czy nieład? Bezpieczeństwo europejskie u progu XXI wieku*, Warszawa 1998, s. 23-26.

Dominujący w tych dążeniach czynnik ekonomiczny powoduje bowiem, że *wzrost efektywności w skali globalnej może pociągać za sobą utratę ośrodków produkcji w skali regionalnej. Wraz z postępującą integracją gospodarki światowej coraz trudniej jest przeciwdziałać wzrastającej konkurencji innych państw i korporacji transnarodowych. Występują obawy, że na rynku światowym będzie więcej przegranych niż wygranych, że osłabienie przywództwa w połączeniu z niestabilnością finansową może doprowadzić do strukturalnego kryzysu i upadku...*[5].

Bezpieczeństwo jest pojęciem używanym do określenia stanu pewności, spokoju i braku zagrożenia. Obejmuje zaspokojenie takich potrzeb jak:

- istnienie;
- przetrwanie;
- całość (integralność);
- tożsamość (identyfikacja);
- niezależność;
- spokój;
- posiadanie;
- pewność rozwoju.

W ujęciu wewnętrznym obejmuje stabilność i harmonijność danego organizmu bądź podmiotu, a w ujęciu zewnętrznym - brak zagrożenia ze strony innych podmiotów lub czynników zewnętrznych. Z kolei ujęcie negatywne bezpieczeństwa wskazuje na brak zagrożeń dla istotnych wartości podmiotu (bezpieczeństwo definiowane jest jako przeciwieństwo zagrożenia), pozytywne natomiast – uwypukla kształtowanie pewności przetrwania, posiadania i swobód rozwojowych podmiotu (zapewnienie kreatywnej aktywności podmiotu).

Uwzględnienie czynnika czasu pozwala na śledzenie priorytetów bezpieczeństwa i traktowanie go jako procesu dynamicznego, gdyż bezpieczeństwo jest ciągłym procesem społecznym, w ramach którego działające podmioty starają się doskonalić mechanizmy zapewniające im poczucie bezpieczeństwa.

Bezpieczeństwo narodowe obejmuje problematykę przeciwstawiania się wszelkim zagrożeniom dla istnienia oraz rozwoju narodu i państwa (zewnętrznym oraz

[5] *Ibidem*, s. 25.

wewnętrznym). Bezpieczeństwo narodowe można zdefiniować jako cechę takiego układu stosunków zewnętrznych i wewnętrznych państwa, w którym nie występują żadne zagrożenia lub są one neutralizowane przez potencjał obronny[6].

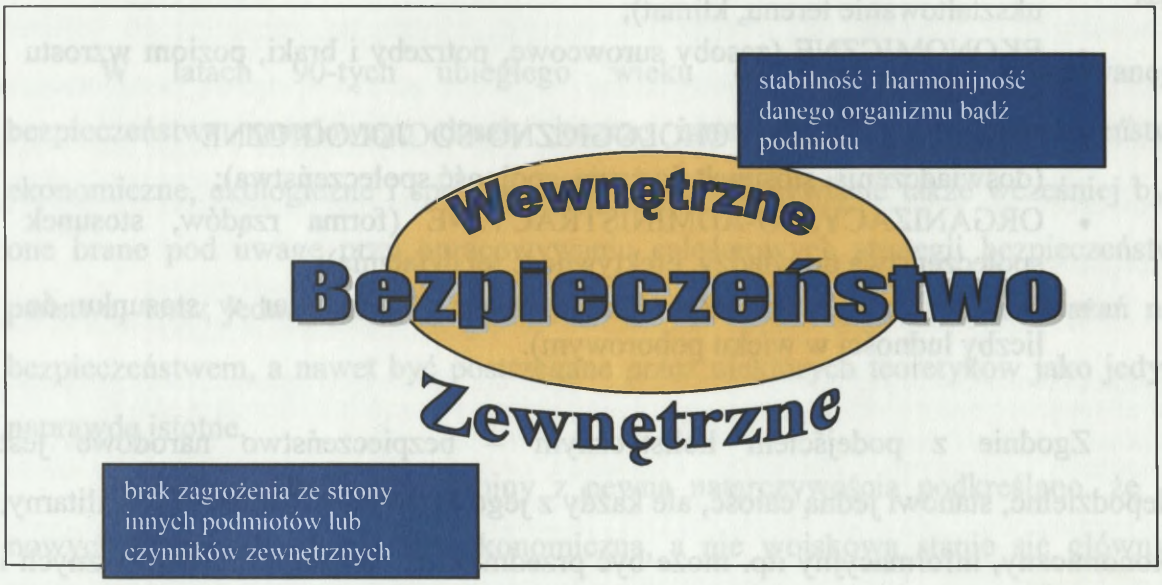


Diagram 4: ***Ogólny układ bezpieczeństwa narodowego***

Źródło: opracowanie własne

Zbiór wartości, które powinny być chronione:

- przetrwanie (biologiczne przeżycie narodu (grupa etniczna) oraz państwa (jednostka polityczna);
- integracja terytorialna;
- niezależność polityczna (w sensie ustrojowym, samowładności i afiliacji);
- jakość życia (standard życia, szczebel rozwoju społ.-gospodarczego, zakres praw i swobód obywatelskich, system kulturalny, stan środowiska naturalnego, możliwości i perspektywy dalszego rozwoju).

Bezpieczeństwo narodowe określają wartości, które powinny być chronione, gdyż stanowią podstawę określenia narodowej polityki bezpieczeństwa.

Zakres i dobór środków zależy głównie od percepcji zagrożeń przez organy kierownicze państwa oraz od pozostających w dyspozycji państwa zasobów materialnych, intelektualnych, umiejętności efektywnego wykorzystywania tych środków. Po zdefiniowaniu tych czynników i wypełnieniu ich treścią pojęcie bezpieczeństwa narodowego transformuje się na ***bezpieczeństwo państwa***. Do głównych czynników bezpieczeństwa państwa należą:

[6] M. Sułek. *Podstawy potęgonomii i potęgometrii*. WSEiA Kielce 2001, s. 144

- POLITYCZNE (wewnętrzne i zewnętrzne);
- DEMOGRAFICZNE (liczba ludności, struktura i tendencje demograficzne);
- GEOGRAFICZNE (położenie przestrzenne, rozmiary terytorium, ukształtowanie terenu, klimat);
- EKONOMICZNE (zasoby surowcowe, potrzeby i braki, poziom wzrostu gospodarczego);
- HISTORYCZNO-PSYCHOLOGICZNO-SOCJOLOGICZNE (doświadczenia, stosunek do życia, spójność społeczeństwa);
- ORGANIZACYJNO-ADMINISTRACYJNE (forma rządów, stosunek społeczeństwa do władzy, efektywność jej działania);
- MILITARNE (organizacja i efektywność SZ, rozmiar w stosunku do liczby ludności w wieku poborowym).

Zgodnie z podejściem holistycznym – bezpieczeństwo narodowe jest niepodzielne, stanowi jedną całość, ale każdy z jego czynników: polityczny, militarny, ekonomiczny, informacyjny itp. może być przedmiotem oddziaływań zewnętrznych i wewnętrznych. Do priorytetowych wymiarów bezpieczeństwa narodowego XXI wieku zaliczono bezpieczeństwo informacyjne i ekonomiczne, jako stanowiące podstawę stabilizacji układu globalnego.

Definiując pojęcie bezpieczeństwa należy nadmienić o współczesnych, wynikających z procesów globalizacyjnych, tendencjach do „oddelegowywania" bezpieczeństwa z poziomu państwa na dół – w kierunku bezpieczeństwa osobistego jednostki (tym NATO usprawiedliwiało interwencję w Jugosławii), lub w górę – w kierunku bezpieczeństwa struktur ponadnarodowych (tym niektórzy zwolennicy europejskiej tożsamości obronnej motywują konieczność zerwania więzi trans-atlantyckiej z USA). Wszystkie te zabiegi mają na celu podważenie, najczęściej tylko w odniesieniu do państw średnich i małych, klasycznego pojmowania bezpieczeństwa narodowego, ze wszystkimi tego konsekwencjami.

Podsumowując powyższe rozważania autor definiuje **bezpieczeństwo** jako *zespół wszystkich działań podejmowanych w celu eliminacji obecnych i przyszłych zagrożeń dla harmonijnego rozwoju, stabilności i istnienia danego systemu (państwa, organizacji...), lub stan, w którym podmiot bezpieczeństwa jest wolny od tych zagrożeń.*

2.1. Wykorzystanie metod potęgometrycznych do oceny bezpieczeństwa państwa

„Matematyka jest archetypem piękna świata"
Kepler

W latach 90-tych ubiegłego wieku do tradycyjnie pojmowanego bezpieczeństwa narodowego doszły jeszcze inne czynniki, jak bezpieczeństwo ekonomiczne, ekologiczne i społeczno-kulturowe[7]. Oczywiście także wcześniej były one brane pod uwagę przy opracowywaniu całościowych strategii bezpieczeństwa państwa, teraz jednak zaczęły coraz częściej wysuwać się na czoło rozważań nad bezpieczeństwem, a nawet być postrzegane przez niektórych teoretyków jako jedyne naprawdę istotne.

Po zakończeniu zimnej wojny z pewną natarczywością podkreślano, że „w nowych realiach to raczej siła ekonomiczna, a nie wojskowa stanie się głównym wskaźnikiem potęgi i - odpowiednio - wielkości tego lub innego państwa"[8]. Chodziło też o to, by zdefiniować amerykańską odpowiedź na zakończenie zimnej wojny, na powstanie nowej ery, w której bezpieczeństwo narodowe będzie coraz bardziej definiowane w kategoriach ekonomicznych.

P. Kennedy we wstępie do swego fundamentalnego dzieła „*Mocarstwa świata*", koncentruje się na interakcji ekonomii i strategii, interakcji, z jaką mamy do czynienia, kiedy każde z czołowych państw systemu międzynarodowego stara się powiększyć swe bogactwo i swą potęgę, by stać się (lub pozostać) zarówno bogatym, jak i silnym. Badanie tej interakcji jest ważne w czasie pokoju i wojny[9].

A. D. Rotfeld, były dyrektor Międzynarodowego Instytutu Badań nad Pokojem w Sztokholmie (*SIPRI - Stockholm International Peace Research Institute*), omawiając czynniki wpływające na bezpieczeństwo państw, stwierdził, że *„...dawniej był to przede wszystkim potencjał wojskowy, dzisiaj zbrojenia są wprawdzie nadal ważne, ale o stanie bezpieczeństwa państw decyduje z reguły ich potencjał gospodarczy"*[10].

---

[7] *Ibidem*, s. 24.
[8] *Powerecomics. Economics and Strategy After the Cold War*, Economic Strategy Institute, Washington, D.C. 1991.
[9] P. Kennedy, *Mocarstwa świata - narodziny, rozkwit, upadek*, KiW, Warszawa 1994, s. 7.
[10] *Niespokojny świat* (rozmowa z prof. Adamem Rotfeldem), "*Polska Zbrojna*" z 13 stycznia 1994 r.

2.1.1. Modelowanie i pomiar potęgi państw

Nazwa „**potęgometria**" wiąże „potęgę" i „pomiar". Potęgometria odsyła nas do zagadnień modelowania i pomiaru potęgi. Ten kierunek badań można traktować jako równoległy w stosunku do istniejących nurtów. Można też rozumieć go bardziej dobitnie - jako dalszy rozwój potęgonomii. Zgodnie ze swoją nazwą **potęgonomia** powinna zajmować się potęgą państw (jednostek politycznych). Potęga ma wiele wymiarów, ale w tej dyscyplinie chodzi nie tyle o ich odrębne opisywanie, co raczej o przedstawienie nowej jakości[11].

*W najogólniejszym znaczeniu (*pisze R. Aron*) - **potęga** jest zdolnością do czynienia, tworzenia lub niszczenia. (...). Potęgą na scenie międzynarodowej nazywam zdolność jakiejś jednostki politycznej do narzucenia swej woli innym jednostkom politycznym. Krótko mówiąc, potęga polityczna nie jest niczym absolutnym, lecz stosunkiem między ludźmi*[12].

Pojęcie potęgi używane jest, poza fizyką (gdzie oznacza moc), politologii, socjologii, psychologii i ekonomii, gdzie na ogół oznacza ,zdolność do stosowania przymusu, aby osiągnąć określone zachowanie przedmiotu oddziaływania. Ale, jak zauważa amerykański politolog K. Knorr, nie jest to dostatecznie jasne. Jeśli potęgę określa się jako zdolność wpływania na zachowanie innych, to pojęcie to może być traktowane dwojako. Pierwsza interpretacja utożsamia potęgę z uzyskanym wpływem (zmiany w zachowaniu są widoczne i wymierne). Jest to potęga zrealizowana (*actualized power*). Zgodnie z drugą interpretacją - potęga jest zdolnością do wymuszania wpływu, jest więc tylko potencjalną przyczyną zmian w zachowaniu, wyprzedzającą osiągnięcie konkretnego wpływu. Jest to potęga domniemana (*putative power*)[13].

Według J. G. Stoessingera „*...potęga w stosunkach międzynarodowych to zdolność państwa do użycia swych materialnych i niematerialnych zasobów w sposób, który wpłynie na zachowanie innych państw*"[14].

---

[11] M. Sułek. *Podstawy potęgonomii i potęgometrii.* WSEiA Kielce 2001, s. 18
[12] R. Aron. *Pokój i wojna między narodami (teoria)*, CAS, Warszawa 1995 s. 100-106
[13] K. Knorr, *Military Power and Potential*, Lexington, Mass. 197O, s. 3.
[14] J. G. Stoessinger, *The Might qf Nations: World Politics in Our Time*, New York, 1969, s. 16-27

Różne proporcje elementów składających się na potęgę jednostek politycznych pozwalają wyróżnić kilka charakterystycznych wymiarów (form) potęgi:

- ekonomiczny;
- militarny;
- demograficzno-przestrzenny.

Wyróżnienie profilów potęgi opiera się na kryterium stopnia zharmonizowania grup elementów tworzących daną potęgę. Z tego punktu widzenia można wymienić:

- potęgę jednowymiarową;
- potęgę dwuwymiarową;
- potęgę wielowymiarową.

Wiele kategorii zbliżonych do pojęcia potęgi często definiowane jest prawie tak samo jak pojęcie potęgi. Dotyczy to zwłaszcza potencjału wojennego i potencjału obronnego, a także potencjału militarnego. T. Zakrzewski zauważa, że zagadnienie - gdzie jest kres wszelkich źródeł energii dla siły zbrojnej państwa - było przedmiotem dyskusji na konferencji komisji przygotowawczej do spraw rozbrojenia w Genewie. Stwierdzono tam, że rzeczywisty wyraz potęgi wojennej państwa wyraża się nie tylko w jego zorganizowanej sile zbrojnej, ale także we wszystkich źródłach energii i bogactwa narodowego. Nazwano je potencjałem wojennym[15]. Autor cytowanej książki definiuje go następująco: „*potencjałem wojennym zatem nazywam te środki i zasoby osobowe, materialne, jak również te wartości moralne narodu, które w razie wykroczenia wojny poza ramy przewidywań i planów operacyjnych pozwalają sile zbrojnej państwa trwać, które pozwalają na jej wzmocnienie lub też powodują jej stopniowy upadek*"[16].

Według ujęcia encyklopedycznego „*potencjał wojenny (obronny) państwa to całokształt możliwości materialnych i moralnych państwa (lub koalicji państw), które mogą być wykorzystane do realizacji celów wojny. Skład i wzajemne powiązania elementów potencjału wojennego stanowi jego strukturę (...). Najogólniej potencjał wojenny dzieli się na potencjał moralno-polityczny, potencjał wojskowy, potencjał obrony cywilnej i potencjał ekonomiczno-wojenny*"[17].

---

[15] T.Zakrzewski, *Organizowanie siły zbrojnej* w *państwie,* Wojskowy Instytut Naukowo-Oświatowy, Warszawa 1938, s. 3-4.
[16] *Ibidem*, s. 34
[17] *Mała Encyklopedia Wojskowa*, Warszawa 1970, s. 761.

2.1.2. Metody i modele potęgometryczne

Według A. Muszyńskiego *„Pomiar potencjału wojenno-ekonomicznego ma na celu porównanie możliwości tkwiących w strukturze gospodarki narodowej z potrzebami systemu obrony na wypadek wojny, określenie na podstawie pomiaru potencjału wojenno-ekonomicznego innych krajów warunków bezpieczeństwa oraz określenie zadań dla gospodarki narodowej na podstawie powyższych porównań"*[18].

Zgodnie z poglądami wielu ekonomistów zajmujących się oceną potencjału wojenno-ekonomicznego - łączy się siłę militarną z bogactwem państwa, przypisując główną rolę miernika potęgi dochodowi narodowemu i jego pochodnym. Jednak, według M. Sułka, zarówno dochód narodowy, jak i wydatki wojskowe mogą służyć jako pierwsze przybliżenie, ale jako miary potencjału pomijają dwa ważne z punktu widzenia obronności elementy – demograficzny i geograficzny[19].

Dążenie do potęgometrycznego ujęcia wszystkich czynników bezpieczeństwa państwa doprowadziło do prób wypracowania szeregu matematycznych odwzorowań (modeli) potęgi państwa. Do najważniejszych z nich należą:

Model R.S. Cline'a

Model Cline'a[20] odnosi się zasadniczo do siły, jaką państwo dysponuje na arenie międzynarodowej. Składa się on z dwóch wyraźnych części: pierwszej, odpowiadającej w przybliżeniu pojęciu potencjału gospodarczo-obronnego oraz drugiej, wskazującej na możliwości i kierunek jego uruchomienia, co w sumie daje ocenę roli, jaką państwo może odegrać na arenie międzynarodowej, a w tym również (a może nawet przede wszystkim) w czasie konfliktu zbrojnego.

Formułę Cline'a można zapisać jak niżej:

$$P_p = (C + E + M) \times (S + W), \qquad \text{gdzie:}$$

P_p - *potęga państwa (Cline mówi o „potędze postrzeganej");*
C - *masa krytyczna, czyli ludność i terytorium;*
E - *potencjał gospodarczy (economic capability);*
M - *potencjał militarny (military capability);*
S - *strategia państwa (strategic purpose);*
W - *wola urzeczywistnienia strategii państwa (will national strategy).*

[18] A. Muszyński. *Związki struktury gospodarki narodowej z systemem obronnym i jego potencjałem*, „Materiały i studia WAP", Warszawa 1980, nr 88, s. 93
[19] M. Sułek. *Podstawy potęgonomii i potęgometrii*. WSEiA Kielce 2001, s. 57
[20] R.S. Cline. *World Power Trends and US Foreign Policy for 1980s*, Boulder 1980

Model Fucksa

Jako odwzorowanie potęgi przyjmuje *wskaźniki o charakterze gospodarczym*. Opiera się on na koncepcji trzech czynników potęgotwórczych: *ludności, stali* i *energii elektrycznej*. Konkretna postać modelu jest następująca:

$$M = \frac{M_e + M_s}{2}, \qquad \text{przy czym:}$$

$$M_e = \sqrt[3]{L}E, \qquad M_s = \sqrt[3]{L}S, \qquad \text{gdzie:}$$

M - *syntetyczny wskaźnik potęgi,*
M_e - *wskaźnik cząstkowy oparty na liczbie ludności i produkcji energii elektrycznej,*
M_s - *wskaźnik cząstkowy oparty na liczbie ludności i produkcji stali,*
L - *liczba ludności,*
E - *produkcja energii elektrycznej,*
S - *produkcja stali*

Zamieszczona poniżej tabela pokazuje wskaźniki potęgi obliczone *metodą Fucksa* w okresie tzw. zimnej wojny (USA =1000)[21]:

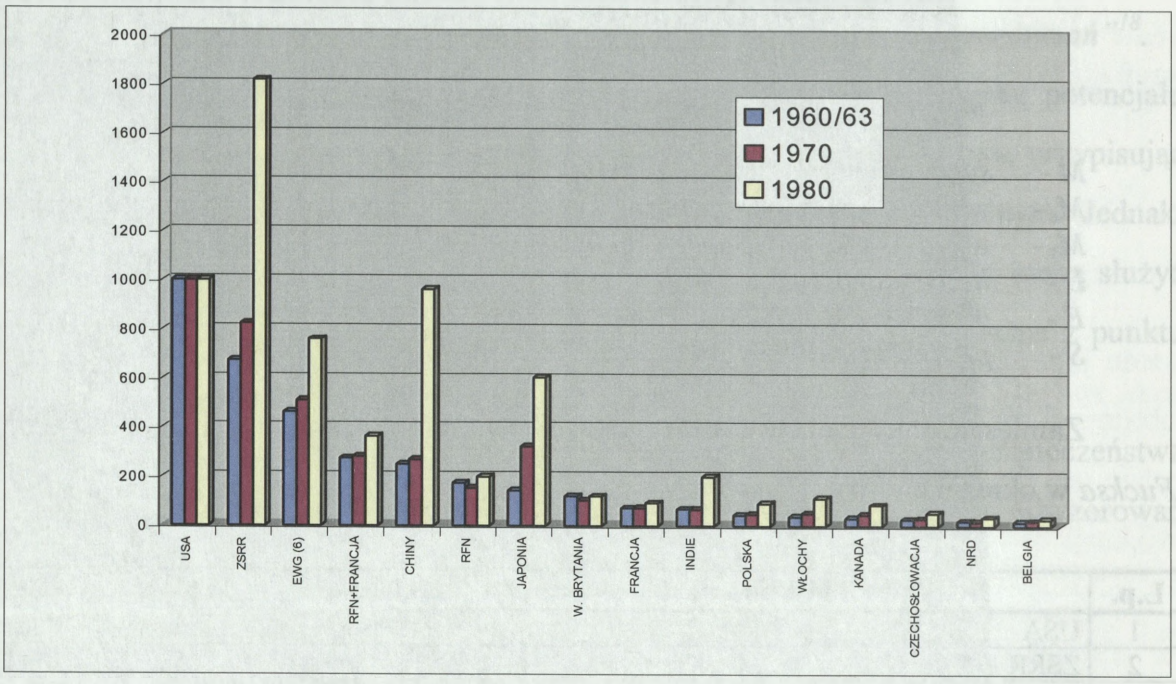
L.p.	Państwa	1960/63	1970	1980
1	USA	1000	10000	1000
2	ZSRR	674	825	1817
3	EWG (6)	463	510	759
4	RFN+FRANCJA	274	281	364
5	CHINY	250	269	963
6	RFN	174	153	198
7	JAPONIA	143	322	603
8	W. BRYTANIA	120	103	119
9	FRANCJA	71	72	92
10	INDIE	67	66	198
11	POLSKA	43	48	91
12	WŁOCHY	37	50	112
13	KANADA	31	46	84
14	CZECHOSŁOWACJA	26	28	51
15	NRD	20	17	34
16	BELGIA	16	20	27

Tabela 1: ***Wskaźniki potęgi obliczone metodą Fucksa***[22]

Model Fucksa jest prosty w stosowaniu, opiera się na danych w postaci naturalnej, łatwo dostępnych. Wadą *modelu Fucksa* jest pewien aprioryzm w wyborze wykładników potęgowych, przyjmowanych empirycznie. We współczesnym,

[21] M. Sułek. Podstawy potęgonomii i potęgometrii. WSEiA Kielce 2001, s. 71
[22] *Ibidem*

zdominowanym elektroniką świecie, nadmiarowym wydaje się także potęgotwórczy charakter wskaźnika produkcji stali. Najbardziej obiektywna wydaje się formuła oparta na energii, ale ona także może przeceniać na przykład przyszłą potęgę Chin, która jest przecież zależna od innych, zwłaszcza politycznych i militarnych, zmiennych. Ilustruje to wykres:



Wykres 1: ***Wskaźniki potęgi obliczone metodą Fucksa za okres zimnej wojny***
Źródło: opracowanie własne

Przedstawione wyliczenia potęgi dla wybranych państw i grup państw wskazują, że stosunkowo duży awans niektórych krajów (ZSRR, Chin, Indii) wynikał raczej z ich względnego zacofania i nadrabiania dystansu. Niewątpliwie doszło w tych krajach do autentycznego postępu, ale nie tak wielkiego, jak sugerowałyby to prezentowane wyniki. Świadczą one raczej o malejącej funkcji eksplanacyjnej modelu Fucksa.

Zaprezentowane modele Cline'a i Fucksa pomijają ważne z punktu widzenia obronności elementy – ludnościowy i geograficzny. M. Sułek zaproponował modelowanie i pomiar potęgi w oparciu o *potencjał demograficzno-geograficzny* i *informacyjno-energetyczny*, rozumiany jako funkcja dochodu narodowego z udziałem wydatków wojskowych[23].

[23] *Ibidem*, s. 87-95

Model Sułka

Model ten opiera się na założeniu o wielofunkcyjności wydatków wojskowych, stanowiących miarę, która może być użyta do interpretacji różnych czynników bezpieczeństwa: militarnego, politycznego, ekonomicznego i informacyjnego. O ile założenie to sprawdza się w dokonanych naliczeniach w zakresie pierwszych trzech czynników bezpieczeństwa w porównaniu z innymi modelami potęgonometrycznymi, informacyjny czynnik bezpieczeństwa wydaje się być niedowartościowany i wymaga odrębnych analiz, co zostanie wykazane i dokonane w dalszej części niniejszej rozprawy.

M. Sułek przyjął , że model obliczania potęgi państw ma postać syntetycznej funkcji produkcji :

$$P = \left(\frac{mD}{T}\right)^{\alpha} L^{\beta} p^{\gamma}, \quad \text{gdzie:}$$

P – *potęga państwa (grupy państw);*
$\frac{D}{T}$ - *dochód narodowy w czasie (najczęściej w ciągu roku);*
L – *liczba ludności;*
p – *terytorium (powierzchnia państwa);*
α, β, γ - *strukturalne dodatnie parametry funkcji, współczynniki elastyczności potęgi względem kolejno: dochodu narodowego (wydatków wojskowych), ludności i terytorium;*
m – *udział wydatków wojskowych w dochodzie narodowym;*

Po przyjęciu założeń dotyczących wykładniczych parametrów przytoczonej funkcji, a mianowicie:

$\alpha, \beta, \gamma > 0;$
$\alpha > \beta > \gamma;$
$\alpha + \beta + \gamma < 1,$

M. Sułek przytacza postać odwzorowania potęgi państwa:

$$P = e^{\lg\left[(mD)^{1,5} L^{0,5} p^{0,25}\right]},$$

a po przekształceniu:

$$P = (mD)^{0,65144} L^{0,21715} p^{0,10857}, P = e^{\lg\left[(mD)^{1,5} L^{0,5} p^{0,25}\right]}$$

Powyższy wzór uzależnia potęgę państwa od części dochodu narodowego przeznaczonej na wydatki obronne. *Model Sułka* rozdziela potęgę państwa naliczoną wyłącznie w stosunku do wydatków wojskowych od potęgi ogólnej, co pozwala na dokonanie oceny o „militarystycznych" skłonnościach jednego z obiektów badań w stosunku do drugiego. Wzory obu rodzajów potęg przyjmują wtedy postać:

$$P_d = D^{0,65144} L^{0,21715} p^{0,10857}, \qquad \text{przy m=1}$$

gdzie P_d - potęga państwa uzależniona od pełnego dochodu narodowego

oraz

$$P_k = W^{0,65144} L^{0,21715} p^{0,10857}, \qquad \text{przy m} \neq 1$$

gdzie P_k - potęga państwa uzależniona od kategorii wydatków wojskowych;

$W=mD$ – *wysokość wydatków na obronność*

Są to dwie podstawowe formuły, które stanowią podstawę obliczeń i analiz w *modelu Sułka*[24]. Poniżej zamieszcza się dane do naliczenia potęg państw NATO:

L.p.	Państwo	D	W	L	P
		mld.$	mld.$	mln	tys. km^2
1	USA	8500	270,2	273,1	9363,5
3	BELGIA	250	2,8	10,1	30,5
4	CZECHY	55	1,1	10,5	78,9
5	DANIA	174	2,7	5,3	43,1
6	FRANCJA	1400	31,3	59,2	551,5
8	GRECJA	121	4,0	10,6	132,0
17	HISZPANIA	553	5,9	39,2	506,0
13	HOLANDIA	372	7,1	15,7	40,8
10	ISLANDIA	8,3		0,28	103,0
2	KANADA	604	6,3	29,2	9976,1
12	LUKSEMBURG	16	0,11	0,42	2,6
7	NIEMCY	2100	26,5	82,1	357,0
14	NORWEGIA	146	3,4	4,4	323,9
15	POLSKA	159	3,4	38,9	312,7
16	PORTUGALIA	105	1,6	9,9	92,4
18	TURCJA	188	7,8	65,2	779,5
19	W. BRYTANIA	1300	37,4	58,8	244,1
9	WĘGRY	48	0,7	10,0	93,0
11	WŁOCHY	1200	17,8	57,9	301,3
	NATO	17299,3	430,11	780,8	23331,9

Tabela 2: ***Dane wyjściowe dla państw NATO (1999 r.)***[25]

[24] *Ibidem*, s. 95

[25] Źródło: The Military Balance 1999/2000

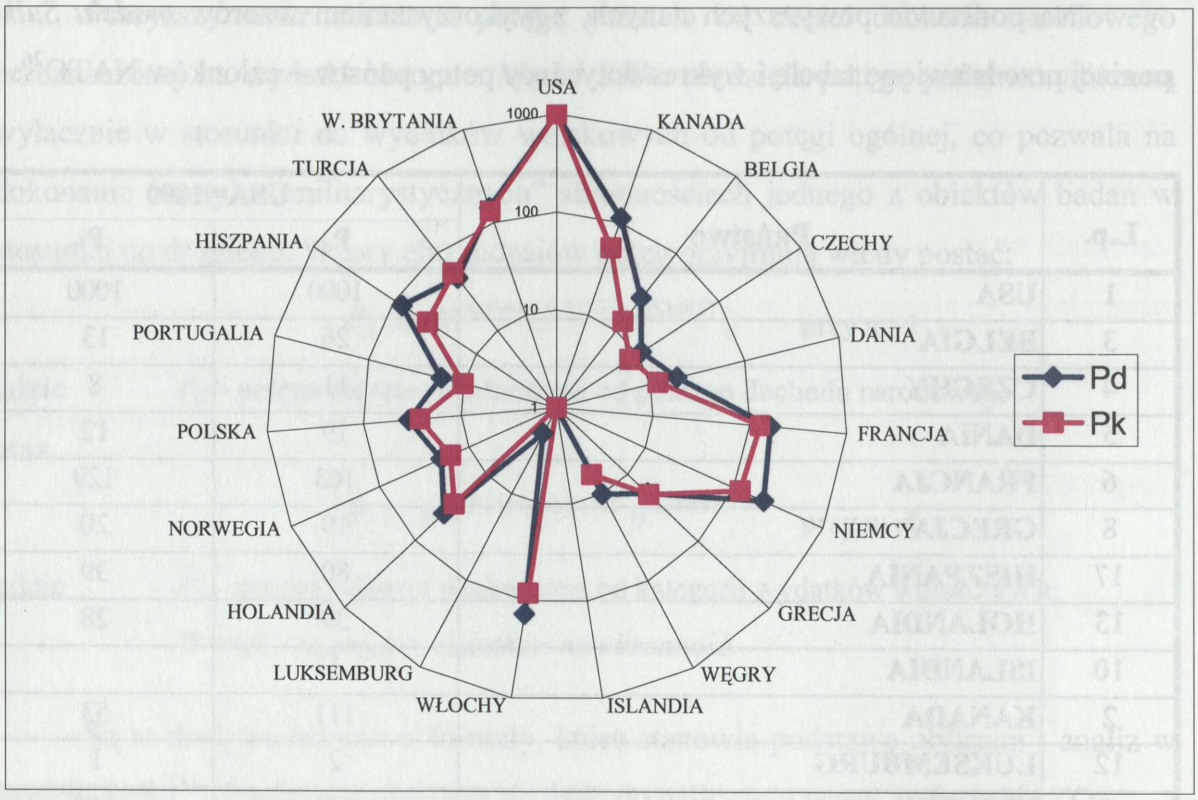
Na podstawie powyższych danych, z wykorzystaniem wzorów *modelu Sułka* poniżej przedstawiono tabelę i wykres dotyczący potęg państw – członków NATO[26]:

L.p.	Państwo	USA= 1000	
		P_d	P_k
1	**USA**	1000	1000
3	**BELGIA**	26	13
4	**CZECHY**	11	8
5	**DANIA**	19	12
6	**FRANCJA**	163	129
8	**GRECJA**	19	20
17	**HISZPANIA**	80	39
13	**HOLANDIA**	39	28
10	**ISLANDIA**	1	
2	**KANADA**	111	53
12	**LUKSEMBURG**	2	1
7	**NIEMCY**	217	119
14	**NORWEGIA**	20	16
15	**POLSKA**	34	26
16	**PORTUGALIA**	17	10
18	**TURCJA**	47	55
19	**W. BRYTANIA**	142	133
9	**WĘGRY**	10	6
11	**WŁOCHY**	137	83
	NATO	2205	1878

Tabela 3: ***Naliczona potęga państw NATO (1999 r.) w kategorii dochodu narodowego i w kategorii wydatków wojskowych***
Źródło: M. Sułek. Podstawy potęgonomii i potęgometrii. WSEiA Kielce 2001, s. 129

Na podstawie przedstawionych w tabeli wyników obliczeń potęg państw NATO w kategorii dochodu narodowego i w kategorii wydatków wojskowych sporządzono ***Wykres Nr 2.***

[26] M. Sułek. *Podstawy potęgonomii i potęgometrii. WSEiA* Kielce 2001, s. 129



Wykres 2: ***Wykres potęg państw NATO (1999 r.) w kategorii dochodu narodowego i w kategorii wydatków wojskowych (logarytmiczny)***

Źródło: Opracowanie własne

Analiza wykresu pozwala na określenie stopnia „zmilitaryzowania" poszczególnych państw (na podstawie proporcji potęgi wynikającej z wydatków wojskowych, wobec potęgi będącej pochodną dochodu narodowego - można zauważyć dominację militarnego czynnika potęgi państwa w przypadku Turcji - M. Sułek określa tę właściwość jako „napięcie mobilizacyjne"[27]).

Metoda Sułka nie jest pozbawiona subiektywizmu w podejściu do potęgi państw. Naliczona na podstawie wypracowanego modelu potęga nie jest wskaźnikiem bezwzględnym, lecz jedynie porównawczym, przy czym twórca metody dla lepszego zobrazowania proporcji dokonuje aproksymacji wyników (przyjmując liczbę 1000 jako wyjściowy wskaźnik dla USA w przypadku obydwu wymiarów potęgi, co z matematycznego punktu widzenia nie wydaje się w pełni uzasadnione).

Zaletą *modelu Sułka* jest możliwość jego rozwinięcia do postaci umożliwiającej dokonywanie oceny ***bezpieczeństwa państwa.***

[27] *Ibidem*, s. 132

2.1.3. Miary potęgi państw jako czynnik oceny bezpieczeństwa

Stosując odwzorowania potęgometryczne do ilościowego określenia poziomu bezpieczeństwa M. Sułek przytacza operacyjną definicję bezpieczeństwa państwa, rozpatrując je w dwóch głównych kategoriach - mocy i potencjału. Bezpieczeństwo definiowane w kategoriach mocy uważa za bardziej realne niż bezpieczeństwo w kategoriach potencjału. *„**Bezpieczeństwo narodowe** można zdefiniować jako cechę takiego układu stosunków zewnętrznych i wewnętrznych państwa, w którym nie występują żadne zagrożenia lub są one neutralizowane przez potencjał obronny. **Zagrożenie** natomiast można określić jako stan wynikający z nierównowagi potencjałów obronnych. Miarą zagrożenia jest **potencjał zagrożenia** (PZ), który jest różnicą dwóch przeciwstawnych potencjałów (**potencjału obronnego** - PO i **potencjału agresywnego** - PA)*[28]*."*

Ze stanem bezpieczeństwa narodowego (BN) mamy do czynienia wówczas, gdy potencjał zagrożenia PZ nie przewyższa potencjału obronnego PO, czyli:

$$PZ=PA-PO$$

warunek bezpieczeństwa: $$PZ \leq PO \rightarrow BN$$

Przy założeniu, że główną determinantą militarnego czynnika bezpieczeństwa państwa jest stosunek sił; który może być określany na podstawie potencjału obronnego, potencjałów bojowych sił zbrojnych - w szczegółowych analizach konieczne jest uwzględnienie wielu innych elementów. Przy rozpatrywaniu problemu przewagi (dominacji) jednej ze stron - rozważaniom teoretycznym (w tym obliczeniom na podstawie przytoczonych wzorów) muszą towarzyszyć założenia empiryczne, mające swoje odzwierciedlenie w doktrynach sztuki wojennej.

W swym modelu M. Sułek nie dokonuje obliczeń wskaźników bezpieczeństwa państwa z zastosowaniem metod potęgometrycznych, ograniczając się do ich zestawienia (wskaźnik potencjału obronnego, nominalny wskaźnik zagrożenia, prawdopodobieństwo wybuchu konfliktu, prognozowany wskaźnik zagrożenia), nie

[28] *Ibidem*, s. 144-145

uwzględnia także roli czynnika informacyjnego w bezpieczeństwie państwa i wpływu systemów walki informacyjnej na przebieg konfliktów zbrojnych. Przyznaje zresztą: *„zdaję sobie sprawę, że w dziedzinie polityki i strategii państw, w tym zwłaszcza polityki i strategii bezpieczeństwa, uwikłanej w kontekst międzynarodowy i wewnętrzny, nie można opierać się wyłącznie na syntetycznych miarach potęgi"*[29].

W kolejnych rozdziałach niniejszej pracy autor postara się uzupełnić metodologię oceny bezpieczeństwa państwa poprzez włączenie roli czynnika informacyjnego i wykazać niezbędność zapewnienia bezpieczeństwa informacyjnego z systemowym wypracowaniem narzędzi służących realizacji tego zamierzenia.

2.2. Bezpieczeństwo narodowe w ujęciu statycznym i dynamicznym

Bezpieczeństwo państwa jest nieodłącznym elementem bezpieczeństwa narodowego, rozpatrywanego w **ujęciu statycznym** – jako brak zagrożeń dla istotnych wartości podmiotu (bezpieczeństwo definiowane jako przeciwieństwo zagrożenia, tzw. podejście negatywne) i kształtowanie pewności przetrwania, posiadania i swobód rozwojowych podmiotu (zapewnienie kreatywnej aktywności podmiotu, tzw. podejście pozytywne) oraz w **ujęciu dynamicznym**, z uwzględnieniem czynnika czasu – jako ciągły proces społeczny, w ramach którego działające podmioty starają się doskonalić mechanizmy zapewniające im poczucie bezpieczeństwa.

2.2.1. Wymiar bezpieczeństwa narodowego

Biuro Bezpieczeństwa Narodowego jako organ Prezydenta Rzeczypospolitej Polskiej określiło obszary zagrożeń bezpieczeństwa państwa i zdefiniowało niżej wymienione priorytetowe płaszczyzny działania:

1. **Podstawy polskiej polityki bezpieczeństwa**
   - 1.1. Strategiczne cele polskiej polityki bezpieczeństwa
   - 1.2. Podstawowe zasady polskiej polityki bezpieczeństwa
2. **Zagrożenia i wyzwania**
   - 2.1. Wojna i agresja zbrojna
   - 2.2. Kryzysy i konflikty lokalne
   - 2.3. Regiony nadmiernej koncentracji potencjału militarnego

[29] *Ibidem*, s. 198

2.4. Proliferacja broni masowego rażenia
2.5. Zagrożenia ekonomiczne
2.6. Niebezpieczeństwo nowych podziałów w Europie
2.7. Niekontrolowane migracje transgraniczne
2.8. Środowisko naturalne
2.9. Terroryzm i przestępczość zorganizowana
2.10. Aktywność obcych służb specjalnych oraz **ochrona informacji**

3. Płaszczyzny aktywności i instrumenty realizacji polskiej polityki bezpieczeństwa
3.1. Działania narodowe
3.1.1. Rozwój cywilizacyjny i projekcja stabilności
3.1.2. Dyplomacja
3.1.3. Kontrola eksportu
3.1.4. Służby specjalne
3.1.5. Policja i Straż Graniczna
3.2. Integracja
3.2.1. Rola Sojuszu Północnoatlantyckiego
3.2.2. Integracja w ramach Sojuszu Północnoatlantyckiego
3.2.3. Integracja z Unią Europejską; Unia Zachodnioeuropejska, Europejska Polityka w dziedzinie
3.2.4. Bezpieczeństwa i Obrony (ESDP)
3.2.5. Przemysł obronny a członkostwo w NATO, UZE i UE
3.3. Zaangażowanie
3.3.1. Aktywna postawa Polski
3.3.2. Organizacja Narodów Zjednoczonych i operacje pokojowe
3.3.3. Organizacja Bezpieczeństwa i Współpracy w Europie (OBWE)
3.3.4. Kontrola zbrojeń i środki budowy zaufania
3.4. Współpraca
3.4.1. Współpraca regionalna i subregionalna
3.4.2. Stosunki dobrosąsiedzkie
3.4.3. Stosunki euroatlantyckie
3.4.4. Współpraca z partnerami pozaeuropejskimi

4. Podstawy strategii obronności Rzeczypospolitej Polskiej
4.1. Istota obronności
4.2. Odstraszanie i obrona
4.3. Polityka nuklearna
4.4. System obronności Rzeczypospolitej Polskiej
4.5. Podsystem kierowania obronnością
4.6. Siły Zbrojne Rzeczypospolitej Polskiej
4.6.1. Zadania Sił Zbrojnych
4.6.2. Organizacja Sił Zbrojnych
4.6.3. Kierunki zmian w Siłach Zbrojnych
4.7. Pozamilitarne ogniwa systemu obronności
4.8. Planowanie, programowanie i finansowanie obronności

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej została 22 lipca 2003 r. zaakceptowana przez Radę Ministrów, a 8 września 2003 r. zatwierdzona przez Prezydenta RP. Opracowanie i wdrożenie *„Strategii..."* zostało niejako wymuszone przez pojawienie się nowych wyzwań globalnych, związanych przede wszystkim z napięciem i destabilizacją wywoływaną przez terroryzm międzynarodowy i proliferację broni masowego rażenia, a także nieprzewidywalną politykę reżimów autorytarnych, co zaostrza groźbę terroryzmu międzynarodowego. Polska jako członek wspólnoty euroatlantyckiej jest wystawiona bezpośrednio na wynikające z tego zagrożenia.

„Strategia..." , nadając priorytety poszczególnym obszarom bezpieczeństwa narodowego omawia następujące obszary przedmiotowe:

I. NOWE WYZWANIA

II. ZAŁOŻENIA OGÓLNE

III. ZADANIA SŁUŻB PAŃSTWOWYCH
1. Aktywność międzynarodowa
   A. Sojusz Północnoatlantycki
   B. Unia Europejska
   C. ONZ i inne instytucje międzynarodowe; kontrola zbrojeń
   D. Regionalne aspekty polityki bezpieczeństwa
2. Siły zbrojne
3. Wywiad
4. Wewnętrzne aspekty bezpieczeństwa
5. Ochrona infrastruktury teleinformatycznej.

IV. GOSPODARCZE PODSTAWY BEZPIECZEŃSTWA PAŃSTWA
1. Finanse
2. Gospodarka.
3. Infrastruktura
4. Środowisko naturalne
5. Edukacja obywatelska

Wśród omówionych obszarów znajdują się priorytety obejmujące tematykę związaną z aspektem bezpieczeństwa wyzwań technologicznych XXI wieku. Proces rozwoju technik informatycznych i komunikacyjnych, globalizacja rynków kapitałowych niosą ze sobą zagrożenia działań naruszających stabilność sytuacji finansowo-kapitałowej i gospodarczej. Nowe wyzwania dyktują potrzebę utworzenia państwowego kompleksowego systemu reagowania kryzysowego, odpowiadającego

na współczesne zagrożenia bezpieczeństwa zarówno międzynarodowego, jak i wewnętrznego. Odpowiednie instytucje państwowe mają prowadzić działania zmierzające do powołania zintegrowanego systemu kierowania i zarządzania na wypadek kryzysu. Niezbędne staje się spójne uregulowanie zadań i kompetencji organów i instytucji państwowych, a także organizacji społecznych działających na rzecz bezpieczeństwa państwa. w świetle charakteru nowych zagrożeń szczególna rola służb wywiadowczych dla bezpieczeństwa państwa polegać ma między innymi na:

- uzyskiwaniu, analizowaniu, przetwarzaniu i przekazywaniu właściwym organom informacji mogących mieć istotne znaczenie dla bezpieczeństwa i międzynarodowej pozycji RP oraz jej potencjału ekonomicznego i obronnego;
- rozpoznawaniu zagrożeń zewnętrznych godzących w bezpieczeństwo, obronność, niepodległość i nienaruszalność terytorium RP oraz przeciwdziałaniu im;
- rozpoznawaniu podmiotów pozarządowych prowadzących, inspirujących bądź finansujących międzynarodową działalność terrorystyczną lub trudniących się przestępczością zorganizowaną;
- rozpoznawaniu międzynarodowego obrotu bronią, amunicją i materiałami wybuchowymi oraz towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także rozpoznawaniu międzynarodowego obrotu bronią masowej zagłady i zagrożeń związanych z jej rozprzestrzenianiem oraz środkami jej przenoszenia;
- rozpoznawaniu i analizowaniu zagrożeń występujących w rejonach napięć, konfliktów i kryzysów międzynarodowych oraz podejmowaniu działań mających na celu eliminowanie tych zagrożeń.

Zadania powyższe mają realizować **służby specjalne**, m.in. poprzez:

- rozpoznawanie zagrożeń dla bezpieczeństwa wewnętrznego i porządku konstytucyjnego, w szczególności suwerenności, nienaruszalności terytorium i obronności państwa, zapobieganie im i ich zwalczanie;
- wykonywanie - w zakresie ochrony informacji niejawnych, w tym także wymienianych w ramach współpracy sojuszniczej i międzynarodowej - zadań służby ochrony państwa i krajowej władzy bezpieczeństwa określonych w ustawach oraz umowach międzynarodowych.

Do służb specjalnych należy więc zwalczanie zagrożeń dla rządowych systemów i sieci teleinformatycznych. Ich zadaniem jest zwalczanie przestępczości komputerowej wymierzonej w rządową i samorządową infrastrukturę telekomunikacyjną, w tym przeciwdziałanie atakom na jej elementy.

Do zapewnienia należytej ochrony tej infrastruktury niezbędny jest rozwój i utrzymanie zdolności do zapobiegania wszelkim zakłóceniom, jakie mogą wystąpić w tej sferze, a także zdolności do koordynacji procesów dochodzeniowych w ramach instytucji posiadających elementy rządowej infrastruktury teleinformatycznej. Działania te prowadzone mają być wspólnie z sojusznikami, a także producentami i dostawcami urządzeń oraz oprogramowania informatycznego, krajowymi operatorami telekomunikacyjnymi i dostawcami usług internetowych, ośrodkami badawczymi i szkoleniowymi. *„Aby podejmowane działania w tej dziedzinie były skuteczne, należy w sposób priorytetowy podejść do **rozwoju i wdrażania rodzimej kryptografii** oraz dostosować przepisy prawa telekomunikacyjnego, które wraz z szybkim postępem technologicznym mogą się okazać niewystarczające do zapewnienia bezpieczeństwa chronionej infrastrukturze teleinformatycznej*[30]*"*.

Strategia zakłada także podjęcie wysiłków na rzecz rozwoju nowoczesnej łączności, w tym sprawnej i bezpiecznej strategicznej infrastruktury teleinformatycznej oraz zapewnienia warunków budowy społeczeństwa informacyjnego.

2.2.2. Priorytetowe aspekty bezpieczeństwa narodowego XXI wieku

Zgodnie z powszechnie przyjętą opinią do nowych płaszczyzn bezpieczeństwa narodowego należeć będą :

- ekonomiczna;
- naukowo-techniczna- **informacyjna**;
- ideologiczna;
- ekologiczna;
- społeczna,

a do priorytetowych aspektów bezpieczeństwa XXI w.:

- **bezpieczeństwo informacyjne**;
- bezpieczeństwo ekonomiczne.

W niniejszej rozprawie główny nacisk zostanie położony na płaszczyznę informacyjną bezpieczeństwa narodowego.

---

[30] *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej* z 22 lipca 2003 r. zatwierdzona przez Prezydenta RP 8 września 2003 roku

2.2.3. Płaszczyzna informacyjna bezpieczeństwa narodowego

"Gdzie się podziała nasza mądrość, którą zastąpiła wiedza.
Gdzie się podziała nasza wiedza, którą zastąpiła informacja."
T. S. Elliot

Jedną z charakterystycznych cech rozwoju współczesnego świata jest nieustanny wzrost roli informacji, która obecnie stanowi coraz częściej główną przesłankę rozwoju wszystkich podstawowych dziedzin życia gospodarczego i społecznego[31]. ***Informacja*** (z języka łacińskiego *„informatio" - wizerunek, zarys, pojęcie; „informo, informare" - kształtować, tworzyć, wyobrażać sobie, przedstawiać, opisywać, kreślić, kształcić) to wyobrażenie, pojęcie oznaczające wiedzę, która może być przekazana w jakiejkolwiek formie, gromadzona oraz przetwarzana*[32].

Definicję informacji przytacza Encyklopedia Powszechna PWN: *„przedmiot myślowy odzwierciedlający każdy czynnik zmniejszający stopień niewiedzy (nieokreśloności) o badanym zjawisku, umożliwiający człowiekowi, organizmowi żywemu lub urządzeniu automatycznemu polepszenie znajomości otoczenia i w sprawniejszy sposób przeprowadzenie działania celowego"*[33]. Inaczej definiuje informację słownik wyrazów obcych: *„**informacja** - wiadomość, wieść, nowina, rzecz zakomunikowana, zawiadomienie, komunikat; pouczenie, powiadomienie, zakomunikowanie o czymś; dane; (ilość informacji) - miara wiedzy o jakimś zdarzeniu, uzyskanej w wyniku przeprowadzenia określonego eksperymentu; mat., cyber. - miara braku entropii (nieokreśloności), miara organizacji systemu"*[34].

Ojciec współczesnej cybernetyki Norbert Wiener określa ***informację*** jako *„treść zaczerpniętą ze świata zewnętrznego w procesie naszego dostosowywania się do niego i przystosowywania się do niego naszych zmysłów*[35]".

Nawiązując do teorii informacji C. E. Shannona (omówiona w ***Rozdziale 2.3.3***) K. Urbanowicz podaje: *„**informacja** jest sposobem opisu jakości w sposób nieciągły; z definicji informacji wynika, że informacja jest skwantowana, czyli jest w pewnych porcjach (kwantach)"*[36], natomiast A. Mazurkiewicz rozwija:

---

[31] R. Szałowski. *Prawna ochrona informacji niejawnych i danych osobowych*, Warszawa 2000, s. 11
[32] *Umowa między stronami Traktatu Północnoatlantyckiego o ochronie informacji* z 6.03.1997r.
[33] Encyklopedia Powszechna, PWN Warszawa 1997
[34] *Słownik wyrazów obcych i zwrotów obcojęzycznych W. Kopalińskiego – OMNIA* – serwis internetowy
[35] N. Wiener, *Cybernetyka, czyli sterowanie i komunikacja w zwierzęciu i maszynie*, PWN, Warszawa 1971.
[36] K. Urbanowicz. *Teoria Informacji*, Politechnika Warszawska 2000

„...informacją nazywamy wielkość abstrakcyjną, która może być przechowywana w pewnych obiektach, przesyłana między pewnymi obiektami, przetwarzana w pewnych obiektach i stosowana do sterowania pewnymi obiektami"[37].

Według P. Sienkiewicza *„**informacja** to zbiór faktów, zdarzeń, cech obiektów itp., zawarty w określonej wiadomości (komunikacie), tak ujęty i podany w takiej formie, że pozwala odbiorcy ustosunkować się do zaistniałej sytuacji i podjąć odpowiednie działania umysłowe lub fizyczne"*[38]. Podejście to harmonizuje z bodaj najkrótszą definicją informacji, przytoczoną przez C. Cempela, według którego **informacja** to *„zawartość przekazu zdolna wzbudzić działanie"*[39].

Wzrost znaczenia informacji powoduje, że ujęcie negatywne bezpieczeństwa informacyjnego jest niewystarczające dla zapewnienia bezpieczeństwa narodowego. Każda płaszczyzna bezpieczeństwa narodowego staje się coraz bardziej zależna od swobodnego przepływu informacji i od zachowania systemów bazujących na informacjach. Środki polityki bezpieczeństwa informacyjnego budowane w oparciu o ujęcie pozytywne muszą uwzględniać, że:

- informacja stanowi zasób strategiczny państw i organizacji XXI w.;
- informacja i wynikająca z niej wiedza oraz technologie informatyczne staną się podstawowym czynnikiem wytwórczym;
- zakłócenie prawidłowości działania systemów informacyjno-sterujących nie wymaga wysokich nakładów materialnych;
- charakter konfliktów przeniesie się na płaszczyznę walki informacyjnej.

Do desygnatu pojęcia *„informacja"* L. Ciborowski przypisuje ustalenie identyfikujące następującej treści: *„**informacja** to bodziec oddziałujący na układ recepcyjny człowieka, powodujący wytwarzanie w jego wyobraźni przedmiotu myślowego, odzwierciedlającego obraz rzeczy materialnej lub abstrakcyjnej (przedmiotu, procesu, zjawiska, pojęcia itp.), który w jego przekonaniu (świadomości) kojarzy się jakoś z tym bodźcem"*[40]. Bezpieczeństwo informacyjne stopniowo staje się w powszechnej świadomości takim przedmiotem myślowym, czego implikacją jest przypisanie właściwej roli czynnikowi informacyjnemu w obszarze militarnym.

---

[37] A. Mazurkiewicz. *Lokalne negocjacje w pewnych strukturach komunikacyjnych*. IPI PAN, 2003
[38] P. Sienkiewicz. *Teoria Informacji. Wykłady otwarte*. Akademia Obrony Narodowej 2002
[39] C. Cempel. *Teoria i inżynieria systemów – skrypt*, Politechnika Poznańska, 2002
[40] L. Ciborowski. *Walka Informacyjna*. Europejskie Centrum Edukacyjne, Wyd. Adam Marszałek Toruń 1999

2.3 Rola czynnika informacyjnego w militarnym obszarze bezpieczeństwa państwa

Współczesne narzędzia walki informacyjnej stwarzają możliwości podejmowania skutecznej działalności ukierunkowanej na sterowanie procesami decyzyjnymi przeciwnika w skali państwowej a także w czasie konfliktu zbrojnego. Wprowadzenie do publicznego i utajnionego systemu informacyjnego państwa złożonych zbiorów precyzyjnie dobranych prawdziwych i sfałszowanych danych może generować podejmowanie błędnych, katastrofalnych w skutkach decyzji. Wraz z budowaniem cywilizacji informacyjnej należy stworzyć środki bezpieczeństwa informacyjnego dla zapewnienia prawidłowego jej funkcjonowania. Proces zmian związanych z przechodzeniem do nowej epoki rozwojowej wzmacnia rolę państwa jako organizatora procesów społecznych i gwaranta interesów narodowych, nakładając jednocześnie obowiązek zapewnienia bezpieczeństwa informacyjnego ze względu na łatwość atakowania systemów informacyjnych[41].

Niezmiernie istotnym czynnikiem jest znaczenie walki informacyjnej w militarnym obszarze bezpieczeństwa państwa, szczególnie w warunkach prowadzenia platformo-centrycznych i sieciocentrycznych operacji informacyjnych w trakcie działań bojowych.

2.3.1. Elementy walki informacyjnej w obszarze działań bojowych

Mierzenie jakości procesów bezpieczeństwa, a zwłaszcza badanie bezpieczeństwa informacyjnego państwa , warunków w jakich te procesy przebiegają i od których są uzależnione - jest trudne z uwagi na brak jednolitych standardów, czytelnych wzorców i wspólnych, przy zróżnicowanych parametrach, narzędzi pomiarowych. Obiektywna ocena nie może więc być wynikiem instrumentalnego pomiaru, lecz efektem pogłębionej, wielostronnej analizy.

[41] T. Jemioło. *Globalizacja. Szanse i zagrożenia.* AON 5215/2000, Warszawa 2000

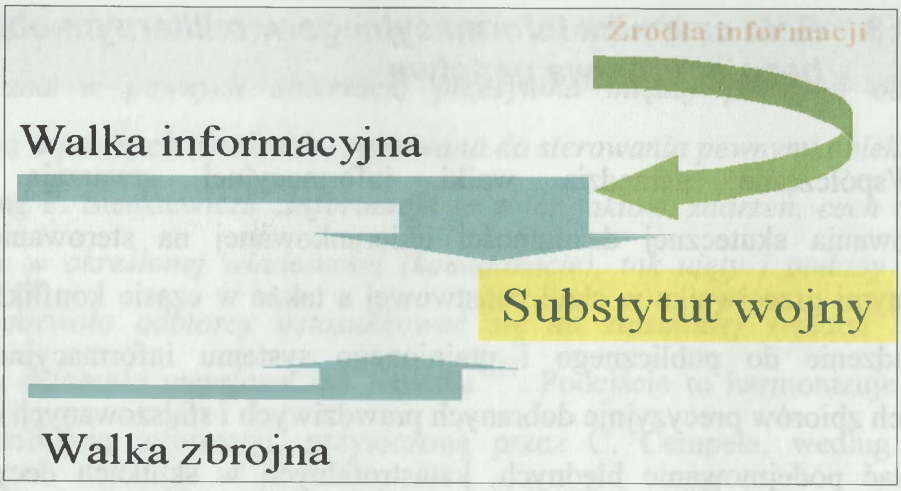


Diagram 5: ***Zrewaloryzowanie roli walki informacyjnej***
Źródło: opracowanie własne

Tradycyjny konflikt zbrojny, wykorzystujący siły lądowe, morskie i powietrzne wspierane przez systemy dowodzenia i kierowania, wywiadu, obserwacji i rozpoznania wymaga informacji o sytuacji na polu walki w czasie rzeczywistym. Sztuka wojenna została wzbogacona trzecim elementem – operacjami informacyjnymi i technologią informacyjną jako wzmocnieniem dla wizji pola walki i systemów dowodzenia.

Walka informacyjna

W. Schwartau uważa, że *„walka informacyjna to konflikt elektroniczny, w którym informacja jest strategicznym celem zdobycia i zabezpieczenia"*[42], a M. Libicki w swojej książce: *„What is Information Warfare?"* nie definiuje wprost walki informacyjnej, podaje natomiast siedem form, jakie może przybrać *IW*:

- *command and control warfare* - walka o przewagę w dowodzeniu;
- *intelligence based warfare* - walka bazująca na wiedzy rozpoznawczej;
- *electronic warfare* - techniki radioelektroniczne i kryptograficzne;
- *psychological warfare* - działania psychologiczne;
- *hacker warfare* - wojna hakerska (ataki na systemy informacyjne);
- *economic information warfare* – walka o dominację ekonomiczną;
- *cyber warfare* walka w wirtualnej rzeczywistości[43].

[42] W. Schwartau, *Information Information Warfare. Cyberterrorism: Protecting Your Personal Security in the Electronic Age,* New York 1996 s. 13
[43] M. Libicki, *What is Information Warfare?,* Washington 1995, s. 7.

W polskiej myśli wojskowej pierwszym, który podjął się zdefiniowania walki informacyjnej był L. Ciborowski. Według niego, *walką informacyjną* są *„działania kooperacji negatywnej wzajemnej, w których cel destrukcyjnego oddziaływania skoncentrowany jest na systemach informacyjno-sterujących przeciwnych sobie stron"*[44].

L. Ciborowski uważa, że przedmiotem konfliktu nie jest informacja, ale system informacyjno-sterujący, zaś *IW* pełni jedynie funkcję wspierającą inne walki. W polskiej myśli wojskowej przyjęła się definicja zaproponowana przez R. Szpyrę (umieszczona została m.in. w *„Słowniku terminów z zakresu bezpieczeństwa narodowego"*, wydanego przez Akademię Obrony Narodowej[45]). Według niej, walka informacyjna to *„zorganizowana w formę 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 przez nie informacji przed podobnym działaniem przeciwnika"*[46].

„Nie istnieje powszechnie uzgodniona definicja walki informacyjnej...", stwierdza R. Stark, *„...jest jednak wspólna treść większości spotykanych definicji"*[47]. Treść ta sprowadza się do tego, że walka informacyjna jest konfliktem, w którym informacja jest jednocześnie *zasobem, obiektem ataku* i *bronią*. IW obejmuje także fizyczną destrukcję infrastruktury, która wykorzystywana jest przez przeciwnika do działań operacyjnych[48]. Na marginesie warto zasygnalizować, że istnieje spór, co do rozumienia pojęcia *Information Warfare*. Termin ten możemy przetłumaczyć na język polski zarówno jako *„walka informacyjna"*, jak i *„wojna informacyjna"*. J. Bloch przetłumaczyła tytuł książki D. E. Denning *„Information Warfare and Security"* jako *„Wojna informacyjna i bezpieczeństwo informacji"*. W niektórych polskich publikacjach można także znaleźć termin *„wojna*

[44] L. Ciborowski, *Walka...*, op. cit., s. 68.
[45] Słownik terminów z zakresu bezpieczeństwa narodowego, Warszawa 2002, s. 157.
[46] R. Szpyra. *Walka informacyjna w przyszłych działaniach sił powietrznych. Opracowanie pod kryptonimem CYBERAWIATOR*, Warszawa 2000, s. 146.
[47] Stark R. *Future Warfare: Information Superiority through Info War.* AUM AFB 1995
[48] Stein G. *Information War - Cyberwar – Netwar Cyber Terrorismt.* NARMS Breda 1999

informacyjna". Jednak R. Szpyra argumentuje, że wojna jest kategorią obejmującą wszystkie formy walki. Jest parasolem rozpostartym nad różnymi rodzajami walki: zbrojną, informacyjną, ekonomiczną itd. Podsumowaniem tych definicji jest uwaga T. L. Sanza, który stwierdził, 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 (*information age warfare*)[49].

W dostępnej literaturze przedmiotu brak jest wyczerpujących opracowań monograficznych na temat walki informacyjnej. Według doktryny USA[50] - funkcjonują trzy terminy dotyczące walki informacyjnej, a mianowicie:

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

Walka informacyjna - są to operacje informacyjne prowadzone w czasie kryzysów lub konfliktów, aby wspierać określone zadania lub osiągnąć specjalne cele nad specyficznym przeciwnikiem lub przeciwnikami. Według niektórych specjalistów wojskowych walka informacyjna dotyczy zmagania się w ogólnych dziedzinach (militarnej, politycznej, dyplomatycznej, ekonomicznej, etnicznej, socjalnej, infrastrukturze, kryminalnej, ideologicznej, religijnej i możliwie jeszcze innych) o uzyskanie kontroli i przewagi dotyczącej wszelkich postaci informacji. Walka informacyjna może zacząć się bez wypowiedzenia (deklaracji) wojny i może być stosowana na szerokim froncie lub na polu walki – otwarcie lub skrycie, izolowana lub szeroko rozprzestrzeniona. Celem walki informacyjnej może być maskowanie lub nie maskowanie faktów wykorzystanie, mylenie (takie jak dezinformacja), przerwanie lub odmowa obsługi i zniszczenie informacji. Atakowanie dowództw i systemów kierowania, telekomunikacji i powiązanej z tym infrastruktury wysoko

[49] T. L. Sanz, *InformationAge Warfare:A Workins Bibliography,* „Military Review", t. LXXVIII, nr 2, marzec kwiecień 1998

[50] Matutszewski J. Rapacki T. *Aktualne Koncepcje Prowadzenia Rozpoznania, Walki Radioelektronicznej i Informacyjnej w państwach NATO.* Konferencja Radiolokacji 2001

uprzemysłowionych państw jest oceniane jako wysoce efektywny sposób do załamania potęgi państwa. Jest to możliwe z następujących powodów: zagrożenie rośnie, jeśli atak na infrastrukturę staje się bardziej opłacalny; zagrożenie wzrasta, jeśli prawdopodobieństwo wtargnięcia/niepokojenia (*intrusion*), zdobywania, manipulacji wzrasta odpowiednio do większej liczby uczestników z większą wiedzą na obszarze globalnym; wzrasta możliwość nie zabezpieczenia się przed atakiem, jeśli maleje niezawodność systemów. Może to być spowodowane przez wzrost złożoności technicznej sprzętu i krytyczne powiązania sprzętowe i programowe; wzrasta możliwość nie zabezpieczenia się przed atakiem, jeśli instalacja systemu, wykonywane operacje i nadzór stają się bardziej scentralizowane. Powody ekonomicznej praktyczne często prowadzą do centralizacji; efekty wzrastają, jeśli zwiększa się w społeczeństwie zależność od technologii w coraz większej liczbie dziedzin działalności ludzkiej; sposoby ochrony są niewystarczające, jeśli wiedza potrzebna do zapewnienia bezpieczeństwa jest niewystarczająca lub inwestycje ekonomiczne są niewystarczające. Walka informacyjna kieruje się na samą informację, na transmisję, zbieranie, przetwarzanie informacji i decyzje ludzkie oparte na informacji. Może mieć duży wpływ na zapobieżenie kryzysu, jeśli jest ostrożnie realizowana, koordynowana i wykonywana. Walka informacyjna jest stosowana we wszystkich fazach wojny począwszy od mobilizacji do rozmieszczenia, przydziału zadań, utrzymania, zachowania i przegrupowania wszystkich operacji militarnych na wszystkich poziomach konfliktu. Defensywna walka informacyjna jest stale stosowana zarówno w czasie pokoju i kryzysu i jest stałą częścią zabezpieczenia i obrony. Ofensywna walka informacyjna może być wykonywana w różnych sytuacjach we wszystkich operacjach militarnych. W pełni rozwinięta i zintegrowana, ofensywna walka informacyjna może oferować olbrzymi potencjał i zwiększyć wsparcie żołnierzom na polu walki.

Przyjmuje się, że walka informacyjna obejmuje trzy fundamentalne komponenty:

- zdobywanie informacji z rozpoznania i wywiadu;
- wykorzystanie systemów informacyjnych;
- kombinację tych działań - C2W *(Command and Control Warfare).*

Zdobywanie informacji z rozpoznania i wywiadu polega na pozyskiwaniu jak największej liczby wiadomości o:

- własnych siłach zbrojnych (ich dyslokacji, skuteczności prowadzenia walki oraz aktualnej działalności);
- siłach zbrojnych przeciwnika (ich dyslokacji, możliwościach bojowych, skuteczności walki, zamiarach), które mogłyby być przydatne dla odniesienia sukcesu w walce.

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

- koordynację działań z siłami powietrznymi i marynarką wojenną,
- niezbędne dane dla nowoczesnych systemów broni,
- ścisłą kontrolę prowadzonych działań oraz ich skuteczność,
- synchronizację różnego typu operacji zarówno na tyłach, jak i wysuniętych rubieżach w jedną połączoną operację.

Operacje informacyjne (*IO – Information Operations*) są to podjęte działania, które mają wpływać na informacje przeciwnika i jego systemy informacyjne podczas ochrony własnych informacji i systemów informacyjnych.

Podstawowym celem operacji informacyjnych jest ich wpływ na podejmowanie decyzji przez ludzi. Operacje informacyjne nie mogą być takie same, tj. mieć te same zadania, cele i rodzaje działania. Wynikają one ze struktury zaangażowania. Należy rozróżniać działania wykonywane w czasie pokoju, w momencie kryzysu i podczas zaangażowania się do walki.

Operacje (działania) informacyjne, w czasie wojny nazywane wprost walką informacyjną, są definiowane jako *„ciągłe działanie sił zbrojnych w ramach wojskowego środowiska informacyjnego, które przyczyniają się do wzmocnienia i obrony możliwości sił własnych w zakresie zdobywania, przetwarzania i przekazywania informacji w celu uzyskania przewagi w całym spektrum walki zbrojnej, prowadzonej wewnątrz globalnego środowiska informacyjnego, przy jednoczesnym pozbawieniu takiej możliwości strony przeciwnej"*[51]. Operacje

[51] *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*

informacyjne zaangażowane są wszystkie instytucje administracji rządowej, publicznych (media) i militarnych (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. Operacje informacyjne są planowane i prowadzone zarówno w czasie pokoju, jak i w okresach kryzysu oraz w czasie wojny.

Walka informacyjna jest pojęciem znacznie szerszym niż ***walka elektroniczna (radioelektroniczna),*** obejmującym swym zasięgiem wiele dziedzin działalności (tak militarnej jak i pozamilitarnej), których podstawowym celem jest oddziaływanie na procesy i systemy informacyjne przeciwnika, przy jednoczesnej ochronie własnych procesów i systemów informacyjnych. Ich złożoność, niejednoznaczność w pojmowaniu zadań i celów, doprowadziły do sytuacji, w której istnieją spore różnice interpretacyjne, podczas gdy *walka radioelektroniczna* została zdefiniowana bardziej precyzyjnie i pomimo drobnych różnic pojęciowych i organizacyjnych jest odbierana jednoznacznie. Zastosowanie instrumentów objętych pojęciem „*walki informacyjnej*" może spowodować, już nie tylko jak dotychczas, straty powstałe w wyniku walk, lecz w krótkim czasie doprowadzić do ekstremalnego zniszczenia nowocześnie zorganizowanego systemu całego państwa. Właśnie dlatego wysoko uprzemysłowione społeczeństwa są zmuszone zastanawiać się nad różnymi środkami ochrony własnych systemów telekomunikacyjnych i informatycznych[52].

W walce zbrojnej układy informacyjne zaangażowanych stron posiadają duży stopień skomplikowania, jak również dwoiste przeznaczenie. Są systemami służącymi do zdobywania informacji o przeciwniku oraz do przekazywania informacji we własnych procesach dowodzenia i kierowania. Dlatego też ich strukturę tworzą dwa sprzężone ze sobą podsystemy:

- pierwszy - rozpoznania, służący do zdobywania informacji o przeciwniku;
- drugi - dowodzenia wojskami i kierowania uzbrojeniem.

Uwzględniając reguły kooperacji negatywnej wzajemnej do działań noszących znamiona walki, należy włączyć dwa przeciwnie skierowane podsystemy:

---

[52] Matutszewski J. Rapacki T. *Aktualne Koncepcje Prowadzenia Rozpoznania, Walki Radioelektronicznej i Informacyjnej w państwach NATO.* Konferencja Radiolokacji 2001

- pierwszy - zakłócania informacyjnego, ukierunkowany w swej funkcjonalności na wnoszenie entropii informacyjnej do systemu informacyjnego przeciwnika i destrukcji fizycznej nośników;
- drugi - obrony informacyjnej, ukierunkowany na przeciwdziałanie rozpoznaniu i zakłócaniu informacyjnemu przeciwnika.

Przyjmując to za właściwe, pojęcie i przestrzeń walki informacyjnej można zdefiniować następująco:

- *walka informacyjna to kooperacja negatywna wzajemna realizowana w sferze zdobywania informacji, zakłócania informacyjnego i obrony informacyjnej, gdzie każdemu działaniu jednej strony przyporządkowane jest działanie antagonistyczne strony drugiej;*

- *istota walki informacyjnej sprowadza się do stworzenia sytuacji utrudniających przeciwnikowi podejmowanie trafnych decyzji, wykonywanie sprawnych ruchów wojskami i precyzyjnych uderzeń ogniowych przy jednoczesnej obronie przed tym samym wojsk własnych;*

- *przestrzeń walki informacyjnej to zbiór wszelkich działań, przynajmniej dwóch przeciwnych sobie stron, których istota, ze względu na relację porządkującą celu, skupiona jest w podprzestrzeniach: zdobywania informacji, zakłócania informacyjnego i obrony informacyjnej*[53].

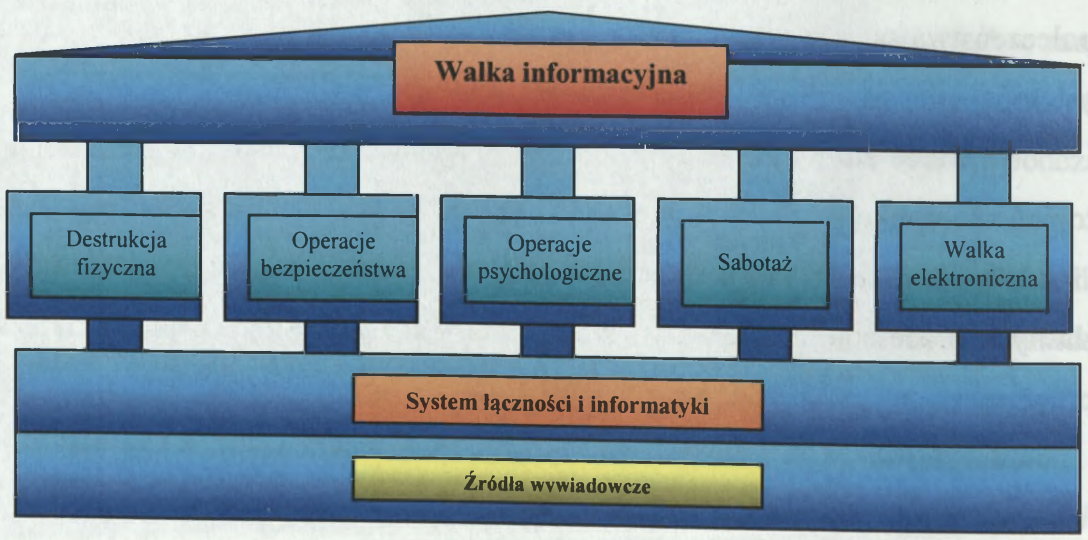


Diagram 6: ***Elementy składowe walki informacyjnej***

Źródło: Kwiatosz J. *Współczesne poglądy na walkę informacyjną*. Materiały VIII Konferencji Naukowej „Automatyzacja Dowodzenia", Jelenia Góra, 2000.

[53] Ciborowski L. *Walka informacyjna*, wyd. ECE, Toruń 1999

Walka informacyjna skierowana przeciwko przeciwnikowi powinna umożliwić:

- utrudnienie procesu dowodzenia;
- obniżenie tempa operacji lub jej przerwanie;
- uniemożliwienie wykorzystania siły ognia;
- redukcję zamiaru działań.

W stosunku do własnych wojsk walka informacyjna powinna umożliwić:

- zmniejszenie zagrożenia własnego systemu dowodzenia i kierowania;
- zmniejszenie wpływu działań walki elektronicznej przeciwnika;
- ochronę systemu przed działaniami bezpieczeństwa ze strony przeciwnika;
- obniżenie wpływu działań psychologicznych przeciwnika.

Uproszczony model funkcjonalny walki informacyjnej jest pokazany na ***Diagramie*** *7*. Model ten zakłada, że walka informacyjna występuje w trzech dziedzinach, a mianowicie: w umyśle ludzkim, w cyberprzestrzeni oraz w przestrzeni fizycznej. Atakujący i obiekty (cele) ataku występują zatem na trzech poziomach (warstwach): percepcyjnym (wiedza ludzka), informacyjnym (infrastruktura informacyjna) i fizycznym (dane). Poziomy te są hierarchiczne z powiązaniem w dół po stronie atakujących i w górę po stronie obiektów ataku.

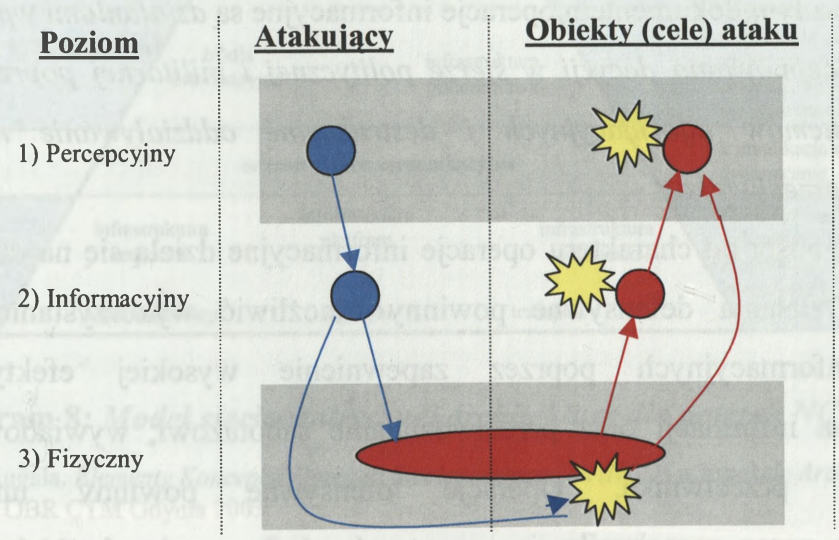


Diagram 7: ***Trójpoziomowy model walki informacyjnej***

Źródło: Kwiatosz J. *Współczesne Poglądy Na Walkę Informacyjną*. Materiały VIII Konferencji Naukowej „Automatyzacja Dowodzenia", Jelenia Góra, 2000.

Na najwyższym poziomie znajduje się warstwa ludzkiej percepcji, postanowień decydentów, polityków, dowódców wojskowych i całej populacji. Na tym poziomie określane są pożądane działania przeciwko obiektom ataku i przewidywane najbardziej prawdopodobne następstwa tych działań. Obiekty ataku są poddawane wpływom tych decyzji i rezultatom podjętych przeciw nim działań.

Na średnim poziomie jest warstwa informacyjna, która zawiera infrastrukturę 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).

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 systemem, które mają ciągły wpływ na jego 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.*

W zależności od charakteru operacje informacyjne dzielą się na defensywne i ofensywne. Działania defensywne powinny umożliwić wykorzystanie własnych systemów informacyjnych poprzez zapewnienie wysokiej efektywności i bezpieczeństwa informacji oraz przeciwdziałanie sabotażowi, wywiadowi i walce elektronicznej przeciwnika. Operacje ofensywne powinny uniemożliwić wykorzystanie przez przeciwnika jego systemów informacyjnych. Należą do nich m.in.: atak fizyczny, sabotaż, działania psychologiczne, walka radioelektroniczna[54].

[54] Kwiatosz J. *Współczesne Poglądy Na Walkę Informacyjną*. Materiały VIII Konferencji Naukowej „Automatyzacja Dowodzenia", Jelenia Góra, 2000.

Charakter współczesnego pola walki ogranicza stosowanie indywidualnych, izolowanych operacji. Nawet konflikty lokalne, stając się zagrożeniem pokoju dla większej populacji, rozwiązywane są przez siły koalicyjne. Tendencja ta wymusza nowe spojrzenie na współdziałanie na polu walki. Zasady, które przyjęto dla tego typu działań, zostały sformułowane w postaci koncepcji zwanej ogólnie *„sieciocentrycznymi działaniami wojennymi*[55]*"* (*Network Centric Warfare*[56]). W kontekście dowodzenia mówi się coraz częściej o *„operacjach sieciocentrycznych"*[57] (*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.

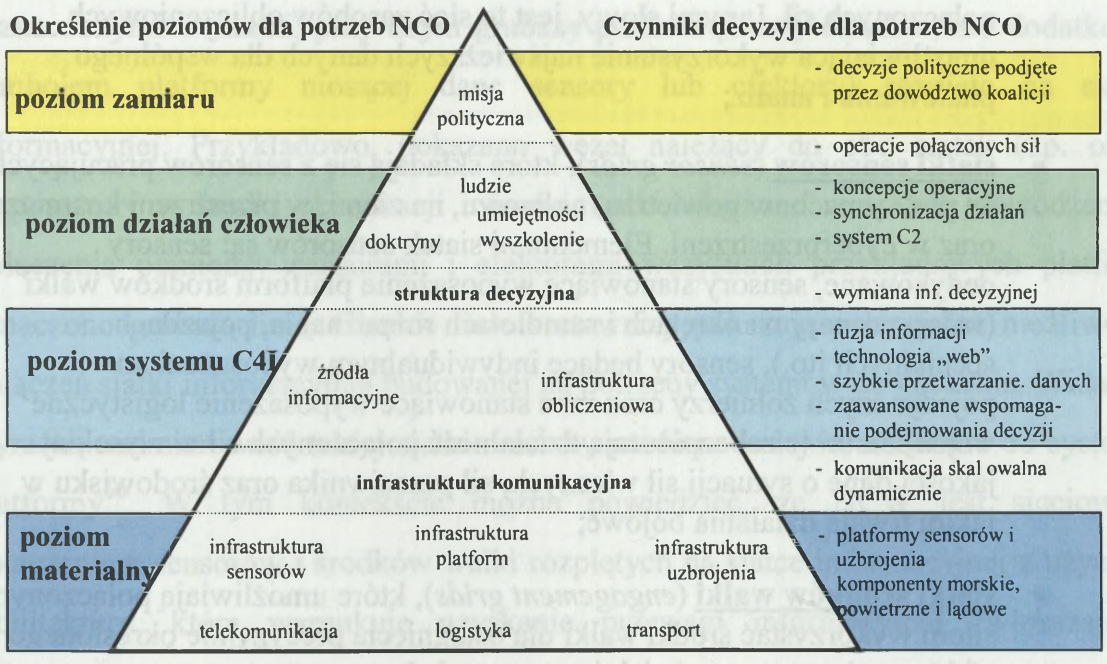


Diagram 8: ***Model sieciocentrycznej architektury dla potrzeb NCO***

Źródło: R. Rugała. *Elementy Koncepcji Operacji Sieciocentrycznych (NCO) w aspekcie Architektury Systemów Dowodzenia.* OBR CTM Gdynia 2003

[55]David S. Alberts, 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.
[56]Network Centric Warfare – przetłumaczono jako sieciocentryczna architektura ZtSyD za: A. Stokalski, *Sieciocentryczna architektura zautomatyzowanych systemów dowodzenia – Bazowa Infrastruktura Informacyjna*, część I, s. 5-17.
[57]Hans E. Keus, *Network Centric Operations. Implications for Allied and Coalition Operations,* Konferencja SMi Conferences on Network Centric Warfare, London, 4-5 October 2000.

Sieciocentryczne działania wojenne (NCW), jako przeciwstawienie dla dotychczasowych działań nazwanych *„platformo-centrycznymi"*, zdefiniowano jako koncepcję działań w celu osiągnięcia przewagi informacyjnej zwiększając w ten sposób efektywność mocy uderzeniowej sił zbrojnych.

Realizacja tej zasady w dobie walki informacyjnej wymaga zaawansowanej wymiany 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[58] są:

- **siatka informacyjna** (*information grid*), która zabezpiecza infrastrukturę dla sieciocentrycznych obliczeń i komunikacji (zwana często *infostrukturą*). Infrastruktura ta obsługuje przyjmowanie, przetwarzanie, przesyłanie, zapamiętywanie i zabezpieczenie informacji niezbędnych dla działania połączonych sił. Innymi słowy, jest to sieć zasobów obliczeniowych umożliwiająca wykorzystanie najświeższych danych dla wspólnego planowania i analiz;

- **siatki sensorów** (*sensor grids*), które składają się z sensorów pracujących na platformach: w powietrzu, na morzu, na ziemi, w przestrzeni kosmicznej oraz w cyberprzestrzeni. Elementami siatek sensorów są: sensory dedykowane, sensory stanowiące wyposażenie platform środków walki (radary, sonary na okrętach i samolotach rozpoznania, pojazdach specjalnych itp.), sensory będące indywidualnym wyposażeniem pojedynczych żołnierzy oraz inne stanowiące 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*), które umożliwiają połączonym siłom wykorzystać środki walki dla osiągnięcia precyzyjnie określonego efektu zarówno w czasie jak i przestrzeni. Jest to zatem system skoordynowanych środków walki, umieszczonych na różnorakich platformach (okręty, samoloty, czołgi), umożliwiający jak najszybsze, lecz we właściwym czasie i przestrzeni, przeciwstawienie się zagrożeniom.

[58] G.R. Maddiso, *The Naval C4I Way Ahead – A Blueprint for 2010*. Materiały NG/5 NATO, s. 44.

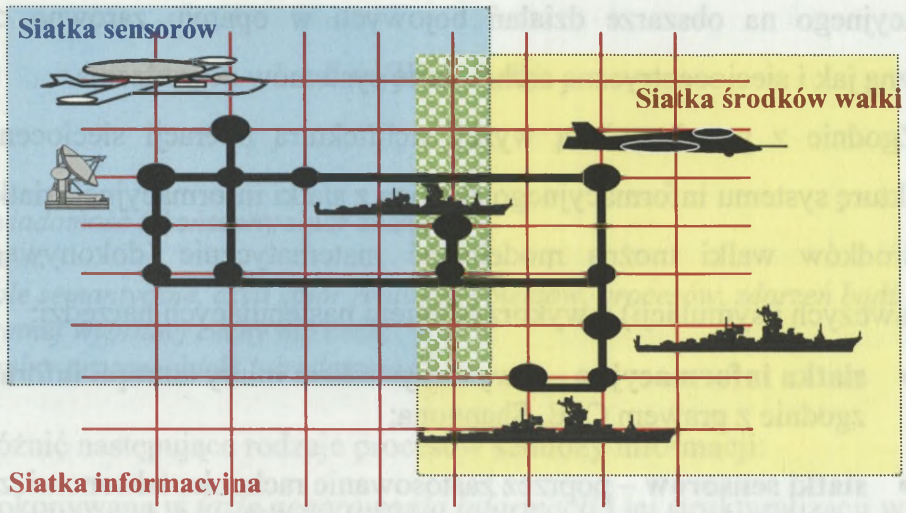


Diagram 9: ***Siatki sensorów i środków walki rozpięte na siatce informacyjnej***[59]

Na diagramie zaznaczono schematycznie siatki sensorów i efektorów (z zaznaczonymi węzłami, przy czym grubszy punkt węzłowy oznakowano dodatkowo symbolem platformy niosącej dane sensory lub efektory) rozpięte na siatce informacyjnej. Przykładowo, pokazano węzeł należący do obu siatek (np. okręt wyposażony w środki obserwacji i środki walki włączone w system dowodzenia). Połączenia pomiędzy sensorami i efektorami wszystkich przykładowych platform oznaczono grubszą linią. Cienkie linie kratownicy pokazują potencjalne możliwości połączeń siatki informacyjnej budowanej na potrzeby systemów dowodzenia. Widać tu wyraźną nadmiarowość takiej siatki oraz otwartość na kolejne, włączane do systemu platformy[60]. W tym kontekście można powiedzieć, że NCW jest sieciowym połączeniem sensorów i środków walki rozpiętych na siatce informacyjnej z użyciem architektury, która warunkuje uzyskanie przewagi informacyjnej zwiększającej efektywność użycia sił uderzeniowych w celu wykonania postawionych zadań bojowych (spełnienia misji).

[59] R. Rugała. *Elementy Koncepcji Operacji Sieciocentrycznych (NCO) w aspekcie Architektury Systemów Dowodzenia.* OBR CTM Gdynia 2003
[60] *Ibidem*

Celem niniejszego rozdziału jest wykazanie determinującej roli czynnika informacyjnego na obszarze działań bojowych w oparciu zarówno o platformo-centryczną jak i sieciocentryczną architekturę systemów dowodzenia.

Zgodnie z przedstawioną wyżej architekturą operacji sieciocentrycznych – infostrukturę systemu informacyjnego złożoną z siatki informacyjnej, siatki sensorów i siatki środków walki można modelować matematycznie (dokonywać pomiarów porównawczych i symulacji) z wykorzystaniem następujących narzędzi:

- **siatka informacyjna** – z wykorzystaniem miary entropii informacyjnej zgodnie z prawem C. E. Shannona;
- **siatki sensorów** – poprzez zastosowanie rachunku taksonomicznego uwzględniającego nasycenie pola walki źródłami informacji;
- **siatki środków walki** – z wykorzystaniem *mieszanego prawa F. W. Lanchestera* uwzględniającego wpływ przewagi informacyjnej na przebieg działań bojowych.

Kolejne podrozdziały prezentują modele matematyczne poszczególnych elementów powyższej architektury i ich zastosowanie.

2.3.2. Identyfikacja, ocena i kwantyfikacja informacji

Proces poznania jest ciągiem pozyskiwania informacji, sprowadzający się do wzbogacania zasobu informacyjnego poprzez wyprowadzanie nowych informacji z posiadanych danych, a wybór jest konsekwencją przeprowadzonego wartościowania. To nabywanie, wzbogacanie, wartościowanie i przekazywanie informacji odbywa się w sposób powiązany (równoległy) i zostało nazwane przez K. Devlina *postawą informacyjną*[61], wymagającą myślenia systemowego. metodycznego, teleologicznego (celowego), a także zaangażowania nabytego doświadczenia.

Współczesne możliwości szybkiego i wydajnego przekazywania informacji w obszarze całego globu ziemskiego przekształciły świat w globalną wioskę.

Zrozumienie znaczenia sygnałów-nośników informacji umożliwia nam zjawisko semiozy. Polega ono na tym, że w procesie generowania informacji każdej wiadomości (W) będącej skończonym zbiorem danych, przypisuje się w ramach przyjętego języka (J) określone pole semantyczności, (P), które odwzorowuje realny

[61] K. Devlin. *Żegnaj Kartezjuszu. Rozstanie z logiką w poszukiwaniu nowej kosmologii umysłu.* Warszawa 1997.

proces, obiekt lub zdarzenie (R). Informacyjnym produktem semiotycznym (S) będzie więc:

$$S = \{W, J, P, R\}$$

gdzie:

W – wiadomość (skończony zbiór znaków);
J – język;
P - pole semantyczne, czyli zbiór realnych obiektów, procesów, zdarzeń bądź ich konkretnej wybranej cechy lub cech;
R - realny proces, obiekt lub zdarzenie[62].

Można wyróżnić następujące rodzaje procesów semiozy informacji:

- dokonywane w *fazie generowania informacji* i jej strukturalizacji w formie
- wiadomości;
- dokonywane w *fazach interpretacji i wykorzystywania* informacji zawartej w wiadomości;
- dokonywane w *fazach gromadzenia, przetwarzania, przekazywania i udostępniania* informacji.

W fazie generowania informacji, na skutek obserwacji cech przedmiotów, procesów i zdarzeń oraz ewentualnych pomiarów wybranych stanów tych zjawisk powstaje pierwotne pole semantyczne wiadomości.

W systemach informacyjnych szczególną rolę pełnią sygnały bądź zbiory sygnałów nadanych (wysłane, przekazane), czyli sygnały wprowadzone przez konkretnego nadawcę do kanału informacyjnego oraz sygnały bądź zbiory sygnałów odebrane przez konkretnego odbiorcę, a więc takie, które dotarły do konkretnego odbiorcy. W systemach informacyjnych, których funkcją jest zaspokajanie potrzeb informacyjnych użytkowników informacji, trzeba uwzględniać, że mogą pojawić się w nich wiadomości zawierające informacje zbędne, że może wystąpić dublowanie informacji i to wielokrotne, że mogą występować luki informacyjne, brak informacji.

Dobry system informacyjny powinien być wyposażony w efektywne metody i narzędzia identyfikacji redundancji luk informacyjnych, niepełnej relewancji procesów wyszukiwania informacji. Te metody i narzędzia powinny umożliwić kontrolę i

[62] J. Kozioł. *Podejmowanie decyzji w warunkach ryzyka*, w: Zeszyty Naukowe AON. *Współczesne Siły Powietrzne - Misje, Zadania, Tendencje Rozwoju,* Nr 2(47) Numer specjalny Warszawa 2002 s. 194

minimalizację rozbieżności między wiedzą użytkownika (decydenta, dowódcy), jego potrzebami informacyjnymi a dostarczaną mu informacją.

Ważne jest rozróżnienie między:

- informacją opisującą sytuację decyzyjną;
- informacją stanowiącą opis procedury decyzyjnej;
- informacją stanowiącą zasób relewantnej wiedzy decydenta I(W).

Wiedza I(R) to wiedza, którą powinien posiadać decydent definiujący swoją sytuację decyzyjną. Jest to informacja o systemie, w którego ramach jest podejmowana decyzja oraz o systemie, którego te decyzje dotyczą. Oba zbiory wiedzy I(R) i I(W) powinny być identyczne. Znaczy to, że decydent wie wszystko, co może być potrzebne do zdefiniowania sytuacji decyzyjnej. W praktyce często zbiór I(W) rzeczywistej wiedzy decydenta nie obejmuje wszystkich informacji należących do zbioru I(R), czyli wiedzy relewantnej, którą powinien posiadać decydent w celu podjęcia poprawnej decyzji.

Zwykle wiedza posiadana przez decydenta jest węższa od relewantnej wiedzy o systemach, do których odnosi się sytuacja decyzyjna. Zbiór informacji opisujący procedurę decyzyjną jest konstruowany na podstawie wiedzy decydenta I(W). Jeżeli wiedza ta zawiera informacje nierelewantne lub fałszywe, procedura decyzyjna może być błędna. Zdarza się też, że decydent posiada wiedzę I(W) obejmującą tylko część informacji I(R). Jest to więc wiedza niepełna[63].

Z taką właśnie sytuacją informacyjną spotykamy się często w systemach zarządzania i dowodzenia. Podejmowanie decyzji w tych systemach odbywa się w warunkach niepełnej informacji i ryzyka. Luki informacyjne, brak pełnej informacji w procesie podejmowania decyzji, powodują, że informację niepełną przyjmuje się jako wystarczającą albo uzupełnia się luki informacyjne informacjami nierelewantnymi, które decydent uznaje tylko za relewantne (np. informacje niesprawdzone, subiektywne szacunki dokonywane na wątpliwych podstawach lub zgoła nieprawdziwe). Jest to jedna z częstych przyczyn popełnienia błędów przy podejmowaniu decyzji.

---

[63] Zeszyty Naukowe AON. *Współczesne Siły Powietrzne - Misje, Zadania, Tendencje Rozwoju, Nr 2(47) Numer specjalny Warszawa* 2002

Kwantyfikację informacji można rozpatrywać w ujęciu:

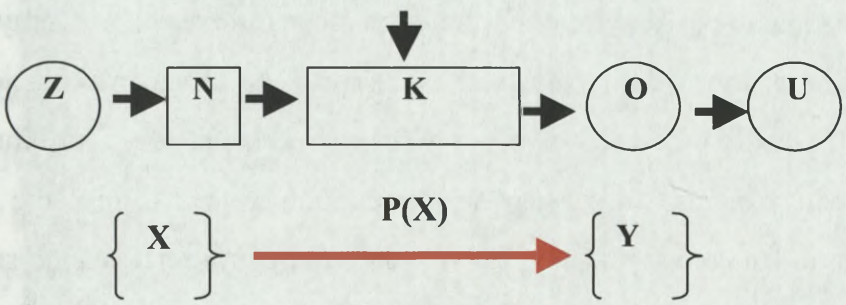
- probabilistycznym (*Shannon, Weaver*);
- nieprobabilistycznym (*Ingarden, Urbaniak*);
- związanym z treścią (*Carnap, Bar-Hillel*);
- związanym z wartością (*Szaniawski, Mazur, Charkiewicz, Roginski*).

W ujęciu wartościowym interesująca jest hipoteza A. Charkiewicza: *ilość informacji rośnie proporcjonalnie do kwadratu wartości potencjału gospodarczego* oraz wzór na wartość informacji:podejście A. Charkiewicza, który przytacza wzór:

$$V(1) = \log_2 \frac{P_1}{P_0}$$

gdzie: $V(1)$ - *wartość informacji;*
P_1 - *prawdopodobieństwo osiągnięcia zamierzonego celu bez uzyskania informacji;*
P_o - *prawdopodobieństwo osiągnięcia zamierzonego celu po uzyskaniu informacji*

Podejście A. Charkiewicza koresponduje z tzw. *shannonowską* teorią informacji, zakładającą, że *informowanie to zmiana stanu niepewności wobec rozpatrywanego zjawiska*, a więc noszącą charakter probabilistyczny. *Model informacji C.E. Shannona* ilustruje ***Diagram Nr 10.***



gdzie: ***Z*** - *źródło informacji;*
N - *nadawca;*
K - *operacja przekształcająca;*
O - *odbiorca;*
U - *użytkownik*
P(X) - *kanał informacyjny*

Diagram 10: ***Model informacji C.E. Shannona***

Źródło: P. Sienkiewicz. *Wykłady otwarte*. AON 2002

Model ten, stanowiący wyjście do dalszych badań nad wartością informacji i jej wpływem na przebieg działań na polu walki, omówiony jest w ***Rozdziale 2.3.3***. Celem weryfikacji trzeciej grup hipotez badawczych, autor rozprawy przeprowadził badania nad możliwością zastosowania modeli matematycznych w odniesieniu do czynnika informacyjnego w sieciocentrycznych działaniach bojowych w oparciu o ogólnodostępne dane źródłowe dotyczące sprzętu walki informacyjnej oraz o przebieg działań w operacji ***Iraqi Freedom***.

2.3.3. Kwantyfikacja informacji według teorii C. E. Shannona

W końcu ostatnich pięciu dekad XX wieku wystąpił olbrzymi wzrost znaczenia informacji, zwany rewolucją informacyjną, która ma miejsce w strukturze informacyjnej zwanej cyberprzestrzenią. Wzrastająca złożoność współczesnych operacji wojennych, często z udziałem sił międzynarodowych, rozproszonych na dużym obszarze oraz pożądana duża szybkość działań wymagają dokładnej koordynacji i synchronizacji pomiędzy poszczególnymi rodzajami sił i środków walki. Jest to możliwe poprzez zastosowanie odpowiedniego układu informacyjnego stanowiącego połączenie militarnych i cywilnych systemów informacyjnych narodowych, międzynarodowych i globalnych. Ten układ informacyjny działający w cyberprzestrzeni powinien zapewniać dowodzenie i kierowanie siłami zbrojnymi[64].

W *układzie informacyjnym*, tak źródła informacji, jak i układy odbierające mają strukturę złożoną.. Jeśli przyjmie się, że adresatem informacji jest umysł ludzki, to człowiek odbierający swoimi zmysłami docierające do niego informacje, czyni tym samym te zmysły zewnętrznym wyjściem układu. W strukturze układu informacyjnego źródłami informacji są układy odbierające informację z otoczenia. Zatem źródła informacji funkcjonujące w ***systemie informacyjnym*** nie są tożsame ze źródłami informacji w ***układzie informacyjnym***[65].

Oddziaływanie na proces informacyjny, poprzez źródła informacji i poprzez układy odbierające, powodować będzie zmiany ***entropii informacyjnej***. Wartość tej entropii będzie tym mniejsza, im mniejsza będzie deformacja źródeł informacji oraz

[64] Kwiatosz J. *Współczesne Poglądy Na Walkę Informacyjną*. Materiały VIII Konferencji Naukowej „*Automatyzacja Dowodzenia*", Jelenia Góra, 2000.
[65] Ciborowski L. *Walka informacyjna*, wyd. ECE, Toruń 1999

zewnętrznych i wewnętrznych wejść układów odbierających. W tym aspekcie bardzo ważną rolę funkcjonalną odgrywają nośniki komunikatów, których znaczenie zostało matematycznie odwzorowane w kolejnym podrozdziale niniejszej rozprawy.

Zależności te jednoznacznie zdefiniował C. E. Shannon w swojej formule o możliwie maksymalnej prędkości bezbłędnej komunikacji[66]. Podstawy ilościowej teorii informacji zawarł w książce *„Mathematical Theory of Communication"*, gdzie po raz pierwszy wprowadzono ilościową miarę informacji przenoszonej przez kanał i wprowadzono jej definicję, przez analogię do termodynamicznej ujemnej entropii - *negentropii* (*entropia - statystyczna miara nieuporządkowania*).

Przez p_{ji} oznaczamy prawdopodobieństwo wystąpienia sygnału y_j pod warunkiem istnienia sygnału y_i (tzn. prawdopodobieństwo warunkowe), czyli $p_{ji} = P\{y_j / y_i\}$. Z własności prawdopodobieństwa wiemy również, że $p_{ji} \geq 0$. Wtedy ilość informacji zawartej w *X (źródłowy układ informacyjny)*, gdy znamy *Y (odbiorczy układ informacyjny)* jest oznaczona przez *H(X/Y)* i jest równa:

$$H(X/Y) = -\sum_{i,j} p_{ji} \log_2 p_{ji}$$ *(stan entropii informacyjnej)*

Formuła C.E. Shannona jest następująca: $C = W \log_2(1 + \frac{U}{S})$

gdzie: *C - przepustowość kanału; U - moc sygnału;*
W - szerokość pasma; S - moc szumu
(podstawa logarytmu „2" świadczy o binarnej postaci informacji)

Układ, który ma choć jedno **wejście** informacyjne oraz jedno **wyjście** informacyjne, jest jednocześnie układem informującym i układem informowanym, tworząc w przypadku wielokrotnych wejść/wyjść - ***siatkę informacyjną***.

Przy pomiarze ilości informacji przekazanej w układzie, stosuje się wzór:

$$I(X) = H(X) - H\left(\frac{X}{Y_{H_{max}}}\right)$$ *(uwzględnienie wielkości entropii informacyjnej)*

Ilość informacji w systemie informacyjnym uzależniona jest od źródeł informacji rozmieszczonych na siatce informacyjnej. W kolejnym podrozdziale

[66] *Ibidem*

zawarto obliczenia taksonomiczne obrazujące strukturalne i ilościowe cechy *siatki sensorów*, oparte na sprzętowych źródłach informacji pola walki.

2.3.4. Taksonomia informacyjna w oparciu o sieciocentryczną architekturę systemów informacyjnych pola walki

Przy pomiarach efektywności analizujemy cechy złożonego obiektu, wyrażające racjonalne zdolności do zaspokojenia określonych potrzeb (osiągania zamierzonych celów działania, funkcjonowania zgodnie z przeznaczeniem i wymaganiami). W przypadku ***siatki sensorów*** można dokonać pomiaru nasycenia sprzętem zdolnym do gromadzenia i przesyłania szeroko rozumianej informacji pola walki w odniesieniu do poszczególnych podmiotów (państw dysponujących danym sprzętem). Pomiary takie oparte być muszą o wyspecyfikowane kryteria:

- ***kryteria operacyjne*** związane z nasyceniem sprzętowym, czyli zdolnością do osiągania zamierzonych celów;
- ***kryteria techniczne*** związane z rodzajami sprzętu wchodzącego w skład systemu (siatki sensorów), wyrażające wpływ techniki na powodzenie operacji;
- ***kryteria porównawcze*** pozwalające na określenie proporcji danych kwantytatywnych w stosunku do wielkości podmiotu pomiaru (państwa).

Wartościowanie polega na dokonaniu:

- pomiaru, czyli ilościowego wyrażenia wartości cechy uznanej za kryterialną w przyjętych jednostkach miary (fizycznych, ilościowych, wartościowych) - obejmuje tzw. **cechy mierzalne;**
- ocen, czyli wypowiedzi wartościujących, wyrażających aprobatę lub dezaprobatę stanu analizowanego obiektu, który to stan wyrażono ilościowo dzięki procedurom pomiaru efektywności - obejmuje tzw. **cechy niemierzalne**.

Do metod pozwalających na analizy wartościujące zaliczamy ***metody taksonomiczne***, które dzięki stosowaniu odpowiednich miar i wskaźników umożliwiają porównanie obiektów (systemów) opisanych przez wiele cech mierzalnych i niemierzalnych.

Stosowanie metod taksonomicznych w znacznym stopniu obiektywizuje oceny, a tym samym proces porównywania rozważanych obiektów (systemów).

Każdy obiekt utożsamiamy z wektorem $\mathbf{z_i} = [z_{i,j}]$, którego składowe $\mathbf{z_{i,j}}$ ($j=1,2,...,k$) obrazują wartości uwzględnione w badaniu cech diagnostycznych opisujących obiekty: *i-ta* wartość *j-tej* cechy. Tak więc rozważane obiekty identyfikowane są z wektorami z *k-wymiarowej* przestrzeni $\mathbf{R^k}$, przy czym wartości stosowanych miar taksonomicznych wyznaczamy w oparciu o wystandaryzowane wartości cech dla cech z poszczególnych grup (kryteriów) oraz dla pełnego zestawu cech.

W celu umożliwienia porównań w zbiorze obiektów oraz konstrukcji list klasyfikacyjnych (rankingów) tych obiektów w oparciu o wartości miar taksonomicznych wprowadza się konstrukcję abstrakcyjną tzw. ***obiekt wzorcowy***, z którym porównuje się wszystkie obiekty rozważanego zbioru.

Obiekt wzorcowy jest opisany wektorem $\mathbf{Z_o} = [\mathbf{Z_{o,j}}]$, którego składowe $\mathbf{Z_{o,j}}$ określa się następująco:

$$\mathbf{Z_{o,j}} = \begin{cases} \max\limits_i \mathbf{z}_{i,j} & - \textit{ dla stymulantów} \\ \min\limits_i \mathbf{z}_{i,j} & - \textit{ dla destymulantów} \end{cases}$$

Miarami taksonomicznymi wykorzystywanymi w procesie konstrukcji rankingów rozważanych obiektów są:

μ - miara podobieństwa obiektów ,

d - miara dystansu między obiektami

Miara podobieństwa obrazuje „*strukturalne*" podobieństwo każdego z obiektów (wektorów $\mathbf{z_i}$) do wzorca $\mathbf{Z_o}$ (pokazuje poprawność wzajemnych proporcji poszczególnych danych w stosunku do obiektu-wzorca), czyli stopień „*przylegania*" jako ***wartość kwalitatywną***, natomiast miara dystansu obrazuje uśredniony wektorowo stopień „*zbliżenia*" danych do parametrów obiektu wzorcowego jako ***wartość kwantytatywną***.

miara **podobieństwa** - $$\mu_{i,o} = \frac{\sum_{j=1}^{k} z_i \mathbf{Z}_o}{\sum_{j=1}^{k} |z_i| \, |\mathbf{Z}_o|} \quad (1)$$

(podobieństwo struktur w badanych obiektach mierzone jest miarą, będącą cosinusem kąta zawartego między wektorami obrazującymi rozważane obiekty[67])

miara **dystansu** - $$\mathbf{d}_{i,o} = \sqrt{\sum_{j=1}^{k} \left(z_{i,j} - Z_{o,j}\right)^2} \quad (2)$$

(dystans między obiektami wyznacza się wykorzystując tzw. metrykę euklidesową, tzn. zróżnicowanie poziomów cech w rozważanych obiektach[68])

W przypadku **cech niemierzalnych**, wynikających np. z *analizy porównawczej* lub opisów charakterystycznych cech systemów (obiektów), dokonuje się rankingu bezpośredniego[69].

Z wykorzystaniem danych z rankingów cech mierzalnych i cech niemierzalnych z uwzględnieniem danych opisowych przedstawiających charakterystyczne cechy obiektu dokonuje się syntezy danych, uzyskując wykaz i opis parametrów mających najkorzystniejszy wpływ na jakość obiektu badań. Wnioski wyciągnięte z przeprowadzonej analizy i syntezy mogą służyć dalszym procesom ewaluacyjnym oraz przyczynić się do bardziej efektywnego planowania sił i środków walki.

W ***Tabelach 4 - 5*** oraz na ***Wykresach 3 - 4*** autor rozprawy przedstawia wynik taksonomicznych obliczeń nasycenia sprzętem walki informacyjnej wybranych państw NATO w oparciu o źródła jawne (*The Military Balance 2002-2003, Jane's C4I Systems 2001-2002, C3I Forecast International, SIPRI Yearbook 2002, Rocznik Strategiczny 2002-2003)* i dokonuje analizy uzyskanych wyników. Źródłowa tabela sprzętu walki informacyjnej, będącego w dyspozycji poszczególnych państw zawarta jest w ***Załączniku Nr 1***. Sprzęt został podzielony na kategorie zastosowań, po czym dokonano zsumowania ilościowego wg państw – członków NATO (nie uwzględniono

[67] T. Michalski. *Polska w drodze do Unii Europejskiej.* Diffin. Warszawa 2000 s. 78
[68] *Ibidem* s. 86
[69] *Ibidem*

niektórych państw ze względu na brak danych, zamieszczono osobne, ogólnodostępne dane za siły wydzielane do NATO).

Ujęte w tabeli pozycje obejmują jedynie dane opublikowane w ww. źródłach, wynik obliczeń nie odzwierciedla zatem pełnego zakresu przedmiotowego (niektóre państwa obejmują klauzulą tajności informacje dotyczące sprzętu walki informacyjnej w poszczególnych kategoriach), pozwalają jednak na wyciągnięcie wniosków ogólnych.

Miary podobieństw i miary dystansów zostały obliczone z wykorzystaniem arkusza EXCEL – przy tabelach podano przekształcenia wzorów taksonometrycznych. Jako współczynniki nasycenia poszczególnych państw sprzętem walki informacyjnej przyjęto zlogarytmizowane (ze względu na potrzebę czytelnego zobrazowania wyniku przyjęto logarytm dziesiętny zwiększony o liczbę 3 celem uniknięcia wartości ujemnych) wskaźniki ilości sprzętu walki informacyjnej *per capita*. W ***Tabeli na s. 36*** zamieszczono dane źródłowe przeliczone na współczynniki zgodnie z ***Zał. Nr 1.***

Obliczenia miar podobieństw przedstawiono w ***Tabeli-Wykresie Nr 3***. Miary dystansów zostały odzwierciedlone w ***Tabeli-Wykresie Nr 4***. Celem dokonania czytelnych porównań wybrano tzw. radarowe typy wykresów.

Nazwa	Ilość	Kraj	Ludność w mln	Nasycenie sprzętem na 1 mln mieszk.	Moduł logarytm
Systemy WOiN	**92**	Francja	58	1,586206897	3,200359834
	68	Hiszpania	39	1,743589744	3,241444306
	454	USA	285	1,592982456	3,202210993
	28	Wlk. Bryt.	58	0,482758621	2,683730038
	9	Włochy	57,1	0,157618214	2,197606401
Systemy Dow. i Kier.	**1600**	Francja	58	27,5862069	4,440691989
	2	Hiszpania	39	0,051282051	1,709965389
	227	Niemcy	82	2,768292683	3,442212005
	10	Turcja	60	0,166666667	2,22184875
	2750	USA	285	9,649122807	3,984487834
	600	Włochy	57,1	10,50788091	4,021515142
Specj. systemy łączn.	**1000**	Francja	58	17,24137931	4,236572006
	750	Hiszpania	39	19,23076923	4,283996656
	453	Holandia	15,5	29,22580645	4,465766504
	2718	Niemcy	82	33,14634146	4,5204356
	2840	Turcja	60	47,33333333	4,67516709
	10666	USA	285	37,4245614	4,573156719
Systemy WRE	**2**	NATO	59	0,033898305	1,530177984
	338	USA	285	1,185964912	3,07407184
	331	Wlk.Bryt.	58	5,706896552	3,7564
Systemy WI Morskie	**24**	Holandia	15,5	1,548387097	3,189879544
	12	Kanada	31	0,387096774	2,587819552
	2	Niemcy	82	0,024390244	1,387216143
	153	USA	285	0,536842105	2,729846571
	85	Wlk.Bryt.	58	1,465517241	3,165990932
	14	Włochy	57,1	0,245183888	2,389491927
Systemy identyf.	**1**	Grecja	10,3	0,097087379	1,987162775
	4	Holandia	15,5	0,258064516	2,411728293
	7	Kanada	31	0,225806452	2,353736346
	4	Niemcy	82	0,048780488	1,688246139
	2	Portugalia	9,8	0,204081633	2,30980392
	18	Turcja	60	0,3	2,477121255
	624	USA	285	2,189473684	3,34033973
Specj. systemy rozp.	**8**	Francja	58	0,137931034	2,139661993
	1700	NATO	59	28,81355932	4,45959691
	4	Niemcy	82	0,048780488	1,688246139
	4257	USA	285	14,93684211	4,17425879
	128	Wlk.Bryt.	58	2,206896552	3,343781976
	5	Włochy	57,1	0,087565674	1,942333896
Satelitarne Syst. WI	**22**	Francja	58	0,379310345	2,578994687
	2	NATO	59	0,033898305	1,530177984
	53	USA	285	0,185964912	2,26943101
	13	Wlk.Bryt.	58	0,224137931	2,350515359
	6	Włochy	57,1	0,105078809	2,021515142

(celem przybliżonego porównania zasobów NATO – uśredniono wskaźnik liczmy ludności)

Tabela 4: ***Nasycenie sprzętem walki informacyjnej w wybranych państwach NATO***

Po obliczeniu na podstawie danych źródłowych z ***Tab. Nr 4*** modułów logarytmicznych nasycenia sprzętem walki informacyjnej i przeniesieniu ich wg poszczególnych państw i wg kategorii sprzętu do ***Tab. Nr 5*** - dokonano obliczenia składowych wektora państwa wzorca. Składowe wektorów $z_{i,j}$ poszczególnych państw oraz składowe wektora $Z_{o,j}$ posłużyły do obliczenia i zobrazowania miar podobieństw $\mu_{i,o}$ i miar dystansów $d_{i,o}$ na ***Wykresach Nr 3 i Nr 4***.

Kraj	Satelitarne syst. WI	Specj. systemy łączn.	Specj. systemy rozp.	Systemy dow. i kier.	Systemy identyf.	Systemy WI morskie	Systemy WOiN	Systemy WRE
Francja	2,578994687	4,236572006	2,139662	4,440692			3,20036	
Grecja					1,987163			
Hiszpania		4,283996656		1,709965			3,241444	
Holandia		4,465766504			2,411728	3,18988		
Kanada					2,353736	2,58782		
NATO	1,530177984		4,459597					1,530178
Niemcy		4,5204356	1,688246	3,442212	1,688246	1,387216		
Portugalia					2,309804			
Turcja		4,67516709		2,221849	2,477121			
USA	2,26943101	4,573156719	4,174259	3,984488	3,34034	2,729847	3,202211	3,074072
Wlk.Bryt.	2,350515359		3,343782			3,165991	2,68373	3,7564
Włochy	2,021515142		1,942334	4,021515		2,389492	2,197606	

(pola niewypełnione oznaczają brak ogólnie dostępnych danych)

Państwo wzorzec	**2,578994687**	**4,67516709**	**4,459597**	**4,440692**	**3,34034**	**3,18988**	**3,241444**	**3,7564**

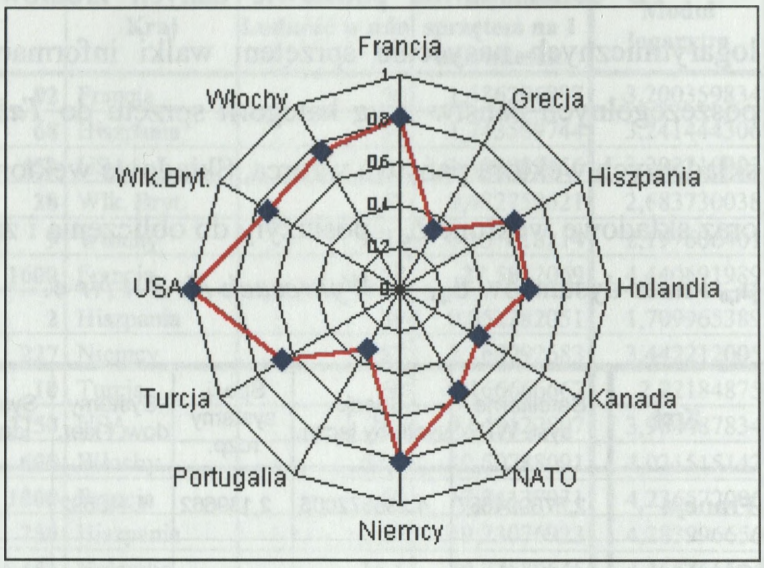
składowe wektora państwa-wzorca: $$Z_{o,j} = \begin{cases} \max\limits_{i} z_{i,j} & - \text{ dla stymulantów} \\ \min\limits_{i} z_{i,j} & - \text{ dla destymulantów} \end{cases}$$

(w przedstawionych cechach obiektów nie występują destymulanty)

Tabela 5: ***Obliczenie wskaźników taksonomicznych obiektu-wzorca***

Źródło tabel: opracowanie własne

	$\mu_{i,o}$
Francja	0,804707863
Grecja	0,312759786
Hiszpania	0,633245282
Holandia	0,610864676
Kanada	0,431391961
NATO	0,55878086
Niemcy	0,800549361
Portugalia	0,312759786
Turcja	0,652626768
USA	0,997918733
Wlk.Bryt.	0,727877193
Włochy	0,740159926
Państwo wzorzec	1



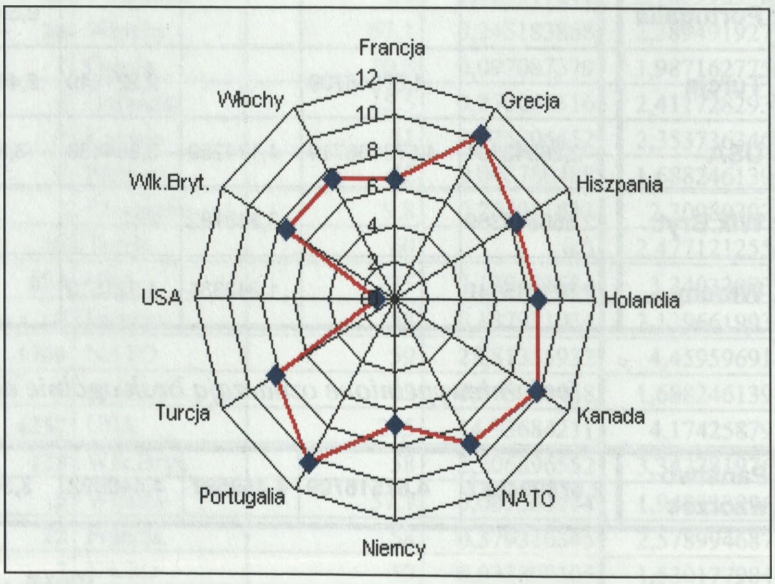
wzór (1) dostosowany do obliczeń w arkuszu EXCEL:

$$\mu_{i,o} = \frac{\sum_{j=1}^{k} z_{i,j} z_{o,j}}{\sqrt{\sum_{j=1}^{k} z_{i,j}^{\,2}} \sqrt{\sum_{j=1}^{k} z_{o,j}^{\,2}}}$$

Wykres 3: ***Miary podobieństw nasycenia sprzętem walki informacyjnej***

Źródło tabel-wykresów: opracowanie własne

	$d_{i,o}$
Francja	6,404677476
Grecja	10,23425974
Hiszpania	8,34223245
Holandia	8,472463248
Kanada	9,698944039
NATO	8,914772897
Niemcy	6,778570168
Portugalia	10,19661653
Turcja	8,185381072
USA	1,036589199
Wlk.Bryt.	7,371815503
Włochy	7,461830971
Państwo wzorzec	0



wzór (2) do obliczeń w arkuszu EXCEL:

$$d_{i,o} = \sqrt{\sum_{j=1}^{k} \left(z_{i,j} - Z_{o,j}\right)^2}$$

Wykres 4: ***Miary dystansów nasycenia sprzętem walki informacyjnej***

Na podstawie wyników obliczeń taksonomicznych, nawet przy ograniczonej ilości danych, można jednoznacznie dostrzec sprzętową przewagę informacyjną USA, Francji, Niemiec i Wielkiej Brytanii nad pozostałymi państwami członkowskimi NATO, zarówno pod względem struktury asortymentowej sprzętu (wysokie miary podobieństw do naliczonego wzorca), jak i ilościowej (niskie miary dystansów). Wynik obliczeń zbieżny jest ze wskaźnikami potęg państw członków NATO liczonych *metodą Sułka* wg wskaźników wydatków wojskowych, przedstawionymi w ***Tabeli Nr 3*** i na ***Wykresie Nr 2*** - *s. 54*. Można zaobserwować wręcz pełną zbieżność wyników badań taksonomicznych z uśrednionymi wskaźnikami potęg państw NATO (wg dochodu narodowego i wydatków wojskowych), pomimo zastosowania zróżnicowanych modeli matematycznych.

Wyniki obliczeń pokazują również (niezależnie od obarczenia błędem wynikającym z niekompletności danych i z uśrednień) względną słabość miar strukturalno-ilościowych sprzętu wydzielonego do sił NATO, co potwierdza konieczność włączania sił narodowych do operacji sojuszu na dużą skalę.

2.3.5. Miary efektywności informacyjnej pola walki

Szeroko pojęty czynnik informacyjny pola walki we współczesnych działaniach bojowych stał się czwartym rodzajem sił zbrojnych. Mimo, iż jest oczywiste, że informacja będzie miała daleko idący wpływ na przebieg operacji, to jednak kwantyfikowanie, czy też pomiar tego wpływu – sposób realizacji – jest daleki od zadowalającego. Rozwiązanie tego zagadnienia jest ważne dla sił zbrojnych, szczególnie w czasie, gdy przeznaczają one znaczną część swojego kapitału inwestycyjnego na rozwijanie sił i środków wieku informacyjnego, w tym na środki łączności i informatyki, systemy dowodzenia i kierowania ogniem, sieciocentryczne systemy zarządzania informacją, a także na kosztowne elementy zapewniania bezpieczeństwa informacyjnego. Ze względu na trwające procesy transformacji w siłach zbrojnych występuje potrzeba stosowania narzędzi analitycznych zapewniających wsparcie w procesie dokonywania najlepszych możliwych wyborów.

Pośród stosowanych narzędzi analitycznych, główną pozycję stanowią miary efektywności, które są w stanie wykazać wartość informacji w ujęciu militarnym. Tradycyjnie stosowane zestawy miar, np. zmiany zasobów ludzkich i ich koncentracja

w terenie oraz straty, niezbędne nadal do kwantyfikacji - nie są w stanie odzwierciedlić rosnącego udziału informacji. Ponadto, wielkości uzyskiwane za pomocą tych miar są często wyliczane w oparciu o indywidualne uproszczone modele myślowe, pomijające ważne procesy, w których informacja odgrywa dużą rolę.

Jedną z implikacji przyszłej przewagi informacyjnej jest nowy zestaw koncepcji dla wszystkich rodzajów sił. Koncepcje te, zawarte w dokumencie *Joint Vision 2010* – manewr dominujący, precyzyjny kontakt bojowy, obrona pełnowymiarowa i zogniskowana logistyka – są widziane jako pewne *„transformacje"* (przejścia) bardziej tradycyjnych funkcji (manewr, uderzenie, obrona i logistyka) *„nadające taką moc, że funkcje te w rzeczywistości stają się nowymi koncepcjami"*[70].

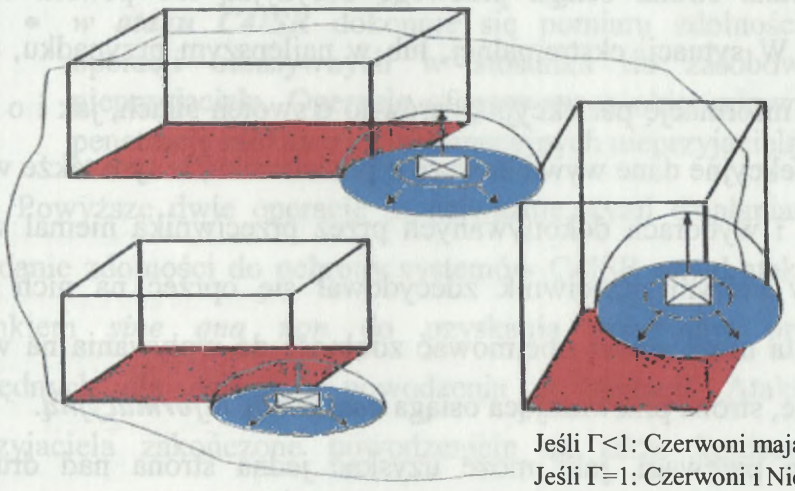
- ***przejście od manewru do manewru dominującego*** - wielkość przestrzeni bojowej oraz terytorium, jakie dowolna jednostka o danej wielkości będzie zdolna kontrolować, wraz z poprawą strategicznego i operacyjnego rozmieszczenia sił;
- ***przejście od uderzenia do precyzyjnego kontaktu bojowego*** - zdolność dowolnej jednostki do precyzyjnego wykorzystania swoich sił i środków;
- ***przejście od obrony do obrony pełnowymiarowej*** - pewne kluczowe wymaganie dla wszystkich operacji wojskowych spowodowane globalnymi trendami w kierunku dokładniejszego i skuteczniejszego manewru;
- ***przejście od logistyki do logistyki zogniskowane*** - zdolność do logistycznego wsparcia sił przeprowadzających operacje z wykorzystaniem systemów informacyjnych zapewniających zdecydowaną poprawę skuteczności logistycznej.

Koncepcje te zależą od informacji, będącej czynnikiem usprawniania dowodzenia, kierowania i wywiadu. Nowe technologie z natury wykorzystują przewagę informacyjną i powodują, że wynikiem takich transformacji jest przewartościowanie (*rewaloryzacja*) roli walki informacyjnej **(*Diagram Nr 5*).**

Pomimo, iż koncepcje te odzwierciedlają także dotychczasowy charakter operacji bojowych, opracowanie *Joint Vision 2010* utrzymuje, że w wieku informacji stanie się on przetransformowany z wykorzystaniem nowych koncepcji, które charakteryzują informację jako *wiedzę*. Wiedza różni się od informacji tym, że uwzględnia dwa kluczowe atrybuty informacji: *jakość* i *wartość*. Informacja pola

[70] RAND

walki posiada wartość wtedy, gdy dociera w odpowiedniej formie i treści do właściwego adresata-dowódcy i przez to przekazuje mu wiedzę o sytuacji bojowej. W rezultacie, kiedy odwołujemy się do *wiedzy*, rzeczywiście mamy na myśli odpowiednią i dlatego *wartościową* informację. Jakość informacji zależy od jej dokładności, terminowości i kompletności. Nie zawsze informacja lub wiedza wartościowa jest najwyższej jakości. Odwrotnie, informacja jakościowa może mieć niską lub żadną wartość tj. może to być uboczna informacja o niewielkiej użyteczności, a więc może nawet zmniejszyć wiedzę.



Γ - wiedza względna: stosunek wiedzy Niebieskich do wiedzy Czerwonych.

$$\Gamma = \frac{K_B}{K_R}$$

K_B,K_R – wiedza uzyskana;
Γ - wiedza relatywna

Jeśli Γ<1: Czerwoni mają przewagę informacyjną
Jeśli Γ=1: Czerwoni i Niebiescy mają jednakowe możliwości
Jeśli Γ>1: Niebiescy mają przewagę informacyjną.

D= Mobilność x Γ ➡ Wiedza jest zwielokrotnieniem siły

Diagram 11: ***Efekt wiedzy***

Źródło: *RAND Corporation. 1700, Main Street, Santa Monica CA USA* - Instytut zajmujący się od 1948 r. studiami strategicznymi i inżynierią systemów

Zbierając informację ze znaczników (*sensorów*) i źródeł osobowych, dowódca poszukuje informacji wartościowej, zawierającej elementy krytyczne, tworzące wiedzę. Wiedza jest to stopień posiadanej przez dowódcę znajomości dyspozycji sił własnych i nieprzyjaciela wewnątrz promienia kontroli, tzn. *stopień posiadanej świadomości sytuacyjnej*[71]. Problemem jest trudność w ocenie jakości otrzymanej informacji. Nasuwa to potrzebę ***taksonomicznej oceny informacji***[72] (przykład

[71] *RAND Corporation. 1700, Main Street, Santa Monica CA USA* - Instytut zajmujący się od 1948 r. studiami strategicznymi i inżynierią systemów
[72] *Ibidem*

wykorzystania rachunku taksonomicznego w porównaniu potencjału źródeł informacji zawarto w ***Rozdziale Nr 2.3.4*).**

Informacja jest *krytyczną zmienną* przy określaniu charakteru sił zbrojnych *wieku informacyjnego*. Większość mierzalnych potrzeb w zakresie efektywności sił zbrojnych może być potencjalnie wyrażona przez stopień przewagi informacyjnej, jaki może być zdolna osiągnąć jedna strona nad drugą.

Przewaga informacyjna może być, z punktu widzenia analizy, traktowana jako wynik dwustronnych oddziaływań między przeciwnikami (tzn. jako pewna gra lub walka), w którym jedna strona osiąga przewagę decyzyjną lub pewien stopień dominacji nad drugą. W sytuacji ekstremalnej, lub w najlepszym przypadku, strona przeważająca posiada informację perfekcyjną zarówno o swoich siłach, jak i o siłach przeciwnika, oraz perfekcyjne dane wywiadowcze o przeciwniku, w tym także wiedzę o planach, intencjach i wyborach dokonywanych przez przeciwnika niemal w tym samym momencie, w którym przeciwnik zdecydował się oprzeć na nich swoje działania; informacja ta może nawet obejmować zdolność do wpływania na wiedzę przeciwnika. W skrócie, strona przeważająca osiąga ***dominację informacyjną***.

Wysoki stopień przewagi, jaki może uzyskać jedna strona nad drugą w działaniach bojowych wieku informacyjnego, jest tym czynnikiem, który powoduje, że zmienna ta staje się krytyczna. Jeśli jednak żadna ze stron nie może osiągnąć dominacji informacyjnej nad drugą – ani nawet znaczącego stopnia przewagi informacyjnej – technologie wdrażane w dobie walki informacyjnej nie muszą być w takim stopniu decydujące dla którejkolwiek ze stron. Pośród miar efektywności informacyjnej najważniejszymi są więc te, które mierzą sposób, w jaki można osiągnąć i utrzymać *przewagę informacyjną* oraz, jeśli to jest możliwe, *dominację informacyjną*.

Jak scharakteryzowano to w ***Rozdziale 2.3.1*** - w zależności od charakteru, operacje informacyjne dzielą się na *defensywne* i *ofensywne*. Działania defensywne powinny umożliwić wykorzystanie własnych systemów informacyjnych poprzez zapewnienie wysokiej efektywności i bezpieczeństwa informacji oraz przeciwdziałanie sabotażowi, propagandzie, wywiadowi i walce elektronicznej

przeciwnika. Operacje ofensywne powinny uniemożliwić wykorzystanie przez przeciwnika jego systemów informacyjnych.

Przekładając powyższe na systemy *C4ISR* (*Command, Control, Communication, Coordination, Intelligence, Sourveillance and Reconnaissance - Systemy Dowodzenia, Kierowania, Łączności, Koordynacji, Wywiad i Rozpoznanie)* można określić pomiar efektywności informacyjnej jak niżej:

- ***w obronie C4ISR*** mierzy się stopień, w jakim siły zbrojne w operacjach sieciocentrycznych są zdolne do przeprowadzenia operacji defensywnych, które pomogą zachować lub zapewnić *przewagę informacyjną*;
- ***w ataku C4ISR*** dokonuje się pomiaru zdolności do przeprowadzenia operacji ofensywnych w stosunku do zasobów i procedur C4ISR nieprzyjaciela. Operacje ofensywne są ukierunkowane na degradację lub penetrację możliwości informacyjnych nieprzyjaciela.

Powyższe dwie operacje są najważniejszymi działaniami miar efektywności. Posiadanie zdolności do ochrony systemów C4ISR przed atakami nieprzyjaciela jest warunkiem *sine qua non* do uzyskania poziomów przewagi informacyjnej niezbędnych dla osiągania powodzenia w operacji. Ataki na systemy C4ISR nieprzyjaciela zakończone powodzeniem są także konieczne dla wspomagania przełożenia tej *przewagi informacyjnej* na *dominację informacyjną*.

W opracowaniu *Joint Vision 2010* przewaga informacyjnej definiowana jest jako *„zdolność do zbierania, przetwarzania i rozprowadzania dowolnego nieprzerwanego strumienia informacji przy wykorzystaniu lub dementowaniu zdolności przeciwnika do wykonywania tego samego"*[73].

W odróżnieniu od przewagi informacyjnej, termin *dominacja informacyjna* jest mniej jasny. Zamiast stwierdzić, że operacje informacyjne są przeprowadzane w celu uzyskania dominacji informacyjnej, opracowanie *Joint Vision 2010* stwierdza: *„operacje informacyjne obejmują zarówno wysiłki ofensywne, jak i defensywne, których celem jest* ***stworzenie różnicy między tym, co my wiemy o naszej przestrzeni bojowej i operacjach w niej prowadzonych, a tym, co nieprzyjaciel wie o swojej przestrzeni bojowej"***[74] (podkreślenie autora).

[73] *Ibidem*
[74] *Ibidem*

Z powyższymi definicjami koresponduje celne w swej lakoniczności sprowadzenie powyższych pojęć do:

- przewaga informacyjna: „*wiem więcej, ale przeciwnik o tym nie wie*";
- dominacja informacyjna: „*wiem więcej, a przeciwnik o tym wie*"[75].

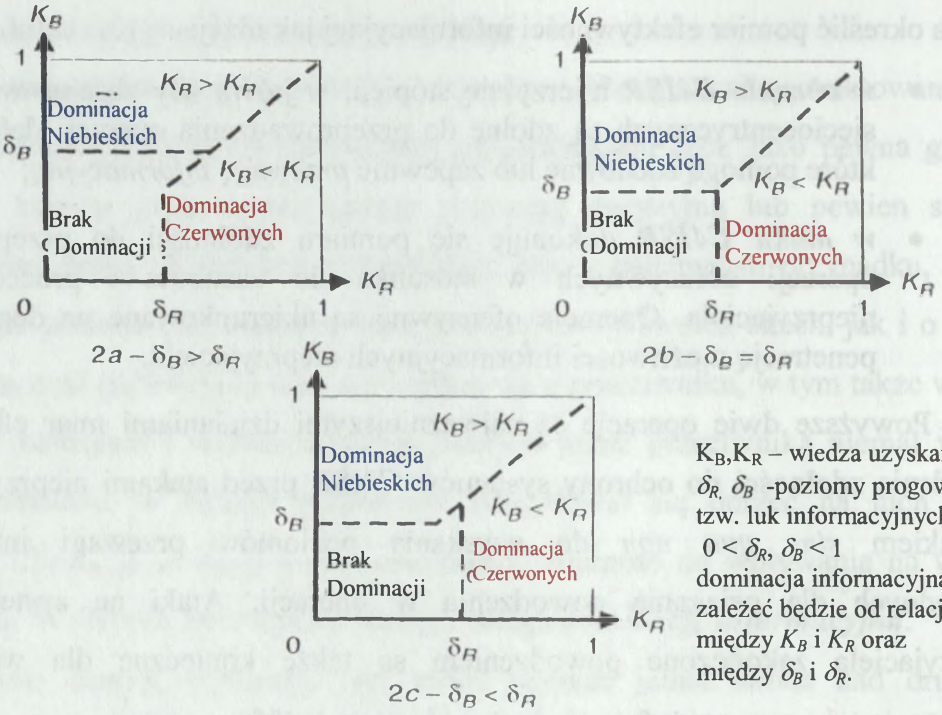


Diagram 12: ***Zobrazowanie przewagi/dominacji informacyjnej***

Źródło: *RAND Corporation. 1700, Main Street, Santa Monica CA USA* - Instytut zajmujący się od 1948 r. studiami strategicznymi i inżynierią systemów

Pomiar efektywności sił w walce pozostanie centralnym zadaniem dla sił zbrojnych *wieku informacyjnego*. Jedynie w najbardziej skrajnym przypadku – np. totalna dominacja informacyjna nad nieprzyjacielem, który całkowicie rezygnuje z walki – prawdopodobne jest, że walka informacyjna zapobiegnie potrzebie walki zbrojnej. Bardziej prawdopodobne wydaje się, że przyszłość będzie charakteryzowała się sporami, których kwestią będzie przewaga informacyjna, przy czym obie strony konkurować będą o nią w sposób dynamiczny (np. za pomocą środków podejmowanych jako inicjatywy i kontr-środków podejmowanych w odpowiedzi na te inicjatywy). Wyniki takiej walki zawierać będą pewną silną pozytywną zależność jako wkład, który wniosą nowe technologie, łącznie – choć nie tylko, z technologiami

[75] P. Sienkiewicz. *Przewaga informacyjna*, - wykład otwarty w AON 9.10. 2002 r.

informacyjnymi. Stąd nowe miary efektywności są pożądanym wyznacznikiem wkładu nowych technologii do walki.

Procesy walki według F. W. Lanchestera są prawdopodobnie najlepiej znanymi modelami matematycznymi. Zostały one opracowane tuż przed włączeniem się Stanów Zjednoczonych do I Wojny Światowej (nb. włączenie USA do wojny nastąpiło w wyniku przechwycenia, dekryptażu i opublikowania istotnych tajnych informacji strony niemieckiej – jest to przykład *skutków niskiego stopnia bezpieczeństwa informacji*) i najpierw były opublikowane w jego słynnej książce *Aircraft in Warfare: The Dawn of the Fourth Arm - Samoloty w Walce: Początki Czwartej Broni*[76].

Lanchester wyróżnia dwie formy walki: *tradycyjną* i *nowoczesną*. Ta pierwsza forma została przez niego scharakteryzowana za pomocą sformułowanego przez niego prawa liniowego, a druga forma – za pomocą jego prawa kwadratowego. W ***Rozdziale 2.3.6*** przedstawiono obie te formy, a także zaprezentowano trzeci wariant, przedstawiający obraz statyczny pola walki w określonym czasie z uwzględnieniem asymetrii informacyjnej, który określa się mianem *mieszanego prawa Lanchestera*. To trzecie prawo jest pewną próbą oceny implikacji przewagi informacyjnej. Efektywność jednostek, zdolność wojsk do przetrwania oraz wielkość wojsk i ich struktura mogą ulegać zmianom w wyniku pozyskania informacji lepszej jakościowo. *Prawa Lanchestera* zapewniają przydatny zestaw modeli do badania tych zmian.

W wyniku rozważań nad matematycznym modelowaniem walki powstała tablica wszystkich *praw Lanchestera* (***Tabela Nr 6***), która obejmuje pewną liczbę różnych przypadków mieszanych. Następnie, rozdział ten prezentuje wzory symulacji oparte na zmianach głównych parametrów. Wzory te wskazują stany przejściowe od prawa liniowego do mieszanego oraz od prawa kwadratowego do mieszanego.

[76] F. W. Lanchester. *Aircraft in Warfare: The Dawn of the Fourth Arm*

Warunek powodzenia	Rodzaj prawa	Interpretacja
$\frac{M}{N} > \left(\frac{R}{B}\right)^2$	Kwadratowe	Obie strony polegają wyłącznie na zbiorze swoich zasobów organicznych. Żadna informacja nie jest dostępna z dowództw wyższego szczebla.
$\frac{Mg}{N} > \left(\frac{R}{B}\right)^2$	Kwadratowe	W tych dwóch przypadkach, jedna strona ma jedynie zbiór swoich zasobów organicznych, a druga otrzymuje pewną informację z dowództwa wyższego szczebla ($0 < g < R$ i $0 < h < B$).
$\frac{M}{Nh} > \left(\frac{R}{B}\right)^2$	Kwadratowe	
$\frac{M}{N} > \frac{R}{B}$	Liniowe	Obie strony posiadają pełną informację z dowództw wyższego szczebla oraz informację zebraną ze swoich organicznych zasobów. Jest to najlepszy przypadek tego, co każda ze stron może zrobić w odniesieniu do informacji.
$\frac{dB}{dt} = -\alpha R - gB + B_\alpha$ $\frac{dR}{dt} = -\beta B - hR + R_\beta$ $\frac{Mg}{N} > \frac{R^2}{B}$	Mieszane	W tych dwóch przypadkach jedna ze stron posiada pełną wiedzę o siłach swojego przeciwnika, podczas gdy druga strona posiada jedynie pewną wiedzę o sile swojego przeciwnika ($0 < g < R$ i $0 < h < B$). Obie strony posiadają informację dostępną ze swoich własnych organicznych zasobów.
$\frac{dB}{dt} = -\alpha R - gB + B_\alpha$ $\frac{dR}{dt} = -\beta B - hR + R_\beta$ $\frac{M}{Nh} > \frac{R}{B^2}$	Mieszane	
$\frac{M}{N} > \frac{R^2}{B}$	Mieszane	Te dwa ostatnie przypadki ilustrują ekstremalny brak dostosowania. Jedna strona otrzymuje informacje z dowództwa wyższego szczebla dotyczącą pełnych sił nieprzyjaciela, podczas gdy druga strona posiada jedynie informację dostępną ze swoich własnych organicznych zasobów.
$\frac{M}{N} > \frac{R}{B^2}$	Mieszane	

Tabela 6: ***Prawa Informacji Lanchestera***

Źródło: *RAND Corporation. 1700, Main Street, Santa Monica CA USA* - Instytut zajmujący się od 1948 r. studiami strategicznymi i inżynierią systemów.

Obliczenia matematyczne wykazują, że jeśli zmienia się stosunek wiedzy względnej, tzn. to, co jedna strona wie w stosunku do tego, co wie strona druga, wyniki przechylają się na rzecz strony, która posiada *większą wiedzę względną*. Zostało to matematycznie wykazane w ***Rozdziale 2.3.6*** w oparciu o operację *Iraqi Freedom*, gdzie pokazano algorytm wykorzystania *równań Lanchestera* do zilustrowania wpływu asymetrii informacyjnej na osiągnięcie korzyści w walce przez stronę posiadającą przewagę informacyjną.

Zastosowanie *praw Lanchestera* w niniejszej rozprawie obarczone jest pewnymi uproszczeniami, głownie w zakresie parametrów wejściowych (wykorzystano ogólnodostępne dane z operacji *Iraqi Freedom*). Bardziej złożone modelowanie walki wymaga symulacji (w ***Rozdziale 2.3.6*** posłużono się przykładowymi symulacjami matematycznymi, odzwierciedlającymi asymetrię informacyjną).

Miary efektywności oraz wyrażające je wielkości powinny pomóc w ukierunkowaniu poszukiwań w dziedzinie nowych aplikacji technologicznych, niezależnie od oceny aplikacji już rozwijanych. Bez miar efektywności pozwalających na wymierne ujęcie założonych korzyści wynikających z technologii *wieku informacyjnego – przewagi informacyjnej* i *manewru dominującego*, ucierpi w siłach zbrojnych zdolność do pomiaru rzeczywistego potencjału prawdopodobnych przeciwników oraz umotywowania własnych wydatków na rozwój nowych technologii.

2.3.6. Pomiar efektywności informacyjnej w oparciu o doświadczenia operacji Iraqi Freedom – prawa F. W. Lanchestera

Sapiens nihil affirmat quod non probet
(badacz nie ogłasza, póki nie udowodni...)
przysłowie rzymskie

Wobec operacji informacyjnych, szczególnie w aspekcie prognozowania rozwoju sytuacji oraz pomiaru przewagi informacyjnej, podobnie jak wobec innych rodzajów działań pola walki można stosować odwzorowania matematyczne.

Modelowanie matematyczne jest narzędziem do badania różnych zjawisk, trzeba jednak pamiętać o kilku trudnościach w jego stosowaniu. Na początek należy odpowiednio opisać model, czyli przy wykorzystaniu języka matematycznego zapisać poznane zależności. Ważnym zadaniem jest wybranie krytycznego zbioru parametrów jako podzbioru wcześniej określonych parametrów opisujących zjawisko. Określenie zbioru krytycznego jest kluczowym etapem modelowania, dalsza część to zbudowanie modelu w oparciu o te parametry i przeprowadzenie symulacji. Jeśli wyniki symulacji są zgodne z przewidywaniami teoretycznymi to znaczy, że model jest poprawny..

Jednym z ważniejszych sposobów modelowania zjawisk jest ich opis przy pomocy równań różniczkowych.

Złożoność zjawisk opisywanych równaniami różniczkowymi powoduje, że często nie udaje się ich rozwiązać metodami analitycznymi lub rozwiązanie analityczne nie nadaje się do efektywnego zastosowania. Czasem też nie interesuje nas dokładne rozwiązanie, a jedynie jego dostatecznie dobre przybliżenie. Innym zagadnieniem związanym z równaniami różniczkowymi jest ocena stabilności rozwiązań układów równań różniczkowych. Liczbowe wartości parametrów modelu wyznaczamy jako wynik doświadczeń lub w gorszym przypadku są jedynie wartościami przewidywanymi. Podobnie jest z wartościami początkowymi. W związku z tym na rozwiązanie układu równań opisującego badane zjawisko nakładamy pewne warunki. Podstawowym warunkiem, niezbędnym do praktycznej użyteczności rozwiązania jest założenie, że niewielkim zmianom wartości początkowych odpowiadają niewielkie zmiany wyniku (czyli de facto rozwiązania) równania. Podstawowe zastosowanie praktyczne ma zbadanie stabilności *w sensie Lapunowa* lub asymptotycznej stabilności układu równań różniczkowych.

Aby matematycznie modelować walkę załóżmy, że w konflikcie uczestniczy jedno państwo i koalicja państw. Model musi opisywać relacje pomiędzy tymi elementami. W matematycznych odwzorowaniach działań bojowych posłużono się ***prawami F. W. Lanchestera*** **(*Rozdział Nr 2.3.5*)**.

Wśród znanych odwzorowań - kwadratowe prawo *F. W. Lanchestera* jest pewną próbą oceny implikacji przewagi informacyjnej dla walki lądowej poprzez odwołanie się do mechanizmu polegającego na tym, że efektywność jednostek, zdolność wojsk do przetrwania oraz wielkość wojsk i ich struktura mogą ulegać zmianom w wyniku pozyskania informacji lepszej jakościowo. Zastosowanie prawa kwadratowego polega na matematycznym zmodelowaniu wpływu informacji i szeroko pojętej, z różnych źródeł uzyskiwanej wiedzy o przeciwniku, na efekt operacyjny działań bojowych. Na podstawie układów równań można wykazać, że jeśli jedna strona posiada znaczną ilość informacji, w przeciwieństwie do strony drugiej - wówczas przypadek pierwszej strony podąża w kierunku *liniowego prawa Lanchestera*, podczas gdy przypadek strony drugiej podąża w kierunku *prawa kwadratowego*. Przy dokonywaniu symulacji pola walki za pomocą modeli matematycznych w sytuacji asymetrii informacyjnej zasadnym więc jest zastosowanie

tzw. *mieszanego prawa Lanchestera* (układ równań różniczkowych i nierówność kwadratowa). Ma tu zastosowanie nierówność w odniesieniu do statycznego obrazu przewagi bojowej, a układ równań różniczkowych w oparciu o zróżnicowane dane początkowe pozwala na dynamiczne zobrazowanie przebiegu działań bojowych w funkcji czasu.

Niech $x=x(t)$ opisuje potencjał koalicji w walce, a $y=y(t)$ ten sam potencjał dla drugiego strony. Prędkość zmiany x zależy oczywiście od parametrów y drugiej strony (efektywności strat) oraz od różnic w wiedzy o przeciwniku. W uproszczeniu można przedstawić te zależności jako ky i αx, gdzie k i α są stałymi dodatnimi. Te dwa elementy powodują zmianę x. Z drugiej strony wielkość początkowa potencjału bojowego ogranicza ten wpływ na dx/dt. Przedstawmy ten człon jak g, gdzie g jest stałą dodatnią. Podobnie sytuacja wygląda dla dy/dt. W rezultacie $x=x(t)$ i $y=y(t)$ są rozwiązaniami liniowego układu równań różniczkowych:

$$\begin{cases} \dfrac{dx}{dt} = -\alpha x - ky + g, \\ \dfrac{dy}{dt} = -lx - \beta y + h, \end{cases} \tag{1}$$

Rozwiązaniem układu (1) jest (wyprowadzenie - ***Załącznik Nr 2***):

$$\begin{cases} x(t) = -2kC_1 e^{-\frac{t}{2}\left[(\alpha+\beta)+\sqrt{(\alpha-\beta)^2+4kl}\right]} - 2kC_2 e^{-\frac{t}{2}\left[(\alpha+\beta)-\sqrt{(\alpha-\beta)^2+4kl}\right]} + \dfrac{g\beta-kh}{\alpha\beta-kl}, \\ y(t) = \left(\alpha-\beta-\sqrt{(\alpha-\beta)^2+4kl}\right)C_1 e^{-\frac{t}{2}\left[(\alpha+\beta)+\sqrt{(\alpha-\beta)^2+4kl}\right]} + \left(\alpha-\beta+\sqrt{(\alpha-\beta)^2+4kl}\right)C_2 e^{-\frac{t}{2}\left[(\alpha+\beta)-\sqrt{(\alpha-\beta)^2+4kl}\right]} + \dfrac{h\alpha-gl}{\alpha\beta-kl}, \end{cases} \tag{2}$$

gdzie: $C_1, C_2 \in \Re$, stanowiąc stałe należące do zbioru liczb rzeczywistych, które należy wyliczyć z warunków początkowych

przy: $x_0(t_0) = 0$;
$y_0(t_0) = 0$

$$\begin{cases} C_1 = \dfrac{-2kgl + kh(\alpha+\beta-\sqrt{(\alpha-\beta)^2+4kl}) + \beta g(\alpha-\beta+\sqrt{(\alpha-\beta)^2+4kl})}{4k\sqrt{(\alpha-\beta)^2+4kl}\,(\alpha\beta-kl)} \\ C_2 = \dfrac{2kgl - kh(\alpha+\beta+\sqrt{(\alpha-\beta)^2+4kl}) - \beta g(\alpha-\beta-\sqrt{(\alpha-\beta)^2+4kl})}{4k\sqrt{(\alpha-\beta)^2+4kl}\,(\alpha\beta-kl)} \end{cases} \tag{3}$$

Rozwiązanie układu równań różniczkowych pozwala na ukazanie dynamiki działań bojowych z uwzględnieniem czynnika informacyjnego oraz strat obydwu stron

Dysponując danymi obejmującymi wartości podanych współczynników można oszacować pozostałe parametry modelu, a tym samym dokonać prognozowania przebiegu walki zbrojnej. Rozwiązanie układu równań różniczkowych zgodnie z *mieszanym prawem Lanchestera* zawarte jest w ***Załączniku Nr 2***.

Poniżej zamieszczono prezentację modelu odwzorowania przebiegu działań bojowych w oparciu o konflikt iracki za pomocą *liniowego prawa Lanchestera* uwzględniającego potencjał informacyjny (miary efektywności informacyjnej).

Model matematyczny oparto na danych z operacji *Iraqi Freedom* uzyskanych ze źródeł ogólnodostępnych:

- A. Cordesman. *The Lessons of the Iraq War – Main Report July 2003.* Center for Strategic and International Studies. Waszyngton 2003;
- L. Konopka. *Operacja Iraqi Freedom – próba podsumowania.* W: "Myśl Wojskowa" – dodatek specjalny „Iracka Wolność" Bellona, Warszawa 2003;
- M. Krauze (red). *Operacja Iracka Wolnośc. Materiały z Konferencji Naukowej.* AON, Warszawa, 2003.

Ze względu na rozbieżność w przedziale ok. 20% i niejednorodność danych zawartych w ww. źródłach – dokonano ich analizy i uśrednienia, co zamieszczono w ***Załączniku Nr 3***. Do modelu matematycznego użyto danych uśrednionych w zakresie stanów osobowych i sprzętu pola walki na I dzień działań (wejście do walki przy $t_0 = 0$). Dane powyższe zawiera ***Tabela Nr 7***. Na ***Wykresie Nr 5*** zobrazowano wyraźną przewagę sprzętową strony irackiej (za wyjątkiem środków walki powietrznej). Strona iracka miała także przewagę w liczebnym stanie wojsk.

Tabela Nr 8 wraz z odwzorowaniami matematycznymi przedstawia wynik obliczeń (z wykorzystaniem *układu równań różniczkowych Lanchestera*) ($x(t)$ i $y(t)$ jako potencjału zaangażowanego w walce, odpowiednio *Koalicji* i *Iraku*. Do przedstawionego w tabeli obliczenia przyjęto następujące parametry początkowe:

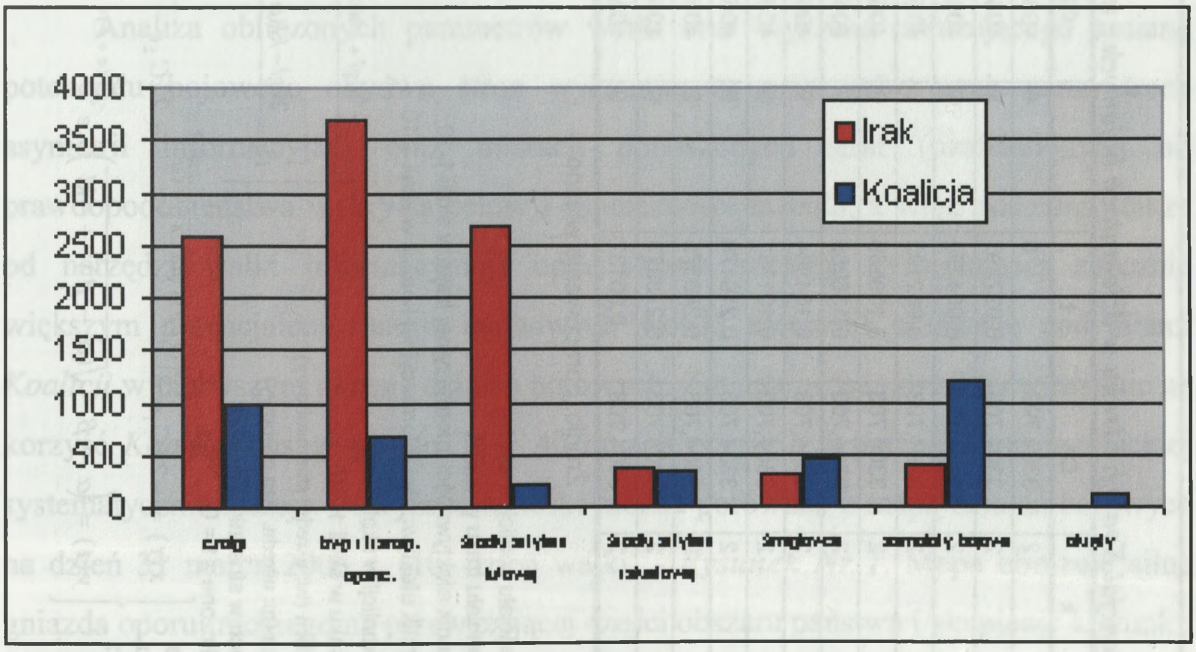
- α - *współczynnik efektywności informacyjnej Iraku w skali 1-10, przyjęto pierwsze założenie* $\alpha = 3$;
- β - *współczynnik efektywności informacyjnej koalicji w skali 1-10, przyjęto pierwsze założenie* $\beta = 9$;
- k - *miara strat koalicji w skali 1 – 10, przyjęto pierwsze założenie* $k = 2$;
- l - *miara strat Iraku w skali 1 – 10, przyjęto pierwsze założenie* $l = 9$;

- *t - czas w dniach w stosunku rocznym (przeliczany w n przedziałach dziesięciodniowych jako zmienna 10n/365 celem zachowania wyrazistości obliczeń i czytelności wykresu z przyjęciem 110 dni trwania działań bojowych).*

Dane uśrednione	Irak	Koalicja
Stany Osobowe	**463333**	**278393**
Sprzęt		
czołgi	2600	981
bwp i transportery opanc.	3700	689
środki artylerii lufowej	2683	220
środki artylerii rakietowej	382	333
śmigłowce	300	459
samoloty bojowe	391	1191
okręty	12	127
średnia geometryczna sił	**1266**	**995**

Tabela 7: ***Uśrednione dane wartości bojowych Iraku I Koalicji***

Źródło: opracowanie własne



Wykres 5: ***Wykres przewagi sprzętowej strony irackiej***

Źródło: opracowanie własne

Tabela 8: ***Potencjał Koalicji i Iraku w działaniach bojowych z uwzględnieniem miar efektywności informacyjnej***

dni	k	C1	t	l	C2	h	g	α	β	x(t)	y(t)
1	2	3304,703	0	9	40552,82	463333	278393	3	9	0	0
10	2	3304,703	0,027397	9	40552,82	463333	278393	3	9	7025,259	10430,146
20	2	3304,703	0,054795	9	40552,82	463333	278393	3	9	13051,13	17164,649
30	2	3304,703	0,082192	9	40552,82	463333	278393	3	9	18322,96	21200,239
40	2	3304,703	0,109589	9	40552,82	463333	278393	3	9	23021,68	23269,901
50	2	3304,703	0,136986	9	40552,82	463333	278393	3	9	27280,85	23912,557
60	2	3304,703	0,164384	9	40552,82	463333	278393	3	9	31199,1	23524,343
70	2	3304,703	0,191781	9	40552,82	463333	278393	3	9	34849,42	22396,331
80	2	3304,703	0,219178	9	40552,82	463333	278393	3	9	38285,87	20742,294
90	2	3304,703	0,246575	9	40552,82	463333	278393	3	9	41548,6	18719,138
100	2	3304,703	0,273973	9	40552,82	463333	278393	3	9	44667,51	16441,926
110	2	3304,703	0,30137	9	40552,82	463333	278393	3	9	47664,96	13994,946

Źródło: opracowanie własne

gdzie:

x(t) - moduł potencjału koalicji w walce

y(t) - moduł potencjału Iraku w walce

α - współczynnik efektywności informacyjnej Iraku w skali 1-10

β - współczynnik efektywności informacyjnej koalicji w skali 1-10

k - miara strat koalicji w skali 1- 10

l - miara strat Iraku w skali 1 - 10

g - potencjał koalicji (tu: uśredn. stan osobowy)

h - potencjał Iraku (tu: uśredn. stan osobowy)

t - czas w dniach w stosunku rocznym

C1, C2 - stałe wyliczone z t = 0

układ równań

$$\begin{cases} \frac{dx}{dt} = -\alpha x - ky + g, \\ \frac{dy}{dt} = -lx - \beta y + h, \end{cases}$$

$$\begin{cases} C_1 = \frac{-2kgl + kh(\alpha + \beta - \sqrt{(\alpha-\beta)^2 + 4kl}) + \beta g(\alpha - \beta + \sqrt{(\alpha-\beta)^2 + 4kl})}{4k\sqrt{(\alpha-\beta)^2 + 4kl}(\alpha\beta - kl)} \\ C_2 = \frac{2kgl - kh(\alpha + \beta + \sqrt{(\alpha-\beta)^2 + 4kl}) - \beta g(\alpha - \beta - \sqrt{(\alpha-\beta)^2 + 4kl})}{4k\sqrt{(\alpha-\beta)^2 + 4kl}(\alpha\beta - kl)} \end{cases}$$

wyliczenie C1, C2:

C2: 40552,82

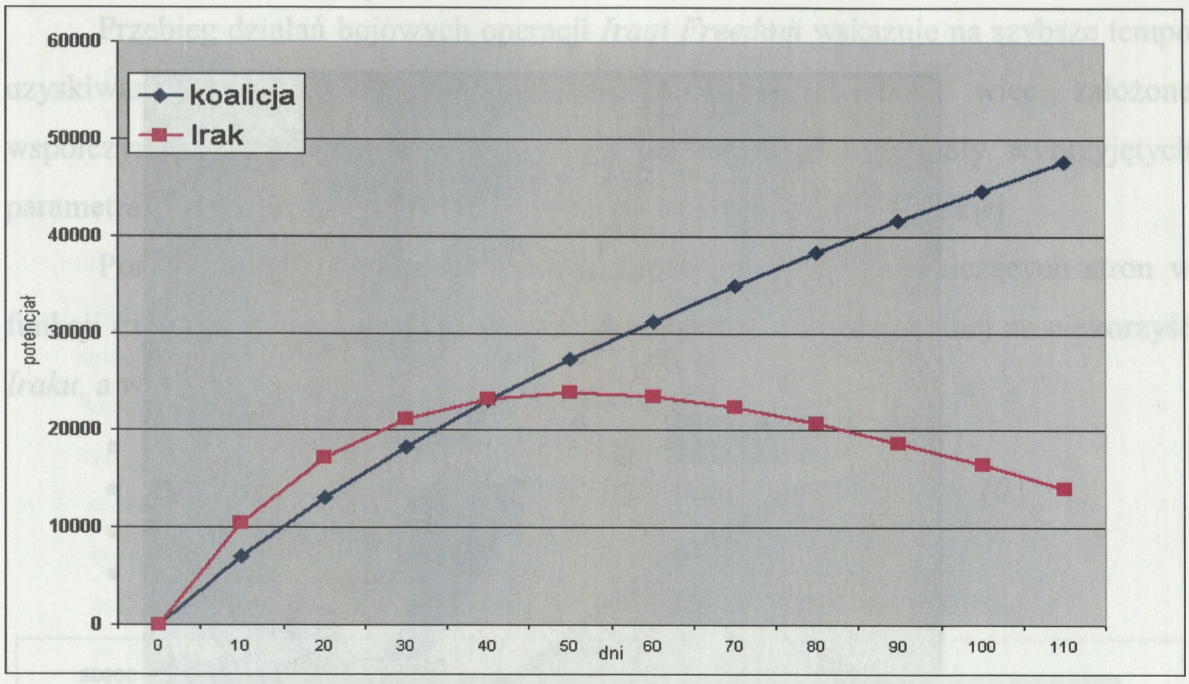
C1: 3304,703

rozwiązanie układu równań:

$$\begin{cases} x(t) = -2kC_1 e^{-\frac{t}{2}\left[(\alpha+\beta)+\sqrt{(\alpha-\beta)^2+4kl}\right]} - 2kC_2 e^{-\frac{t}{2}\left[(\alpha+\beta)-\sqrt{(\alpha-\beta)^2+4kl}\right]} + \frac{g\beta - kh}{\alpha\beta - kl}, \\ y(t) = \left(\alpha - \beta - \sqrt{(\alpha-\beta)^2+4kl}\right)C_1 e^{-\frac{t}{2}\left[(\alpha+\beta)+\sqrt{(\alpha-\beta)^2+4kl}\right]} + \left(\alpha - \beta + \sqrt{(\alpha-\beta)^2+4kl}\right)C_2 e^{-\frac{t}{2}\left[(\alpha+\beta)-\sqrt{(\alpha-\beta)^2+4kl}\right]} + \frac{h\alpha - gl}{\alpha\beta - kl}, \end{cases}$$

warunek stabilności

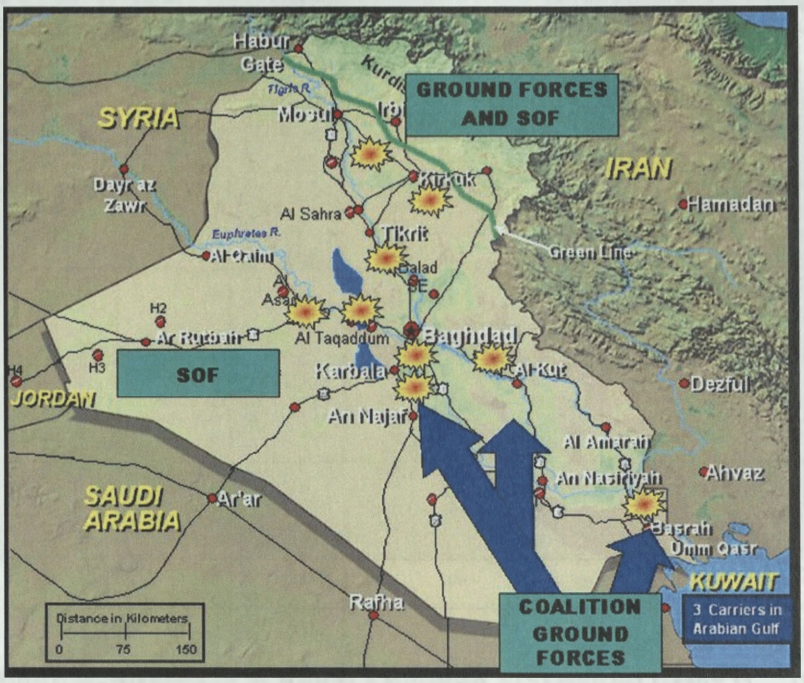
$\alpha\ \beta$ - kl = 9



Wykres 6: ***Wykres potencjału koalicji i Iraku w działaniach bojowych z uwzględnieniem efektywności informacyjnej (stany liczebne wojsk)***

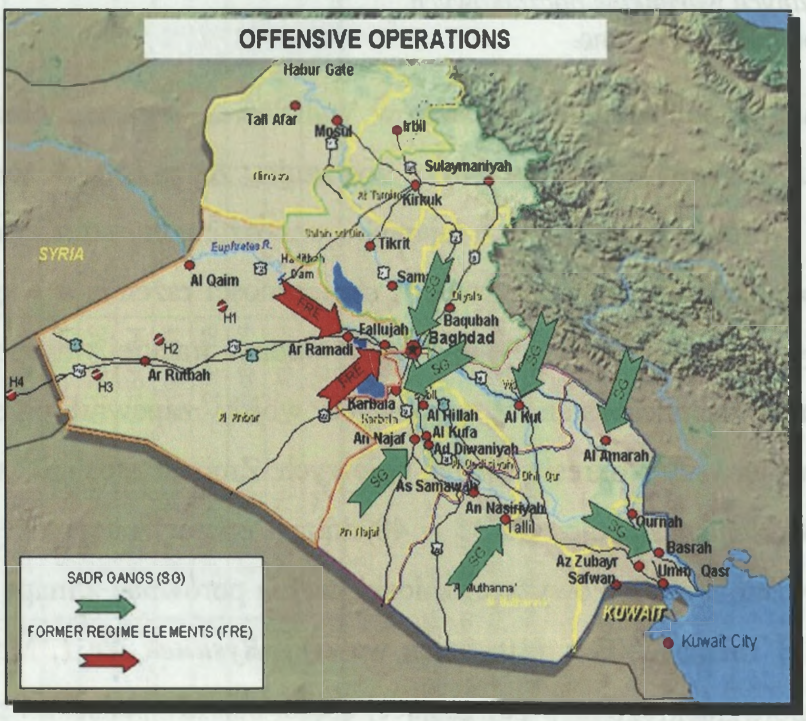
Uwaga: wartości bezwzględne x(t) i y(t) nie wyrażają wielkości liczbowej potencjałów, a jedynie ich moduły porównawcze i mogą przyjmować różne rzędy wielkości w zależności od wprowadzanych warunków początkowych.
Źródło: opracowanie własne

Analiza obliczonych parametrów walki oraz wykresu obrazującego zmianę potencjału bojowego obydwu stron wykazuje, że przy założonych parametrach asymetrii informacyjnej oraz miarach ponoszonych strat (uzależnionych od prawdopodobieństwa wykrycia celów i skuteczności rażenia, a więc pośrednio także od narzędzi walki informacyjnej) opór strony irackiej, dysponującej znacznie większym potencjałem stanów osobowych wojsk, zapewnił przewagę nad siłami *Koalicji* w pierwszym okresie działań bojowych. Zmiana stosunku sił, przełamanie na korzyść *Koalicji* następuje po 35 – 40 dniach operacji, a potencjał strony irackiej systematycznie maleje. Powyższe wnioski można porównać z mapą działań bojowych na dzień 31 marca 2003 r. (10. dzień walki) - ***Rysunek Nr 1.*** Mapa obrazuje silne gniazda oporu irackiego na przeważającej części obszaru państwa i skupienie kierunku uderzenia sił koalicyjnych. Porównanie wyników obliczeń z kolejną mapą działań rzeczywistych odzwierciedla różnicę tempa uzyskiwania przewagi przez *Koalicję* - ***Rysunek Nr 2.***



Rysunek 1: ***Mapa działań bojowych operacji Iraqi Freedom z 31 .03. 2003 r.***

Źródło: http://www.freewebs.com/jeffhead/iraqifreedom/maps.htm



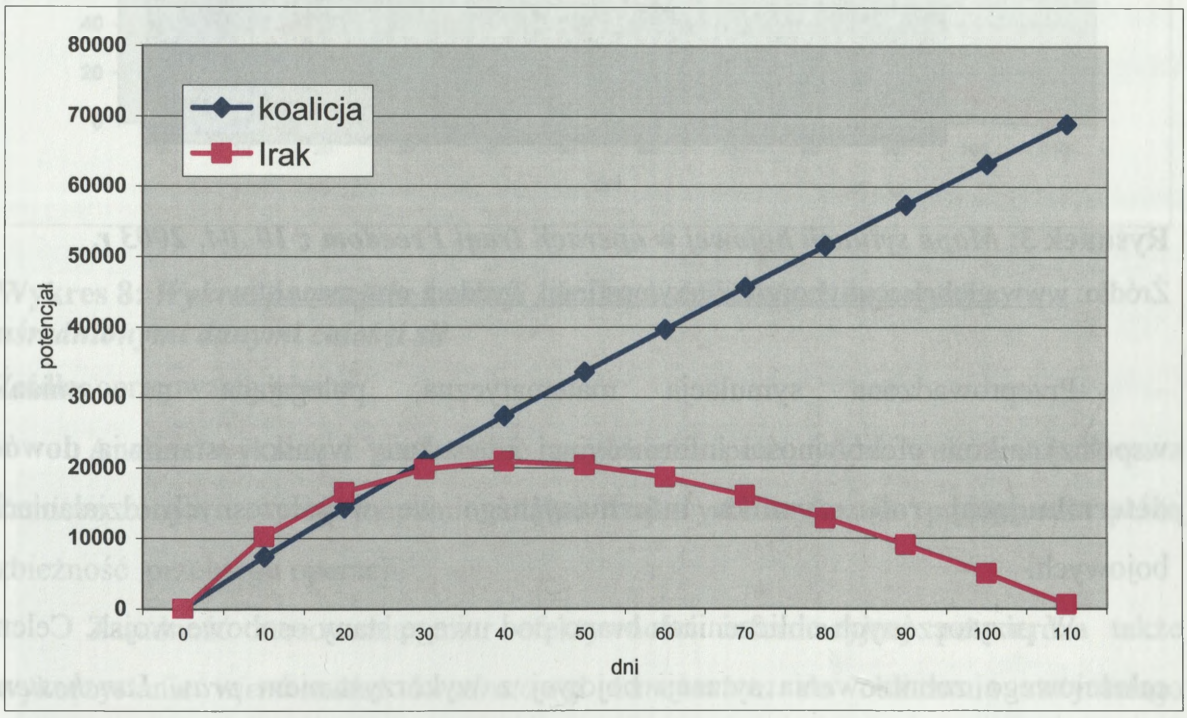
Rysunek 2: ***Mapa działań bojowych operacji Iraqi Freedom z 8 .04. 2003 r.***

Źródło: www.globalsecurity.org/military/ops/iraqi_freedom-ops-maps.htm

Przebieg działań bojowych operacji *Iraqi Freedom* wskazuje na szybsze tempo uzyskiwania przez Koalicję dominacji nad przeciwnikiem, więc założone współczynniki efektywności informacyjnej oraz miary strat zostały w przyjętych parametrach równań różniczkowych zawyżone na korzyść strony irackiej.

Poniżej zamieszczony jest wykres obrazujący potencjał walczących stron w funkcji czasu po zmianie współczynników efektywności informacyjnej na niekorzyść *Iraku*, a więc:

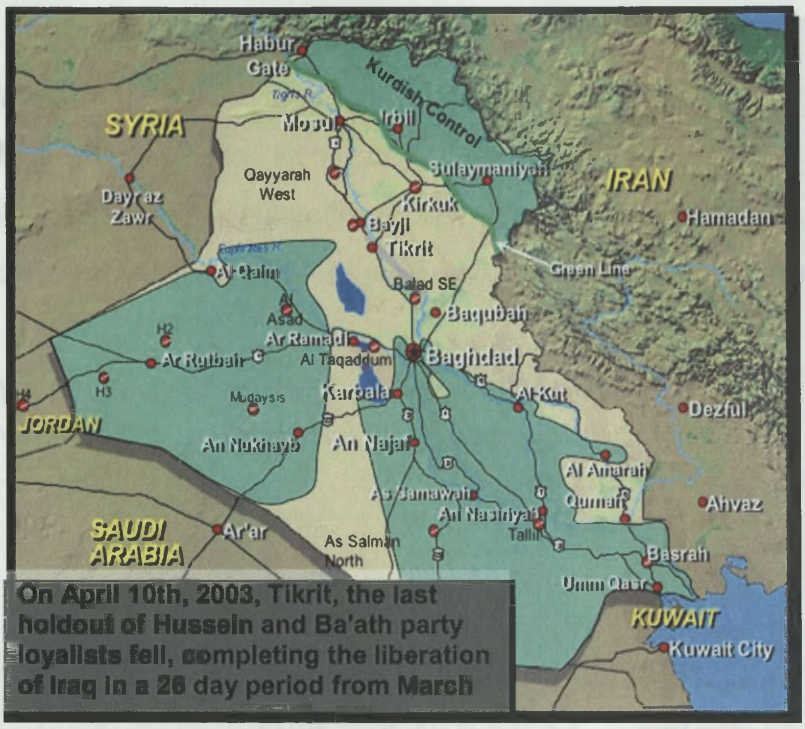
- α - *współczynnik efektywności informacyjnej Iraku* $\alpha = 1$;
- β - *współczynnik efektywności informacyjnej koalicji* $\beta = 10$;
- k - *miara strat koalicji* $k = 1$;
- l - *miara strat Iraku* $l = 9$;



Wykres 7: ***Wykres potencjału koalicji i Iraku w działaniach bojowych z uwzględnieniem zmaksymalizowanej efektywności informacyjnej Koalicji***

Źródło: opracowanie własne

Analiza wykresu pozwala na wyciągnięcie wniosku o przełamaniu oporu irackiego przez *Koalicję* już ok. 20. dnia działań bojowych, a prawdopodobna pełna likwidacja zdolności operacyjnych sił zbrojnych *Iraku* ma miejsce po ok. 110 dniach walki. Wynik ten znajduje potwierdzenie przy analizie mapy sytuacyjnej z 10 kwietnia 2003 r. – ***Rysunek Nr 3***.



Rysunek 3: ***Mapa sytuacji bojowej w operacji Iraqi Freedom z 10 .04. 2003 r.***
Źródło: www.globalsecurity.org/military/ops/iraqi_freedom-ops-maps.htm

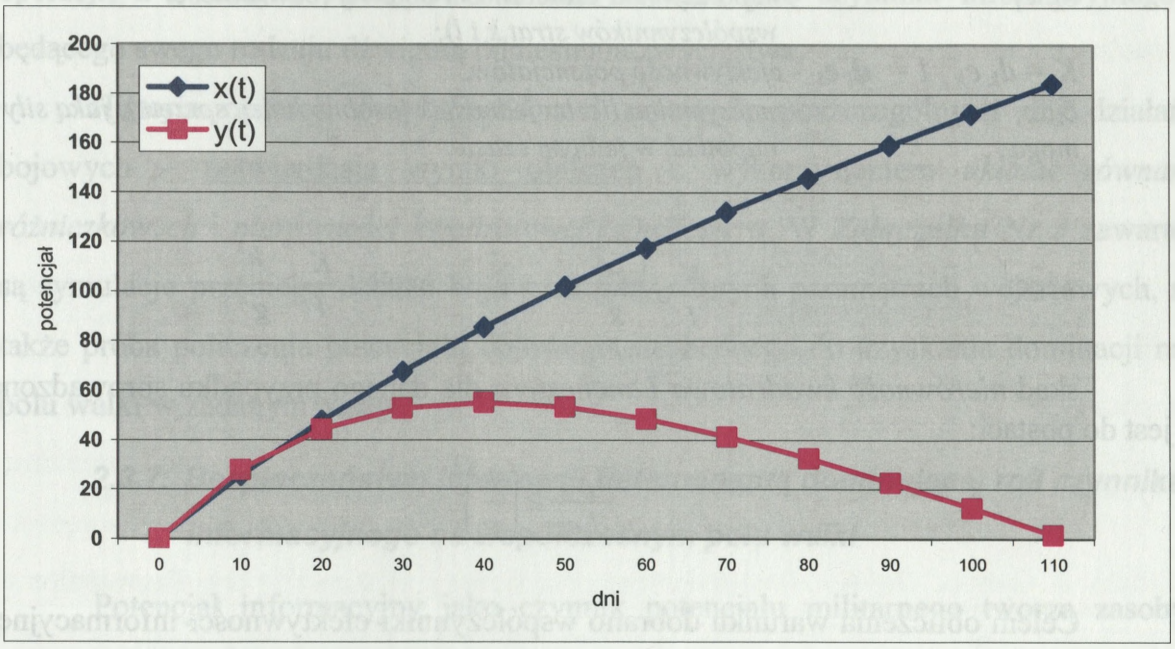
Przeprowadzona symulacja matematyczna, polegająca na zmianie współczynników efektywności informacyjnej i uzyskany wynik – stanowią **dowód determinującej roli czynnika informacyjnego** we współczesnych działaniach bojowych.

W przytoczonych obliczeniach brano pod uwagę stany osobowe wojsk. Celem całościowego zobrazowania sytuacji bojowej z wykorzystaniem *praw Lanchestera* dokonano obliczenia rozkładu potencjału obydwu walczących stron w czasie z zastosowaniem średniej geometrycznej całości sił (***Tabela Nr 7***) wg wzoru:

$\acute{S}rG_{\bar{h}} = \sqrt[n]{h_1 h_2 \ldots . h_n}$ - strona iracka; $\acute{S}rG_{\bar{g}} = \sqrt[n]{g_1 g_2 \ldots . g_n}$ - strona koalicyjna

Obliczenie oparte na odwzorowaniach zgodnych z ***Tabelą Nr 7*** zawarte jest w ***Załączniku Nr 3***. Poniżej zamieszcza się wykres będący odzwierciedleniem wyniku obliczeń przy pierwotnie założonych parametrach efektywności informacyjnej, czyli:

- α - *współczynnik efektywności informacyjnej Iraku* $\alpha = 3$;
- β - *współczynnik efektywności informacyjnej koalicji* $\beta = 9$;
- k - *miara strat koalicji* $k = 2$;
- l - *miara strat Iraku* $l = 9$;



Wykres 8: ***Wykres potencjału koalicji i Iraku w działaniach bojowych z uśrednionymi danymi całości sił***

Źródło: opracowanie własne

Analiza wykresu i porównanie przebiegów potencjałów walczących stron z zamieszczonymi wyżej mapami działań bojowych wykazuje praktycznie pełną zbieżność przebiegu operacji.

Zasadność stosowania miar efektywności informacyjnej potwierdza także wykorzystanie *nierówności kwadratowej Lanchestera* do obliczenia statycznego potencjału bojowego stron przy asymetrii informacyjnej. Zgodnie z *kwadratowym prawem Lanchestera* (***Tabela Nr 6***), w przypadku, gdy jedna ze stron (*Koalicja*) otrzymuje z dowództwa wyższego szczebla pełną informację dotyczącą sił nieprzyjaciela, podczas gdy druga strona (*Irak*) posiada jedynie informację dostępną ze swoich własnych ograniczonych zasobów, występuje poniżej przedstawiony warunek powodzenia *Koalicji (K)*:

$$\frac{K}{I} \geq \frac{c_k^2}{c_i},$$ przy czym: $c_k = \frac{h}{g}$, $c_i = \frac{g}{h}$ - naliczenia jednostkowe,

gdzie:

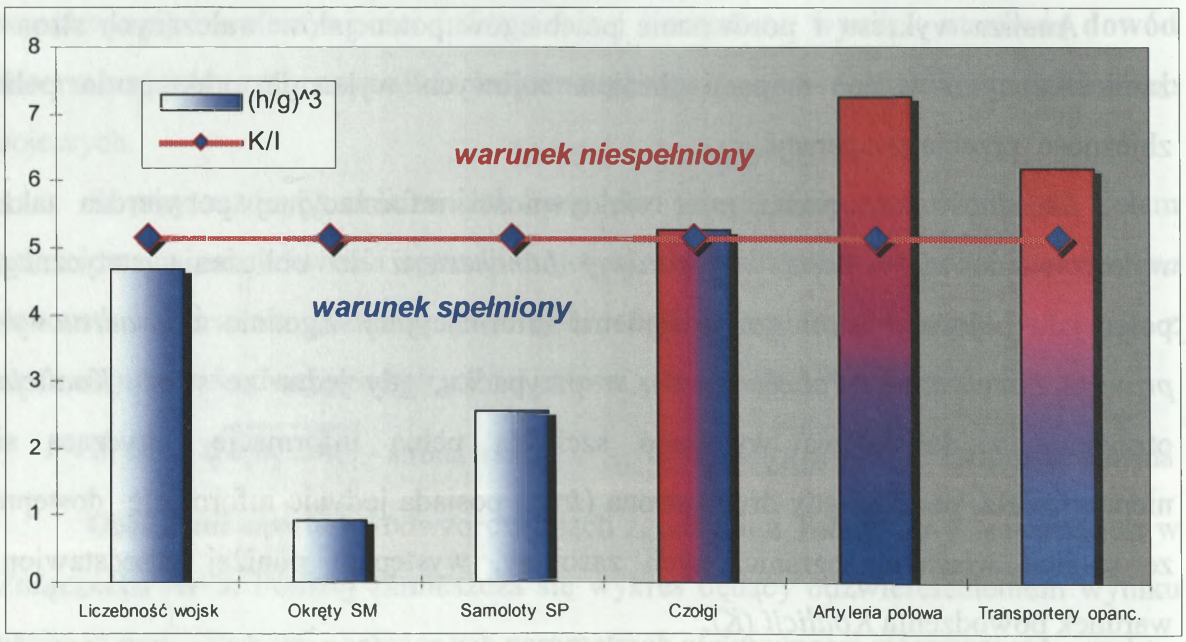
g	*- potencjał Koalicji (stany osobowe, sprzęt);*
h	*- potencjał Iraku (stany osobowe, sprzęt);*
d_k, d_i,	*- współczynniki efektywności informacyjnej;*
e_k, e_i	*- współczynniki skuteczności bojowej (odwrotności współczynników strat k i l);*
$K = d_k e_k$, $I = d_i e_i$	*- efektywność potencjałów,*
c_k, c_i	*- maksymalna liczba jednostek (osobno ludzi, sprzętu), jaką siły*
mogą	*napotkać w jednym czasie.*

więc: $$\frac{K}{I} \geq \frac{\left(\frac{h}{g}\right)^2}{\frac{g}{h}}, \qquad \text{czyli} \quad \frac{K}{I} \geq \frac{h^3}{g^3},$$

skąd *nierówność kwadratowa Lanchestera* dla danego przypadku sprowadzona jest do postaci:

$$\frac{d_k e_k}{d_i e_i} \geq \left(\frac{h}{g}\right)^3$$

Celem obliczenia warunku dobrano współczynniki efektywności informacyjnej i skuteczności bojowej (odwrotność miary strat) jak w ***Tabeli Nr 8***, a uśrednione parametry potencjałów bojowych zgodnie z ***Tabelą Nr 7***. Wynik obliczeń, zawarty w ***Załączniku Nr 3*** zobrazowany jest na wykresie:



Wykres 9: ***Spełnianie warunków powodzenia Koalicji w operacji Iraqi Freedom***

Źródło: opracowanie własne

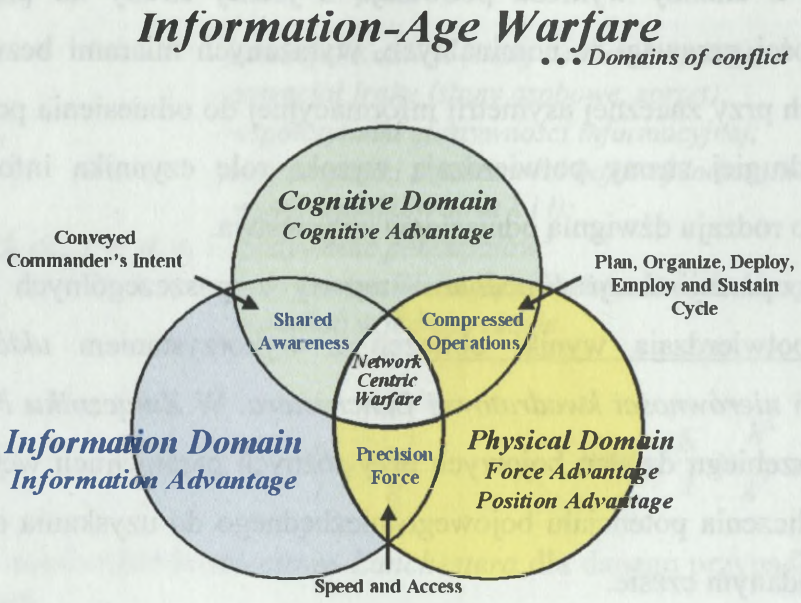
Wnioski z analizy wykresu pozwalają z jednej strony na przekonanie o niewystarczalności przewagi w nominalnych, wyrażanych miarami bezwzględnymi, siłach i środkach przy znacznej asymetrii informacyjnej do odniesienia powodzenia w operacji, a z drugiej strony potwierdzają wysoką rolę czynnika informacyjnego, będącego swego rodzaju dźwignią odniesienia zwycięstwa.

Historia operacji *Iraqi Freedom* i raporty z poszczególnych dni działań bojowych – potwierdzają wyniki obliczeń z wykorzystaniem *układu równań różniczkowych* i *nierówności kwadratowej Lanchestera*. W ***Załączniku Nr 3*** zawarte są symulacje przebiegu działań bojowych przy różnych parametrach wejściowych, a także próba policzenia potencjału bojowego niezbędnego do uzyskania dominacji na polu walki w zadanym czasie.

2.3.7. Bezpieczeństwo informacji determinantą dominującej roli czynnika informacyjnego na współczesnym polu walki

Potencjał informacyjny jako czynnik potencjału militarnego tworzą zasoby informacyjne systemu obronnego państwa oraz systemy kształtujące infrastrukturę informacyjną państwa. Oznacza to, że potencjał informacyjny to wszelkie *zasoby informacyjne* (dane, informacje, wiedza), które tworzą *infosferę* określonego systemu działania, a także *systemy informacyjne* (informatyczne, telekomunikacyjne), jako uporządkowane układy elementów, w których przeprowadza się analizy informacji wejściowych i wyjściowych niezbędne do efektywnego prowadzenia określonych, zamierzonych działań.

Nowoczesne koncepcje walki zbrojnej bazują na tworzeniu wieloczynnikowej przewagi militarnej (*multifactor military superiority*) w oparciu o kontrolowaną, rozstrzygającą przewagę informacyjną (*information superiority*) i technologiczną (*technological superiority*). Szczególnym odzwierciedleniem tych koncepcji jest sieciocentryczna architektura pola walki, zobrazowana na ***Rysunku Nr 4.***



Rysunek 4: ***Sieciocentryczna architektura pola walki uwypuklająca znaczenie czynnika informacyjnego***

Źródło: J. Garstka. *Defense Transformation and Network Centric Warfare.* Presentation to Polish MOD NCW Conference 23-25 June 03

Przykładem dobrze obrazującym zjawisko asymetrii informacyjnej są praktycznie wszystkie współczesne konflikty zbrojne. Wśród głównych przyczyn klęski armii irackiej w operacji *Iraqi Freedom* uznano przestarzałe, niedostosowane do wymogów współczesnego pola walki systemy informacyjne, głównie elementy pozyskiwania informacji i wypracowywania decyzji. Były one mało wydajne, oparte na łatwo zakłócalnej technice analogowej, uniemożliwiającej efektywną, kompleksową automatyzację systemów dowodzenia, łączności, rozpoznania i kierowania środkami walki. Przestarzały i źle funkcjonujący system nie był w stanie dostarczyć danych niezbędnych do planowania i wykonania uderzeń na obiekty przeciwnika (niskie współczynniki efektywności informacyjnej i skuteczności bojowej przyjęte w modelu matematycznym – ***Rozdział 2.3.6***). W tych obszarach występowała zdecydowana przewaga *Koalicji*, co można wyrazić jako konfrontację systemów informacyjnych, należących do dwóch różnych generacji technologicznych (klasyczny przykład asymetrii informacyjnej, której konsekwencją na współczesnym polu walki jest wprowadzenie *„stosunku wiedzy względnej" (relative knowledge)* stron walczących, jako czynnika decydującego).

Strona koalicyjna nie uniknęła błędów w sztuce posługiwania się własnymi systemami informacyjnymi. Specjaliści z *Departamentu Obrony USA* stwierdzili, że około 25% informacji przekazywanych przez organa dowodzenia USA do ośrodków decyzyjnych dyslokowanych poza obszarem działań wojennych zostało przechwyconych przez nieuprawnione osoby, ponieważ przesyłano je w sposób niezaszyfrowany z wykorzystaniem Internetu. Występowały także błędy w identyfikacji obiektów pola walki, doprowadzające do wykonywania uderzeń ogniowych na wojska własne. Zjawiska te potęgują potrzebę zapewnienia bezpieczeństwa przetwarzanym informacjom.

Udowodniona w ***Rozdziale 2.3.6*** teza o dominującej roli czynnika informacyjnego na współczesnym polu walki implikuje wnioski obejmujące problematykę ochrony zasobów informacyjnych. Dotyczy to w szczególności następujących dziedzin (wg poglądów NATO, w kolejności priorytetów)[77]:

- operacje związanych z procesem walki;
- obraz wspólnych działań operacyjnych;
- rozpoznanie wojskowe;
- logistyka / transport;
- systemy łączności oraz systemy informatyczne;
- zarządzanie informacją;
- plany operacyjne;
- analiza operacyjna.

Według oszacowań ekspertów NATO:

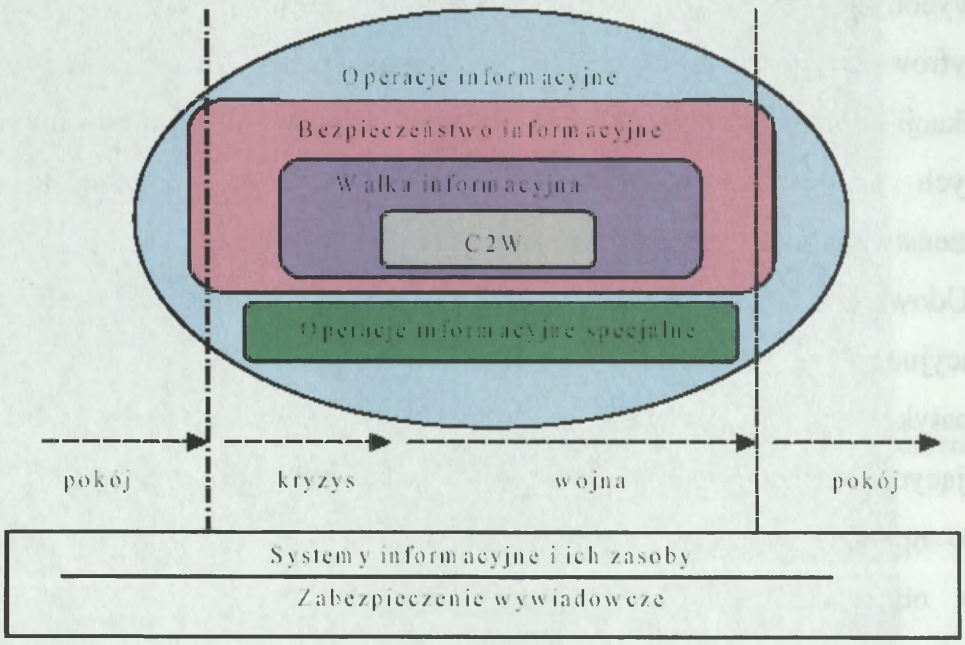
- w ciągu najbliższych 3 do 5 lat można spodziewać się znacznego wzrostu wszelkiego rodzaju ataków na szeroko rozumiane systemy teleinformacyjne,
- właściwe zabezpieczenie informacji jest problemem globalnym i stanowi niezwykłe wyzwanie dla sił zbrojnych,
- zabezpieczenie zasobów informacyjnych wymaga połączenia wysiłków wszystkich podmiotów dysponujących tymi zasobami oraz władz (służb) odpowiedzialnych za bezpieczeństwo państwa[78].

---

[77] Górniak A., Matuszewski J., Jańczak J., Godlewski A.: *Koncepcja prowadzenia walki radioelektronicznej (WRE) w ramach operacji informacyjnej w aspekcie zapewnienia interoperacyjności z NATO.* Praca studyjna. GZRW. Warszawa 2000

[78] J. Gardeta, *Information Operations – the NATO Perspective,* Netherlands Annual Review of Military Studies, Breda 1999

Miejsce bezpieczeństwa informacyjnego we współczesnych operacjach informacyjnych obrazuje ***Rysunek Nr 5***.



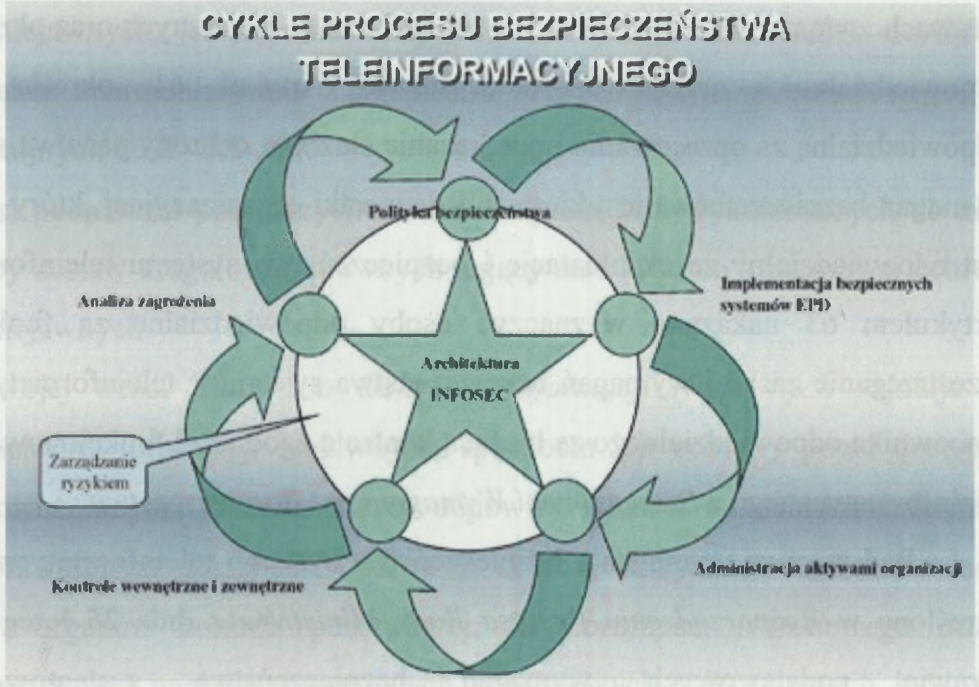
Rysunek 5: ***Współzależność różnych rodzajów operacji informacyjnych***

Źródło: J. Matuszewski, T. Rapacki . *Aktualne koncepcje prowadzenia rozpoznania, walki radioelektronicznej i informacyjnej w państwach NATO*. Instytut Radiolokacji Wydziału Elektroniki, WAT, 2002

Nowoczesne myślenie o bezpieczeństwie narodowym musi obejmować analizę systemową pojęcia bezpieczeństwa informacyjnego państwa oraz świadomość związanych z nim zagrożeń. *Bezpieczeństwo informacyjne* jest trwałym elementem *bezpieczeństwa narodowego* (*międzynarodowego*) tak, jak globalizacja informacyjna jest nieodłącznym elementem (*czynnikiem*) procesu globalizacji.

2.4. Prawno-organizacyjne determinanty bezpieczeństwa informacyjnego

Polityką bezpieczeństwa informacyjnego można nazwać zespół środków i posunięć organizacyjnych, które mają zapewnić bezpieczne funkcjonowanie systemów informacyjnych[79]. (*Polska Norma PN-I-13335-1* wprowadza pojęcie *polityka zabezpieczeń)*. Przepisy bezpieczeństwa *RS-100* które obowiązują w krajach Unii Europejskiej dokładniej charakteryzują powyższe pojęcie „jest to przeciwdziałanie zagrożeniom przypadkowej lub celowej utraty poufności, integralności lub dostępu do informacji". Architektura procesów bezpieczeństwa teleinformacyjnego *(INFOSEC)* nie jest skomplikowana. Właściwie najistotniejszym jej przesłaniem jest cykliczność realizacji poszczególnych procesów[80]. Schematyczny układ jest przedstawiony na ***Rysunku Nr 6.***



Rysunek 6: ***Cykle procesu bezpieczeństwa teleinformacyjnego***
Źródło: http://ochrona.euro-media.pl/archiwum

Politykę bezpieczeństwa informacyjnego buduje się rozpoczynając od analizy ryzyka i jego efektów w postaci szczególnych wymagań bezpieczeństwa.

[79] *Teleinfo* nr 41/2000
[80] http://ochrona.euro-media.pl/archiwum

2.4.1. Obowiązujące ustawodawstwo w zakresie bezpieczeństwa informacji i ochrony danych

„Kto zdradza tajemnicę, traci zaufanie
Bo rana może być opatrzona, obelga darowana,
ale ten kto wyjawił tajemnicę nie ma już nadziei"
Stary Testament, Mądrość Syracha (27, 16, 21)

Nadrzędnym dokumentem definiującym politykę bezpieczeństwa informacyjnego w odniesieniu do informacji niejawnych jest *Ustawa o Ochronie Informacji Niejawnych* z dnia 22 stycznia 1999 r..(*Dz. U. Nr 11, poz. 95*).

Rozdział 10 powyższej ustawy poświęcony jest *bezpieczeństwu systemów i sieci teleinformatycznych.* Ustawodawca pokazał w nim, że szczególne wymagania bezpieczeństwa systemów teleinformatycznych powinny być kompletnym i wyczerpującym opisem ich budowy, zasad działania i eksploatacji wraz z procedurami bezpieczeństwa . Procedury bezpieczeństwa obejmują zasady i tryb postępowania w sprawach związanych z bezpieczeństwem informacji niejawnych oraz określają zakres odpowiedzialności użytkowników systemu. Artykuł 61 określa, że osobą odpowiedzialną za opracowanie i przekazanie służbom ochrony państwa szczególnych wymagań bezpieczeństwa jest kierownik jednostki organizacyjnej, który jednocześnie jest odpowiedzialny za eksploatację i bezpieczeństwo systemu teleinformatycznego. Artykułem 63 nakazano wyznaczyć osoby odpowiedzialne za funkcjonowanie, przestrzeganie zasad i wymagań bezpieczeństwa systemów teleinformatycznych oraz pracownika odpowiedzialnego za bieżącą kontrolę zgodności funkcjonowania systemu teleinformatycznego z *Szczególnymi Wymaganiami Bezpieczeństwa.*

Podstawowe wymagania bezpieczeństwa systemu teleinformatycznego zostały określone w *Rozporządzeniu Prezesa Rady Ministrów* z dnia 25 lutego 1999 r. w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych *(Dz. U. Nr 18, poz. 162*). Rozporządzenie przewiduje, że bezpieczeństwo teleinformatyczne zapewnia się przez:

- ochronę fizyczną;
- ochronę elektromagnetyczną;
- ochronę kryptograficzną;
- bezpieczeństwo transmisji;
- kontrolę dostępu do urządzeń

oraz wskazuje sposób, w jaki osiąga się wyżej wskazane środki bezpieczeństwa.

Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz. U. Nr 133, poz. 883) oraz związane z nią *Rozporządzenie Ministra Spraw Wewnętrznych i Administracji* z dnia 3 czerwca 1998 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. (Dz. U. Nr 80, poz. 521 z późniejszymi zmianami) określa zadania jakie musi wykonać administrator danych wraz z administratorem bezpieczeństwa informacji przed uruchomieniem systemu oraz w czasie jego pracy.

Do powyższych ustaw można jeszcze doliczyć - ustawę prawo bankowe, ustawę o kontroli skarbowej, ustawę o nieuczciwej konkurencji itd. Każda z tych ustaw w swoisty sposób porusza problemy bezpieczeństwa i ochrony danych w przetwarzanych systemach informatycznych. Należy zaznaczyć, że ustawa o ochronie informacji niejawnych, jest zgodna z odpowiednimi przepisami NATO - AC/*35 - D/1016,* a także zharmonizowana z przepisami bezpieczeństwa przemysłowego, wg przepisów unijnych *UZE - RS-100.*

Dzięki połączeniu powyższych ustaw i rozporządzeń wykonawczych do nich, otrzymaliśmy zestaw uregulowań prawnych dający narzędzia do systemowej ochrony informacji niejawnych.

W swojej treści *Ustawa o Ochronie Informacji Niejawnych* zajmuje się systemem ochrony informacji niejawnych, sposobem ich ochrony przed dostępem osób nieupoważnionych. Określa zakres odpowiedzialności za ochronę informacji przed nieuprawnionym dostępem. Ustawa ta dotyczy wszystkich organów władzy publicznej , organów kontroli państwowej, *Sił Zbrojnych, Narodowego Banku Polskiego* oraz innych banków państwowych, państwowych osób prawnych, jednostek organizacyjnych oraz przedsiębiorców, instytutów naukowych, badawczo-rozwojowych i innych, ubiegających się o wykonywanie lub wykonujący prace związane z dostępem do informacji stanowiących tajemnicę państwową lub służbową.

2.4.2. Zasady polityki bezpieczeństwa informacyjnego

Generalną zasadą bezpieczeństwa systemów i sieci teleinformatycznych jest ochrona informacji przed nieuprawnionym dostępem, ujawnieniem, losowym lub nieuprawnionym zniszczeniem i modyfikacją, a także przez opóźnieniem lub nieuzasadnioną odmową jej dostarczenia[181].

W związku z powyższym, w systemach i sieciach teleinformatycznych wprowadzane są środki i metody zabezpieczeń, które powinny zapewnić utrzymanie następujących atrybutów bezpieczeństwa informacji:

1) ***Poufność*** – dostęp do informacji musi być ograniczony jedynie do kręgu użytkowników uprawnionych;
2) ***Integralność*** – informacja musi być zachowana w swej postaci oryginalnej, za wyjątkiem przypadków, gdy jest ona legalnie aktualizowana lub usuwana przez osoby do tego uprawnione;
3) ***Dostępność*** – informacja musi być dostępna dla uprawnionych użytkowników zawsze, kiedy mają taką potrzebę;
4) ***Rozliczalność*** – dostęp użytkownika do informacji może być przypisane w sposób jednoznaczny tylko temu użytkownikowi;
5) ***Autentyczność*** – tożsamość informacji lub podmiotu z nią związanego jest taka jak zadeklarowana;
6) ***Niezawodność*** – zachowanie i skutki działania są takie jak zamierzone.

Bezpieczeństwo informacji w systemie lub sieci teleinformatycznej jest stanem pożądanym, którego osiągnięcie jest zagadnieniem złożonym. Bezpieczeństwo to osiąga się poprzez wprowadzanie zabezpieczeń. Nie jest możliwe osiągnięcie bezpieczeństwa informacji w systemach i sieciach teleinformatycznych drogą zastosowania tylko wybranych środków i metod zabezpieczeń. Stosowane zabezpieczenia muszą mieć charakter kompleksowy. Ponadto, muszą one być adekwatne do wartości zasobów informacyjnych oraz dobrane stosownie do zagrożeń.

Bezpieczeństwo informacji niejawnych stanowiących tajemnicę państwową lub służbową w systemach lub sieciach teleinformatycznych powinno być zagwarantowane zgodnie z:

[81] *Ustawa o Ochronie Informacji Niejawnych*. z dnia 22 stycznia 1999 r. (*Dz.U.99.11.95 z późn. zm.*)

- *Ustawą o Ochronie Informacji Niejawnych* z dnia 22 stycznia 1999 r.;
- *Rozporządzeniem Prezesa Rady Ministrów* z dnia 25 lutego 1999 r. w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych.

W rozumieniu *Ustawy...* :

- *systemem teleinformatycznym* - jest system, który tworzą urządzenia, narzędzia, metody postępowania i procedury stosowane przez wyspecjalizowanych pracowników, w sposób zapewniający wytwarzanie, przechowywanie, przetwarzanie lub przekazywanie informacji;
- *siecią teleinformatyczną* - jest organizacyjne i techniczne połączenie systemów teleinformatycznych wraz z łączącymi je urządzeniami i liniami telekomunikacyjnymi.

Systemy i sieci teleinformatyczne, służące do wytwarzania, przechowywania, przetwarzania lub przekazywania informacji niejawnych stanowiących tajemnicę państwową, **podlegają szczególnej ochronie** przed nieuprawnionym ujawnieniem tych informacji, a także przed możliwością przypadkowego lub świadomego narażenia ich bezpieczeństwa.

Kierownik jednostki organizacyjnej jest obowiązany zapewnić bezpieczeństwo systemom i sieciom teleinformatycznym przed przystąpieniem do wytwarzania, przechowywania, przetwarzania lub przekazywania informacji niejawnych stanowiących tajemnicę państwową lub służbową w tych systemach lub sieciach.

Bezpieczeństwem teleinformatycznym nazywamy wszystkie zagadnienia związane z bezpieczeństwem systemów i sieci teleinformatycznych w których wytwarzane, przetwarzane, przechowywane lub przesyłane są informacje niejawne. Wszystkie zagadnienia związane z bezpieczeństwem teleinformatycznym są ściśle związane z szeroko rozumianą ochroną informacji niejawnych.

Bezpieczeństwo *systemu* lub *sieci teleinformatycznej* (bezpieczeństwo teleinformatyczne) zapewnia się poprzez przedsięwzięcia realizowane w następujących obszarach:

OCHRONA FIZYCZNA

Ochronę fizyczną systemu lub sieci teleinformatycznej wytwarzającej, przetwarzającej, przechowującej lub przekazującej informacje niejawne stanowiące tajemnice państwową lub służbową stosuje się w celu uniemożliwienia dostępu do systemów i sieci teleinformatycznych przez osoby nieuprawnione.

Ochronę fizyczną systemu lub sieci teleinformatycznej wytwarzającej, przetwarzającej, przechowującej lub przekazującej informacje niejawne stanowiące tajemnice państwową lub służbową zapewnia się przez:

- umieszczenie urządzeń systemu lub sieci teleinformatycznej w odpowiednich strefach bezpieczeństwa w zależności od:
  - klauzuli tajności wytwarzanych, przetwarzanych, przechowywanych lub przekazywanych w systemie lub sieci teleinformatycznej informacji niejawnych;
  - ilości wytwarzanych, przetwarzanych, przechowywanych lub przekazywanych w systemie lub sieci teleinformatycznej informacji niejawnych;
  - zagrożeń w zakresie ujawnienia, utraty, modyfikacji przez osobę nieuprawnioną wytwarzanych, przetwarzanych, przechowywanych lub przekazywanych w systemie lub sieci teleinformatycznej informacji niejawnych;
- instalację środków zabezpieczających pomieszczenia, w których znajdują się urządzenia systemu lub sieci teleinformatycznej wytwarzającej, przetwarzającej, przechowującej lub przekazującej informacje niejawne stanowiące tajemnice państwową lub służbową, przed:
  - nieuprawnionym dostępem;
  - podglądem;
  - podsłuchem.

Wytwarzanie, przetwarzanie, przechowywanie lub przekazywanie w systemie lub sieci teleinformatycznej informacji niejawnych, stanowiących tajemnicę państwową lub tajemnicę służbową, oznaczonych klauzulą „*poufne*" w urządzeniach systemu lub sieci teleinformatycznych odbywa się w strefach bezpieczeństwa.

OCHRONA ELEKTROMAGNETYCZNA

Ochronę elektromagnetyczną systemu lub sieci teleinformatycznej wytwarzającej, przetwarzającej, przechowującej lub przekazującej informacje niejawne stanowiące tajemnice państwową lub służbową stosuje się w celu uniemożliwienia przejęcia informacji zawartej w ubocznym promieniowaniu elektromagnetycznym urządzeń wytwarzających, przetwarzających, przechowujących i przesyłających informacje niejawne.

Ochronę elektromagnetyczną systemu lub sieci teleinformatycznej wytwarzającej, przetwarzającej, przechowującej lub przekazującej informacje niejawne stanowiące tajemnice państwową lub służbową, zapewnia się przez:

- umieszczenie urządzeń wytwarzających, przetwarzających, przechowujących lub przekazujących informacje niejawne, połączeń transmisyjnych, linii zasilających i sygnałowych w strefach bezpieczeństwa gwarantujących spełnienie wymagań zabezpieczenia elektromagnetycznego;
- zastosowanie urządzeń wytwarzających, przetwarzających, przechowujących lub przekazujących informacje niejawne, połączeń transmisyjnych, linii zasilających i sygnałowych o obniżonym poziomie emisji;
- ekranowanie urządzeń wytwarzających, przetwarzających, przechowujących lub przekazujących informacje niejawne oraz filtrowanie zewnętrznych linii zasilających i sygnałowych.

OCHRONA KRYPTOGRAFICZNA

Ochronę kryptograficzną systemu lub sieci teleinformatycznej wytwarzającej, przetwarzającej, przechowującej lub przekazującej informacje niejawne stanowiące tajemnice państwową lub służbową stosuje się w celu utrudnienia przejęcia informacji poprzez ich przekształcenie w sposób znany tylko upoważnionemu użytkownikowi.

Przekazanie informacji niejawnych stanowiących tajemnicę państwową (powyżej klauzuli „*poufne*") za pośrednictwem systemów i sieci teleinformatycznych, które składają się z certyfikowanych urządzeń i narzędzi kryptograficznych, może nastąpić pod warunkiem zastosowania kryptograficznych metod i środków ochrony, dopuszczonych do eksploatacji na podstawie szczególnych wymagań bezpieczeństwa.

Ochrona kryptograficzna systemu lub sieci teleinformatycznej polega na stosowaniu metod i środków zabezpieczających informacje niejawne stanowiące tajemnicę państwową przez:

- szyfrowanie informacji niejawnych;
- stosowanie innych mechanizmów kryptograficznych gwarantujących integralność i zabezpieczenie przed nieuprawnionym ujawnieniem tych informacji;
- uwierzytelnienie podmiotów;
- uwierzytelnienie informacji.

Do kryptograficznej ochrony informacji niejawnych stanowiących tajemnicę państwową stosuje się, odpowiednie dla klauzuli „*tajne*" i „*ściśle tajne*", algorytmy kryptograficzne oraz środki gwarantujące ochronę tych algorytmów, kluczy kryptograficznych oraz innych istotnych parametrów zabezpieczenia, a w szczególności haseł dostępu.

BEZPIECZEŃSTWO TRANSMISJI

Bezpieczeństwo transmisji systemu lub sieci teleinformatycznej wytwarzającej, przetwarzającej, przechowującej lub przekazującej informacje niejawne stanowiące tajemnice państwową lub służbową stosuje się w celu utrudnienia rozpoznania sieci teleinformatycznej.

Bezpieczeństwo transmisji systemu lub sieci teleinformatycznej wytwarzającej, przetwarzającej, przechowującej lub przekazującej informacje niejawne stanowiące tajemnice państwową lub służbową, zapewnia się przez:

podłączenie urządzenia systemu lub sieci teleinformatycznej, w którym są wytwarzane, przetwarzane, przechowywane lub przekazywane informacje niejawne stanowiące tajemnicę państwową, do powszechnie dostępnego urządzenia systemu lub sieci jest dopuszczalne pod warunkiem zastosowania metod i środków ochrony kryptograficznej:

- szyfrowanie informacji niejawnych;
- stosowanie innych mechanizmów kryptograficznych gwarantujących integralność i zabezpieczenie przed nieuprawnionym ujawnieniem tych informacji;

- uwierzytelnienie podmiotów;
- uwierzytelnienie informacji.

Podłączenie urządzenia systemu lub sieci teleinformatycznej, w którym są wytwarzane, przetwarzane, przechowywane lub przekazywane informacje niejawne stanowiące tajemnicę służbową, do powszechnie dostępnego urządzenia systemu lub sieci jest dopuszczalne pod warunkiem zastosowania właściwych mechanizmów kontroli dostępu.

KONTROLA DOSTĘPU

Kontrolę dostępu do systemu lub sieci teleinformatycznej wytwarzającej, przetwarzającej, przechowującej lub przekazującej informacje niejawne stanowiące tajemnice państwową lub służbową stosuje się w celu uniemożliwienia dostępu do systemów i sieci teleinformatycznych oraz zasobów informacyjnych przez osoby nieuprawnione.

- kierownik jednostki organizacyjnej określa warunki i sposób przydzielania uprawnień ich użytkownikom;
- administrator systemów i sieci teleinformatycznych określa warunki oraz sposób przydzielania tym użytkownikom kont i haseł, a także zapewnia właściwe wykorzystanie mechanizmów kontroli dostępu do systemu lub sieci teleinformatycznej odpowiednio do klauzuli tajności informacji.

System lub sieć teleinformatyczną wyposaża się w mechanizmy kontroli dostępu odpowiednie do klauzuli tajności informacji niejawnych wytwarzanych, przetwarzanych, przechowanych lub przekazywanych w tych systemach lub sieciach.

System lub sieć teleinformatyczna, w której są wytwarzane, przetwarzane, przechowywane lub przekazywane informacje niejawne stanowiące tajemnicę państwową, projektuje się, organizuje i eksploatuje w sposób uniemożliwiający niekontrolowany dostęp jednej osoby do wszystkich zasobów systemu lub sieci, a w szczególności do danych, oprogramowania i urządzeń[82].

[82] *Rozporządzeniu Prezesa Rady Ministrów* z dnia 25 lutego 1999 r. w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych.(*Dz. U. Nr 18, poz. 162*).

2.4.3. Rola krajowych władz bezpieczeństwa i służb ochrony państwa w zakresie ochrony informacji niejawnych

Rola i miejsce służb specjalnych w III RP były jednymi z najważniejszych problemów przemian demokratycznych, które dokonały się po roku 1989. Wraz z przemianami politycznymi, które przekształciły Polskę z państwa autokratycznego w państwo demokratyczne musiała ulec zmianie rola służb specjalnych, zakres zadań które miały realizować i uprawnienia, które posiadały oraz ich organizacja. Formułowane przez ówczesnych polityków koncepcje przewidywały różne możliwości rozwiązania problemu służb specjalnych. Jedni uważali, że należy je całkowicie rozwiązać, gdyż są zbyt mocno związane z poprzednim systemem politycznym aby je reformować, inni uważali, że należy je pozostawić, dokonując głębokich zmian kadrowych. Ostatecznie przyjęte rozwiązania charakteryzowały się poważną weryfikacją kadr, szczególnie zajmujących kierownicze stanowiska oraz powołaniem nowych struktur organizacyjnych.

Podstawowym zadaniem *służb ochrony państwa* jest sprawowanie nadzoru nad funkcjonowaniem *systemu ochrony informacji niejawnych*. Służby ochrony państwa są powołane do szkolenia i doradztwa, a także przeprowadzania kontroli wprowadzonych rozwiązań i przestrzegania przepisów w zakresie bezpieczeństwa informacji niejawnych.

Zgodnie z art. 2 pkt 3 *Ustawy o Ochronie Informacji Niejawnych* z dnia 22 stycznia 1999 r. *służbami ochrony państwa* w Rzeczypospolitej Polskiej są:

- ***Agencja Bezpieczeństwa Wewnętrznego;***
- ***Wojskowe Służby Informacyjne.***

Zadania *służb ochrony państwa*, na podstawie art. 14 pkt. 1 *Ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych* obejmują:

- kontrolę ochrony informacji niejawnych oraz kontrolę przestrzegania przepisów wydanych w tym zakresie,
- **realizację zadań w zakresie bezpieczeństwa systemów i sieci teleinformatycznych,**
- prowadzenie postępowania sprawdzającego,
- ochronę informacji niejawnych wymienianych przez Rzeczpospolitą Polską z innymi państwami i organizacjami międzynarodowymi,

- szkolenie i doradztwo w zakresie ochrony informacji niejawnych,
- wykonywanie innych zadań, w zakresie ochrony informacji niejawnych, określonych odrębnymi przepisami.

Jak widać, do ustawowych zadań *służb ochrony państwa* należy m.in. zapewnienie bezpieczeństwa systemów i sieci teleinformatycznych, w których są wytwarzane, przechowywane, przetwarzane lub przekazywane informacje niejawne stanowiące tajemnicę państwową lub służbową.

Ogólny podział kompetencji pomiędzy *służby ochrony państwa* przebiega po linii rozgraniczającej sferę cywilną od sfery wojskowej. Dla sfery cywilnej służbą ochrony państwa jest *Agencja Bezpieczeństwa Wewnętrznego*, dla sfery wojskowej są *Wojskowe Służby Informacyjne*. Trudność sprawia określenie przebiegu linii rozgraniczającej, gdyż w Ustawie... nie ma jednoznacznych zapisów określających rozdział kompetencji w zakresie ochrony informacji niejawnych pomiędzy *Agencją Bezpieczeństwa Wewnętrznego* a *Wojskowymi Służbami Informacyjnymi*. Można domyślnie wytyczyć linię rozgraniczającą, opierając się na art. 29 Ustawy... dotyczącym właściwości służb ochrony państwa do przeprowadzania postępowań sprawdzających. Zgodnie z tym artykułem, kompetencje *Wojskowych Służb Informacyjnych* związane z ochroną informacji niejawnych, w tym z bezpieczeństwem teleinformatycznym, obejmują:

- Siły Zbrojne i jednostki organizacyjne podległe *Ministrowi Obrony Narodowej*;
- jednostki organizacyjne nadzorowane przez *Ministra Obrony Narodowej*;
- przedsiębiorstwa, jednostki naukowe lub badawczo-rozwojowe, których organem założycielskim jest *Minister Obrony Narodowej*, a także inne jednostki organizacyjne, w zakresie w jakim realizują one produkcję lub usługi, stanowiące tajemnicę państwową ze względu na obronność państwa i na potrzeby *Sił Zbrojnych*;
- przedsiębiorstwa zajmujące się obrotem wyrobami, technologiami i licencjami objętymi tajemnicą państwową ze względu na obronność państwa, jeżeli uczestnikami tego obrotu są Siły Zbrojne lub jednostki organizacyjne podległe *Ministrowi Obrony Narodowej*
- wojskowe organy ochrony prawa i wojskowe organy porządkowe.

W pozostałych przypadkach kompetencje należą do *Agencji Bezpieczeństwa Wewnętrznego*. Szczegółowy rozdział kompetencji w ramach realizacji swoich zadań pomiędzy *Agencję Bezpieczeństwa Wewnętrznego* i *Wojskowe Służby Informacyjne* zobowiązany jest określić Prezes Rady Ministrów w drodze zarządzenia, na mocy art. 42 pkt. 2 *Ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu*. Zarządzenie to dotychczas nie zostało wydane. Jednocześnie ww. ustawa w art. 42 ust. 1 nakłada na szefów obydwu organów obowiązek współdziałania w ramach realizacji swoich zadań.

Wojskowe Służby Informacyjne zostały powołane do życia rozkazem Ministra Obrony Narodowej w 1991 r. Nastąpiło to w skutek połączenia wywiadu i kontrwywiadu wojskowego. Jednocześnie WSI zostały podporządkowane bezpośrednio Ministrowi Obrony Narodowej. Prawnym oparciem tej decyzji organizacyjnej był przepis art. 2 ustawy z dnia 6 kwietnia 1990 r. o Urzędzie Ochrony Państwa,[83] ustalający, że zadania przewidziane dla UOP wykonują także „służby wywiadu i kontrwywiadu podległe Ministrowi Obrony Narodowej". W 1994 r. nastąpiło przejściowe podporządkowanie WSI Szefowi Sztabu Generalnego Wojska Polskiego i w tym samym roku ponownie powróciły pod bezpośrednią zwierzchność Ministra Obrony Narodowej[84].

Konstytutywnym dla WSI przepisem prawnym stał się art. 15 ustawy o powszechnym obowiązku obrony RP, wprowadzony ustawą nowelizującą z dnia 25 października 1991 r.[85] Ustawodawca nie przyjął wówczas nazwy własnej służb, ale posłużył się ogólnym określeniem „*wojskowe służby informacyjne*." Pod nazwą własną *WSI* pojawiły się w ustawodawstwie dopiero w przepisach ustawy z dnia 8 sierpnia 1996 r. w związku z dokonywaną nowelizacją ustawy o UOP[86], które zdefiniowały równocześnie pojęcie „*służby specjalne*", zaliczając do nich obok *UOP* także *WSI*.

---

[83] *Ustawa z dnia 6 kwietnia 1990 r. o Urzędzie Ochrony Państwa (Dz. U. nr 30, poz.180).*
[84] S. Zalewski, *Służby specjalne w państwie demokratycznym*. Warszawa 2002, s.47.
[85] *Ustawa z dnia 21.11.1967 r. o powszechnym obowiązku obrony RP (Dz. U. 92.4.16). „Wojskowe służby informacyjne wykonują zadania związane z rozpoznawaniem i przeciwdziałaniem zagrożeniom godzącym w obronność Państwa oraz naruszeniom tajemnicy państwowej w zakresie obronności jak również przygotowują dla organów państwowych informacje i analizy istotne dla obronności Państwa."*
[86] *Dz. U. Nr 106, poz. 496 art. 34 pkt* 1.

Ważnym uregulowaniem prawnym dotyczącym statusu *WSI* był przepis art. 5 pkt. 1 *ustawy z dnia 14 grudnia 1995 r. o urzędzie Ministra Obrony Narodowej*[87]. Przepis ten ustawowo usankcjonował rozwiązanie przyjęte przy tworzeniu *WSI*, dokonując bezpośredniego podporządkowania *WSI* Ministrowi Obrony Narodowej.

Spośród aktów prawnych o charakterze wykonawczym ważnym dla działalności WSI w okresie sprzed wejścia w życie *ustawy o WSI* należy wymienić:

- *Rozporządzenie Rady Ministrów z dnia 9 lipca 1996 r. w sprawie szczegółowego zakresu działania Ministra Obrony Narodowej.*[88] Jego przepis § 1 pkt 16 powierza Ministrowi Obrony Narodowej sprawowanie nadzoru na działalnością *WSI „w tym zwłaszcza nad działalnością operacyjno-rozpoznawczą"*;

- *Uchwała Rady Ministrów nr 42 z dnia 16 czerwca 1998 r.* (niepublikowana) sprecyzowała, że Szef *WSI* wykonuje funkcję *Krajowej Władzy Bezpieczeństwa* w sprawach współpracy międzynarodowej w zakresie spraw wojskowych;

- *Decyzja Ministra Obrony Narodowej nr 165/MON z dnia 7 września 1999 r.* w sprawie realizacji w resorcie obrony narodowej zadań wynikających z ustawy o ochronie informacji niejawnych - szefowi *WSI* powierzone zostało zadanie nadzoru nad działaniami w tym zakresie.

Istotnego wzmocnienia i ugruntowania statusu *WSI* dokonały przepisy *Ustawy o Ochronie Informacji Niejawnych* z dnia 22 stycznia 1999 r.[89] Ustanowiły one *WSI* obok *UOP „służbą ochrony państwa"*, zaś szefowi *WSI*, obok szefa *UOP*, powierzyły pełnienie funkcji *„krajowych władz bezpieczeństwa w stosunkach międzynarodowych"*. Zakres właściwości *WSI* został pośrednio, lecz zgodnie z konstytutywnym art. 15 ust. 1 ustawy o powszechnym obowiązku obrony RP określony w art. 29 ustawy o ochronie informacji niejawnych jako odpowiedni w sprawach obronności.

Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu[90] stała się kolejną podstawą prawną do działalności *WSI*. Na podstawie art. 3 ustawy, działalność powołanych agencji oraz *WSI* została poddana

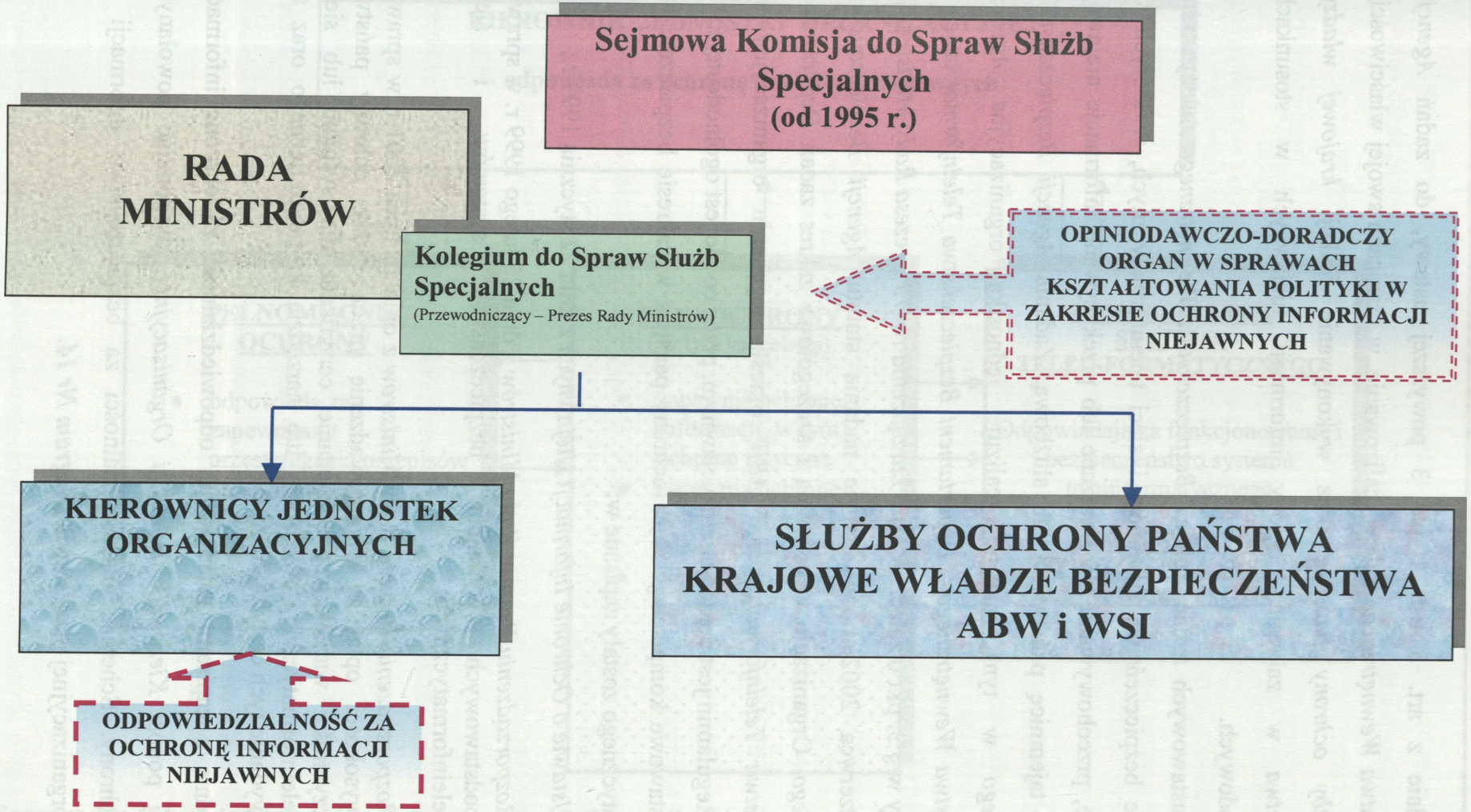
[87] *Ustawa z dnia 14 grudnia 1995 r. o urzędzie Ministra Obrony Narodowej (Dz. U. z 1996 r. nr 10, poz. 56 z późn. zm.).*
[88] *Rozporządzenie Rady Ministrów z dnia 9 lipca 1996 r. w sprawie szczegółowego zakresu działania Ministra Obrony Narodowej (Dz. U. nr 94, poz. 426).*
[89] *Ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (DZ. U. nr 11, poz. 95).*
[90] *Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. nr 74 poz. 676).*

kontroli Sejmu RP. Na mocy art. 11 służby specjalne miały być nadzorowane przez *Kolegium do Spraw Służb Specjalnych przy Radzie Ministrów* - ***Diagram Nr 13***.

Po trwających z przerwami 12 latami prac znalazła się wola polityczna do wprowadzenia racjonalnych rozwiązań w zakresie właściwości, usytuowania w strukturach wojskowych i państwowych oraz nadania odpowiednich narzędzi prawnych *WSI* warunkujących realizację przez nie zadań i w dniu 9 lipca 2003 r. Sejm RP uchwalił *Ustawę o Wojskowych Służbach Informacyjnych.*[91]

W odniesieniu do służb ochrony państwa sfery wojskowej - *Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu*, w art. 3 ust. 2 określa, że szef *Agencji Bezpieczeństwa Wewnętrznego* podlega bezpośrednio Prezesowi Rady Ministrów.

[91] *Ustawa z dnia 9 lipca 1003 r. o Wojskowych Służbach Informacyjnych (Dz. U. nr 139. poz. 1326).*



Źródło: opracowanie własne

Diagram 13: ***Schemat organizacji ochrony informacji niejawnych w Rzeczypospolitej Polskiej***

Zgodnie z art. 5 ust. 1 pkt 3 powyższej ustawy, do zadań *Agencji Bezpieczeństwa Wewnętrznego* należy realizowanie, w granicach swojej właściwości, zadań *służby ochrony państwa* oraz wykonywanie funkcji *krajowej władzy bezpieczeństwa* w zakresie ochrony informacji niejawnych w stosunkach międzynarodowych.

Do ustawowych zadań *Agencji Bezpieczeństwa Wewnętrznego* należy m.in. zapewnienie bezpieczeństwa systemów i sieci teleinformatycznych, w których są wytwarzane, przechowywane, przetwarzane lub przekazywane informacje niejawne stanowiące tajemnicę państwową lub służbową. Zadania *Agencji Bezpieczeństwa Wewnętrznego* w tym zakresie realizuje jednostka organizacyjna *Agencji Bezpieczeństwa Wewnętrznego - Departament Bezpieczeństwa Teleinformatycznego*, wymieniony w § 3. pkt 6 załącznika do *Zarządzenia Nr 73 Prezesa Rady Ministrów* z dnia 26 czerwca 2002 r. w sprawie nadania statutu *Agencji Bezpieczeństwa Wewnętrznego*. Organizację wewnętrzną i szczegółowy zakres zadań *Departament Bezpieczeństwa Teleinformatycznego ABW* określa regulamin organizacyjny tej jednostki. Regulamin jest dokumentem niejawnym, przez co nie jest ogólnodostępny.

Podstawowe kompetencje służb ochrony państwa w zakresie bezpieczeństwa teleinformatycznego zostały zapisane w:

- *Ustawie o Ochronie Informacji Niejawnych* z dnia 22 stycznia 1999 r.;
- *Rozporządzeniu Prezesa Rady Ministrów* z dnia 25 lutego 1999 r. w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych;
- *Rozporządzeniu Prezesa Rady Ministrów* z dnia 16 lipca 2001 r. w sprawie wysokości opłat za przeprowadzenie przez służbę ochrony państwa czynności warunkujących wydanie certyfikatu dla systemu lub sieci teleinformatycznej, urządzenia lub narzędzia kryptograficznego oraz za wydanie tych certyfikatów.

Zgodnie z zapisami ustawowymi odpowiedzialność za ochronę informacji niejawnych ponosi *Kierownik Jednostki Organizacyjnej*, dysponując powołanym pionem ochrony. Schemat odpowiedzialności za bezpieczeństwo informacji w jednostce organizacyjnej przedstawia ***Diagram Nr 14***.

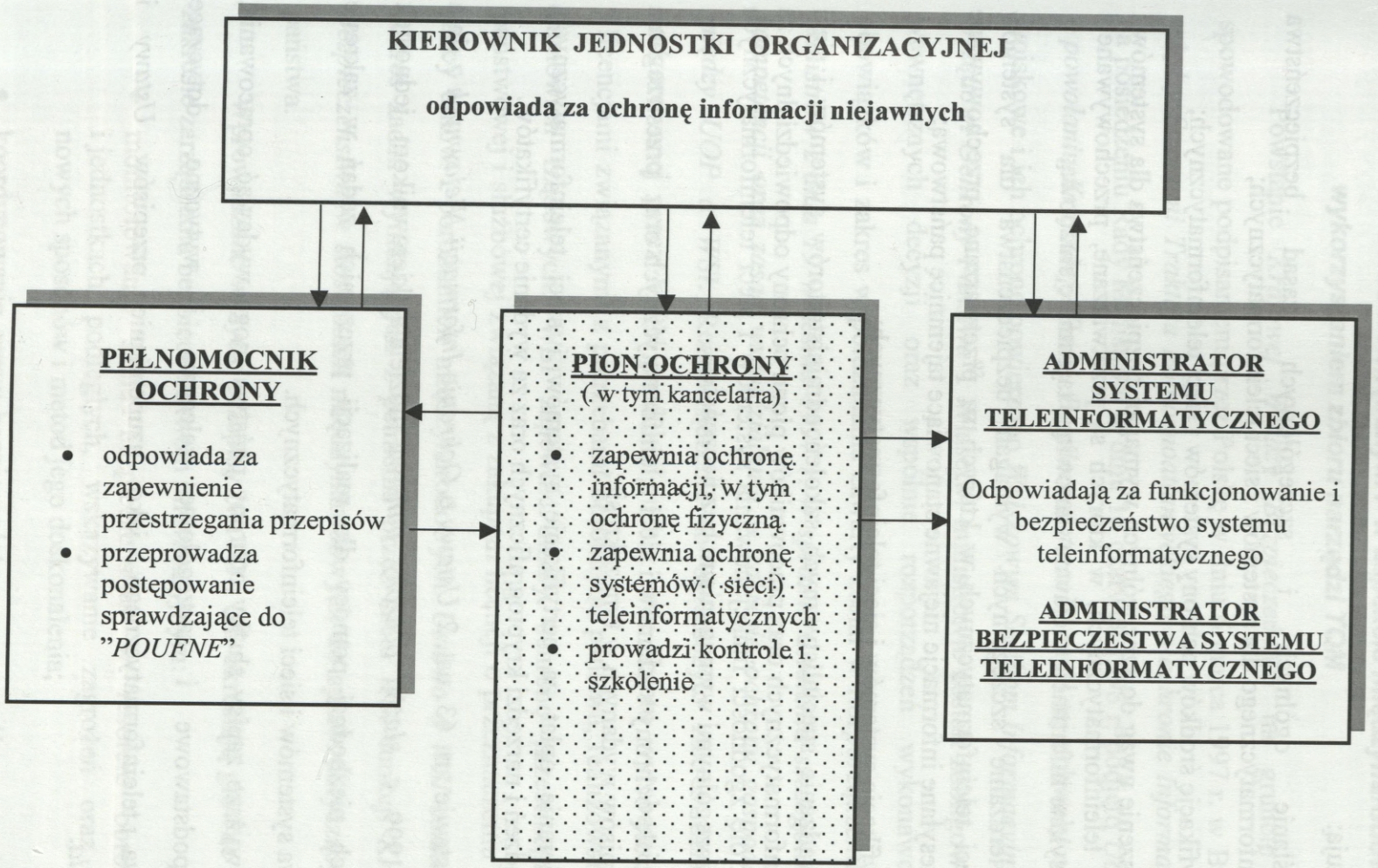


Diagram 14: ***Odpowiedzialność za bezpieczeństwo informacji niejawnych w jednostce organizacyjnej***

Źródło: opracowanie własne

Na podstawie powyższych dokumentów prawnych kompetencje służb ochrony państwa obejmują:

- określanie ogólnych i szczegółowych zasad bezpieczeństwa teleinformatycznego dla systemów i sieci teleinformatycznych;
- certyfikację środków ochrony systemów i sieci teleinformatycznych;
- wnoszenie uwag do szczególnych wymagań bezpieczeństwa dla systemów i sieci teleinformatycznych, w których są przetwarzane, przechowywane i przesyłane informacje niejawne stanowiące tajemnicę służbową;
- zatwierdzanie szczególnych wymagań bezpieczeństwa dla systemów i sieci teleinformatycznych w których są przetwarzane, przechowywane i przesyłane informacje niejawne stanowiące tajemnicę państwową;
- certyfikacja systemów i sieci teleinformatycznych;
- prowadzenie specjalistycznych szkoleń administratorów systemów i sieci teleinformatycznych oraz pracowników pionu ochrony odpowiedzialnych za kontrolę zgodności funkcjonowania systemów i sieci teleinformatycznych ze szczególnymi wymaganiami bezpieczeństwa;
- kontrolę ochrony systemów i sieci teleinformatycznych oraz przestrzegania przepisów wydanych w tym zakresie;
- pobieranie opłat za certyfikację systemów i sieci teleinformatycznych, urządzeń i narzędzi kryptograficznych oraz za wydanie certyfikatów.

Na podstawie art. 63. ust. 2 *Ustawy o Ochronie Informacji Niejawnych* z dnia 22 stycznia 1999 r. *służby ochrony państwa* udzielają kierownikom jednostek organizacyjnych niezbędnej pomocy dla realizacji przez nich zadań w zakresie bezpieczeństwa systemów i sieci teleinformatycznych.

Realizując powyższe zapisy służby ochrony państwa mogą wydawać opracowania, stanowiące podstawowe i szczegółowe zalecenia i wytyczne, dotyczące bezpieczeństwa teleinformatycznego, jako uzupełnienie przepisów *Ustawy* i *Rozporządzenia*.

2.4.4. Zarządzanie bezpieczeństwem informacyjnym państwa w obszarze wewnętrznym i w aspekcie międzynarodowym z wykorzystaniem zbioru narzędzi TQM

Powstanie *Krajowej Władzy Bezpieczeństwa* na gruncie polskim było spowodowane podpisaniem przez Polskę w dniu 6 marca 1997 r. w Brukseli, *Umowy między Stronami Traktatu Północnoatlantyckiego o ochronie informacji*[92]. Następnie na posiedzeniu Rady Ministrów w dniu 16 czerwca 1998 r. podjęto *Uchwałę nr 42/98 o powołaniu Krajowej Władzy Bezpieczeństwa*. W myśl tej uchwały niejawne sprawy wojskowe i ich ochronę powierzono *Wojskowym Służbom Informacyjnym*, pozostałe - *Urzędowi Ochrony Państwa*[93]. Właściwi ministrowie zostali zobligowani do wydania wewnętrznych decyzji oraz wspólnie rozporządzeń wykonawczych. Podział obowiązków i zakres współdziałania zawarty został w *Rozporządzeniu Prezesa Rady Ministrów z dnia 19 września 1997 r. w sprawie ustalenia szczegółowego rozdziału kompetencji oraz zasad współdziałania w zakresie ochrony gospodarki narodowej między UOP a WSI*. Rozporządzenie to ograniczyło zakres działania WSI do nadzorowanej przez MON produkcji, usług oraz obrotu wyrobami, technologiami i licencjami związanymi z potrzebami obronnymi państwa, realizowanymi w ramach zamówień rządowych. WSI zapewnić miały ochronę przestrzegania tajemnicy państwowej i służbowej związaną z zakupem licencji o przeznaczeniu wojskowym na mocy umów i porozumień międzynarodowych. *Ustawa o WSI* ostatecznie określiła zakres zadań wynikających z pełnienia przez szefa *WSI* funkcji *Krajowej Władzy Bezpieczeństwa* w stosunkach międzynarodowych do spraw dotyczących obronności państwa.

Wprowadzane w życie przepisy NATO i UE określają główne zadania *WSI* w zakresie zarządzania bezpieczeństwem informacyjnym:

- monitorowanie stanu bezpieczeństwa w resorcie obrony narodowej i jednostkach podległych, wskazywanie zagrożeń oraz wypracowanie nowych sposobów i metod jego doskonalenia;
- koordynowanie spraw bezpieczeństwa oraz współpraca z *ABW* jako drugą *KWB* w Polsce;

---

[92] *Umowa między stronami Traktatu Północnoatlantyckiego o ochronie informacji (Dz. U. 00.64.740)*.

[93] *Ustawa z dnia 24 maja 2002 r. o ABW oraz AW* mocą art. 221 zniosła *UOP*, a zadania *KWB* na mocy art. 5 ust. 1 pkt 3 zostały przypisane *ABW*.

- przetwarzanie decyzji *Biura Bezpieczeństwa NATO* i UE w zakresie bezpieczeństwa w sprawach dotyczących obronności na dyrektywy krajowe;
- informowanie *Biura Bezpieczeństwa NATO* i UE na temat stanu bezpieczeństwa w resorcie obrony narodowej;
- przeprowadzanie okresowych kontroli systemów bezpieczeństwa służących ochronie informacji niejawnych NATO i UE;
- prowadzenie postępowań w sprawach dotyczących naruszenia bezpieczeństwa informacji niejawnych NATO i UE celem ustalenia wszystkich okoliczności, oceny i minimalizacji skutków oraz powiadamianie odpowiednich władz o tych zdarzeniach;
- określanie środków bezpieczeństwa i zapewnienie ich właściwego stosowania we wszystkich jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej;
- uczestniczenie przedstawiciela *KWB* w spotkaniach *Komitetu Bezpieczeństwa NATO* i UE.

Wojskowe Służby Informacyjne zadania *KWB* realizują w zakresie bezpieczeństwa osobowego, fizycznego, informacyjnego oraz przemysłowego.

Zadaniem *WSI* w zakresie bezpieczeństwa osobowego jest realizowanie specjalnych procedur sprawdzeniowych wobec osób z resoru obrony narodowej, które będą upoważnione do dostępu do informacji niejawnych NATO i UE oraz otrzymają po ich przeprowadzeniu stosowne *certyfikaty bezpieczeństwa* (NATO) i *poświadczenia bezpieczeństwa* (UE). Problem bezpieczeństwa osobowego jest kluczowy, gdyż czynnik ludzki jest najsłabszym ogniwem w systemie ochrony informacji niejawnych[94]. Zakres prowadzonego postępowania sprawdzającego zależy od klauzuli informacji klasyfikowanych, do których dana osoba będzie miała dostęp. Wydanie decyzji potwierdzającej, że dana osoba spełnia warunki bezpieczeństwa, nie stanowi zakończenia działań w zakresie bezpieczeństwa osobowego. Prowadzona jest weryfikacja, czy osoba wciąż spełnia określone wymogi. Certyfikat (poświadczenie) bezpieczeństwa może zostać cofnięty jeżeli *WSI* otrzymają sygnał, mogący świadczyć o braku lojalności czy rzetelności danej osoby. Cofnięcie certyfikatu (poświadczenia)

[94] Istnieje pogląd, że około 80-90% informacji niejawnych wypływa za pośrednictwem pracowników organizacji. Por.: *Ochrona informacji niejawnych...*, op. cit., s. 67.

wyklucza możliwość dalszego zatrudniania osoby na stanowisku wymagającym dostępu do informacji klasyfikowanych NATO lub UE.

Zapewnienie bezpieczeństwa fizycznego polega przede wszystkim na wypracowaniu i wdrażaniu przez *WSI* zasad skutecznego zapobiegania uzyskaniu dostępu osób nieupoważnionych do informacji niejawnych w resorcie obrony narodowej. W tym celu określa się strefy bezpieczeństwa, w których przechowywane są informacje niejawne NATO i UE oraz zapewniona jest im skuteczna kontrola. Stworzenie skutecznego systemu kontroli polega przede wszystkim na rejestrowaniu osób wchodzących i wychodzących ze stref najbardziej newralgicznych, wprowadzenie systemów alarmowych oraz stałego monitoringu wydzielonego obszaru. W dziedzinie bezpieczeństwa informacyjnego działalność *WSI* polega przede wszystkim na:

- zapewnieniu wykonania polityki bezpieczeństwa wobec systemów i sieci *Automatycznego Przetwarzania Danych (APD),* służących do przechowywania, przetwarzania i wymiany informacji niejawnych NATO w resorcie obrony narodowej;
- określeniu środków bezpieczeństwa dla systemów i sieci *APD*, zmierzających do zapobiegania ujawnianiu informacji, zmian jej treści bądź zniszczeniu materiału klasyfikowanego;
- przeprowadzaniu w resorcie obrony narodowej kontroli sieci i systemów informatycznych, w których przetwarza się informacje niejawne NATO;
- udzielaniu akceptacji dla sieci, systemów, urządzeń zabezpieczających oraz innego sprzętu telekomunikacyjnego i elektronicznego w resorcie obrony narodowej na podstawie certyfikacji tych urządzeń.

Realizacja tych zadań odbywa się przez powołaną przez Ministra Obrony Narodowej *Jednostkę Certyfikującą Wyroby*.

Zapewnienie bezpieczeństwa przemysłowego polega na zapewnieniu bezpieczeństwa informacji i materiałów klasyfikowanych NATO i UE w podmiotach gospodarczych uczestniczących w przedsięwzięciach związanych z obronnością państwa. Wynika to z podpisanych przez Polskę porozumień o ochronie niejawnych informacji wojskowych. *WSI* odpowiadają w tym zakresie za:

- informowanie przemysłu powiązanego z resortem obrony narodowej o obowiązujących przepisach z zakresu ochrony informacji niejawnych i zapewnienie pomocy we wprowadzaniu ich w życie;
- określenie środków i metod ochrony informacji klasyfikowanych NATO i UE, monitorowanie przestrzegania przepisów w przemyśle;
- sprawdzanie i dokonywanie oceny podmiotu gospodarczego pod względem bezpieczeństwa osobowego, fizycznego i informacyjnego oraz wydawanie w tym zakresie świadectw bezpieczeństwa przemysłowego;
- egzekwowanie w przedsiębiorstwach wykorzystujących informacje niejawne NATO i UE wyznaczania osoby odpowiadającej za ich ochronę;
- wyjaśnianie i informowanie zainteresowanych państw członkowskich o wszelkich przypadkach zagubienia lub nieuprawnionego dostępu do informacji udostępnianych przez NATO i UE.

Szef Wojskowych Służb Informacyjnych dysponuje aparatem wykonawczym, który pozwala na realizację zadań z zakresu ochrony informacji niejawnych wynikających z pełnienia przez niego funkcji *Krajowej Władzy Bezpieczeństwa* dotyczących spraw obronności. Szef *WSI* uczestniczy również w posiedzeniach *Kolegium ds. Służb Specjalnych Rady Ministrów*, gdzie może przedstawiać problemy ochrony informacji niejawnych oraz zgłaszać propozycje działań doskonalących. Aparat którym dysponuje pozwala mu na specjalistyczną kontrolę przestrzegania ochrony informacji w różnych dziedzinach, np. fizycznej, teleinformatycznej. Posiadane siły umożliwiają szybkie tłumaczenie, analizę i wdrażanie dokumentów normatywnych zarówno NATO i UE. Ponadto, na mocy ustawy o *WSI*, ich szef, w celu realizacji zadań, ma prawo zawierania za zgodą Ministra Obrony Narodowej porozumień z właściwymi organami i służbami zarówno krajowymi jak i zagranicznymi.

Przedstawione powyżej uwarunkowania dotyczące ochrony informacji niejawnych przedstawiają obecny stan formalno-prawny w tym zakresie. Niewątpliwie członkostwo w NATO i integracja Polski z Unią Europejską będą powodowały ewolucję i dostosowywanie polskiego prawa w zakresie ochrony informacji niejawnych do ich standardów. Proces ten stworzy nowe uwarunkowania dla funkcjonowania w Polsce służb specjalnych, w tym *WSI*. Wiąże się to oczywiście z nowymi zadaniami przed którymi staną *WSI* jako *służba ochrony państwa*. Ich zakres,

w dużej mierze będzie zależny od zmieniających się relacji między państwami o różnych interesach narodowych, odmiennych potrzebach, różnym poziomie rozwoju oraz zróżnicowaniu kulturowym tworzących unię. Wymagać to będzie stosowania nowoczesnych narzędzi pomiaru i jakości działania.

Zbiorem narzędzi do wspomagania realizacji takich zadań jest *TQM* – omówione w ***Rozdziale 2.4.4*** *Kompleksowe Zarządzanie Jakością*. Przewodnią ideą tego zbioru narzędzi jest łańcuch stałego doskonalenia systemu-obiektu, zobrazowany jako tzw. *Cykl Deminga* na ***Diagramie Nr 15*** .

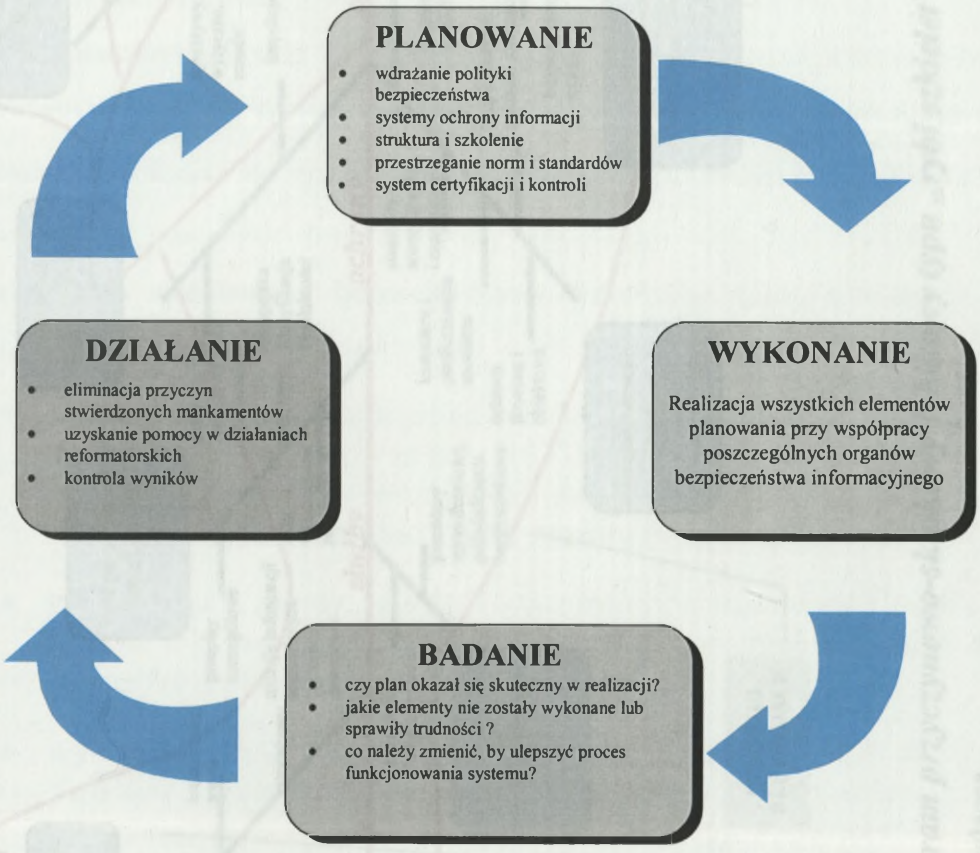


Diagram 15: ***Cykl Deminga***

Źródło: opracowanie własne

Szczególnie przydatnym narzędziem do nadania większej czytelności wskazanym parametrom decydującym o stanie bezpieczeństwa - jest *szczegółowa sieć działań*. Wzajemne powiązania wyszczególnionych parametrów narzucają wybór sieci typu pionowego. Pionowa sieć działań może stanowić narzędzie ciągłego doskonalenia przeanalizowanych procesów, będzie więc miała zastosowanie w końcowym etapie niniejszej rozprawy. Na podstawie przeglądu szczegółowej sieci działań, nadal korzystając z systemu TQM i jego narzędzi, można zdefiniować parametry będące przyczynami stanu systemu oraz te, które stanowią czynniki wpływające na ten stan. Narzędziem umożliwiającym przeprowadzenie tej procedury jest *diagram przyczynowo-skutkowy Ishikawy typu „rybi szkielet"*. Narzędzie to, w odniesieniu do bezpieczeństwa informacyjnego przedstawia ***Diagram Nr 16***.

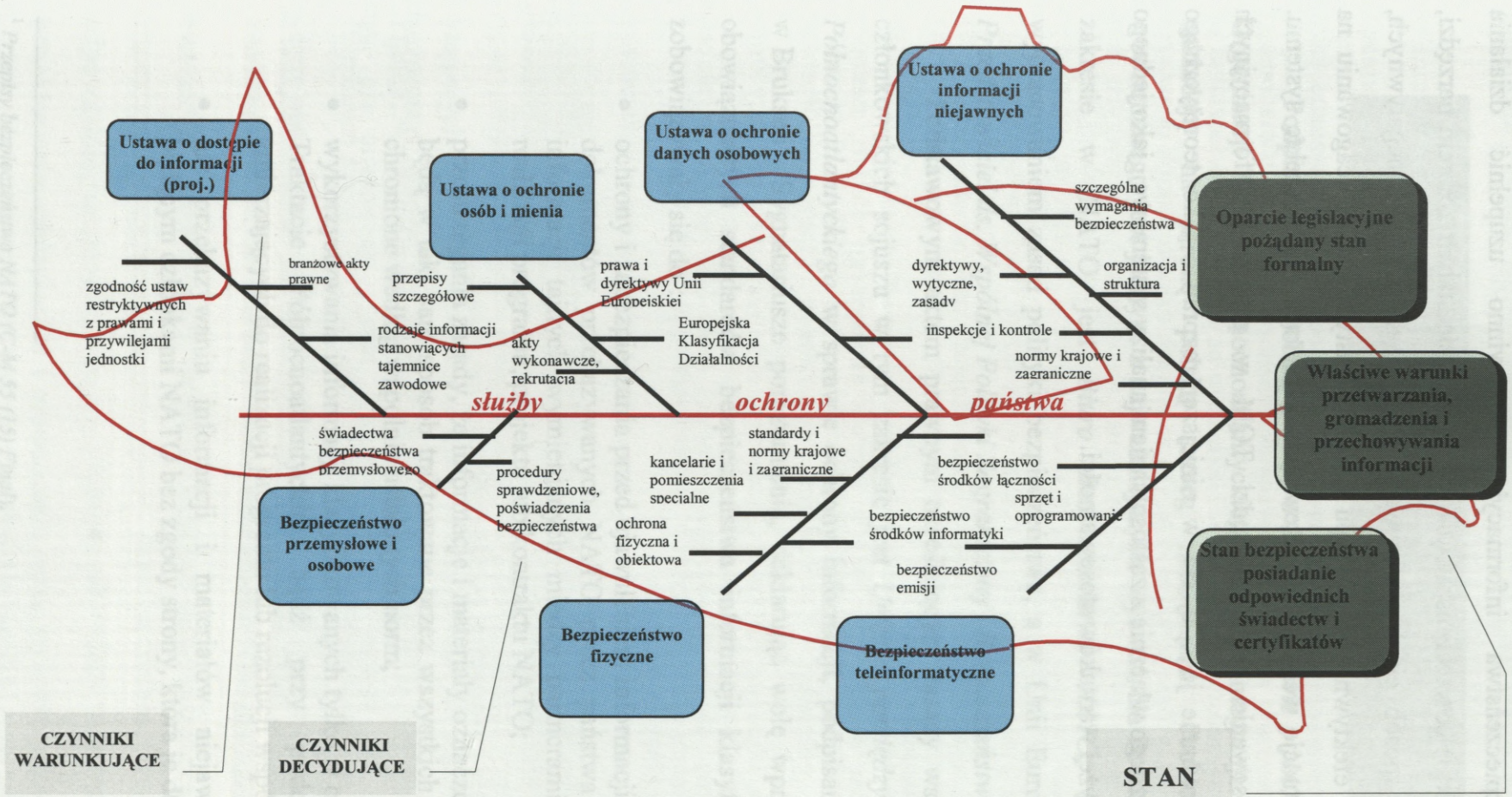


Diagram 16: ***Diagram przyczynowo-skutkowy Ishikawy typu „rybi szkielet" dot. systemu bezpieczeństwa informacyjnego***

Źródło: opracowanie własne

Zastosowanie zbioru narzędzi TQM w procesach zarządzania, kontroli i doskonalenia bezpieczeństwa informacyjnego powinno uzupełnić działania doskonalące ten sektor bezpieczeństwa państwa, stając się stałym zbiorem narzędzi, zapewniającym w sposób ciągły wykrywanie i eliminację zjawisk negatywnych, właściwą jakość i efektywność tego typu działań, elastyczność w reagowaniu na zmieniającą się sytuację wewnętrzną i zewnętrzną, bieżącą samo-korektę systemu. Wnioskowi o stosowanie zbioru narzędzi TQM w procesach informacyjnych towarzyszy konsekwentne jego ujęcie w niniejszej rozprawie jako teoretycznego „*szkieletu*" analitycznego włącznie z zastosowaniem analizy systemowej, jako jednego z wykazanych powyżej warunków stosowalności.

Rozdział 3

3. Standardy NATO i Unii Europejskiej w zakresie bezpieczeństwa informacyjnego

Podpisanie przez Polskę *Umowy o Bezpieczeństwie z NATO*, przystąpienie do Organizacji Traktatu Północnoatlantyckiego, a także integracja z Unią Europejską, nakładają na stronę polską szereg zobowiązań. Problem bezpieczeństwa wewnętrznego jest jednym z najważniejszych wyzwań dla Polski. Partnerem w tym zakresie w NATO jest *Biuro Bezpieczeństwa NATO*, które zajmuje się wypracowaniem zasad polityki bezpieczeństwa, a w Unii Europejskiej - *Wysokim Przedstawiciel ds. Wspólnej Polityki Zagranicznej i Bezpieczeństwa*.

Podstawowym aktem prawnym określającym zasady współdziałania krajów członkowskich sojuszu w tym zakresie jest *Umowa pomiędzy Stronami Traktatu Północnoatlantyckiego* w sprawie ochrony informacji, podpisana 6 marca 1997 r. w Brukseli[1]. Sygnatariusze porozumienia, deklarując wolę wprowadzenia w życie obowiązujących standardów bezpieczeństwa informacji klasyfikowanych NATO, zobowiązywały się do[2]:

- ochrony i zabezpieczania przed ujawnieniem informacji niejawnych NATO, dokumentów przekazywanych NATO przez państwa członkowskie oraz informacji tajnych wymienianych między partnerami sojuszu w ramach realizacji programu, projektu lub kontraktu NATO;
- przestrzegania zasady, że informacje i materiały oznaczone klauzulą tajności będą w taki sam sposób traktowane przez wszystkich członków sojuszu i chronione według wspólnie ustalonych norm;
- wykorzystywania informacji klasyfikowanych tylko w celach określonych w Traktacie Północnoatlantyckim bądź przy podejmowaniu decyzji zmierzających do realizacji programu lub rezolucji wspólnoty;
- nie przekazywaniu informacji i materiałów niejawnych stronom nie będącym członkami NATO bez zgody strony, która je dostarczyła;

[1] *Przepisy bezpieczeństwa NATO (C-M 55 (15) Final)*.
[2] *Ochrona informacji niejawnych...*, op. cit., s. 69.

- powołania *Krajowych Władz Bezpieczeństwa*, które wprowadzą w życie środki bezpieczeństwa, zapewniając jednolity system ochrony informacji niejawnych we wszystkich krajach członkowskich.[3].

Normy „*natowskie*" ściśle określają prawa dostępu do informacji i materiałów chronionych klauzulami tajności. Warunkiem dopuszczenia do informacji stanowiących tajemnice sojuszu jest stwierdzenie, że osoba, której przyznano takie prawo nie będzie stanowiła zagrożenia – wskutek świadomego bądź nieświadomego działania – dla bezpieczeństwa organizacji. Nakłada to na organy odpowiedzialne za ochronę informacji klasyfikowanych w NATO i w krajach członkowskich obowiązek uprzedniego sprawdzenia czy osoby dopuszczone do informacji niejawnych dają rękojmię zachowania tajemnicy, czy są godne zaufania i można im powierzyć tajemnice określone klauzulą tajności bez obawy ich utraty, bądź nieuprawnionego ujawnienia. Służyć temu mają procedury sprawdzające, prowadzone przez *KWB* według wspólnie ustalonych reguł[4].

Po podpisaniu w kwietniu 2003 r. traktatu akcesyjnego do UE, nastąpiła wymiana listów pomiędzy *Sekretarzem Generalnym Rady UE/Wysokim Przedstawicielem ds. Wspólnej Polityki Zagranicznej i Bezpieczeństwa*, na mocy której rząd RP zobowiązywał się do przestrzegania decyzji *Rady UE*, głównie w zakresie wymiany informacji klasyfikowanych.

3.1. Międzynarodowe standardy i normy bezpieczeństwa informacyjnego

3.1.1. Kryteria i procedury bezpieczeństwa informacyjnego

Na wstępie należy zwrócić uwagę, że wybierając do swoich zastosowań określony produkt lub system teleinformatyczny, należy zastanowić się nad następującymi problemami:

- w jakim stopniu może zapewnić on bezpieczeństwo dla eksploatowanych w instytucji zasobów;
- na jakiej podstawie można twierdzić, że wybór danego rozwiązania zapewni to bezpieczeństwo, zaś tak zabezpieczone zasoby będzie można wyeksponować w środowisku zagrożeń.

[3] *Art. 18 Przepisów bezpieczeństwa NATO (CM 55 (15) Final).*
[4] *CM (2002) 49, AC/35-D (2002).*

Można wskazać na trzecią możliwość, jaką może być korzystanie z ocen środków teleinformatycznych, przeprowadzonych przez niezależnych ekspertów, którzy posiadając niezbędną wiedzę, metodykę i potencjał, są w stanie ocenić produkt lub system - *„zmierzyć jego bezpieczeństwo"* - a ściślej określić poziom zaufania do niego. Zaufanie to nie może brać się znikąd – musi bowiem być uzasadnione, zaś wspomniane oceny – powtarzalne, niezależnie od tego, w jakim laboratorium byłyby prowadzone. Te i podobne stwierdzenia legły u podstaw opracowania metod niezależnej oceny zabezpieczeń, których podsumowaniem na dzień dzisiejszy wydają się być *Wspólne Kryteria do Oceny Zabezpieczeń Teleinformatycznych* (*CC - Common Criteria for Information Technology Security Evaluation*).

Bez niezależnej i wnikliwej oceny zabezpieczeń trudno jest sobie wyobrazić rozwój *technologii zaufania i poufności (Trust and Confidence Technologies)*, stanowiących podstawę rozwoju technologii społeczeństwa informacyjnego (*Information Society Technologies*), dlatego też prace w tej dziedzinie prowadzone są intensywnie – do tej pory oceniono już około 50 produktów lub systemów, ale wyłącznie w krajach przodujących w rozwoju technologii teleinformatycznych. Wejście do tego grona stanowi poważne wyzwanie, wymaga jednak sporych nakładów i wysiłków, w tym upowszechnienia wiedzy na ten temat wśród wszystkich potencjalnie zainteresowanych stron.

3.1.2. Standardy i normy bezpieczeństwa teleinformatycznego

Wspólne Kryteria opracowane zostały przez siedem organizacji rządowych – krajowych koordynatorów bezpieczeństwa teleinformatyki z Kanady, USA, Niemiec, Francji, Wielkiej Brytanii i Holandii, zwanych *Organizacjami Sponsorującymi Projekt Wspólnych Kryteriów*, które udzieliły praw niewyłącznych dla komitetu *ISO/IEC JTC1* celem opracowania normy *ISO/IEC 15408*. W 1999 roku stała się ona standardem *ISO (ISO/IEC-15408)*, zaś pierwszy i trzeci arkusz normy osiągnęły już status projektu PN.

W krajach przodujących pod względem rozwoju technologii teleinformatycznych trwają intensywne prace wdrożeniowe – organizowane są odpowiednio umocowane prawnie laboratoria oceny, rozwijana jest metodyka projektowania zabezpieczeń i prowadzenia ocen, wykonano już sporą liczbę ocen i podpisano pierwsze umowy o wzajemnym uznawaniu certyfikatów. Wdrożenie

Wspólnych Kryteriów Oceny Zabezpieczeń posiada kilka aspektów, z których warto wymienić:

- prawny i normatywny – standaryzacja, powołanie i akredytacja laboratoriów, podpisanie stosownych porozumień międzynarodowych o wzajemnym uznawaniu certyfikatów;
- techniczny, związany z umiejętnością projektowania zabezpieczeń i korzystania z raportów ocenionych produktów;
- organizacyjny, związany z procedurami prowadzenia i dokumentowania ocen w tych laboratoriach.

Niezwykle istotną kwestią jest upowszechnienie wiedzy na temat stosowania *Wspólnych Kryteriów (CC)* wśród osób, dla których je opracowano, a więc wśród konstruktorów, programistów, administratorów i innych, zwanych odbiorcami kryteriów.

3.1.3. Znaczenie wprowadzenia pakietu standardów bezpieczeństwa teleinformatycznego – Common Criteria

Certyfikacja wiąże się z oceną (potocznie ewaluacją) tych środków, prowadzoną przez niezależną, prestiżową instytucję, według uzgodnionych procedur i kryteriów, w zakresie spełnienia zakładanych wymagań dotyczących poufności, integralności i dostępności informacji. Ocena ta ma poświadczyć, że produkt lub system, zwany dalej *Przedmiotem Oceny (TOE - Target of Evaluation)* realizuje prawidłowo określone funkcje zabezpieczające, czyli występują w nim pożądane zachowania i posiada przy tym mierzalny poziom wiarygodności – zaufania, to znaczy brak jest w nim niepożądanych zachowań.

Na ogół proces oceny i certyfikacji przebiega dwuetapowo. W pierwszym etapie laboratoria państwowe lub komercyjne, ale działające pod kontrolą państwowych instytucji nadzorujących (wspomnianych już *krajowych władz bezpieczeństwa - służb ochrony państwa*), dokonują szeroko pojętej oceny produktu w zakresie spełnienia wymagań. W drugim etapie, instytucje nadzorujące dokonują dodatkowego przeglądu ocen i poświadczają swym autorytetem w formie certyfikatu zgodność produktu z obowiązującymi wymaganiami oraz możliwość jego zastosowania w określonych warunkach. Tak więc, certyfikacja to w pewnym sensie „*ocena ocen*".

Certyfikat stanowi poświadczenie dotyczące zachowań *Przedmiotu Oceny*, wydane na podstawie wnikliwych badań. Zwróćmy uwagę na fakt, że w praktyce wykazanie pożądanych zachowań jest znacznie łatwiejsze, niż wykazanie braku niepożądanych zachowań, a na tym właśnie opiera się istota pojęcia uzasadnionego zaufania (*assurance*).

3.1.4. Ewaluacja i certyfikacja w oparciu o Wspólne Kryteria Oceny Zabezpieczeń Teleinformatycznych

Podstawą do certyfikacji środków teleinformatycznych było stworzenie jednolitych kryteriów opisu i oceny produktów i systemów tak, by ich własności bezpieczeństwa miały charakter transparentny i można je było ze sobą porównywać. Nie zawsze spełniały to starsze kryteria o znaczeniu regionalnym, choć ogrom doświadczeń zgromadzony podczas ich stosowania wykorzystano przy opracowaniu CC. Dla porządku wypada tylko wspomnieć, że były to standardy:

- *TCSEC/FC „Orange Book"* - USA;
- *CTCPEC*– Kanada;
- *ITSEC*– kraje Unii Europejskiej, również Polska.

Obecnie są one sukcesywnie zastępowane przez bardziej szczegółowe i kompleksowe *Wspólne Kryteria*.

Ujednolicenie kryteriów pozwoliło uniknąć konieczności powtarzania kosztownych procesów certyfikacji w każdym z krajów czy w grupie krajów. Pierwszą umowę o wzajemnym uznawaniu certyfikatów bezpieczeństwa dla CC (do tzw. poziomu *EAL 4*), w 1998 roku podpisały: Niemcy, Francja, Wielka Brytania, USA i Kanada, zaś później do porozumienia przystąpiły też inne kraje. Nasz kraj do tej pory nie jest sygnatariuszem tej umowy.

Istotą oceny jest określenie poziomu zaufania do produktu lub systemu - pewnej miary gwarantowanej, że wbudowane w nie funkcje zabezpieczające oraz środki uzasadniające zaufanie do tych funkcji, spełniają zbiór wymagań zadeklarowany w dokumentach przedłożonych razem z TOE do oceny.

W miarę upowszechniania się *Wspólnych Kryteriów*, należy spodziewać się wzrostu liczby udzielonych certyfikatów o charakterze międzynarodowym. Samo

wdrożenie kryteriów nie jest łatwym zadaniem, o czym świadczy fakt, że nawet w krajach przodujących w rozwoju technologii informatycznych i biorących czynny udział w tworzeniu normy, nie tak dawno wydano pierwsze certyfikaty.

Wspólne Kryteria dedykowane są do następujących grup docelowych:

- odbiorcy teleinformatyki;
- twórcy produktów;
- oceniający;
- pozostali odbiorcy.

Odbiorcy teleinformatyki korzystają najczęściej z raportów oceny. Same wyniki, jak i możliwość ich porównywania dla wielu produktów, pomagają im zorientować się, czy dany produkt zaspokoi potrzeby dotyczące bezpieczeństwa, czy też nie. Potrzeby te zostają zwykle zidentyfikowane po przeprowadzeniu analizy ryzyka w instytucji i ukształtowaniu jej polityki bezpieczeństwa. Pomocnym w wyrażaniu tych potrzeb jest hierarchiczne uporządkowanie wymagań na uzasadnienie zaufania.

Twórcom środków teleinformatycznych, czyli projektantom, konstruktorom i programistom, kryteria pomagają precyzyjnie wyrazić wymagania bezpieczeństwa, jakie tworzony produkt powinien spełniać. Samych konstruktorów wspomagają w żmudnym przygotowaniu swoich produktów lub systemów do oceny a więc definiują zawartość i formę niezbędnej dokumentacji i wprowadzają jasne formy współpracy przy ocenie. Istnieje możliwość deklarowania zgodności *Przedmiotu Oceny* ze wskazanymi wymaganiami, osiągniętej dzięki zastosowaniu podlegających ocenie funkcji zabezpieczających i środków uzasadniających zaufanie. CC zawierają propozycje funkcji zabezpieczających, które twórca może zaimplementować.

Wraz z rozpowszechnieniem wiedzy praktycznej w stosowaniu kryteriów rysuje się możliwość ich stosowania jako *„języka formułowania wymagań bezpieczeństwa"* w procedurach przetargowych.

W normie *ISO/IEC15408* uwagę skupiono na problemie ochrony informacji, głównie przed takimi zagrożeniami, jak:

- ***nieupoważnione ujawnienie***, czyli zapewnieniem jej poufności;
- ***modyfikacja***, czyli zapewnieniem jej integralności;
- ***utrata dostępności***.

Wśród wszelkich możliwych rozpatrywanych kategorii zagrożeń, w szczególny sposób traktowane są zagrożenia dla informacji wprowadzane przez czynnik ludzki, zarówno te celowe, jak i przypadkowe.

Kluczowym pojęciem jest wspomniany już wcześniej *Przedmiot Oceny (TOE)*. Ogólnie rzecz biorąc, może nim być produkt teleinformatyczny lub system wraz ze swoją dokumentacją, na przykład:

- urządzenie teleinformatyczne, na przykład procesor kryptograficzny lub telefon komórkowy z szyfratorem;
- oprogramowanie systemowe, na przykład bezpieczny system operacyjny;
- oprogramowanie układowe, na przykład system operacyjny karty elektronicznej;
- aplikacje, np. bazodanowe czy tzw. portmonetka elektroniczna;
- narzędzia do rozwoju produktów;
- różne ich kombinacje, na przykład system operacyjny współpracujący z kartami elektronicznymi.

Wspólne Kryteria posiadają pewne ograniczenia:

- nie obejmują one zabezpieczeń administracyjnych (personalnych, organizacyjnych) - nie pozwalają bowiem oceniać tego typu zabezpieczeń, jednak uwzględniają je w formie tak zwanych założeń podczas oceny skuteczności zabezpieczeń teleinformatycznych;
- nie uwzględniają zabezpieczeń fizyko-technicznych związanych z emisją ujawniającą;
- w ograniczonym zakresie uwzględniają zabezpieczenia fizyczne;
- nie przedstawiają w pełni tak zwanego kontekstu oceny, choć są jego elementem, w ramach którego mogą być stosowane przez organy nadzorujące oceny; wspomniany kontekst, to metodyka oceny wraz z otaczającą ją strukturą prawno - administracyjną;
- nie przedstawiają procedury użycia wyników oceny do akredytacji produktu lub systemu, gdyż akredytacja jest działaniem administracyjnym, prowadzącym do wydania decyzji o zezwoleniu na eksploatację produktu lub systemu teleinformatycznego w jego środowisku rzeczywistym.

Poddanie produktu procesowi oceny przynosi wiele korzyści, głównie technicznych i marketingowych, gdyż:

- wymusza to staranne opracowanie produktu i jego dokumentacji;
- znacząco podnosi jakość i bezpieczeństwo, co zwłaszcza dotyczy oceny prowadzonej równolegle z powstawaniem produktu;
- może być wykorzystane w celach reklamowych i jako argument w rozmowach handlowych, co wpływa niewątpliwie na zwiększenie sprzedaży;
- dzięki międzynarodowemu zasięgowi standardów, produkty certyfikowane są rozpoznawane i łatwiej wchodzą na obce rynki.

W tym miejscu wypada wspomnieć, że rygorystyczne zasady tworzenia produktów, pracochłonna ich ocena, wpływają jednak na wzrost ich ceny.

Norma ISO/IEC-15408 (CC) składa się z trzech części:

1. **Wprowadzenie i model ogólny**

   Część pierwsza przedstawia przyjęty ***model bezpieczeństwa***, który ma odzwierciedlenie w specyfikacjach wymagań bezpieczeństwa opisanych w jego załącznikach. Prezentuje także konstrukcje pomagające wyrażać cele bezpieczeństwa i tworzyć specyfikacje produktów na wysokim poziomie abstrakcji.

2. **Wymagania dotyczące funkcjonalności zabezpieczeń**

   Część drugą poświęcono tworzeniu wymagań na funkcjonalne zabezpieczenia dla *Przedmiotu Oceny*. Zawiera ona ***katalog komponentów funkcjonalnych*** (*functional components*), podzielonych na rodziny i klasy, za pomocą których modeluje się bezpieczeństwo środków teleinformatycznych, czyli wspomniane ich pożądane zachowanie.

3. **Wymagania dotyczące uzasadnienia zaufania do zabezpieczeń**

   Część trzecia zawiera ***katalog komponentów uzasadniających zaufanie*** (*assurance components*), również podzielonych na rodziny i klasy, służących do wyrażenia wymagań na uzasadnienie zaufania do TOE. W części tej przedstawiono kryteria oceny dokumentów formalnych określających wymagania dla zabezpieczeń, czyli tak zwanych *Zadań Zabezpieczeń* lub *Profili Zabezpieczeń* a także zdefiniowano skalę ***poziomów uzasadnionego zaufania*** (miary wiarygodności) *EAL1-EAL7* (*EAL - Evaluation Assurance Level*).

Powyższa trzyczęściowa norma podstawowa określa więc tylko wymagania funkcjonalne i wymagania dotyczące uzasadnienia zaufania do zabezpieczeń, co nie

jest wystarczające do pełnego wdrożenia CC. Trwają prace nad normami uzupełniającymi, dotyczącymi projektowania i oceny zabezpieczeń.

Metodyka prowadzenia ocen zabezpieczeń - *Common Evaluation Methodology for Information Technology Security,* powstaje z myślą o oceniających. Znajduje się ona ciągle w fazie opracowania. Nie posiada statusu normy *ISO/IEC*, jednak jest dość powszechnie stosowana. Przedstawiona jest w oddzielnym dokumencie, składającym się z dwóch części:

Part 1: *Introduction and General Model*,

Part 2: *Evaluation Methodology*.

Z myślą o konstruktorach i programistach, a więc o twórcach zabezpieczeń, trwają prace nad poradnikiem tworzenia *Profili i Zadań Zabezpieczeń* oraz nad kilkoma innymi normami pomocniczymi.

Wyróżnia się trzy typy ocen w zależności od stadium rozwoju produktu:

- ***ocena towarzysząca opracowywaniu*** produktu lub systemu zawierającego zabezpieczenia (na etapie planowania, koncepcji, projektu, implementacji lub prototypu); to podejście jest najbardziej efektywne, gdyż ewentualne niedomagania w zakresie bezpieczeństwa korygowane są już we wczesnym stadium rozwoju produktu;
- ***ocena gotowego produktu*** – obarczona jest dość dużym ryzykiem, gdyż ewentualne błędy projektowe powodujące obniżenie bezpieczeństwa produktu mogą być bardzo trudne lub wręcz niemożliwe do usunięcia;
- powtórna ***ocena powstałej nowej wersji*** produktu (związana z recertyfikacją) – CC zapewniają środki do utrzymywania założonego poziomu bezpieczeństwa produktu, podczas, gdy w czasie jego życia tworzone są kolejne wersje.

Oceny produktów i systemów powinny być przeprowadzane w ramach obowiązującego systemu oceny, któremu muszą się podporządkować instytucje dokonujące ocen i sami oceniający. Twórcy *Wspólnych Kryteriów* położyli nacisk na zapewnienie przezroczystości i porównywalności ocen.

Uwarunkowane jest to tak zwanym kontekstem oceny (ewaluacji) – kryteria powinny być właściwie stosowane. Kontekst ewaluacji tworzą:

- same ***kryteria***;
- ***metodyka*** ich stosowania - jednolita metodyka ewaluacji jest warunkiem koniecznym, ale niewystarczającym powtarzalności i obiektywności wyników;
- ***schemat ewaluacji*** (inne standardy, nadzór nad jakością procesu prowadzenia oceny, administrowanie jego przebiegiem, odpowiednia organizacja laboratoriów, itp.); *Wspólne Kryteria* nie narzucają wymagań na strukturę tych regulacji, natomiast istotna jest spójność pomiędzy strukturami regulacji różnych organów nadzorujących - ma to umożliwić wzajemne uznawanie wyników oceny.

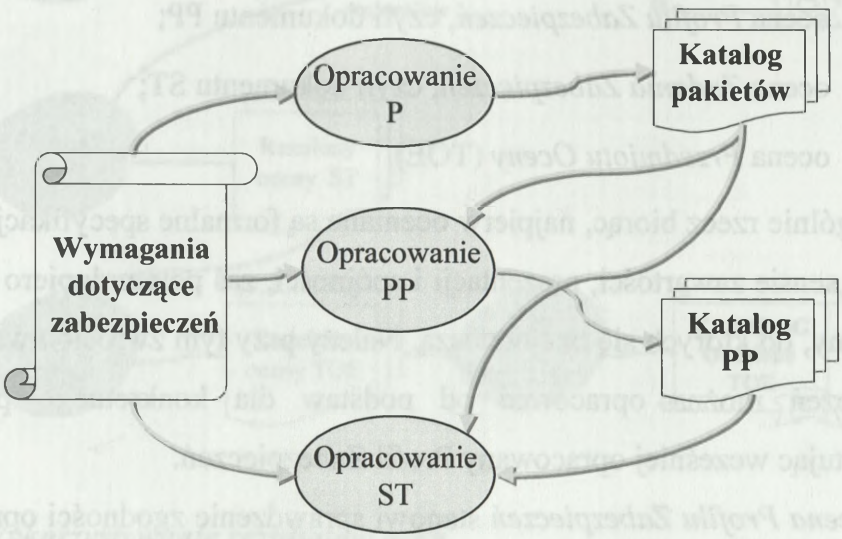
Główną przeszkodą w osiąganiu powtarzalności i spójności ocen jest jednak konieczność opierania się na wiedzy ekspertów, dogłębnej, ale często również intuicyjnej i subiektywnej - formalizacja opisu własności bezpieczeństwa posiada swoje granice. Certyfikacja, związana z dodatkową i niezależną kontrolą wyników oceny, prowadzi do wydania końcowego certyfikatu lub aprobaty. Poprawia to powtarzalność ocen i wzmacnia ich spójność. Jak już wspomniano, system, metodyka i procesy certyfikacji leżą w zakresie odpowiedzialności organów nadzorujących oceny, więc nie zostały one przedstawione w *ISO/IEC-15408*.

Barierami w tym względzie są niewątpliwie:

- niewystarczająca wiedza, zwłaszcza praktyczna, dotycząca stosowania CC i brak odpowiedniej liczby specjalistów;
- brak standardów wspomagających *ISO/IEC 15408*, w tym dotyczących projektowania i sposobów prowadzenia ocen;
- pewna niedojrzałość samych *Wspólnych Kryteriów* – zgłoszono do rozstrzygnięcia około 40 problemów interpretacyjnych;
- dość słaba stymulacja ze strony rynku;
- trudności w powoływaniu akredytowanych laboratoriów.

Procesy projektowania i oceny są niezwykle złożone, wymagają dużej szczegółowości, precyzyjnych uzasadnień na każdym kroku, a przy tym są trudne do sformalizowania. Wszystko to razem stanowi dodatkowe obciążenie dla twórców zabezpieczeń. Łatwiejszym wydaje się samo korzystanie z raportów ocenionych produktów, podczas wyboru środków do budowy własnych systemów – inwestor znajdzie tam zawsze osąd, jaki produkt, do czego się nadaje, zaś administrator – wskazówki, jak go stosować w zgodzie z polityką bezpieczeństwa swojej instytucji.

Wspólne Kryteria określają trzy rodzaje specyfikacji wymagań *(Profil Zabezpieczeń PP, Zadanie Zabezpieczeń ST* i *pakiet P*), co przedstawiono na ***Rys. 7.***



Rysunek 7: ***Rodzaje specyfikacji wymagań***
Źródło: Białas A.: *Budowa zaufania do zabezpieczeń teleinformatycznych... [20]*

Profil Zabezpieczeń (PP - Protection Profile) jest konstrukcją wymagań niezależną od implementacji i nadającą się przy tym do wielokrotnego wykorzystania. Profile podlegają ocenie i po pomyślnym jej zakończeniu zostają skatalogowane jako pewne wzorce wymagań, z których można korzystać przy opracowywaniu *Zadań Zabezpieczeń* dla konkretnego produktu w ramach rodziny produktów. Istniejące PP mogą być wykorzystywane również do tworzenia innych profili.

Zadanie Zabezpieczeń (ST - Security Target), stanowi specyfikację wymagań bezpieczeństwa dla konkretnego *TOE (TOE - Target of Evaluation*), więc uwzględnia aspekty implementacyjne.

Pakiet (P - Package) ma charakter tymczasowy, pomocniczy, bowiem grupuje wymagania dotyczące pewnego podzbioru celów zabezpieczeń i służy do wielokrotnego wykorzystania. Może on w sobie zawierać inne pakiety. Często występuje w dokumentach typu PP lub ST. W tym miejscu należy wspomnieć o zbiorze dość specyficznych pakietów, jakimi są poziomy uzasadnionego zaufania

EAL1 do EAL7. Mają one charakter predefiniowanych w *ISO/IEC-15408-3* pakietów, zawierających komponenty uzasadniające zaufanie.

Wspólne Kryteria pozwalają realizować trzy rodzaje oceny:

- ocena *Profilu Zabezpieczeń*, czyli dokumentu PP;
- ocena *Zadania Zabezpieczeń*, czyli dokumentu ST;
- ocena *Przedmiotu Oceny* (TOE).

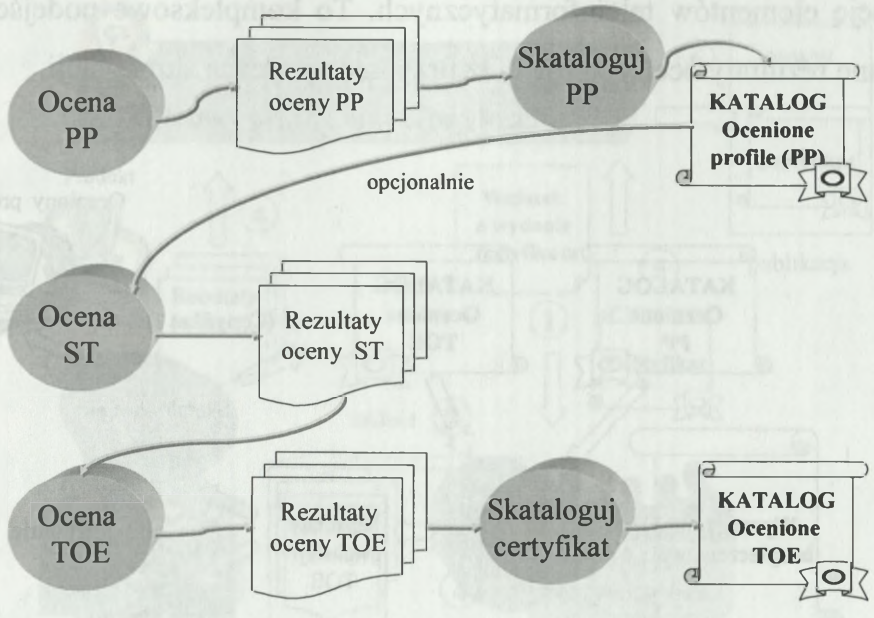
Ogólnie rzecz biorąc, najpierw oceniane są formalne specyfikacje wymagań PP lub ST w sensie zawartości, prezentacji i spójności, zaś potem dopiero same produkty lub systemy, do których się one odnoszą. Należy przy tym zwrócić uwagę, że Zadanie Zabezpieczeń można opracować od podstaw dla konkretnego produktu, bądź wykorzystując wcześniej opracowany Profil Zabezpieczeń.

Ocena Profilu Zabezpieczeń stanowi sprawdzenie zgodności opracowanego PP ze *Wspólnymi Kryteriami*, a w szczególności, czy dokument PP jest kompletny, spójny wewnętrznie i poprawny pod względem technicznym, przez co może stanowić bazę do tworzenia rodziny podobnych TOE (produktów, systemów) a także innych profili.

Ocena Zadania Zabezpieczeń stanowi sprawdzenie zgodności opracowywanego ST z kryteriami. Również i w tym przypadku, celem jest zbadanie, czy dokument ST jest kompletny, spójny wewnętrznie i poprawny pod względem technicznym oraz ponadto, jeśli opracowano go na podstawie PP, to dodatkowym celem jest wykazanie jego zgodności z danym profilem. Wymagania ST po pozytywnej ocenie, stanowią podstawę do rozpoczęcia procesu oceny samego TOE.

Celem oceny TOE jest sprawdzenie, czy *Przedmiot Oceny* spełnia wymagania na zabezpieczenia zawarte w jego *Zadaniu Zabezpieczeń*.

Na ***Rysunku Nr 8*** przedstawiono różnorodność uzyskiwanych form ocen. Zweryfikowane i skatalogowane profile stanowią bazę ocenionych wzorców dla abstrakcyjnie opisanych produktów, które można wykorzystać przy tworzeniu różnorodnych ich implementacji, co wpływa na redukcję kosztów rozwoju nowych produktów lub systemów.



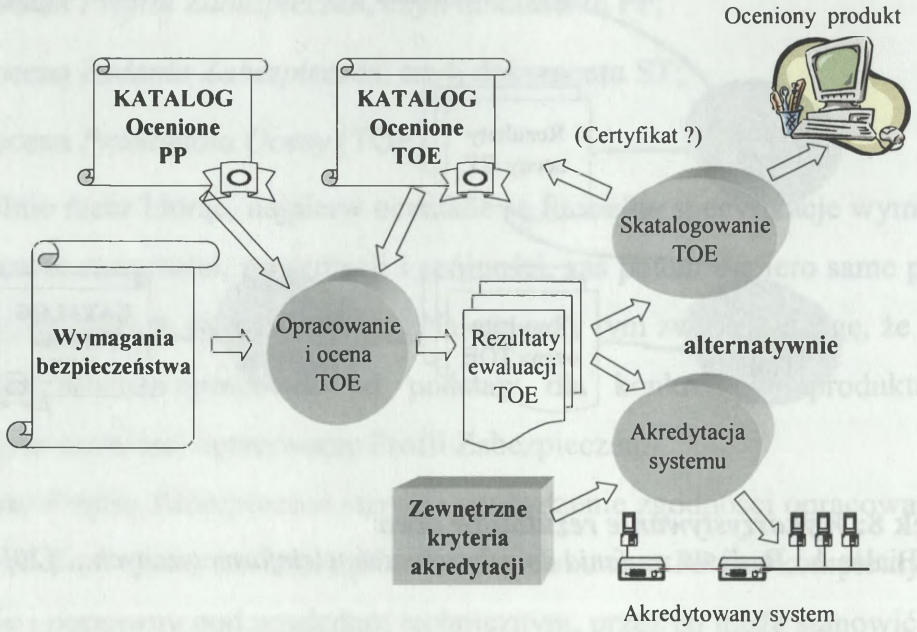
Rysunek 8: ***Wykorzystywanie rezultatów ocen***
Źródło: Białas A.: *Budowa zaufania do zabezpieczeń teleinformatycznych... [20]*

Na podstawie profilu, stosunkowo szybko może powstać dokument ST dla konkretnego produktu. Istotnym w tym przypadku jest sprawdzenie, nie tylko czy tworzony produkt spełnia wymagania na zabezpieczenia, ale również, czy należy do rodziny produktów opisanych w profilu. Produkt, który pozytywnie przeszedł proces oceny może, ale nie musi ubiegać się o uzyskanie certyfikatu bezpieczeństwa.

Rysunek Nr 9 przedstawia praktyczne aspekty wykorzystania wyników ewaluacji przedmiotów oceny. Tworząc określony produkt, można korzystać z ocenionych profili, do których produkt się odwołuje lub z wcześniej ocenionych produktów, występujących jako jego części składowe. TOE typu program, urządzenie lub narzędzie, umieszczony zostaje w publicznie dostępnym katalogu ocenionych produktów. Ocena TOE będącego systemem lub produktem, wchodzącym w jego skład, może stać się podstawą jego akredytacji, czyli dopuszczenia do pewnych odpowiedzialnych zastosowań, co nie stanowi jednak przedmiotu rozważań samej normy.

Należy zwrócić uwagę, że ocena zabezpieczeń koncentruje się na elementach zabezpieczeń teleinformatycznych produktu lub systemu oraz na elementach środowiska eksploatacyjnego, które mają bezpośredni wpływ na bezpieczną

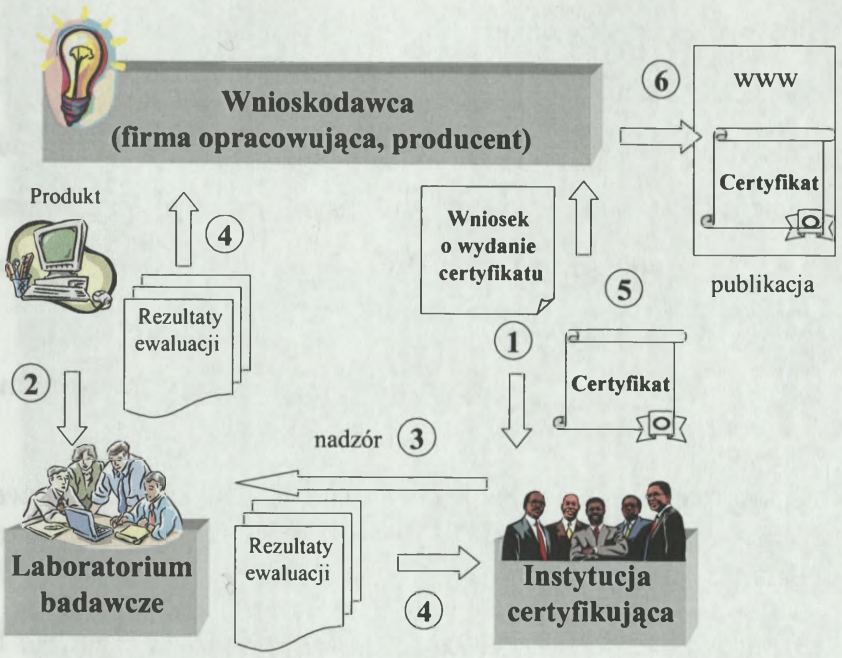
eksploatację elementów teleinformatycznych. To kompleksowe podejście zapewnia, że uzyskane rezultaty oceny są również przydatne podczas akredytacji.



Rysunek 9: ***Wykorzystanie rezultatów oceny TOE***
Źródło: Białas A.: *Budowa zaufania do zabezpieczeń teleinformatycznych... [20]*

W pewnym uproszczeniu (***Rysunek Nr 10***), procedurę oceny zabezpieczeń i ich certyfikacji można przedstawić następująco:

1. Wnioskodawca (producent, konstruktor) pragnący uzyskać certyfikat na swój produkt, składa odpowiedni wniosek do Instytucji Certyfikującej, wskazując przy tym specjalistyczne laboratorium zajmujące się tego typu produktami.
2. Wnioskodawca przekazuje także opracowane formalne wymagania bezpieczeństwa (ST lub PP) i produkt do wskazanego laboratorium.
3. Pod nadzorem *Instytucji Certyfikującej* rozpoczyna się proces oceny zgodnie z zadeklarowanym we wniosku poziomem uzasadnionego zaufania EAL.
4. Wyniki oceny kierowane są do wnioskodawcy oraz do Instytucji Certyfikującej.
5. Na ich podstawie (weryfikacja ocen) podejmowana jest decyzja o wydaniu, bądź nie wydaniu certyfikatu bezpieczeństwa.
6. Wymagania bezpieczeństwa opracowane przez wnioskodawcę, raporty z oceny i sam certyfikat zostają udostępnione publicznie (witryna).



Rysunek 10: Organizacja procesu oceny i certyfikacji wg PCA
Źródło: Białas A.: *Budowa zaufania do zabezpieczeń teleinformatycznych... [20]*

Prace nad wdrożeniem *Wspólnych Kryteriów do Oceny Zabezpieczeń Teleinformatycznych* prowadzone są dość intensywnie, zwłaszcza w krajach przodujących w rozwoju technologii teleinformatycznych, gdyż kraje te są żywotnie zainteresowane jak najszerszym rozpowszechnieniem swych produktów, zwłaszcza na rynkach trzecich. Certyfikaty znacznie im to ułatwiają, gdyż mają one zasięg globalny.

Mimo znacznego postępu w tej dziedzinie, ciągle jeszcze certyfikaty udzielone według starszych kryteriów regionalnych są w większości. W chwili obecnej udzielono już około 50 certyfikatów według Wspólnych Kryteriów[5].

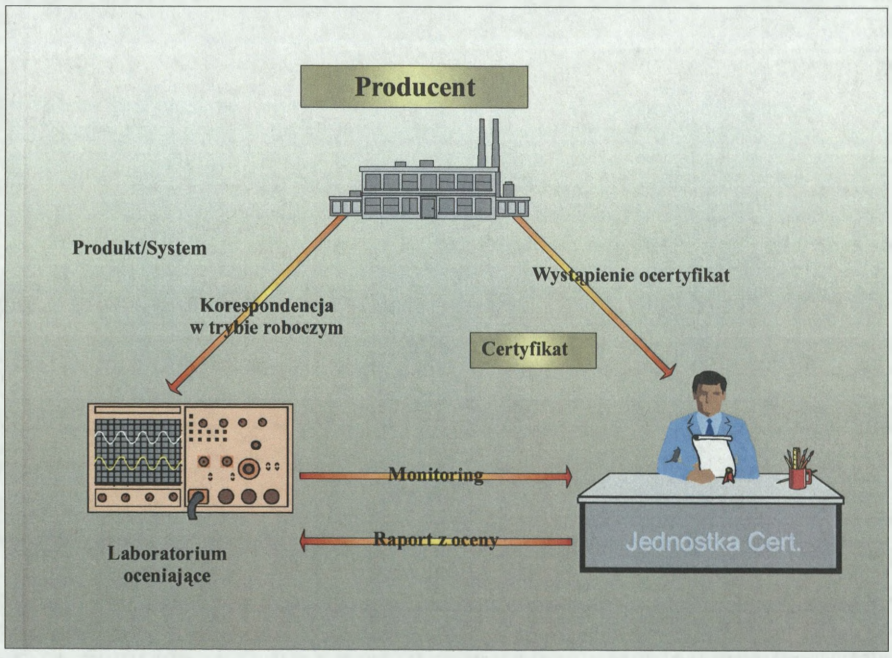
Jak wielokrotnie podkreślano już w rozprawie - systemy i sieci teleinformatyczne, służące do wytwarzania, przechowywania, przetwarzania lub przekazywania informacji niejawnych stanowiących tajemnicę państwową, podlegają szczególnej ochronie przed nieuprawnionym ujawnieniem tych informacji, a także przed możliwością przypadkowego lub świadomego narażenia ich bezpieczeństwa. Powyższe przepisy dostosowały wymagania dotyczące bezpieczeństwa teleinforma-

[5] Białas A.: *Budowa zaufania do zabezpieczeń teleinformatycznych poprzez ich ocenę i certyfikację*, W: Grzywak A. [red].: *Internet wspołeczeństwie informacyjnym*, Wyd. WSB Dąbrowa Górnicza, 2003.

tycznego do poziomu wymagań jakie obowiązują w krajach członkowskich Organizacji Traktatu Północnoatlantyckiego.

Jednym z podstawowych wymogów, które wprowadziła ustawa, jest wymóg posiadania certyfikatu przez system w którym ma być przetwarzana informacja niejawna stanowiąca tajemnicę państwową. Certyfikat taki wydaje właściwa służba ochrony państwa po uprzednim:

- uzyskaniu, przez cały personel mający dostęp do systemu, *poświadczeń bezpieczeństwa*;
- zatwierdzeniu przez właściwą *służbę ochrony państwa* dokumentów *szczególnych wymagań bezpieczeństwa (SWB)* oraz *procedur bezpieczeństwa (PB)*;
- przeprowadzeniu przez właściwą *służbę ochrony państwa* badania i oceny zdolności systemu do ochrony informacji niejawnych (sprawdzenia zgodności zapisów w SWB oraz PB ze stanem faktycznym).



Rysunek 11: ***Proces certyfikacji***
Źródło: opracowanie własne

W stosunku do resortu obrony narodowej oraz do podmiotów gospodarczych założonych przez MON funkcję *służby ochrony państwa* realizują *Wojskowe Służby Informacyjne* (*Decyzją nr 100/MON Ministra Obrony Narodowej* z dnia 06 czerwca 2000 r. została utworzona w *WSI Jednostka Certyfikująca Wyroby*).

W sferze cywilnej funkcje *służby ochrony państwa* wykonuje *Agencja Bezpieczeństwa Wewnętrznego*, w zakresie bezpieczeństwa teleinformatycznego w imieniu szefa *ABW - Departament Bezpieczeństwa Teleinformatycznego (DBTI)*.

Jednostka Certyfikująca Wyroby może wydawać następujące rodzaje certyfikatów:

- *certyfikat typu* (bezpieczeństwa dla urządzeń i aplikacji w rozumieniu ustawy);
- *certyfikat zgodności*;
- *certyfikat systemów i sieci teleinformacyjnych* (w rozumieniu ustawy).

Certyfikat typu wydaje się na moduł kryptograficzny, urządzenie lub oprogramowanie wchodzące w skład systemu. Zawiera on szczegółowe zastrzeżenia dotyczące wydanego certyfikatu oraz termin jego ważności. Uzyskanie tego certyfikatu dla przedmiotu oceny jest warunkiem umieszczenia wyrobu na liście wyrobów preferowanych.

Certyfikat zgodności jest urzędowym dokumentem, formalnym poświadczeniem stwierdzającym zgodność (powtarzalność) przedmiotu oceny z dokumentacją i wzorami wyrobów, stanowiącymi podstawę wydania certyfikatu typu.

W zależności od rodzaju przedmiotu oceny, wyróżnia się trzy podstawowe modele dokonywania oceny zgodności *(5 ISO, 7 ISO, 8 ISO)*.

Badania przeprowadza się na wybranej przez jednostkę certyfikującą próbce wyrobu. Pozytywne zakończenie procesu certyfikacji kończy się wydaniem certyfikatu, który (w myśl ustawy) upoważnia do wdrożenia przedmiotu oceny i zastosowania go w resorcie obrony narodowej.

Certyfikat zgodności zawiera szczegółowe zastrzeżenia dotyczące wydanego certyfikatu oraz termin jego ważności.

Certyfikat systemów i sieci teleinformacyjnych (w rozumieniu ustawy) jest urzędowym dokumentem (formalnym poświadczeniem) gwarantującym, że oceniane przez laboratorium badawcze zabezpieczenia systemu lub sieci teleinformatycznej, odpowiadają określonym wymaganiom związanym z ich bezpieczeństwem. Wynika to z faktu, iż w sieciach tych są wytwarzane, przechowywane przetwarzane lub przekazywane informacje niejawne, stanowiące tajemnicę państwową.

3.2. Stan prawno-organizacyjny ochrony informacji niejawnych NATO

W ostatnim czasie wyzwaniem stały się nowe zagrożenia dla bezpieczeństwa państw i narodów (terroryzm). Istotnym problemem jest takie organizowanie działań czynników odpowiedzialnych za funkcjonowanie państwa, aby zagwarantować stabilizację i poczucie bezpieczeństwa. Polska pełni istotną rolę w kształtowaniu polityki bezpieczeństwa europejskiego i dlatego też musiała dostosować swoją strategię bezpieczeństwa do uwarunkowań zalecanych przez NATO. Utrzymujące się zagrożenia związane z terroryzmem, aktywnością obcych służb specjalnych wymagają od nas zagwarantowania bezpiecznego funkcjonowania, wytwarzania, przetwarzania i przekazywania informacji, w tym przede wszystkim niejawnych, które właściwie chronione gwarantują prawidłowe funkcjonowanie struktur państwowych i społecznych. W związku z wejściem Polski do struktur NATO zostaliśmy zobligowani do zorganizowania systemu ochrony informacji oraz odpowiedzialności za ochronę informacji niejawnych krajowych i sojuszniczych. Konsekwencją tego było przyjęcie przez Sejm w dniu 22.01.1999 r. *Ustawy o ochronie informacji niejawnych*, w której znaczącą funkcję w jej realizacji powierzono Pełnomocnikowi Ochrony.

3.2.1. Struktura instytucjonalna bezpieczeństwa informacyjnego NATO

W Organizacji Traktatu Północnoatlantyckiego przywiązuje się priorytetowe znaczenie bezpieczeństwu informacji niejawnych. Głównym organem bezpieczeństwa sojuszu jest *Biuro Bezpieczeństwa NATO (NOS – NATO Office of Security)*. Jego usytuowanie organizacyjne pokazuje ***Diagram Nr 17***. *NOS* jako organ wykonawczy współpracuje z *Komitetem Bezpieczeństwa NATO (NSC – NATO Security Committee),* będącym kolegialnym ciałem doradczym *Rady Północnoatlantyckiej* – ***Diagram Nr 19***

.

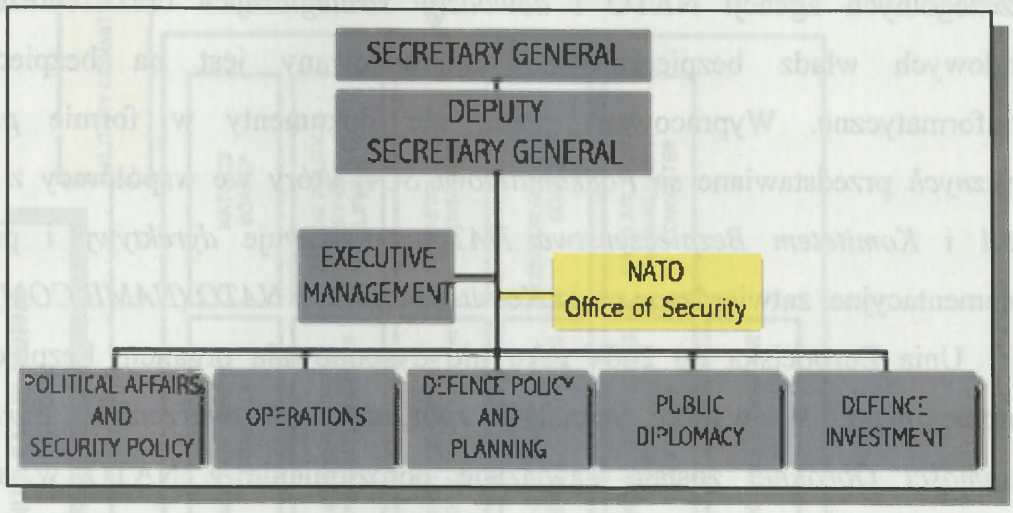


Diagram 17: ***Usytuowanie Biura Bezpieczeństwa NATO (NOS) w strukturze sojuszu***
Źródło: strona internetowa NATO: http://www.nato.int/structur/

Obok etatowych struktur bezpieczeństwa informacyjnego NATO działają liczne grupy robocze, zajmujące się problematyką szczegółową. Obejmują swą działalnością wszystkie elementy polityki bezpieczeństwa informacyjnego (*INFOSEC*).

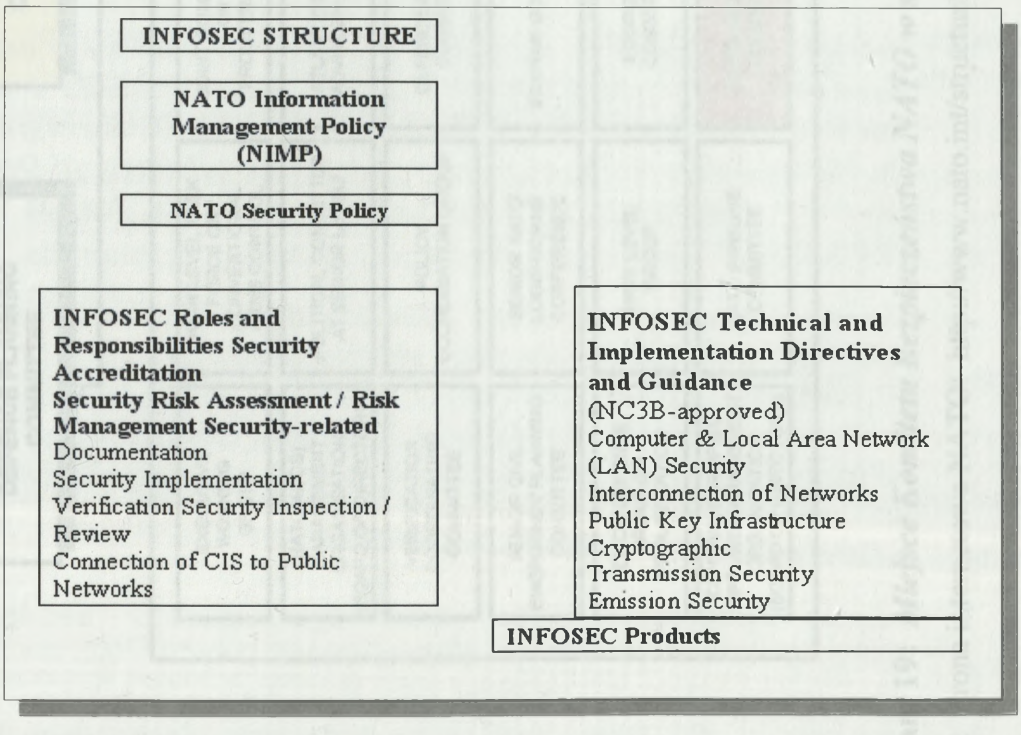


Diagram 18: ***Rola i zadania bezpieczeństwa informacyjnego (INFOSEC) NATO***
Źródło: opracowanie własne

Główny wysiłek w działalności grup roboczych, złożonych z przedstawicieli poszczególnych agencji NATO i *dowództw strategicznych* oraz reorezentantów narodowych władz bezpieczeństwa, ukierunkowany jest na bezpieczeństwo teleinformatyczne. Wypracowane przez nie dokumenty w formie *projektów wytycznych* przedstawiane są *Podkomitetowi SC4*, który we współpracy z *Agencją NC3A* i *Komitetem Bezpieczeństwa NATO* opracowuje *dyrektywy* i procedury implementacyjne, zatwierdzane przez *Komitet Wojskowy NATO (NAMILCOM)*.

Unia Europejska do 2004 roku nie dysponowała organem bezpieczeństwa informacyjnego. W wyniku inicjatyw związanych z tworzeniem *Europejskiej Tożsamości Obronnej* zostało nawiązane porozumienie z NATO w sprawach bezpieczeństwa informacji, wprowadzające zasadę wzajemnego uznawania procedur związanych z polityką bezpieczeństwa. *Parlament Europejski* powołał z dniem 1.01. 2004 r. *Europejską Agencję ds. Bezpieczeństwa Sieciowego i Informacyjnego (ENISA - European Network and Information Security Agency)*. Trwają prace związane z rozwinięciem działalności tej agencji i pogłębieniem współpracy z *Komitetem Bezpieczeństwa NATO*.

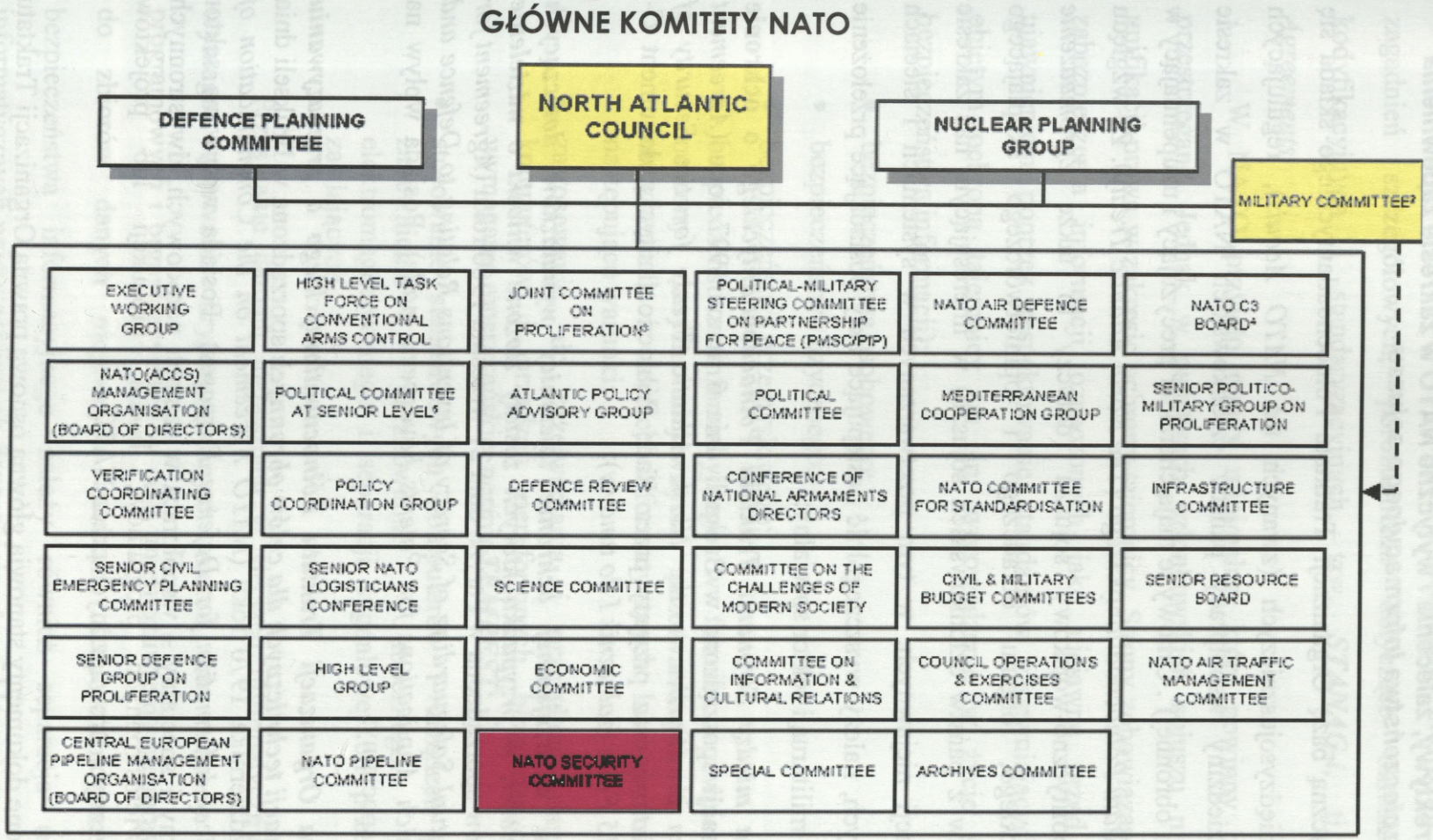


Diagram 19: ***Miejsce Komitetu Bezpieczeństwa NATO w strukturze władz sojuszu***

Źródło: strona internetowa NATO: http://www.nato.int/structur/

3.2.2. Dyrektywy, zalecenia i wytyczne NATO w zakresie zapewnienia bezpieczeństwa informacyjnego sojuszu

Na jurydyczną bazę Organizacji Tratktatu Północnoatlantyckiego składa się osiem umów międzysojuszniczych (zwanych też *NATO Acquis*), regulujących najważniejsze dziedziny współpracy państw członkowskich NATO w zakresie jednolitej polityki obronnej)[6]. Umowy te mają charakter precyzujący i uzupełniający w stosunku do *Traktatu Północnoatlantyckiego (The North Atlantic Treaty)*. Ze względu na charakter polityczno-wojskowy sojuszu (dotyczy to także *Zgromadzenie Północnoatlantyckiego*, organu doradczego i opiniotwórczego skupiającego parlamentarzystów z państw członkowskich sojuszu) w interesującym nas zakresie ochrony informacji niejawnych, w tym przetwarzanych w systemach i sieciach teleinformatycznych, należy wyszczególnić następujące akty posiadające przełożenie na sferę cywilną, militarną i sektor specjalny:

- ***Umowa między Stronami Traktatu Północnoatlantyckiego* o ochronie informacji** sporządzona w Brukseli dnia 6 marca 1997 roku (*Agreement between the Parties to the North Atlantic Treaty for the Security of Information*) oraz przyjęty przez Radę Północnoatlantycką dokument *C-M/55/15 Final (załącznik I do umowy)*;
- ***Umowa o wzajemnej ochronie tajemnicy wynalazków dotyczących obronności, w przypadku których zostały złożone wnioski o udzielenie patentów*** sporządzona w Paryżu dnia 21 września 1960 roku (*Agreement for the Mutual Safeguarding of Secrecy of Inventions Relating to Defence and for which Applications for Patents have been made*). Posiada wpływ na sektor specjalny;
- ***Umowa Organizacji Traktatu Północnoatlantyckiego o przekazywaniu informacji technicznych dla celów obronnych*** sporządzona w Brukseli dnia 19 października 1970 roku (*NATO Agreement on the Communication of Technical Information for Defence Purposes*). Posiada wpływ na sektor militarny i specjalny – współpraca w ramach narodowych, dwustronnych lub wielostronnych programów, badań, produkcji lub projektów logistycznych prowadzonych przez NATO.

Wymienione dokumenty stanowią główną osnowę prawną Organizacji Traktatu Północnoatlantyckiego.

[6] B. Jabłoński, S. Kamiński. *Dorobek prawny NATO.* http://www.bbn.gov.pl/pl/nato/dorobek.html

Istnieją również inne dokumenty o charakterze prawnym, odnoszące się do zagadnień szczegółowych, porozumienia dotyczące określonych zagadnień kodyfikacyjnych i standaryzacyjnych, tzw. ***STANAG-i,*** tj. *Standardization Agreements*.

W NATO przyjęto reguły minimalne, które powinny być bezwzględnie przestrzegane. Jednak w państwach członkowskich sojuszu nie nastąpił nakaz unifikacji prawa w zakresie ochrony tajemnicy. Strony zobowiązane są do ochrony i zabezpieczenia informacji oznaczonych jako niejawne przed nieuprawnionym ujawnieniem poprzez respektowanie standardów zapewniających wiadomościom objętym ochroną tajemnicy (m. in. wprowadzenie w życie środków ochrony bezpieczeństwa informacji):

- bezpieczeństwa osobowego;
- bezpieczeństwa fizycznego;
- bezpieczeństwa przemysłowego;
- bezpieczeństwa informacyjnego w formie zapewnienia odpowiedniej ochrony danych niejawnych, przetwarzanych i przesyłanych w urządzeniach i sieciach informatycznych lub łączności, spełniających następujące warunki:
- zastosowanie, do przetwarzania i przesyłania danych niejawnych, komputerów i urządzeń peryferyjnych bezpiecznych, spełniających wymagania amerykańskiej normy ***TEMPEST***;
- stosowanie standardowych komputerów i urządzeń peryferyjnych po zapewnieniu ekranowania ubocznego promieniowania elektromagnetycznego i separacji sygnałowej od przemysłowych sieci zasilających.

Przesyłanie danych niejawnych w sieciach informatycznych lub łączności wymaga stosowania kryptograficznych metod ich ochrony a także metod programowych i organizacyjnych w celu uniemożliwienia nieuprawnionego dostępu do zbiorów danych niejawnych osobom nieupoważnionym. Do standardu bezpieczeństwa informacyjnego należy również separacja urządzeń i sieci informatycznych przetwarzających dane o najwyższej klauzuli tajności od urządzeń i sieci informatycznych przetwarzających dane jawne lub o niższych klauzulach tajności.

Standardy NATO mają zapewniać również ochronę przed:

- podsłuchem w pomieszczeniach (w urządzeniach);
- podsłuchem aktywnym (ulot informacji stymulowany z zewnątrz);
- przechwytem sygnałów radioelektronicznych;
- promieniowaniem sygnałów elektromagnetycznych.

Prace legislacyjne w naszym kraju w zakresie unormowania problematyki ochrony informacji niejawnych zbiegły się z dążeniem do przystąpienia do NATO. W tej sytuacji, priorytetem stało się dostosowanie przepisów polskich do obowiązujących już w państwach członkowskich sojuszu. Powołany w 1997 roku przez *Prezesa Rady Ministrów*[7)] *Międzyresortowy Zespół do Spraw Ochrony Wiadomości Stanowiących Tajemnicę Państwową Wymienianych na Podstawie Umów Międzynarodowych* wypracował projekty rozwiązań zapewniających spójność prawa polskiego w zakresie ochrony wiadomości niejawnych uwzględniające zakres wymogów stron Traktatu Północnoatlantyckiego i Unii Zachodnioeuropejskiej.

Na podstawie przyjętych przez parlament RP ustaw ratyfikacyjnych w marcu 2000 r.8), prezydent Aleksander Kwaśniewski podpisał akty przystąpienia Polski do umów tworzących tę multilateralną konstrukcję prawną sojuszu. Przyjęte przez Polskę zobowiązania sojusznicze miały zasadniczy wpływ na kształt polskiej ustawy o ochronie informacji niejawnych w kontekście ujednolicenia stopnia ich ochrony, szczególnie w zakresie[9]:

- utworzenia krajowych władz bezpieczeństwa do spraw działalności NATO;
- utworzenie i wprowadzenie standardów bezpieczeństwa;
- certyfikacja i akredytacja.

Krajowy ustawodawca nałożył na ministrów *Spraw Wewnętrznych* oraz *Obrony Narodowej,* a także szefa *Urzędu Ochrony Państwa* obowiązek uregulowania w trybie rozporządzeń kilku bardzo ważnych problemów ochrony tajemnic (m.in. *procedura*

[7] Zarządzenie nr 107 Prezesa Rady Ministrów z 3 października 1997 roku *„w sprawie utworzenia Międzyresortowego Zespołu do Spraw Ochrony Wiadomości Stanowiących Tajemnicę Państwową Wymienianych na Podstawie Umów Międzynarodowych" (M.P. Nr 73/97, poz. 693).* Zespół był kontynuatorem analogicznego, funkcjonującego w ramach programu Partnerstwo dla Pokoju.

[8] *„Umowa między Stronami Traktatu Północnoatlantyckiego o ochronie informacji sporządzona w Brukseli 6 marca 1997 roku (Dz. U. nr 64/00 poz. 740) oraz oświadczenie rządowe z dnia 29 grudnia 1999 roku „w sprawie ratyfikacji przez Rzeczpospolita Polską Umowy między stronami Traktatu Północnoatlantyckiego o ochronie informacji" (Dz. U. nr 64/00 poz. 741).*

[9] Art. 2 *„Umowy między Stronami Traktatu Północnoatlantyckiego o ochronie informacji".*

sprawdzeniowa, bezpieczeństwo przemysłowe, autoryzacja dostępu), bazujących na przyjętych w NATO standardach.

Przepisy NATO w zakresie bezpieczeństwa teleinformatyki, opierają się na podstawowym dokumencie *C-M (55) 15 (Final) Security within NATO*, do którego inne dokumenty (standardy, dyrektywy, zalecenia, itp.) odwołują się jako do *NATO Security Policy.*

Opracowana przez Departament Obrony USA tzw. „*Orange Book*" stała się podstawą kryteriów oceny wykorzystywanych przez kraje członkowskie NATO)[10]. Ze względu na międzynarodowy charakter oraz dużą elastyczność i łatwość w nadążaniu za postępem technologicznym *Wspólne Kryteria* (CC) będą wprowadzone jako obowiązujące w NATO zastępując kryteria *NTCSEC.* Na drugi kwartał 2003 roku planowane jest zakończenie okresu przejściowego do pełnego stosowania kryteriów.

Zadanie przygotowania podstaw do wprowadzenia CC w NATO realizuje grupa robocza *Common Criteria Ad Hoc Working Group (CC AHWG)* przy *Komitecie bezpieczeństwa Teleinformatycznego NATO (INFOSEC Sub-Committee – SC/4).* Kolejnymi, zasadniczymi dla wprowadzenia kryteriów CC do stosowania w NATO dokumentami są obecnie opracowywane dyrektywy:

- *INFOSEC Technical and Implementation Directive on the Use of the Common Criteria within NATO* – zobowiązująca do stosowania w opracowaniu, ocenie i certyfikacji produktów dla NATO kryteriów CC;
- *INFOSEC Technical and Implementation Directive on the Registration of Protection Profiles, Packages and INFOSEC Products within NATO* – opisująca obowiązkowe procedury rejestracji profili zabezpieczenia i pakietów wymagań oraz zadań zabezpieczenia w *Repozytorium NATO.*

Podstawowe standardy NATO dotyczące ochrony informacji przed przejęciem jej metodami infiltracji środowiska elektromagnetycznego:

- *MC 315: NATO Policy on Control of Compromising Emanations;*
- *AMSG 719: Installation of Electrical Equipment for The Processing of Classified Information;*
- *AMSG 720: Compromising Emanations Laboratory Test Standard;*

[10] *AC/35-D1012 (Revised) „NATO Trusted Computer System Evaliation Criteria"*, Maj 1990.

- *AMSG 784 B: vol.1-Laboratory Test Standard for Tactical Mobile Equipment/System; vol.2 -Test Procedures for Tactical Mobile Platforms;*
- *AMSG 788: Compromising Emanations Laboratory Test Standard s for Protected Facility Equipment;*
- *AMSG 799: NATO TEMPEST Zoning Concept and Evaluation Procedures.*

Wymienione normy obowiązują w danym kraju stowarzyszonym w odniesieniu do systemów organizowanych przez NATO lub systemów narodowych, w których jest przetwarzana informacja NATO.

Wymagania zostały zdefiniowane w roku 1982 i zawarte w dokumencie *AMSG 720B „Compromising Emanations Laboratory Tests Standard"*. Wymagania tego dokumentu zbieżne są z wymaganiami pierwszego poziomu dokumentu *NSTISSAM TEMPEST/1-92*. Wyroby, które spełniają wymagania powyższej normy umieszczane są na liście sprzętu zalecanego (*NATO Recommended Product List*).

Mniej restrykcyjne wymagania zawierają dokumenty *AMSG 788A* i *AMSG 784*, które odpowiadają odpowiednio *NSTISSAM TEMPEST/1- 92 – Level II* oraz *NSTISSAM TEMPEST/1-92 – Level III.*

Poszczególne kraje członkowskie NATO posiadają również własne, narodowe wymagania i pracujące na potrzeby swoich rządów instytucje zajmujące się ochroną informacji przed przenikaniem elektromagnetycznym

3.2.3. Instytucjonalne formy reagowania na naruszenia bezpieczeństwa informacyjnego - CIRC - Computer Incidents Response Capabilty

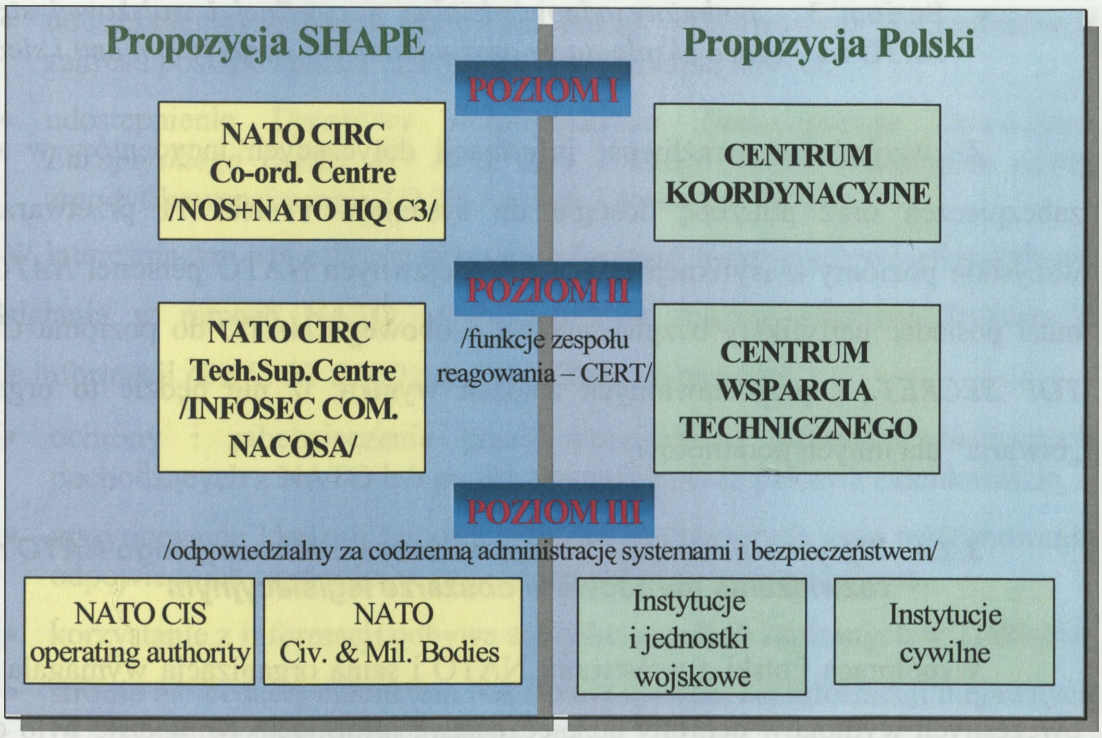
NATO przykłada wielką wagę do zabezpieczenia systemów teleinformatycznych używanych przez państwa członkowskie i dlatego opracowano dokument definiujący strukturę bezpieczeństwa teleinformatycznego NATO – *INFOSEC Framework*[11]. Dokument ten zakłada utworzenie *NATO CERT* w celu przekazywania użytkownikom systemów teleinformatycznych aktualnych ostrzeżeń i porad w zakresie zabezpieczeń. Kolejną inicjatywą NATO w zakresie bezpieczeństwa teleinformatycznego jest stworzenie możliwości szybkiego i efektywnego reagowania na zagrożenia w systemach i sieciach teleinformatycznych poprzez powołanie *NATO CIRC (Computer Incident Response Capability)*. Głównym zadaniem jest ciągła zdolność do reagowania na incydenty w chwili, gdy wystąpią. Jest to możliwe pod

[11] prezentacja *Biura Bezpieczeństwa Łączności i Informatyki UOP* na konferencji SECURE 2001

warunkiem centralizacji i przy zaangażowaniu wszystkich struktur cywilnych i wojskowych NATO. *NATO CIRC* powinien realizować następujące zadania12:

- prowadzenie oceny podatności systemów i sieci TI,
- prowadzenie testów penetracyjnych,
- prowadzenie szkoleń i warsztatów,
- opracowywanie materiałów szkoleniowych,
- analizowanie i/lub opracowywanie narzędzi dla administratorów systemów do lepszego zapobiegania i wykrywania incydentów,
- prowadzenie prac badawczych związanych z incydentami w zakresie zabezpieczeń

W koncepcji funkcjonowania *NATO CIRC* przyjęto 3-warstową strukturę zarządzania, wykorzystując w maksymalnym stopniu obecne zasoby i strukturę organizacyjną, przedstawioną na ***Rysunku Nr_12***[13].



Rysunek 12: ***Diagram przedstawiający strukturę organizacyjną CIRC***

Źródło: prezentacja *Biura Bezpieczeństwa Łączności i Informatyki UOP* na konferencji SECURE 2001

[12] *Ibidem*
[13] *Ibidem*

W strukturze *NATO CIRC* wyróżnia się następujące poziomy :

- Poziom 1 - *Centrum Koordynacyjne NATO CIRC (NATO Computer Incident Response Capability Coordination Centre)* – stanowi je *Biuro Bezpieczeństwa NATO (NATO Office of Security - NOS)* w połączeniu z *Pionami Bezpieczeństwa Teleinformatycznego Sztabów Konsultacji, Dowodzenia i Kontroli Kwatery Głównej NATO (INFOSEC Branch NATO HQ C3 Staffs)* w celu uwzględnienia odpowiedzialności *Komitetu Bezpieczeństwa NATO (NATO Security Committee - NSC)* i *Rady Konsultacji, Dowodzenia i Kontroli NATO (NATO Consultation Command Control Body – NC3B);*
- Poziom 2 *Centrum Wsparcia Technicznego NATO CIRC (NATO CIRC Technical Support Centre),* wykonujące funkcje CERT - jest to personel techniczny udzielający na żądanie lub w razie potrzeby bezpośredniej pomocy technicznej – personel wywodzi się ze struktury bezpieczeństwa teleinformatycznego *Agencji Eksploatacji i Serwisowania Systemów Teleinformatycznych NATO (INFOSEC Command NACOSA*) z dodatkowym wsparciem technicznym ze strony *Agencji Konsultacji Dowodzenia i Kontroli NATO (NATO C3 Agency – NC3A*);
- Poziom 3 – *podmioty odpowiedzialne w cywilnej i wojskowej strukturze NATO za bieżącą eksploatację oraz administrowanie systemami i sieciami .*

Ze względu na wrażliwość informacji dotyczących incydentów w zakresie zabezpieczeń oraz potrzebę dostępu do systemów i sieci TI przetwarzających wszystkie poziomy klasyfikacji informacji niejawnych NATO personel *NATO CIRC* musi posiadać certyfikaty bezpieczeństwa osobowego NATO do poziomu *COSMIC TOP SECRET.* Z przedstawionych założeń wynika, iż nie będzie to organizacja „otwarta" dla innych podmiotów.

3.2.4. Wpływ standardów bezpieczeństwa informacyjnego NATO na rozwiązania narodowe w obszarze legislacyjnym

Współpraca Polski z państwami NATO i samą organizacją wymagała zmiany ówczesnych wymogów ochrony bezpieczeństwa informacji. Konieczne było odejście od zasad ujętych w ustawie o tajemnicy państwowej i służbowej z 1982 roku. Dążenie do opracowania właściwych zasad posługiwania się informacjami niejawnymi było procesem wieloetapowym:

- podpisanie przez premiera rządu RP w Brukseli w dniu 2 lutego 1194r. *„Dokumentu Ramowego Partnerstwa dla Pokoju (PdP)''*;
- przedłożenie przez Polskę w dniu 25 kwietnia 1994r. w Kwaterze Głównej NATO *Dokumentu Prezentacyjnego PdP NATO-PL*;
- zatwierdzenie w dniu 5 lipca 1994r. *„Indywidualnego Programu Partnerstwa Rzeczpospolita Polska – NATO''*;
- przekazanie przez ambasadora pełnomocnego RP przy NATO w Brukseli w dniu 3 listopada 1994r. podpisanej deklaracji zobowiązań co do *„Zasad Postępowania''* z oferowanymi dla RP przez NATO informacjami niejawnymi;
- podpisanie przez Sekretarza Generalnego NATO i przez ambasadora pełnomocnego RP przy NATO w Brukseli w dniu 3 listopada 18994r. *„Umowy o Bezpieczeństwie'' związanej z przystąpieniem Polski do programu „Partnerstwo dla Pokoju (PdP)''*;
- przyjęcie z dniem 12 kwietnia 1995r. przez NATO przedstawionych przez Polskę rękojmi ochrony powierzanych tajemnic układu w zakresie PdP - była to akceptacja *Uprawnień Rzeczypospolitej Polskiej*;
- udostępnienie agendom rządowym Polski podstawowych dokumentów z zakresu postępowania z informacją poufną i tajną NATO;
- udostępnienie *Dyrektywy Bezpieczeństwa Zjednoczonego Dowództwa Europejskiego (ACE) AD 70* z dnia 1 lutego 1989r. i następnie nowej zmodyfikowanej wersji *AD 70-1* z dnia 1 stycznia 1997r.

W interesującym nas zakresie ochrony informacji niejawnych wszelkie kwestie współdziałania w ramach NATO reguluje umowa między stronami *Traktatu* o ochronie informacji.*(Dz.U. Nr 64/00 poz.740)*. Obliguje nas do:

- ochrony i zabezpieczenia przed ujawnieniem informacji niejawnych pochodzących z NATO lub przekazywanych przez państwa członkowskie,
- utrzymywania klauzuli tajności informacji niejawnych oraz podejmowania odpowiednich czynności w celu odpowiedniego zabezpieczenia,
- korzystanie z informacji odbywa się tylko w celach zapisanych w Traktacie,
- stronie nie będącej członkiem NATO nie ujawnia się informacji niejawnych bez zgody organu zastrzegającego.

W celu odpowiedniego zabezpieczenia informacji strony zobligowane są do utworzenia *Krajowych Władz Bezpieczeństwa*. Zgodnie z art.15 ustawy o ochronie informacji niejawnych w stosunkach międzynarodowych *Szef Agencji Bezpieczeństwa Wewnętrznego oraz Szef Wojskowych Służb Informacyjnych* pełnią funkcję *Krajowych Władz Bezpieczeństwa.*

Umowa nakłada na strony obowiązek właściwego sprawdzenia wszystkich osób, które z racji pełnionych obowiązków służbowych będą miały dostęp do informacji niejawnych. Ma to na celu zabezpieczenie informacji przed niedopuszczalnym ryzykiem jej ewentualnego ujawnienia, dlatego też sprawdzenie powinno być zakończone przed przystąpieniem do wykonywania obowiązków służbowych. Uzupełnieniem umowy o ochronie informacji niejawnych między stronami Traktatu Północnoatlantyckiego jest *Dyrektywa Bezpieczeństwa AD 70–1*, która ustanawia strefy bezpieczeństwa i strefy administracyjne jako podstawę ochrony informacji niejawnych. Dało to sposobność dostosowania się do wymogów Traktatu poprzez wprowadzenie pojęcia strefy bezpieczeństwa w ustawie z dnia 22 stycznia 1999 roku o ochronie informacji niejawnych. Celem strefy bezpieczeństwa jest utworzenie systemu nadzoru chroniącego niejawne informacje przed dostępem osób niepowołanych. Istotne jest, aby system nadzoru i zabezpieczeń fizycznych był starannie przemyślany, aby właściwie spełniał swoją funkcję. Strefy administracyjne przylegają do stref bezpieczeństwa. W strefach tych powinna istnieć możliwość kontroli pojazdów i ludzi.

Umowa między stronami Traktatu Północnoatlantyckiego o ochronie informacji nie zabrania stronom zawierania innych umów w sprawie wymiany informacji niejawnych, jeżeli te umowy nie wpływają na zakres obowiązywania Traktatu. (*art.4. Traktatu Północnoatlantyckiego o ochronie informacji*). Przyjęte reguły to zobowiązania minimalne, które powinny być bezwzględnie przestrzegane.

3.3. Standardy Unii Europejskiej w zakresie bezpieczeństwa informacyjnego

Bezpieczeństwo sieci, systemów teleinformatycznych oraz przetwarzanych w nich informacji funkcjonuje jako część unijnej prawnej struktury obejmującej telekomunikację, elektronikę, handel i podpis elektroniczny. Jest domeną powołanego w tym celu gremium ustawodawczego działającego w strukturze Unii Europejskiej.

Standardy ochrony informacji niejawnych w państwach członkowskich UE, mające wpływ na kształt polskiej ustawy, regulowane są przez następujące akty prawne:

- Decyzja Komisji Europejskiej z 30 listopada 1994 r. dotycząca zasad ochrony klasyfikowanych informacji, przygotowywanych lub wymienianych przez członków Unii Europejskiej;
- *Decyzja Rady Europejskiej* z 12 maja 1998 r. dotycząca autoryzacji procedur osób zatrudnionych w sekretariacie generalnym Rady, którzy mają dostęp do informacji chronionych przez Radę;
- Regulacje *EUROPOLU z* 1 listopada 1995 r.;
- Wskazówki *Rady EURATOMU* dotyczące art. 24 traktatu o Europejskiej Wspólnocie *EURATOM* z 6 października 1958 r.

Powyższe dokumenty gwarantują standardy ochrony informacji niejawnych w państwach członkowskich na zasadzie wzajemności i zapewniają utrzymywanie jednakowego poziomu zabezpieczeń danych informacji w poszczególnych państwach. Dostęp do informacji posiadają jedynie osoby,[14] które uzyskały uprawnienia na podstawie postępowań sprawdzających, jednakowych dla wszystkich państw członkowskich.

Jednym z wniosków, jakie *Komisja Europejska* przyjęła w konkluzji swej Opinii przedstawianej podczas szczytu Rady Europejskiej w Luksemburgu w grudniu 1997 roku, było stwierdzenie, że do skutecznego stosowania i egzekwowania polskiego prawa zharmonizowanego ze wspólnotowym niezbędne będą dalsze reformy administracyjne. W konsekwencji strategii przedakcesyjnej przygotowanej przez Radę Europy zwrócono szczególną uwagę na wzmocnienie struktur administracyjnych i stworzenie warunków do ich sprawnego funkcjonowania, w tym przygotowanie kadr weryfikowanych w oparciu o ujęte w narodowej ustawie postępowania sprawdzające oraz obieg niejawnych informacji i materiałów.

Ewolucyjny proces dostosowawczy polskiego ustawodawstwa do obowiązującego w państwach członkowskich Unii Europejskiej w zakresie ochrony informacji niejawnych oraz całości problematyki bezpieczeństwa systemów i sieci teleinformatycznych je przetwarzających, jest wynikiem postępu technologicznego i wynikających z tego faktu zagrożeń. Opracowany przez Polskę *Narodowy Program Przygotowania do Członkostwa w Unii Europejskiej (NPPC)*[15] wyznaczył dalsze

[14] *Art. 10-12 traktatu z Maastricht.*
[15] *Narodowy Program Przygotowania do Członkostwa w U.E.* http://www.polindustry.org.pl/npp/02.htm

kierunki działań dostosowawczych zmierzających do spełnienia przez Polskę wymogów.

Niewątpliwie wpływ na przyszłe, ewentualne zmiany w polskim ustawodawstwie będzie miała *rezolucja Rady Unii Europejskiej*[16] z dnia 28 stycznia 2002 r. Nr 2002/C 43/02 *W sprawie wspólnego podejścia i określenia działań dotyczących bezpieczeństwa informacji oraz sieci teleinformatycznych*. Zamiarem jest praktyczne wprowadzenie w życie wniosków z posiedzenia Rady Europy[17] w zakresie strategii bezpieczeństwa informacji i sieci teleinformatycznych

3.3.1. Programy rozwoju społeczeństwa informacyjnego w dyrektywach Unii Europejskiej

Już w roku 1994 na zlecenie *Rady Europejskiej* został opracowany raport *Europe and the global information society; Recommendations to the European Counci*", znany powszechnie jako *Raport Bangemanna*. Był to dokument wyrażający zainteresowanie Europy tzw. społeczeństwem informacyjnym, czyli kształtem przyszłego stanu społeczno-gospodarczego naszego kontynentu na tle działań podjętych przez administrację Stanów Zjednoczonych w kierunku rozwoju infrastruktury informatycznej. Raport wyraźnie wskazywał, iż te kraje, które najwcześniej zainwestują w rozwój technologii dostępu do informacji i jej przesyłania, uzyskają przewagę ekonomiczną. Istotnym elementem mającym zapewniać rozwój *Egospodarki* jest zapewnienie odpowiedniego poziomu bezpieczeństwa korzystania z elektronicznych mediów przesyłania danych. W czasie sesji Rady Europejskiej w Lizbonie dn. 23-24 marca 2000 roku szefowie rządów i państw Unii Europejskiej wytyczyli dla Europy ambitny cel na następne dziesięciolecie: ma ona stać się "*najbardziej konkurencyjną i dynamiczną, opartą na wiedzy gospodarką na świecie*". Rada uznała, że istnieje pilna potrzeba szybkiego wykorzystania przez Europę możliwości, jakie stwarza właśnie taka gospodarka, a zwłaszcza Internet. Aby zaspokoić tę potrzebę, w Feirze w dniach 19-20 czerwca 2000 r. ogłoszono *Plan Działania eEuropa.*

[16] Na podstawie fragmentów tłumaczenia zrealizowanego przez *zespół - ENSI Sp. z o.o.*
[17] Sztokholm, 23 i 24 marzec 2001 r.

Implikacją zwrócenia uwagi na znaczenie bezpieczeństwa korzystania z elektronicznych mediów przesyłania danych jest sporządzenie w dniu 23 listopada 2001 roku w Budapeszcie Konwencji o cyberprzestępczości („*Convention on Cybercrime*"[18]). W preambule, między innymi, wyraźnie zaznaczono, iż stworzono ją w „ przekonaniu o potrzebie prowadzenia, jako kwestii priorytetowej, wspólnej polityki kryminalnej mającej na celu ochronę społeczeństwa przed cyberprzestępczością, między innymi poprzez przyjęcie właściwych przepisów prawnych i wspieranie międzynarodowej współpracy". Konwencja wskazuje jakie działania muszą podjąć kraje, które ją ratyfikują. Są to zarówno działania na szczeblu krajowym w obszarze prawa karnego, prawa procesowego (szczególnie w zakresie dowodu cyfrowego), jak też współpracy międzynarodowej w zakresie wzajemnej pomocy prawnej (w zabezpieczeniu przechowywanych danych informatycznych, udostępnianiu tych danych, przechwytywaniu). Kolejnym krokiem państw europejskich na drodze wzmocnienia bezpieczeństwa informacji jest wydanie przez Radę Europy 28 stycznia 2002 r. rezolucji „w sprawie wspólnego podejścia i określenia działań dotyczących bezpieczeństwa informacji oraz sieci teleinformatycznych" („*Resolution on a common approach a specific actions in the area of network and information security*"[19]). Rezolucja wymienia osiem konkretnych punktów, których zrealizowanie powinno zbliżyć nas do osiągnięcia stanu, w którym możemy uznać, iż informacja jest bezpieczna:

- Do końca roku 2002 rozpocząć kampanię informacyjną i edukacyjną zmierzającą do wzrostu świadomości na temat bezpieczeństwa sieciowego i bezpieczeństwa informacji. Kampania ta powinna dotyczyć zarówno użytkowników indywidualnych, sektora komercyjnego, jak i administracji publicznej.
- Promować najlepsze praktyki w zarządzaniu bezpieczeństwem, zwłaszcza w małych i średnich przedsiębiorstwach, bazując na międzynarodowych standardach z tej dziedziny.
- Do końca roku 2002 wzmacniać lub promować elementy bezpieczeństwa w programach edukacyjnych i szkoleniowych dotyczących informatyki.
- Do połowy roku 2002 dokonać ustaleń i planów związanych z odpowiedzią na sytuacje awaryjne; powinny one zawierać systemy alertów wirusowych,

[18] *Convention on Cybercrime*. http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm
[19] European *Council. „Council Resolution on a common approach a specific actions in the area of network and information security (2002/C 43/02).*

z uwzględnieniem tam, gdzie jest to konieczne, poprawy możliwości zapobiegania, wykrywania i skutecznego reagowania na poziomie krajowym i międzynarodowym na przypadki ataków i zakłócania działania systemów informatycznych.

- Promować stosowanie standardu *ISO-15408 (Common Criteria)*, co zmierza do wzajemnego uznawania odpowiednich certyfikatów.
- Do końca roku 2002 udoskonalić rozwiązania związane z *Egovernment* i *Eprocurement*, bazujące na rozwiązaniach międzynarodowych. Aby umożliwić działanie serwisów *on-line*, powinno się je powiązać ze stosowaniem podpisów elektronicznych.
- Promować systemy identyfikacji elektronicznej i biometrycznej.
- W celu zacieśniania współpracy międzynarodowej pracować nad wymianą informacji pomiędzy organizacjami, odpowiedzialnymi w danych regionach za aspekty bezpieczeństwa teleinformatycznego[20].

Przedstawione w dokumencie terminy wyraźnie pokazują, że zadania te już powinny być realizowane. Równocześnie zapisy rezolucji wymieniają warunki, jakie powinny być spełnione, aby można było powiedzieć, że dana informacja jest bezpieczna:

- zapewniona jest dostępność serwisów i danych,
- istnieje zabezpieczenie przed zakłóceniem i nieautoryzowanym przechwyceniem komunikacji,
- jest potwierdzenie, że dane – które zostały wysłane, otrzymane lub są przechowywane – są kompletne i niezmienione,
- zabezpieczona jest poufność danych,
- system jest zabezpieczony przed nieautoryzowanym dostępem,
- jest zabezpieczenie przed atakami wykorzystującymi złośliwe oprogramowanie,
- zapewnione jest niezawodne zabezpieczenie[21].

Stanowisko Unii Europejskiej dotyczy wszystkich krajów członkowskich, jak również krajów kandydujących (w tym Polski). Realizację stawianych przez Komisję Europejską celów mają wspomóc dwa projekty:

---

[20] K. Silicki, M. Maj *Ochrona Krytycznej Infrastruktury Państwa. Koordynacja działań w skali kraju.* Materiały z konferencji IT.Forum „*Bezpieczna Infrastruktura*" Warszawa 18.04.2002 r.
[21] *Ibidem*

- *eCSIRT.NET*: stworzenie wspólnej terminologii dla incydentów naruszających bezpieczeństwo teleinformatyczne, stworzenie roboczego systemu wymiany informacji na temat odnotowywanych przypadków naruszenia bezpieczeństwa teleinformatycznego, przygotowywanie informacji, która będzie podstawą Europejskiego systemu wczesnego ostrzegania. W skład konsorcjum, które ma realizować te cele, wchodzą następujące zespoły reagujące: *CERT Polska(Polska), DFN-CERT (Niemcy), DK-CERT (Dania), GARR-CERT (Włochy), IRIS CERT (Hiszpania), JANET-CERT (Wielka Brytania), RENATER (Francja)*.
- *COCISA (Centre of Competence in Internet Security Area)*, którego założenia przygotował zespół *CERT Polska*. Głównym jego celem jest stworzenie na terenie Polski *Centrum Kompetencji* w dziedzinie bezpieczeństwa teleinformatycznego, które będzie realizowało zadania zmierzające do poprawy bezpieczeństwa polskich zasobów Internetu oraz koordynowało polskie inicjatywy z tym, co w dziedzinie bezpieczeństwa teleinformatycznego dzieje się w Europie[22].

Przedstawione działania i plany w zakresie bezpieczeństwa teleinformacyjnego i ochrony krytycznej infrastruktury na poziomie instytucji Rady Europy opierają się głównie na narodowych zespołach *CERT (Computer Emergency Response Team – Grupa Reagowania Komputerowego)*. Zespoły *CERT* realizują następujące zadania:

- rejestrowanie oraz analiza zdarzeń naruszających bezpieczeństwo systemów i sieci;
- likwidowanie oraz pomoc przy likwidacji skutków ataków;
- prowadzenie działalności informacyjno-zapobiegawczej oraz szkoleń;
- audit bezpieczeństwa oraz prowadzenie testów penetracyjnych systemów i sieci teleinformatycznych;
- wydawanie analiz technicznych oraz tworzenie sprawozdań dotyczących oprogramowania „złośliwego”[23].

Przedstawione zadania zespołów *CERT* wskazują na ograniczony obszar działania w stosunku do zakresu ochrony krytycznej infrastruktury i bezpieczeństwa informacyjnego do incydentów w odniesieniu do otwartych systemów i sieci teleinformatycznych. Mogą stanowić tylko struktury pomocnicze, acz o znaczącym wpływie dla organizacji powołanych przez państwo dla zapewnienia bezpieczeństwa państwa i wyposażonych we właściwe instrumenty prawne.

---

[22] *Ibidem*

[23] D. Mąka *Elementy analizy zagrożeń i zarządzania ryzykiem w świetle polityki bezpieczeństwa informacyjnego*; IT Security Magazine nr 8-9 z 2001 r.

3.3.2. Regulacje prawne związane z ochroną kluczowych zasobów informacyjnych Unii Europejskiej

Do głównych dokumentów regulujących ochronę informacji w Unii Europejskiej należą:

- Zalecenie[24] *Rady UE 95/144/EC z* 7 kwietnia 1995 r. w zakresie wspólnych kryteriów oceny informatycznej technologii bezpieczeństwa;
- Komunikat z posiedzenia *Komisji Europejskiej* dotyczący tworzenia bezpieczniejszego społeczeństwa poprzez unowocześnianie infrastruktury bezpieczeństwa informatycznego i zwalczanie przestępstw komputerowych;
- *Dyrektywa 97/66/EC Parlamentu Europejskiego i Rady Europy* z 15 grudnia 1997 r. dotycząca przetwarzania danych osobowych i ich ochrony sektorze telekomunikacyjnym;
- *Dyrektywa 99/93/EC Parlamentu Europejskiego i Rady Europy* z 13 grudnia 1999 r. dotycząca ramowych warunków Wspólnoty dla podpisu elektronicznego.
- *Rezolucja Rady* z 30 maja 2001 r. dotycząca – *eEuropejskiego Planu Działania* w zakresie bezpieczeństwa informacji i sieci teleinformatycznych. Dział bezpieczeństwa informacji i sieci teleinformatycznych dotyczy:
  - zapewniania dostępności do usług i danych;
  - zapobiegania zakłóceniom i nieautoryzowanemu przechwytywaniu transmisji danych w systemach teleinformatycznych;
  - zapewnienia integralności przesłanym i przechowywanym informacjom;
  - zabezpieczenia informacjom poufności25);
  - ochrony systemów informatycznych przed nieautoryzowanym dostępem;
  - stałej ochrony przed zaatakowaniem złośliwym oprogramowaniem (wirusem);
  - uwierzytelniania.

[24] *Zalecenie* - nie jest aktem prawa i nie ma mocy wiążącej. Może być wydane przez Radę lub Komisję celem przekonania adresatów do podejmowania określonych działań, zwłaszcza w dziedzinach, w których nie można wprowadzać ustawodawstwa wspólnotowego.

[25] *Poufność* (confidentiality) w pojęciu UE: zagwarantowanie, że do danych przechowywanych w systemach komputerowych, przetwarzanych i przesyłanych pomiędzy tymi systemami oraz do informacji o systemie mogą mieć dostęp tylko uprawnione osoby. Mechanizmami zapewniającymi poufność są m.in. kontrolowanie dostępu MAC *(Mandatory Access Control)*/ DAC *(Discretionary Access Control),* szyfrowanie i kodowanie informacji stosowne w łączach i logicznych połączeniach pomiędzy użytkownikami sieci komputerowych (end-to-end).

Na posiedzeniu *COREPER (Komitet Stałych Przedstawicieli przy Wspólnotach Europejskich*) w dniu 27.07.2000r. państwa członkowskie Unii Europejskiej podjęły jednomyślną decyzję dotyczącą ograniczenia dostępności jej dokumentów związanych z polityką bezpieczeństwa i obronną.

Z przyjętych przez Unię Europejską planów działania wynika konieczność wzmożenia kontroli dostępu do zasobów systemów i sieci teleinformatycznych, zwiększenia efektywności ochrony przed nieuprawnionym dostępem, zwiększenia zdolności w wykrywaniu i skutecznym reagowaniu na zakłócenia oraz ataki w narodowych a także międzynarodowych sieciach i systemach teleinformatycznych. W celu ułatwienia wzajemnego uznania odpowiednich certyfikatów, dążeniem Unii Europejskiej jest stosowanie wspólnych kryteriów (*standard ISO-15408*) do zdefiniowania wymogów bezpieczeństwa dla produktów, jakim są systemy i sieci teleinformatyczne26) oraz oceny, czy określone produkty spełniają te wymagania. W tym też duchu *Międzynarodowy Standard ISO-17799* (technika informatyczna – praktyczne zasady zarządzania bezpieczeństwem informacji) i podobne narodowe wytyczne są uznanymi zasadami dla zarządzania bezpieczeństwem w prywatnych i publicznych organizacjach.

Należy zaznaczyć, że Unia Europejska nie posiada odrębnych uregulowań w aspekcie bezpieczeństwa elektromagnetycznego; zawarte są one pośrednio w problematyce ochrony sieci i systemów teleinformatycznych przetwarzających informacje prawnie chronione. Problem elektromagnetyzmu, obejmujący również wchodzącą w zakres niniejszej pracy studyjnej ochronę przed zaburzeniami, zawarty jest głównie w dyrektywie *89/336/EWG* dotyczącej kompatybilności elektromagnetycznej[27].

[26] UE stosuje kryteria *ITSEC*

[27] *Dyrektywa 89/336/EWG* z 3 maja 1989 r. *„W sprawie ujednolicenia w państwach członkowskich praw dotyczących kompatybilności elektromagnetycznej”* (wraz ze zmianami wprowadzonymi *Dyrektywami 91/263/EWG* z 29 kwietnia 1991 r. *92/31/EWG* z 28 kwietnia 1992 r. i *93/68/EWG* z 22 lipca 1993 r.).

3.3.3. Problematyka cyberprzestępczości w polityce bezpieczeństwa informacyjnego Unii Europejskiej

Cyberterroryzm (zwany czasem *soft terrorism*) – definiowany jest jako działania blokujące, niszczące lub zniekształcające w stosunku do informacji przetwarzanej, przechowywanej i przekazywanej w systemach teleinformatycznych oraz niszczące (obezwładniające) te systemy.

W pojęciu tym mieści się także wykorzystywanie systemów teleinformatycznych do dezinformacji, walki psychologicznej itp. Celem ataku jest najczęściej informacja przetwarzana, a nie system jako taki.

Pojawia się też czasem określenie cyberterroryzmu jako nowego rodzaju broni masowego rażenia (*WMD – Weapon of Mass Destruction*).

Cyberterroryzm jest określeniem wieloznacznym, któremu nadaje się różny sens w zależności o kontekstu, w jakim pojęcie to jest używane. Amerykańscy wojskowi specjaliści od bezpieczeństwa komputerowego uznają każdy zamach na serwery departamentu obrony USA za *akt cyberterrorystyczny*, tylko z tego powodu, że w chwili jego nastąpienia nie wiadomo, kto „za nim stoi" i jakie ma intencje. Dla FBI przejawem cyberterroryzmu są politycznie motywowane przestępstwa o charakterze destrukcyjnym popełniane przy pomocy systemów komputerowych, które są skierowane przeciwko obiektom cywilnym i mają na celu wywołanie niepokoju społecznego. W ramach tej definicji mieści się więc zarówno spowodowanie katastrofy lotniczej na skutek ingerencji w komputerowo wspomagany system kontroli lotów, jak i odcięcie dostaw energii elektrycznej lub gazu do wielkiej metropolii, a także gwałtowna destabilizacja notowań na *Wall Street* wywołana elektronicznym atakiem na systemy informatyczne giełdy. Z cyberterroryzmem utożsamia się niekiedy podejmowane z pobudek politycznych lub ideologicznych ataki na serwery i strony www *"wrogich"* instytucji lub organizacji. Kojarzy się z nim wreszcie wykorzystywanie Internetu i poczty elektronicznej przez członków ugrupowań terrorystycznych, takich jak np. *Hamas*, do komunikowania się ze sobą, rekrutowania ochotników i publikowania informacji o planowanych operacjach zbrojnych lub ich skutkach.

Według D. Denning – autorki wielu książek z tego zakresu definicja cyberterroryzmu powinna uwzględniać kilka elementów. Przede wszystkim powinna odnosić się do bezprawnych zamachów lub groźby takich ataków na sieci i systemy komputerowe oraz przetwarzane w nich informacje. Zamachy te powinny być dokonywane w celu zastraszenia lub zmuszenia władz lub reprezentujących je osób do spełnienia określonych żądań politycznych lub społecznych. Aby atak uznać za cyberterrorystyczny, powinien on wywoływać skutki o cechach przemocy wobec osób lub mienia, lub powodować na tyle poważne szkody, by wzbudzać w ludziach uczucie strachu. Warunek ten będą spełniać ataki prowadzące do śmierci, uszczerbku na zdrowiu, eksplozji lub poważnych szkód majątkowych. Poważne ataki na elementy „*krytycznej infrastruktury*" mogą być uznane za ataki cyberterrorystyczne w zależności od ich skutków. Ataki powodujące dysfunkcjonalność mniej istotnych usług, nawet gdy narażają ich administratorów na poważne koszty, nie spełniają natomiast kryterium cyberterroryzmu[28].

W 2001 roku *Komitet Problemów Przestępczości Rady Europy* przyjął projekt konwencji międzynarodowej dotyczącej przestępczości popełnianych w sieciach komputerowych (*Draft Convention on Cybercrime*).

Projekt konwencji przewiduje nowe, niezależne międzynarodowemu prawu karnemu rozwiązania, które mają umożliwić ściąganie sprawców przestępstw popełnianych przy pomocy Internetu.

Projekt konwencji wyróżnia cztery grupy przestępstw:

1) przestępstwa przeciwko poufności, integralności i dostępności danych i systemów komputerowych, do których należą:
   - nielegalny dostęp do systemu komputerowego;
   - nielegalne przechowywanie danych przy użyciu środków technicznych;
   - ingerencja w system, która powoduje poważne zakłócenia w funkcjonowaniu systemu komputerowego na skutek wprowadzenia, uszkodzenia, usunięcia pogorszenia, zmiany lub zablokowania danych;
   - wytwarzanie, sprzedaż, oferowanie do używania, import, rozpowszechnianie lub udostępnianie w inny sposób, a także posiadanie:

[28] D. Denning . *Wojna informacyjna i bezpieczeństwo informacji*, Warszawa 2002

- przyrządów lub narzędzi, w tym programów komputerowych, przeznaczonych lub specjalnie przystosowanych do celów związanych z popełnieniem ww. przestępstw;
- haseł, kodów dostępu lub innych podobnych danych umożliwiających dostęp do systemu komputerowego lub jego części, w zamiarze użycia ich w celu popełnienia któregokolwiek z ww. przestępstw.

2) przestępstwa związane z użyciem komputera (fałszerstwo i oszustwo komputerowe) - przestępstwa przeciwko własności intelektualnej.

3.3.4. Elementy wspólnej polityki NATO i Unii Europejskiej w obszarze bezpieczeństwa informacyjnego

Prace w zakresie unormowania problematyki ochrony informacji niejawnych w związku z przystąpieniem Polski do NATO zbiegły się z procesem dostosowawczym funkcjonowania dziedzin gospodarki i administracji do wymogów Unii Europejskiej i Unii Zachodnioeuropejskiej umożliwiającej nam udział w budowie *Europejskiej Tożsamości Obronnej*. Stowarzyszenie z instytucjami europejskimi i euroatlantyckimi stanowiło dla naszego kraju priorytet w zakresie dostosowania przepisów do obowiązujących w państwach członkowskich wymienionych organizacji i wskazywały na szeroko pojętą konieczność legislacyjnego unormowania problematyki ochrony informacji niejawnych.

Standardy ochrony informacji niejawnych w państwach członkowskich UE, mające wpływ na kształt polskiej ustawy, regulowane są przez następujące akty prawne:

- *decyzja Komisji Europejskiej* z 30 listopada 1994r dotycząca zasad klasyfikowanych informacji, przygotowywanych lub wymienianych przez członków Unii Europejskiej;
- *decyzja Rady Europejskiej* z 12 maja 1998r. dotycząca autoryzacji procedur osób zatrudnionych w sekretariacie generalnym Rady, którzy mają dostęp do informacji chronionych przez Radę;
- *regulacje EUROPOLU* z 1 listopada 1995r.;
- *wskazówki Rady EURATOMU* dotyczące art. 24 *Traktatu o Europejskiej Wspólnocie EURATOM* z 6 października 1958r.

Powyższe dokumenty gwarantują standardy ochrony informacji niejawnych w państwach członkowskich na zasadzie wzajemności i zapewniają utrzymanie poziomu

zabezpieczeń danych informacji w poszczególnych państwach. Dostęp do informacji posiadają jedynie osoby, które uzyskały uprawnienia na podstawie postępowań sprawdzających, jednakowych dla wszystkich państw członkowskich.

Prace legislacyjne w naszym kraju w zakresie unormowania problematyki ochrony informacji niejawnych zbiegły się z dążeniem do przystąpienia Polski do Paktu Północnoatlantyckiego. W tej sytuacji powołano w 1997 r. międzyresortowy *Zespół do Spraw Ochrony Wiadomości Stanowiących Tajemnicę Państwową*, który to był kontynuatorem analogicznego, funkcjonującego w ramach programu Partnerstwo dla Pokoju, aby wypracował projekty rozwiązań zapewniających spójność prawa polskiego w zakresie ochrony informacji niejawnych uwzględniające zakres wymogów traktatu Północnoatlantyckiego i Unii Zachodnioeuropejskiej.

3.4. Analiza zagrożeń informacyjnych imperatywem wynikającym z uwarunkowań międzynarodowych oraz z dominującej roli informacji w bezpieczeństwie państwa

W czasie, w których nie tylko w Polsce znaczenie informacji występujących w postaci elektronicznej rośnie w niespotykanym dotychczas tempie - środki teleinformatyczne wprzęgnięto do realizacji bardzo odpowiedzialnych zadań. Rośnie stąd ranga bezpieczeństwa procesów wytwarzania, przetwarzania, przesyłania i przechowywania informacji. Ranga ta jest tym większa, im przetwarzane informacje stanowią obszar wrażliwych czy też niejawnych. Jedną z dróg prowadzących do tego celu jest ***analiza zagrożeń bezpieczeństwa informacyjnego i zarządzanie ryzykiem w systemach informacyjnych***.

W polityce bezpieczeństwa informacyjnego NATO prowadzenie *analizy ryzyka* przy wdrażaniu rozwiązań techniczno-administracyjnych dotyczących gromadzenia, przechowywania, przetwarzania, przesyłania i niszczenia informacji niejawnych – jest *obligatoryjne*, a wobec państw członkowskich zastosowano klauzulę – *zalecane*.

W ***Rozdziale 2.3*** wykazano szczególną rolę informacji w obszarze militarnym bezpieczeństwa narodowego. Wzrastająca rola czynnika informacyjnego w pozostałych wymiarach bezpieczeństwa, szczególnie w świetle coraz częstszych przypadków *utraty poufności* informacji na skutek braku właściwych procedur

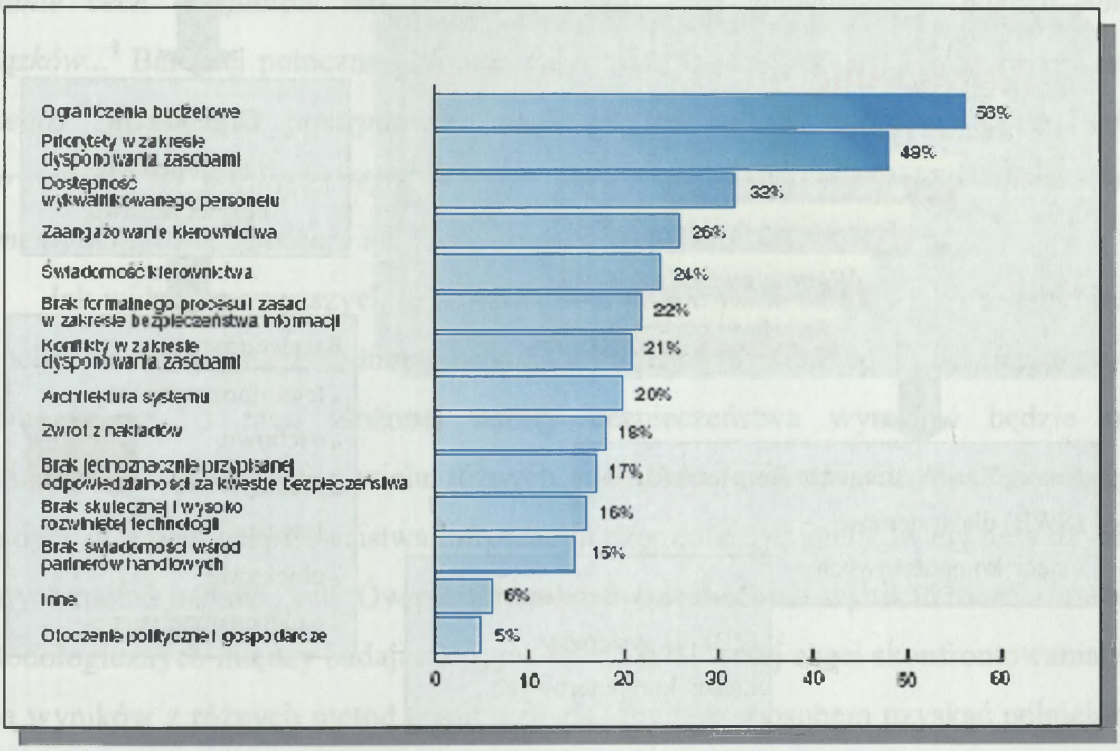
bezpieczeństwa lub nierzetelności w ich przestrzeganiu, implikuje potrzebę doskonalenia narzędzi ochrony. Po 11 września 2001 roku wzrosła liczba zagrożeń, które należy wziąć pod uwagę, chcąc dobrze przygotować się na ewentualność utraty bezpieczeństwa.

Badania pt. *Bezpieczeństwo Informacji 2003* przeprowadzone przez ośrodek analityczny *Ernst & Young* wykazały, co następuje:

- 90% przedsiębiorstw twierdzi, że bezpieczeństwo informacji stanowi ważny czynnik w osiąganiu ich celów;
- 78% przedsiębiorstw twierdzi, że ograniczanie ryzyka jest najważniejszym czynnikiem decydującym o wydatkach związanych z bezpieczeństwem informacji;
- ponad 34% przedsiębiorstw uważa, że nie jest w stanie wykrywać ataki na swoje systemy;
- ponad 33% przedsiębiorstw twierdzi, że nie jest w stanie odpowiednio reagować na incydenty dotyczące bezpieczeństwa informacji;
- jedynie 34% przedsiębiorstw twierdzi, że przestrzega wymogów dotyczących bezpieczeństwa informacji narzuconych przez przepisy prawne;
- 56% przedsiębiorstw wskazuje, że główną przeszkodą uniemożliwiającą osiągnięcie zadowalającego poziomu bezpieczeństwa informacji są ograniczenia budżetowe;
- blisko 60% przedsiębiorstw twierdzi, że rzadko oblicza wskaźnik zwrotu z inwestycji (ROI) w odniesieniu do wydatków związanych z bezpieczeństwem informacji lub nie robi tego wcale;
- tylko 29% przedsiębiorstw wskazuje na szkolenia pracowników oraz na budowanie świadomości w zakresie bezpieczeństwa informacji jako jednego z trzech podstawowych obszarów wydatków związanych z bezpieczeństwem informacji.
- jednocześnie w przypadku 83% przedsiębiorstw największą pozycję kosztową związaną z bezpieczeństwem informacji stanowią wydatki na technologię;
- zaledwie 35% przedsiębiorstw deklaruje, że prowadzi systematyczne programy edukacyjne oraz szkolenia dotyczące budowania świadomości swych pracowników w zakresie bezpieczeństwa informacji.

Ponad jedna trzecia ankietowanych przez ośrodek analityczny *Ernst & Young* przedsiębiorstw stwierdziła, że minimalizowanie ryzyka jest kluczowym czynnikiem wpływającym na podejmowanie decyzji o wydatkach na cele związane z bezpieczeństwem informacji. Niewątpliwie, jednym z filar bezpieczeństwa informacji jest identyfikacja krytycznych dla organizacji informacji oraz określenie ***poziomu związanego z nimi ryzyka***.

Zarządzanie ryzykiem jest z pewnością właściwym uzasadnieniem inwestycji w zakresie bezpieczeństwa informacji. Świadczą o tym istotne sumy będące wynikiem wyceny szkód. Brytyjska firma zajmująca się zarządzaniem ryzykiem, *MI2G Ltd.*, twierdzi, w ciągu 2003 roku może dojść do ponad 180.000 ataków, które mogą spowodować szkody w wysokości od 80 do 100 miliardów dolarów. Według *Centrum Koordynacji CERT Uniwersytetu Carnegie Mellon* liczba zidentyfikowanych podatności system? informatycznych podwoiła się od 1998 roku. Trudno się więc dziwić, że zarządzanie ryzykiem stanowi główny czynnik motywujący do inwestowania w bezpieczeństwo informacji[29].



Wykres 10: ***Przyczyny braku skuteczności we wdrażaniu zabezpieczeń informacji***
Źródło: *Ernst & Young. Bezpieczeństwo Informacji 2003,* http:// www.ey.com/pl/tsrs

*Z **Wykresu Nr 10*** wynika, że według 56% ankietowanych, ograniczenia budżetowe stanowią główną przeszkodę wdrożenia pełnych procedur bezpieczeństwa informacyjnego. Powyższy wynik badań wskazuje kolejny, finansowy aspekt zasadności

[29] *Ernst & Young. Bezpieczeństwo Informacji* 2003. Badania ankietowe. Kwestionariusz obejmował 1400 przedsiębiorstw z 66 państw i składał się z 40 pytań

wypracowania i wdrożenia dobrych jakościowo narzędzi wspomagających pomiar, ocenę i analizę zagrożeń i, poprzez poprawne, wykorzystujące odpowiednio przygotowane programy komputerowego – właściwe zarządzanie ryzykiem bezpieczeństwa informacyjnego zgodnie z polityką bezpieczeństwa, zobrazowaną na ***Diagramie Nr 20*** .

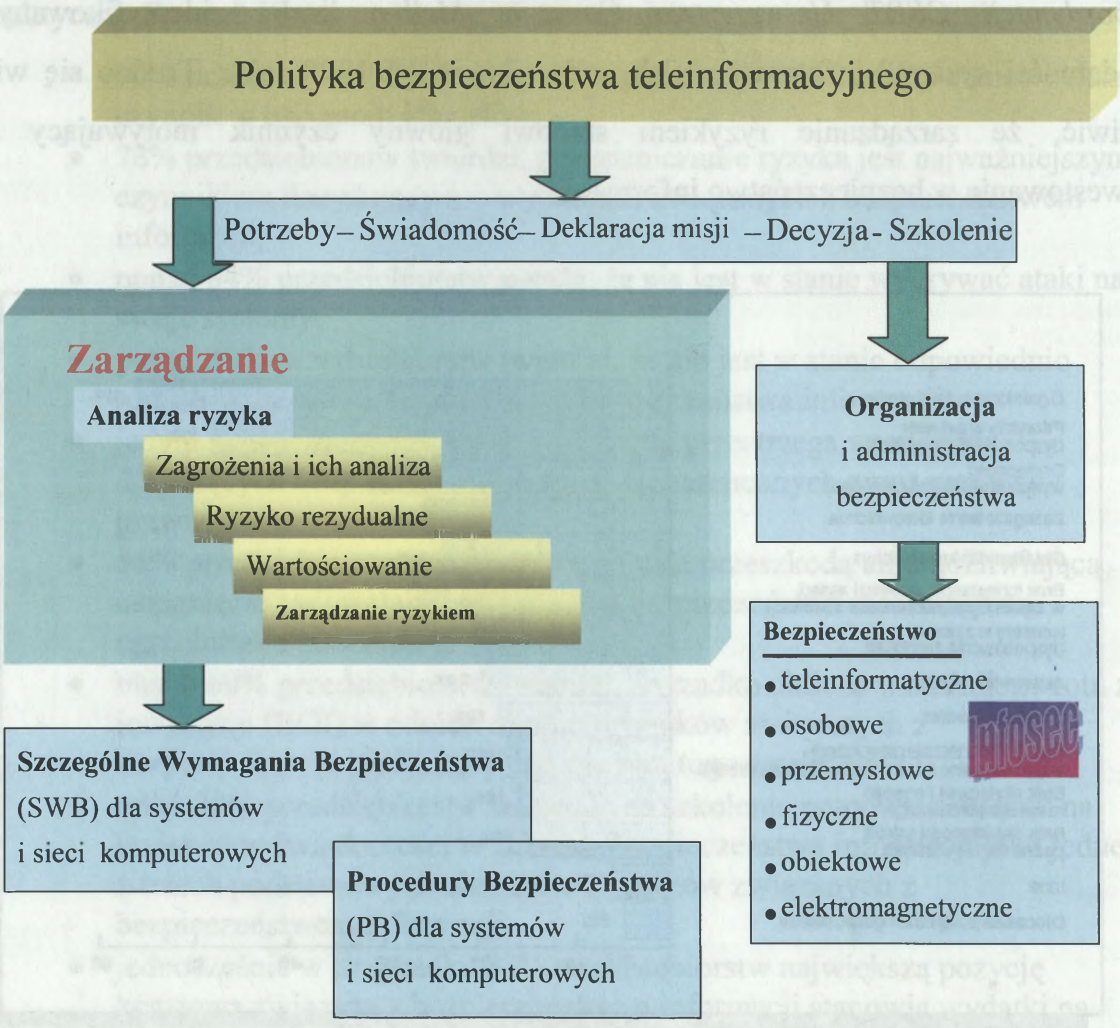


Diagram 20: ***Polityka bezpieczeństwa teleinformacyjnego***
Źródło: opracowanie własne

Analizie zagrożeń bezpieczeństwa informacyjnego i zarządzaniu ryzykiem w systemach informacyjnych w ujęciu systemowym, poświęcony jest kolejny rozdział niniejszej rozprawy.

Rozdział 4

4. Analiza zagrożeń bezpieczeństwa informacyjnego i zarządzanie ryzykiem w systemach informacyjnych

Analiza oznacza badanie, czyli trafne rozpoznanie obiektu (systemu), jego pomiar i opis w oparciu o przeprowadzony proces badawczy umożliwiający wyciągnięcie syntetyzujących wniosków.

Słownik Języka Polskiego PWN definiuje *analizę* jako *myślowe, pojęciowe wyodrębnienie cech, części lub składników badanego zjawiska lub przedmiotu; badanie cech elementów lub struktury czegoś oraz zachodzących między nimi związków...*[1] Bardziej potoczna definicja mówi: *analiza czegoś, np. jakiejś rzeczy lub jakiegoś zjawiska to postępowanie naukowe lub proces myślowy, które mają doprowadzić do poznania tego. Analiza polega zwykle na rozbiciu problemu na elementy składowe, zbadaniu ich i wyciągnięciu wniosków...*[2]

Jak widać z powyższych definicji ogólne pojmowanie analizy jako badania jest w pełni uzasadnione. Przedmiot badania – *ryzyko w systemach bezpieczeństwa informacyjnego* z racji złożonej natury bezpieczeństwa wymagać będzie od analizującego zastosowania wielu różnych metod dochodzenia prawdy. Co więcej, pojedynczy aspekt bezpieczeństwa informacyjnego może być analizowany przy użyciu różnych metod badawczych. Ów pluralizm w równym stopniu wynikać może z różnic metodologicznych między badającymi, jak też ze świadomej chęci skonfrontowania ze sobą wyników z różnych metod analitycznych, aby tym sposobem uzyskać pełniejszy ogląd zgłębianego problemu. Im bogatszego zespołu narzędzi analitycznych użyjemy, tym pełniejszy będzie materiał końcowy naszych dociekań i tym trafniejsza będzie polityka bezpieczeństwa zbudowana w oparciu o przedstawione przez nas wnioski. Należy zatem zająć się przeglądem metod analitycznych, które mogą okazać się przydatnymi w *analizowaniu ryzyka bezpieczeństwa informacyjnego*.

[1] *Słownik Języka Polskiego PWN*, Tom I, Warszawa 1978, s. 49.
[2] *Inny Słownik Języka Polskiego PWN*, Tom I, Warszawa 2002, s. 26.

Narzędzia matematyczno-statystyczne

Współcześnie, w dobie informatyki, niewybaczalnym zaniedbaniem zespołów analitycznych byłoby niewykorzystanie możliwości tkwiących w komputerach podczas badania interesujących zjawisk. Z pomocą przychodzi tu matematyka wyższa – w szczególności statystyka matematyczna, którą dzięki komputerom i odpowiednio przygotowanym programom statystycznym, posługiwać się mogą nawet osoby nieprzygotowane teoretycznie do jej wykorzystania. *„Komputery skróciły proces obliczeń matematycznych i umożliwiły przeprowadzanie precyzyjnych analiz na dużych zbiorach danych. Dlatego rozpowszechnienie technik komputerowych... przyczyniło się do znacznego rozpowszechnienia metod statystyki matematycznej... a zakres ich wykorzystania wzrasta we wszystkich dziedzinach nauki*[3].

Warto w tym miejscu zaznaczyć, że metody niżej opisywane mogą okazać się przydatne po uprzednim rozpoznaniu ewentualnych zagrożeń i ich inwentaryzacji (także zajść, które już miały miejsce, a które chcielibyśmy lepiej poznać, by skutecznie się przed nimi bronić). Metody te pozwolą przede wszystkim trafnie przewidzieć prawdopodobieństwo przyszłych zajść, dokładniej je scharakteryzować i na tej podstawie wypracować wnioski użyteczne dla projektantów systemu bezpieczeństwa.

Jak wykazano wcześniej, za metodami statystyki matematycznej stoją przeważnie rozbudowane i skomplikowane wzory matematyczne, których część autor niniejszej rozprawy zastosował w ***Rozdziale Nr 2.3*** , a przekształcenia matematyczne zamieścił w załącznikach. Pomijając zatem w tym miejscu metody obliczeniowe, autor skupił się na próbie przybliżenia cech charakterystycznych głównych typów analiz statystycznych, które mogą okazać się przydatne w dalszych dociekaniach nad bezpieczeństwem systemów informatycznych, nakreślając ramy ich użyteczności.

M. Dobosz w swojej książce *Wspomagana komputerowo statystyczna analiza wyników badań* wymienia pięć podstawowych metod analizy statystycznej:

- Analiza czynnikowa,
- Analiza kanoniczna,
- Analiza dyskryminacyjna,

[3] M. Dobosz, *Wspomagana komputerowo statystyczna analiza wyników badań*, Warszawa 2001, s. 5.

- Analiza skupień,
- Analiza tabel liczności[4].

Z powyższych metod przydatne wydają się być trzy typy analizy, mające zresztą swoje odpowiedniki w tradycyjnych, pozamatematycznych metodach badawczych.

Analiza czynnikowa

Pierwsza z metod to analiza czynnikowa. Sprawdza się ona wówczas, gdy porównujemy ze sobą *obiekty (problemy, procesy)* tego samego typu warunkowane jednak przez różne czynniki. Bogactwo determinantów powoduje, że porównując ze sobą poszczególne elementy zbioru danych musimy korzystać z wielu różnych parametrów, co komplikuje procesy analityczne. Wskazanym jest wówczas znalezienie jednego lub licznej grupy parametrów, które równie trafnie opisywałyby badany zbiór elementów, czyniąc analizę znacznie prostszą.

„Dzięki odpowiednim przekształceniom matematycznym możemy uzyskać redukcję liczby zmiennych w zbiorze danych i wówczas ten szczególny przypadek analizy czynnikowej występuje zwykle pod nazwą analizy czynników lub składowych głównych..."[5]. Inne korzyści, jakie odnieść można z zastosowania tej metody to *„uzyskanie w wyniku przeprowadzonych przekształceń takiego parametru (zespołu parametrów) opisującego zmienność w danym zbiorze danych, który umożliwi nam bardziej jednoznaczne określenie charakteru zachodzących zmian – w powyższym sensie analiza czynnikowa służy jako metoda klasyfikacji"*[6].

Analiza czynnikowa jest zatem niczym innym, jak sformalizowaną i opisaną przy pomocy wzorów matematycznych, analizą upraszczającą powszechnie stosowaną we wszystkich badaniach porównawczych.

Metoda ta może okazać się bardzo przydatna na przykład przy analizowaniu wymagań względem sprzętu służącego do transmisji, obróbki i przechowywania informacji.

[4] *Ibidem*, s. 277-375.
[5] *Ibidem*, s. 276.

Analiza skupień

Kolejną metodą badawczą która jest *de facto* matematycznym odpowiednikiem tradycyjnych metod porównawczo-analitycznych, jest analiza skupień. Zwana jest ona również *analizą klastrową* i jej istotą jest wyszukiwanie w badanej próbie elementów (wyników doświadczeń, zmiennych, obiektów) w ten sposób, by utworzyć grupy (*skupienia, klastry*), w których pod względem określonej cechy elementy te są do siebie jak najbardziej podobne i jednocześnie maksymalnie inne niż w pozostałych grupach. *„Jeśli w grupie skupiona jest mała liczba elementów (skrajnie 1), to klaster taki nazywamy słabym skupieniem lub skupieniem o najmniejszej odległości aglomeracyjnej. Jeżeli w grupie znajduje się duża liczba elementów, to mamy do czynienia z silnym skupieniem (o największej odległości aglomeracyjnej). Istnieją dwa rodzaje poszukiwania skupień: hierarchiczne i niehierarchiczne"*[7].

Analiza skupień to matematyczna wersja tradycyjnej metody badawczej w historii sztuki czy archeologii znanej w tych naukach pod nazwą *„analizy porównawczej"*. Umiejętne posługiwanie się nią wymaga od prowadzącego badania pewnej wrażliwości (zmysłu estetycznego), opatrzenia i podstawy teoretycznej zapobiegającej elementarnym pomyłkom. Tymczasem zastosowanie *sformalizowanej metody metamatyczno-statystycznej* ułatwia użycie tego typu analizy przez osoby nie posiadające odpowiedniego doświadczenia i warsztatu metodologicznego, co jest niewątpliwą korzyścią. Trzeba jednak uprzednio spełnić jeden warunek – badane zjawisko (*parametr, cecha*) muszą poddać się *skwantyfikowaniu*. Nie zawsze się to udaje.

Ten typ analizy może okazać się pomocny wszędzie tam, gdzie z pożytkiem dla dalszych dociekań jesteśmy w stanie wyodrębnić z całości badanych zjawisk logicznie powiązane ze sobą grupy. Mogą to dla przykładu być typy zagrożeń, słabe punkty systemu itp.

[6] *Ibidem.*
[7] *Ibidem*, s. 337.

Analiza tabel wielodzielnych

Najbardziej chyba matematyczną analizą z przedstawionych przez M. Dobosza jest *analiza tabel wielodzielnych*. Oto jak charakteryzuje on jej mechanizmy: *„...poszukując istotności i siły związków pomiędzy zmiennymi często mamy do czynienia z sytuacją, gdy wyniki badań stanowią dyskretne wartości w postaci liczności przypadków uzyskanych na różnych poziomach czynnika oddziałującego (klasyfikującego). Uzyskane w badaniach liczności zestawiane są w tzw. tabelach liczebności, tabelach wielodzielczych zwanych również tabelami krzyżowymi lub kontyngencji"*[8].

Przy badaniu wyników doświadczeń zapisanych w postaci tabel liczności często zdarza się, że zmienną zależną jest nie tyle liczność przypadków w danej klasie, lecz jedna ze zmiennych klasyfikujących, interesuje nas wówczas zależność między zmiennymi parametrami obiektów, a niekoniecznie udział poszczególnych obiektów o danym parametrze w całym zbiorze badanych elementów.

Upraszczając, można powiedzieć, że ten typ analizy przydatny jest przede wszystkim w tych przypadkach, gdy przychodzi badać zespoły zmieniających się danych poddane różnym, zmieniającym się czynnikom, a celem dociekań jest przede wszystkim uchwycenie dynamiki przebiegających zmian, a niekoniecznie pogrupowanie elementów badanego zbioru.

Wprawdzie i tutaj można poszukiwać wzorca pozamatematycznego, ale skomplikowanie procesu dociekań i mnogość danych, które są ze sobą zestawiane czyniłoby z tej metody badawczej, nie popartej udogodnieniami, jakie daje analitykowi matematyka i komputery, mało użyteczne narzędzie badawcze. Należałoby raczej dążyć do rozbicia badanego zbioru na mniejsze podzbiory i kolejne wyciąganie wniosków. Efekt takich dociekań mógłby jednak znacząco odbiegać od rzeczywistości, bowiem prosta suma zmienności w poszczególnych podzbiorach danych nie musi wcale być tożsama z ogólną zmiennością całego zbioru.

Zatem wszędzie tam, gdzie ogrom badanych zjawisk (*obiektów*) przerasta możliwości prostszych analiz, a jednocześnie przedmiot badań daje się

[8] *Ibidem.*

skwantyfikować, możemy posłużyć się *metodą analizy tabel wielodzielnych*, co zastosowano w niniejszej rozprawie.

Wszędzie tam, gdzie poszukuje się metod sprawdzenia lub zoptymalizowania systemów decyzyjnych, procedur reagowania kryzysowego, skuteczności regulaminów, sprawności zespołów ludzkich możena skorzystać z wygodnego narzędzia testującego, jakim są gry.

Matematyczna teoria gier

Ze względu na to, że *analiza ryzyka w systemach bezpieczeństwa informacyjnego* wiązać się musi nieodzownie z *polityką bezpieczeństwa*, zasadnym będzie krótkie omówienie teorii gier. Jest to teoria podejmowania decyzji w szczególnych, interaktywnych warunkach, w których konsekwencje działań podejmowanych przez poszczególnych uczestników, nazywanych graczami, zależą od działań pozostałych uczestników. Podobnie jak inne teorie, które zajmują się rozwiązywaniem problemu decyzji w pewnych warunkach (jakie np. narzuca nam nasz regulamin reagowania kryzysowego w systemie informacyjnym), teoria gier jest teorią normatywną. Oznacza to, że bada możliwe zachowania i decyzje uczestników w sytuacjach częściowego lub pełnego konfliktu interesów między nimi i poszukuje takich wyborów, jakich powinni dokonać racjonalni uczestnicy tych sytuacji oraz rozwiązań, które powinni zaakceptować[9]. Teoria gier znajduje zastosowanie w wielu dziedzinach życia, przede wszystkim w ekonomii i naukach politycznych.

Teoria gier ma przede wszystkim zastosowanie wszędzie tam, gdzie uczestnicy konfrontacji kierują się kryteriami racjonalnymi, choć wiele naruszeń systemów bezpieczeństwa może nie być obarczone racjonalnymi przesłankami. Wprawdzie zwolennicy tej metody uważają, że pozornie niezrozumiałe i nieracjonalne zachowania można wyjaśnić za pomocą modeli teorii gier[10], jednak wymóg racjonalności ogranicza jej zastosowanie. Nie zmienia to faktu, że z uwagi na logiczność i czytelność kryteriów oceny zachowań graczy, teoria gier jest cennym narzędziem wspomagającym analizę ryzyka w systemach bezpieczeństwa informacyjnego.

[9] G. Lissowski *Przedmowa do wydania polskiego,* w: Philip D. Straffin, *Teoria gier*, Warszawa 2001, s. VII.

Gry decyzyjne (kierownicze i wojenne)

Podobnie jak wiele innych badań prowadzonych nad naturą podejmowania decyzji oraz mających na celu optymalizację procesu decyzyjnego – również gry decyzyjne swój dynamiczny rozwój zawdzięczają ostatnim dziesięcioleciom. Także w tej dziedzinie wykorzystanie symulacji komputerowych znacząco ją wzbogaciło i usprawniło.

W Polsce duże zasługi na polu praktycznego wykorzystania gier decyzyjnych położył *Wydział Cybernetyki Wojskowej Akademii Technicznej*. Wiele cennych uwag i definicji można znaleźć między innymi w pracy A. Barczaka *Komputerowe gry wojenne* wydanej przez Bellonę w 1996 roku. A. Barczak cytuje kilka definicji gry kierowniczej oraz formułuje swoją własną.

Gra decyzyjna – to symulacyjny proces podejmowania decyzji, w konkretnej sytuacji, w warunkach wieloetapowego, krokowego udokładnienia niezbędnych czynników, a także proces *analizy informacji* sukcesywnie napływających do uczestników gry i opracowywanej w trakcie jej przebiegu.

Gra decyzyjna – to model współdziałania ludzi w procesie realizacji materialnych lub (i) prestiżowych celów.

Gra decyzyjna jest symulacyjnym modelem funkcjonowania organizacji[11].

I wreszcie definicja samego A. Barczaka:

Gra kierownicza – to model funkcjonowania określonego systemu działania w sytuacji konfliktowej, w którym odwzorowano procesy robocze i informacyjno-decyzyjne oraz procesy współdziałania decydentów przy realizacji celów systemu[12].

Gry kierownicze mają znacznie szersze zastosowanie niż *matematyczna teoria gier*. Potrafią też symulować sytuacje które kłócą się z wymogiem racjonalności. Nie oznacza to, że teoria gier jest bezużyteczna. Pełni ona jednak wobec gier kierowniczych rolę wspierającą i porządkującą.

Podobnie jak *teoria gier*, także *gry kierownicze* dają analitykowi do ręki doskonałe *narzędzie testowo-optymalizacyjne*. Dobrze przygotowane są też w stanie pomóc dostrzec zagrożenia, które przy pomocy klasycznych metod analitycznych mogły nie zostać ujawnione.

[10] *Ibidem*, s. VIII
[11] A. Barczak, *Komputerowe gry wojenne*, Warszawa 1996, s. 109.
[12] *Ibidem*, s. 110.

4.1. Globalizacja zagrożeń w obszarze bezpieczeństwa informacyjnego

„Cywilizacja, którą zbudujemy, zbliżając się do XXI wieku, nie będzie cywilizacją materialną, symbolizowaną przez ogromne konstrukcje, ale będzie cywilizacją niewidoczną. Precyzyjniej powinno się ją nazwać cywilizacją informacyjną"
Yoneii Masuda. *Computopia*

Pojęcie *globalizacji* staje się jednym z coraz częściej spotykanych terminów nie tylko w literaturze fachowej, ale również w wielu artykułach w prasie. Istnieje wiele prób zdefiniowania pojęcia globalizacji i problemów globalnych, np.:

„Wyodrębniona na podstawie naukowo uzasadnionych kryteriów grupa współczesnych zagadnień, których zidentyfikowanie oraz naukowa analiza i wyprowadzone z niej sposoby rozwiązywania problemów mają zasadnicze znaczenie dla przyszłości całego świata[13]*"*.

Mówiąc o problemach globalnych, mamy na uwadze poważne zagadnienia związane głównie z różnego rodzaju wyzwaniami. Jak się łatwo domyślać wyzwania rodzą zarówno szanse, jak i zagrożenia. Najdobitniejszymi przykładami problemów globalnych związanych z przeszłością, a które miały znaczący wpływ na aktualną sytuację polityczno-wojskową współczesnego świata, są:

- I i II wojna światowa;
- odkrycie energii jądrowej – wykorzystanie do celów pokojowych i militarnych;
- rozwój środków łączności i informatyki

H. P. Martin, autor *„Pułapki globalizacji"* twierdzi: *„Gospodarcza interpretacja w skali globalnej nie jest bynajmniej wydarzeniem naturalnym, ale rezultatem świadomie i celowo uprawianej polityki"*, a dostrzegając ujemne skutki integracji gospodarczej spowodowanej *globalizacją*, dodaje: *„Globalizacja nie musi, ale może prowadzić do konfliktów zbrojnych, jeżeli nie uda się ujarzmić uwolnionych sił międzynarodowej ekonomii"*[14].

[13] T. Jemioło. *Globalizacja. Szanse i zagrożenia.* AON 5215/2000, Warszawa 2000
[14] Martin H. P. *Pułapka globalizacji.* Warszawa 2001

4.1.1. Rozwój elektronicznej wymiany informacji w procesie globalizacji

Gwałtowny rozwój systemów informatycznych (teleinformatycznych) wykorzystywanych do elektronicznej wymiany informacji w zdecydowany sposób przyczynił się do rozwoju globalizacji. Dzięki temu dostęp do informacji i jej przetwarzanie stało się możliwe z dowolnego miejsca na ziemi. Wszelkie rekordy popularności biją dzisiaj tzw. systemy *Ecommerce (elektronic commerce*), które dzięki technologii teleinformatycznej ułatwiają wymianę handlową i wszelką inną wymianę informacji przynoszącą korzyści finansowe. W skład systemów *Ecommerce* wchodzą między innymi takie techniki i rozwiązania, jak:

- *elektroniczna wymiana dokumentacji (Elektronic Data Interchange - EDJ);*
- *elektroniczny transfer środków pieniężnych (Elektronic Funds Transfer - EFT);*
- *interaktywne systemy informacji głosowej (Interactive Voice Response)*
- *bankowość elektroniczna (elektronic banking) i jej „domowa" odmiana (home banking).*

Sprawna realizacja elektronicznej wymiany informacji stała się możliwa dzięki rozwojowi Internetu. Występują następujące formy wykorzystania Intemetu:

- *Intranet* - dla potrzeb wewnętrznej komunikacji w firmie;
- *Extranet* - do tworzenia między organizacyjnych systemów informacyjnych;
- *Internet* - powszechnie dostępne medium informacyjne.

Przykładem najnowszego wykorzystania sieci Internet są następujące techniki:

- *VPN* – prywatne sieci korporacyjne realizowane poprzez Internet
- *VDN* – sieci korporacyjne wykorzystujące połączenia komutowane *(dial-up)*
- *VoIP* – przesyłanie głosu poprzez Internet
- *UMTS, WAP* – dostęp do Internetu z telefonu komórkowego
- *XDSL* – szybki dostęp do Internetu z domu
- powszechne wykorzystanie przeglądarki w dostępie do rozmaitych aplikacji lokalnych i Internetowych.

Do najważniejszych cech Internetu zaliczyć można:

- ogromną liczbę jej użytkowników;
- łatwą i powszechną umiejętność korzystania z niej, niezależność sprzętową;

- dostępność technologiczną i cenową, decydujące o niezwykłej atrakcyjności tego kanału dystrybucji;
- uniwersalność, pozwalającą oferować w sieci dowolne towary i usługi;
- brak instytucji nadzorującej i kontrolującej, gwarantujący niezależność od konkretnych producentów czy organizacji rządowych.

Udoskonalane technologie informacyjne i komunikacyjne z każdym dniem stają się tańsze i łatwiejsze w użyciu. Będą one coraz szerzej przyswajane i stosowane w praktyce, a ich wykorzystanie nie będzie ograniczało się jedynie do wąskich zastosowań w kierowaniu procesami produkcyjnymi czy też w innych wyselekcjonowanych obszarach działalności. W rzeczywistości technologie te będą typowym środkiem wykorzystywanym we wszystkich obszarach ludzkiej działalności. Coraz więcej informacji będzie docierało do pojedynczego elementu systemu międzynarodowego z różnych jego poziomów. Zwiększy się dostępność do informacji, ale jednocześnie wzrośnie na nią zapotrzebowanie. Oprócz wyróżnionych danych narodowych i korporacyjnych, przewiduje się dalsze uzupełnianie zasobów informacyjnych, co związane jest ze zwiększonym dostępem i rozpowszechnianiem danych pochodzących z lokalnych baz danych i sieci.

Przewiduje się dalszy wzrost możliwości przestrzennych oraz ilości odbiorców informacji. Użytkownicy informacji będą posiadali ciągły dostęp do informacji niezależnie od poziomu prowadzonych analiz. Określone korzyści będą płynęły także z faktu wzrastającego rozpraszania informacji. Nie ulega wątpliwości, że pojawi się pilna potrzeba wzmożonej ochrony najbardziej ważnych systemów informacyjnych. Dotyczy to zarówno centrów odpowiedzialnych za gromadzenie, przetwarzanie i zobrazowanie informacji, jak i kanałów jej przesyłania.

4.1.2. Wpływ globalizacji na przestrzeń walki informacyjnej

Informacja odgrywała i nadal odgrywać będzie zasadniczą rolę w organizowaniu i prowadzeniu działań względem *„przeciwnika"*. Szczególnie jest to widoczne w operacjach militarnych, w których o zwycięstwie decyduje posiadanie odpowiedniej informacji, szybkie je wykorzystanie i podjęcie właściwej decyzji. W ***Rozdziale 2.3*** omówiono pojęcie i znaczenie *walki informacyjnej*.

Odmianą *walki informacyjnej* jest tzw. *terroryzm informacyjny* albo *„piractwo informacyjne"*, które faktycznie wykorzystują wojnę informacyjną do osiągnięcia celów terroryzmu. Zakładają one stosowanie przemocy względem obiektów cywilnych i wojskowych, przy czym ryzyko ingerencji w systemy informatyczne będzie wzrastało wraz z rozwojem technologii informatycznej.

W przyszłości działania terrorystyczne będą prawdopodobnie miały na celu zapewnienie terrorystom dostępu do najnowszych technologii stanowiących niejako *„ochronę bogactwa"* państw uprzemysłowionych. Dlatego też grupy terrorystyczne oprócz dotychczasowych zainteresowań bronią masowego rażenia, systemami komunikacji i innymi rozwiązaniami technologicznymi, będą uciekały się do *terroryzmu informacyjnego*.

Skutki konwencjonalnych działań terrorystycznych, jakkolwiek wielce dokuczliwe i bolesne mają na ogół ograniczony zasięg. Natomiast w przypadku piractwa informatycznego *(cyberterroryzm)*, skala destrukcyjnych działań może mieć ogromny zasięg.

Równie groźną odmianę terroryzmu informacyjnego może stanowić ingerencja w sieci informatyczne z zamiarem zniszczenia lub uniemożliwienia ich funkcjonowania czy też sprawowania nad nimi kontroli.

Wielce prawdopodobnym obiektem zainteresowań terroryzmu informacyjnego może być sieć internetowa, mająca charakter globalny. Pierwszymi oznakami tego typu działań są działania *hackerów*. Nie można także wykluczać, że *„cyberterroryzm"* będzie swego rodzaju logicznym modelem przyszłego konfliktu, który będzie prowadzony w *„cyberprzestrzeni"*.

Wzrastające uzależnianie się sił zbrojnych, rządów i organizacji od systemów informatycznych stanowi doskonałe tło dla terrorystów w zakresie oddziaływania stosunkowo niewielkimi siłami.

Rozwój elektronicznej wymiany informacji, rozwój systemów teleinformatycznych, rozwój Internetu przynoszą bardzo wiele korzyści, nie da się jednak nie zauważyć jak wiele niepożądanych skutków mogą powodować i jakie im grożą niebezpieczeństwa. W związku z tym istnieje potrzeba obrony przed wszystkimi zagrożeniami jakie niosą technologie teleinformatyczne.

Omówione w ***Rozdziale 2.4*** akty normatywne (*ustawa o ochronie informacji niejawnych, ustawa o ochronie danych osobowych* i in.) są próbą uporządkowania całego procesu przepływu i przetwarzania różnego rodzaju informacji. Wskazują kierunki i środki ochrony informacji, definiują regulowane aktami prawnymi zadania służb specjalnych w zakresie ochrony informacji.

4.1.3. Globalizacja informacyjna jako nośnik zagrożeń bezpieczeństwa

Istotnym elementem związanym z globalizacją jest ograniczanie władzy państw. Często spotkać można poglądy, iż pomimo wzrostu liczby różnego rodzaju organizacji międzynarodowych i przejmowania przez nie *„zarządzania niektórymi zagadnieniami"* w skali regionu czy całej gospodarki światowej, zakres suwerennej władzy państwa nie uległ ograniczeniu, a globalizacja nie zmniejszyła jeszcze w znaczącym stopniu możliwości podejmowania suwerennych decyzji nie tylko przez wielkie mocarstwa, lecz także przez rządy większości państw średnich i małych.

Jednak według J. Caporoso (Unia Europejska):

„Unia Europejska może integrować się politycznie, jedynie wykraczając poza suwerenność poszczególnych państw, perswadując, aby przyjęły status jednostek podporządkowanych i rekonstruując suwerenność na wyższym poziomie".



Rysunek 13: ***Interpretacja graficzna zjawiska globalizacji***[15]

[15] T. Jemioło. *Globalizacja. Sszanse i zagrożenia.* AON 5215/2000, Warszawa 2000

W procesie integracji europejskiej państwa tracą atrybuty suwerenności, ale pozyskują nowe techniki realizacji swoich celów. Nie zakres podejmowanych przez państwo decyzji jest tu miernikiem, a możliwość realizacji własnych interesów. Nie ulega więc wątpliwości, że praktyczny wybór, przed jakim stoją współczesne państwa, dotyczy przekazania części tradycyjnie rozumianej suwerenności na rzecz instytucji międzynarodowej, gdy jest to w interesie państwa i społeczeństwa, lub też utrzymania kompetencji państwa, nawet jeśli może to być ze stratą dla jakiegoś określonego interesu narodowego[16].

Władza państwa narodowego ulega rozproszeniu w dwóch płaszczyznach: *pionowej* (Unia Europejska oraz szczebel lokalny i regionalny) oraz *poziomej* (*organizacje transnarodowe*, dominujące w sferze produkcji, finansów i usług). Powyższe zjawisko zostało spowodowane przez *integrację europejską, fragmentację i globalizację.*

4.2. Ewaluacja zagrożeń w zakresie bezpieczeństwa informacyjnego

Kierując się strukturą analizy systemowej należy uznać, że zasadniczym narzędziem tej metody badawczej jest modelowanie, czyli odwzorowanie obiektu rzeczywistego, jakim jest np. istniejący, niedoskonały system narodowego bezpieczeństwa informacyjnego. Posługiwanie się modelem obiektu rzeczywistego jest jedną z cech współczesnych badań naukowych. W analizie systemowej jest to koniecznością, chociażby ze względu na brak możliwości przeprowadzenia eksperymentów z takim obiektem, jakim jest w tym przypadku system bezpieczeństwa.

Pojęcia: *bezpieczeństwo* i *zagrożenie* stanowią dla siebie naturalną opozycję. Wraz z postępem technologicznym i cywilizacyjnym sfera bezpieczeństwa publicznego rozszerzyła się na nowe dziedziny. Współczesne pojęcie bezpieczeństwa informacyjnego lub cybernetycznego (*cybersecurity*) odnosi się zatem do prężnie rozwijającej się i bardzo wrażliwej sfery IT.

[16] *Ibidem*

Bezpieczeństwo informacyjne funkcjonuje w powiązaniu z szeregiem tradycyjnych wymiarów bezpieczeństwa państwa: począwszy od bezpieczeństwa systemów obrony militarnej, poprzez skomputeryzowany monitoring ochrony środowiska i podtrzymanie standardów w tym sektorze, bezpieczeństwo komunikacji i transportu, bezpieczeństwo połączeń telemedialnych, zachowanie niejawności informacji, stabilność systemu ochrony zdrowia, życia i mienia obywateli. Odniesienia do tak licznych dziedzin życia publicznego, które w ostatniej dekadzie XX wieku zostały przesycone technologiami informacyjnymi, czynią kwestię bezpieczeństwa państwa bardziej dynamiczną i modyfikowalną, a równocześnie bardziej newralgiczną. Wykazują też nieprzewidywalność nowych zagrożeń, brak pełnego przygotowania służb państwowych do ich zwalczania. Bardzo istotne znaczenie dla bezpieczeństwa informacji ma technologia jej przetwarzania, oparta na bieżących osiągnięciach naukowo-technicznych, wykorzystująca ciągle doskonalone narzędzia automatyzowania procesów informacyjnych. W kontekście historycznym warto przypomnieć etapy prowadzące do współczesnego, dynamicznego rozwoju tych narzędzi.

Wraz ze wzrostem znaczenia informacji w kształtowaniu stosunków społecznych pojawiły się pierwsze zwiastuny technologii komputerowej. Prekursorów możemy szukać już w XVII wieku. Wilhelm Schickard skonstruował w 1623 roku, na zamówienie J. Keplera, pierwszą na świecie maszynę matematyczną, wykonującą proste działania arytmetyczne (dodawanie liczb całkowitych), Blaise Pascal także zaprojektował maszynę dodającą, a Gottfried W. Leibniz koło do wykonywania czterech działań arytmetycznych. Początek informatyki to jednak XIX wiek i prace brytyjskiego matematyka oraz wynalazcy, Charlesa Babbage'a, który zaprojektował „maszynę analityczną", będącą właściwie prototypem współczesnych komputerów. Początek XX wieku to okres zintensyfikowanych prac matematyków nad praktyczną realizacją idei Babbage'a. Warto wymienić chociażby Alana M. Turinga, Norberta Wienera czy Johna von Neumanna. Za pierwszy komputer można uznać skonstruowaną w 1944 roku przez matematyka amerykańskiego Howarda H. Aikena maszynę liczącą, zbudowaną z przekaźników elektromechanicznych *(MARK 1)*. Era współczesnych komputerów rozpoczęła się w momencie zastosowania w nich

elementów elektronicznych, umożliwiających znaczne przyspieszenie wykonywanych działań. Pierwszą całkowicie elektroniczną (zawierała 18 tys. lamp elektronowych) maszyną cyfrową był *ENIAC (Electronic Numerical Integrator And Calculator)* zbudowany w 1946 roku przez amerykańskich uczonych Johna Mauchly'ego i Johna Prospera Eckerta.

R. Kwećka, autor książki *„Informacja w walce zbrojnej"*, uważa, że informacja, jak nigdy przedtem w historii, stanowi o sile tego, kto nią dysponuje, czym m.in. można tłumaczyć potęgę mediów we współczesnym świecie (przede wszystkim mediów elektronicznych, a więc także Internetu)[17]. R. Kwećka stawia także tezę, iż o sile mediów decyduje nie sam fakt dostępu do informacji, ale możliwość jej dowolnej interpretacji. Uważa on, że ocenianie tego, co jest „*dobrem*", a co „*złem*" może w procesach informacyjnych naszej rzeczywistości odegrać rolę strategiczną, może swobodnie kształtować nasze poglądy i zmusić do zachowań, których rezultaty odpowiadają tylko niewielkiej grupie ludzi. „*Czasem wydaje się, że zatracamy naszą własną, obiektywną zdolność postrzegania świata. Powoli jej miejsce zajmuje rzeczywistość wykreowana przez media"* — pisze R. Kwećka[18].

Powojenny postęp techniczny, głównie w dziedzinie elektroniki, spowodował także znaczące zmiany w siłach zbrojnych. Jak wskazuje L. Ciborowski, twórca teoretycznych podstaw walki informacyjnej, na współczesnym polu walki główną rolę zaczyna odgrywać zdolność szybkiego komunikowania się[19]. Według L. Ciborowskiego można wyróżnić cztery wydarzenia, które wpłynęły na powstanie koncepcji walki informacyjnej:

- prace amerykańskiego matematyka, profesora C. E. Shannona, które ukierunkowane były na określenie optymalnych warunków przesyłania informacji (praca: „*The Mathematical Theory of Communication*"). W 1948 roku stworzył podstawy teorii informacji i opracował metodę określenia ilościowej miary informacji, wprowadzając nową jej jednostkę (bit);
- konstrukcja w 1946 roku pierwszej w świecie całkowicie elektronicznej maszyny cyfrowej ENIAC;

[17] R. Kwećka, Informacja w walce zbrojnej, Warszawa 2001, s. 57.
[18] *Ibidem*, s. 95.
[19] L. Ciborowski, Walka informacyjna, Toruń 1999, s. 7.

- konstrukcja pierwszych typów tranzystorów: w 1948 roku tranzystora ostrzowego przez J. Bardeena i W. H. Brattaina i w 1949 roku tranzystora warstwowego przez W. Shockleva. Wynalazki te zainicjowały burzliwy rozwój elektroniki. Powstały komputery trzeciej generacji;
- konstrukcja w 1958 roku pierwszego układu scalonego. Na ich bazie zaczęto tworzyć sieci informacyjne[20].

Współczesnym strategom wojskowym anachroniczne wydają się słowa Karla von Clausewitza: *„wojna jest kontynuacją polityki, prowadzoną jedynie za pomocą innych środków"*[21]. Coraz częściej odwołują się natomiast do tez chińskiego filozofa z VI wieku p.n.e., Sun Tzu, którego uznaje się za prekursora koncepcji walki informacyjnej. *„Osiągnąć sto zwycięstw w stu bitwach nie jest szczytem osiągnięć. Największym osiągnięciem jest pokonanie wroga bez walki"*. To nawiązanie do rewolucyjnej zmiany myślenia na temat wykorzystania sił zbrojnych w walce najdobitniej świadczy o znaczeniu informacji we współczesnej armii.

Wyciągając wnioski z dotychczasowej analizy, można wskazać przynajmniej dwa powody, dla których koncepcja stworzenia globalnej sieci zyskała powszechne uznanie: pierwszym było urzeczywistnienie idei społeczeństwa informacyjnego i *„świata bez granic"*, pozbawionego barier komunikacyjnych; drugim chęć stworzenia sieci komunikacyjnej, służącej celom militarnym, która działałaby nawet w sytuacji zniszczenia tradycyjnych środków komunikacji, na przykład w wyniku ewentualnego ataku nuklearnego. Właśnie taki system mógł zagwarantować zachowanie możliwości przekazywania rozkazów pomiędzy poszczególnymi jednostkami, nawet w przypadku globalnego konfliktu, ponieważ opierał się na braku centralnego punktu dowodzenia. Zakładano, że w odróżnieniu od sieci telefonicznej, układ powinien mieć charakter zdecentralizowany, tzn. każdy z komputerów byłby równorzędny i połączony ze wszystkimi pozostałymi komputerami, toteż w przypadku awarii jednego z nich, sieć mogła nadal funkcjonować.

[20] L. Ciborowski, Walka..., op. cit., s. 35
[21] K. von Clausewitz, O wojnie, Warszawa 1958, s. 15

4.2.1. Wprowadzenie do analizy systemowej

Użytecznym narzędziem optymalizacji jest ***analiza systemowa***. Jak definiuje ją P. Sienkiewicz:

Analiza systemowa jest

- zbiorem technik analitycznych, ocenowych i decyzyjnych, służących racjonalnemu rozwiązywaniu systemowych sytuacji decyzyjnych,
- badaniem wspomagającym działania osób odpowiedzialnych za decyzje lub linie postępowania w warunkach *niepewności i ryzyka*[22].

Ma ona na celu określenie pożądanego działania lub linii postępowania przez rozpoznanie i rozważenie dostępnych wariantów oraz porównanie przewidywanych ich, bliższych i dalszych, następstw[23]. To, co zasadniczo odróżnia *analizę systemową* od analizy jako ogólnej metody badań to fakt, że postrzega ona badany obiekt jako system. Ważną jej cechą jest kompleksowość i wielowątkowość metody badawczej. *Analiza systemowa* posiłkuje się wieloma rodzajami dociekań zaczerpniętymi z różnych dziedzin naukowych. Nadal jednak głównym jej narzędziem poznawczym są *metody matematyczno-statystyczne*.

Z uwagi na swoją kompleksowość *analiza systemowa* stanowi bardzo cenne narzędzie poznania i sprawdzania zaprojektowanych systemów informacyjnych. Ponadto *analiza ryzyka* stanowi jedno z zasadniczych jej zagadnień. Wydaje się zatem, że bez poddania gotowego projektu systemu bezpieczeństwa informacyjnego rygorom *analizy systemowej* nie będzie można mówić o pełnym przebadaniu takiego projektu. Bowiem ze wszystkich narzędzi analitycznych bazujących na metodach obliczeniowych jedynie *analiza systemowa* może dokonać całościowego przeglądu projektu czy funkcjonującego rozwiązania. Nawet, jeśli nie rozstrzygnie wszystkich dylematów, to na pewno znacząco uzupełni nasza wiedzę.

W niniejszej rozprawie posłużono się ***analizą systemową*** w procesie badań nad *bezpieczeństwem informacyjnym państwa*.

---

[22] Piotr Sienkiewicz, *Analiza systemowa. Podstawy i zastosowania,* Warszawa 1994, s. 37.
[23] *Ibidem*, s. 38.

4.2.2. Struktura narzędzi ewaluacyjnych

Zgodnie z teorią analizy systemowej - celem określenia przydatności tego narzędzia badawczego w procesie analizy obiektu-systemu - należy przeprowadzić analizę identyfikacyjną problemu.

Identyfikacja sytuacji problemowej polega na określeniu zadania będącego problemem. W przypadku niniejszej pracy głównym problemem badawczym jest ***wykazanie potrzeby, określenie możliwości i kierunków oraz wskazanie zakresu i sposobu doskonalenia polityki bezpieczeństwa informacyjnego państwa, celem efektywnego włączenia jej w trwający proces transformacji politycznej i społeczno-ekonomicznej Polski z jednoczesnym nadaniem cech sprzyjających zapewnieniu właściwego miejsca i roli w Organizacji Traktatu Północnoatlantyckiego i w Unii Europejskiej.***

Pierwszy krok analizy identyfikacyjnej pozwala na zdefiniowanie obiektu analizy jako systemu, gdyż bezpieczeństwo informacyjne państwa niewątpliwie stanowi **system**. W kolejnych krokach analizy identyfikacyjnej określa się grupę (klasę) sytuacji systemowej.

4.2.3. Integralność systemu analizy zagrożeń bezpieczeństwa informacyjnego – analiza identyfikacyjna

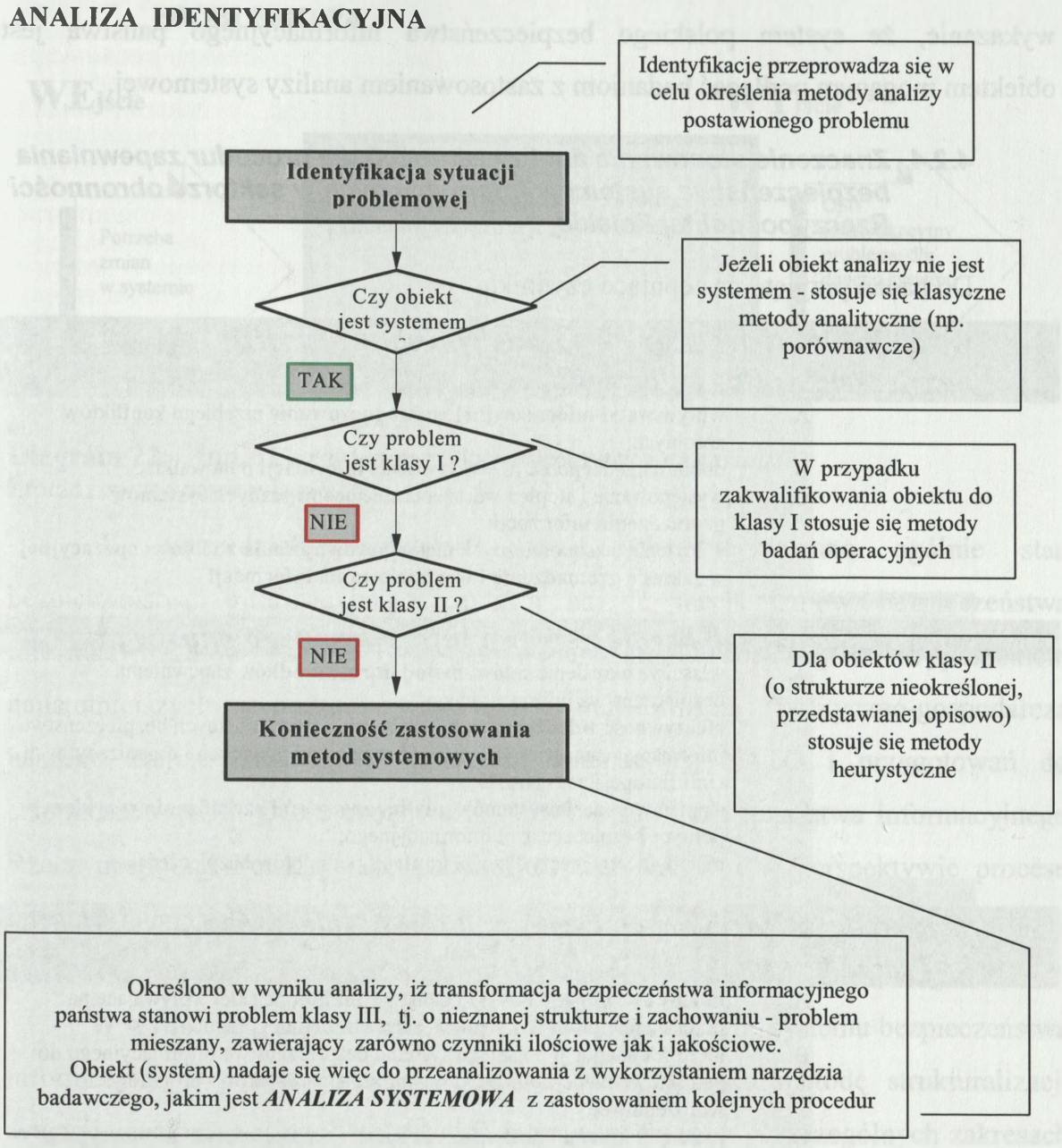


Diagram 21: ***Analiza identyfikacyjna obiektu badań***
Źródło: opracowanie własne

W wyniku analizy identyfikacyjnej określono, że bezpieczeństwo informacyjne państwa stanowi obiekt systemowy, ale w kontekście trwającej integracji z NATO i niezbędnych przeobrażeń uwarunkowanych procesem przystępowania naszego kraju do struktur Unii Europejskiej - nie jest znana jego struktura ani jego zachowanie. Jest to więc *obiekt grupy (klasy) III*, należy więc określić jego prawdopodobne

zachowanie i na tej podstawie wnioskować o strukturze systemu, a następnie określić warunki istnienia struktury pożądanej. Wnioskiem z analizy identyfikacyjnej jest wykazanie, że system polskiego bezpieczeństwa informacyjnego państwa jest obiektem mogącym podlegać badaniom z zastosowaniem analizy systemowej.

4.2.4. Znaczenie stosowania analizy zagrożeń dla procedur zapewniania bezpieczeństwa systemów informacyjnych w sektorze obronności Rzeczypospolitej Polskiej

Do badań przyjęto następujące czynniki:

I. w zakresie ***roli procesów informacyjnych w obszarze bezpieczeństwa narodowego***:

- A. **wpływ walki informacyjnej** na **prognozowanie** przebiegu konfliktów zbrojnych;
- B. dobór narzędzi pomiaru **efektywności informacji** pola walki;
- C. występowanie i stopień wdrożenia **sieciocentrycznych systemów gromadzenia** informacji;
- D. wdrożenie taksonomicznych metod **porównywania zdolności operacyjnej** w zakresie **gromadzenia i wartościowania informacji**

II. w zakresie ***jakości bezpieczeństwa informacyjnego państwa*** :

- A. właściwe określenie **celów, metod, form i środków** zapewnienia bezpieczeństwa informacyjnego;
- B. **efektywność wdrożeniowa** przedsięwzięć zapewniających bezpieczeństwo informacyjne państwa w aspekcie uregulowań prawnych i organizacyjnych Unii Europejskiej i NATO;
- C. stopień wdrożenia systemów **analizy zagrożeń i zarządzania ryzykiem** w polityce bezpieczeństwa informacyjnego;
- D. metody **oceny, certyfikacji i kontroli** podmiotów bezpieczeństwa

III. w zakresie ***międzynarodowych aspektów bezpieczeństwa informacyjnego***:

- A. **normy i standardy** NATO i państw Unii Europejskiej wpływające na podniesienie **jakości bezpieczeństwa informacyjnego;**
- B. kierunek adaptacji polskiego systemu bezpieczeństwa informacyjnego do jakościowo nowej sytuacji w **wymiarze europejskim** - programy wdrożeniowe;
- C. metody **pomiaru** i **doskonalenia** jakości bezpieczeństwa informacyjnego w wymiarze międzynarodowym;
- D. stosowanie zautomatyzowanych **narzędzi analizy zagrożeń i zarządzania ryzykiem** w obszarze ochrony informacji niejawnych

Określenie zbioru cech i zbioru stanów przyjętego do analizy materiału obejmującego system bezpieczeństwa informacyjnego państwa pozwala na przeprowadzenie badań ukierunkowanych na określenie aktualnego stanu systemu, co jest właściwym celem analizy diagnostycznej. Wypełnienie analizy diagnostycznej konkretną treścią stanowić będzie opis przebiegu procesu systemowego na zdefiniowanych i przeanalizowanych warunkach.

4.2.5. Zakres i struktura zagrożeń bezpieczeństwa informacyjnego – analiza problemowa

ANALIZA PROBLEMOWA

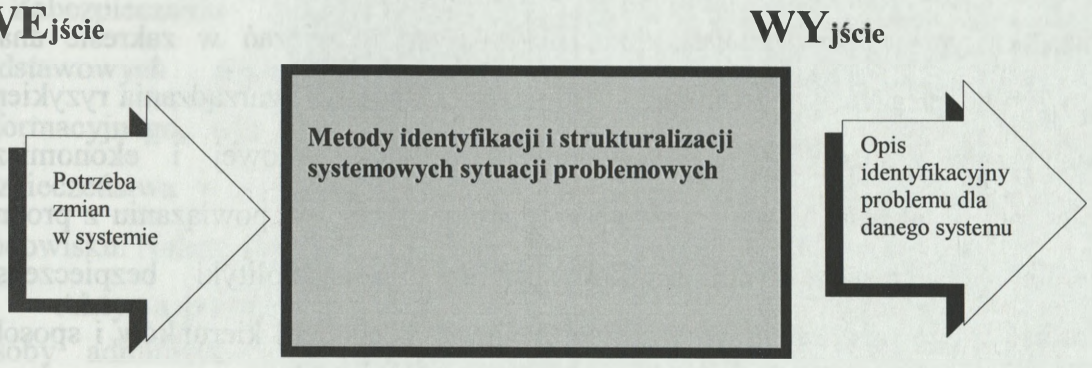


Diagram 22: ***Analiza problemowa przedmiotowego materiału***
Źródło: opracowanie własne

W poprzednich rozdziałach pracy scharakteryzowano ogólnie stan bezpieczeństwa informacyjnego państwa na tle mechanizmów bezpieczeństwa informacyjnego w NATO i w państwach Unii Europejskiej z uwypukleniem najistotniejszych czynników związanych z transformacją polityczno-gospodarczą naszego kraju, postępującym procesem integracji z NATO i przygotowań do członkostwa w UE. Ocena możliwości transformacji bezpieczeństwa informacyjnego Rzeczypospolitej Polskiej jako państwa-członka NATO i w perspektywie procesu integracyjnego z Unią Europejską jest możliwa do dokonania pod warunkiem analizy systemu bezpieczeństwa informacyjnego RP w zakresie zakładanych wymagań.

W wyniku analizy identyfikacyjnej określono, iż ocena systemu bezpieczeństwa informacyjnego państwa stanowi *problem klasy III*. Jako metodę strukturalizacji sytuacji problemowej przyjęto sklasyfikowanie systemu w poszczególnych zakresach składających się na ocenę jakościowo-ilościową przedmiotu badań. W opisie identyfikacyjnym uwzględniono zdefiniowanie kryteriów oceny w zakresie:

- **jakości bezpieczeństwa informacyjnego państwa;**
- **wykazania potrzeby doskonalenia polityki bezpieczeństwa informacyjnego;**
- **określenia kierunków rozwoju polityki bezpieczeństwa informacyjnego;**
- **międzynarodowych aspektów bezpieczeństwa informacyjnego państwa;**
- **wskazania rodzaju i zakresu przedsięwzięć reformatorskich**

Dokonana zgodnie ze schematem analiza problemowa pozwala na zdefiniowanie w powiązaniu z w/w charakterystyką tematycznych zakresów danych niezbędnych do przeprowadzenia procedur badawczych zgodnie z ***celem poznawczym*** pracy, którym jest wykazanie braku efektywnych rozwiązań w zakresie analizy zagrożeń bezpieczeństwa informacyjnego państwa i narzędzi zarządzania ryzykiem w dynamicznie zmieniającej się sytuacji polityczno-wojskowej i ekonomiczno-społecznej, a także analiza przyczyn takiego stanu rzeczy w powiązaniu z prognozą ewentualnych negatywnych skutków zachowawczej polityki bezpieczeństwa informacyjnego oraz ***celem utylitarnym***, a więc wskazaniem kierunków i sposobów kreowania i wdrażania polityki bezpieczeństwa informacyjnego państwa z wykorzystaniem najlepszych doświadczeń NATO i państw członkowskich Unii Europejskiej w tym zakresie.

4.2.6. Istota i źródła zagrożeń w systemach teleinformatycznych

Bezpieczeństwo systemu informacyjnego nie jest kategorią absolutną. Można jednak zdefiniować warunki uznania takiego systemu za bezpieczny. Zdefiniować należy cele, metody i środki zapewnienia bezpieczeństwa w systemach informacyjnych, wychodząc z konieczności spełnienia określonych ustawowo warunków (kryteriów bezpieczeństwa):

- **poufności,** co oznacza ochronę przed ujawnieniem informacji nieuprawnionemu odbiorcy;
- **integralności,** co oznacza ochronę przed modyfikacją lub zniekształceniem aktywów przez osobę nieuprawnioną;
- **dostępności,** co oznacza gwarancję uprawnionego dostępu do aktywów przy zachowaniu określonych rygorów czasowych;
- **rozliczalności,** co oznacza określenie i weryfikowanie odpowiedzialności za działania, usługi i funkcje realizowane za pośrednictwem systemu;
- **autentyczności,** co oznacza weryfikację tożsamości podmiotów lub prawdziwość aktywów systemu informacyjnego;
- **niezawodności,** co oznacza gwarancję odpowiedniego zachowania się systemu informacyjnego i otrzymanych wyników.

Zabezpieczanie systemu informacyjnego obejmuje wszelkie działania związane ze zdefiniowaniem, osiągnięciem i utrzymaniem stanu spełnienia tych kryteriów zabezpieczeń, czyli osiągnięcia stanu bezpieczeństwa tego systemu.

Zabezpieczanie systemów informacyjnych wymaga zdefiniowania grupy podstawowych pojęć, umożliwiających przeprowadzenie analizy systemu informacyjnego, zaproponowanie mechanizmów zabezpieczeń i utrzymanie stanu bezpieczeństwa w warunkach działania obiektu w dynamicznie zmieniającym się środowisku. Należą do nich:

Aktywa (systemu informacyjnego) - wszelkie oprogramowanie, dane, sprzęt, zasoby administracyjne, fizyczne, komunikacyjne oraz osobowe w systemie informacyjnym.

Zagrożenia - przyczyny niepożądanych zdarzeń, których efektami są szkody w systemie informacyjnym.

Słabości - podatności systemu na zagrożenia wyrażone łatwością, z jaką dane zagrożenie może wyrządzić szkodę. Konsekwencją tego są niepożądane zdarzenia, które mogą spowodować straty w systemie informacyjnym lub zakłócić realizację celów systemu.

Zdarzenie - możliwa, aczkolwiek niepożądana konsekwencja zmiany stanu obiektu, spowodowana przez zagrożenie. Analiza zdarzeń umożliwia wyznaczenie punktu równowagi między stratami wynikającymi ze zdarzeń a kosztem przyjętych procedur zabezpieczeń, zmniejszających ryzyko zdarzenia.

Ryzyko - określa prawdopodobieństwo sytuacji, w której dane zagrożenie wykorzystuje określone słabość, powodując stratę lub uszkodzenie elementu systemu informacyjnego, a zatem, pośrednią lub bezpośrednią szkodę dla obiektu. Ryzyko charakteryzują dwa czynniki: prawdopodobieństwo jego wystąpienia oraz miara zdarzenia. Określenie poziomu ryzyka dla każdej kategorii i grupy majątku przedsiębiorstwa, dostrzeżonych zagrożeń, słabości oraz wpływów jest **analizę ryzyka.**

Mechanizmy zabezpieczeń - do zadań mechanizmów zabezpieczeń należy: ochrona przed zagrożeniami, eliminowanie słabości systemu, ograniczanie wpływu niepożądanych zdarzeń, wykrywanie niepożądanych zdarzeń i realizowanie wyjścia z kryzysowych sytuacji.

Ryzyko szczątkowe - mechanizmy zabezpieczeń mogę jedynie zmniejszać ryzyko. Całkowita eliminacja jest zwykle niemożliwa lub zbyt kosztowna. Powoduje to konieczność oszacowania ryzyka szczątkowego i określenia poziomu jego akceptacji.

Dynamiczny układ zależności między różnymi elementami systemu zabezpieczenia przedstawiono na ***Diagramie Nr 23.***

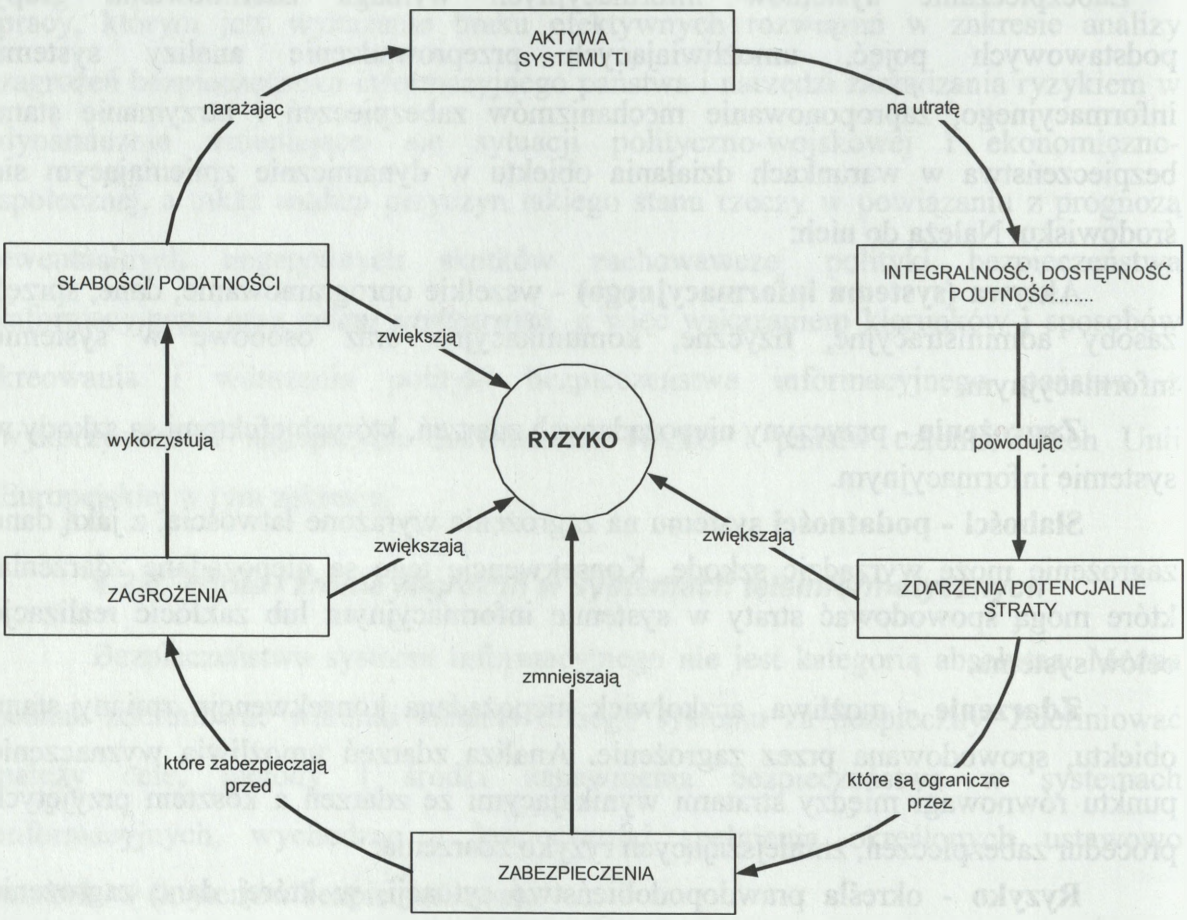


Diagram 23: ***Zależności między elementami zabezpieczenia***[24]

Jeżeli system teleinformatyczny przetwarza informacje niejawne, to problem jego zabezpieczenia należy traktować jak jedną z zasadniczych strategii działania obiektu. Realizacja polityki zabezpieczenia systemu teleinformatycznego wymaga zdefiniowania procesów zarządzania zabezpieczeniem.

Proces zarządzania zabezpieczeniem systemu teleinformatycznego można podzielić na trzy zasadnicze podprocesy:

- podproces planowania zabezpieczenia;
- podproces implementacji;
- podproces eksploatacji zabezpieczenia.

[24] A. Wiśniewski. *Analiza ryzyka. Wytyczne dla administratorów systemów.* AZW Warszawa 2000.

Realizacja procesu zarządzania zabezpieczeniem musi być zgodna z wymogami ustawowymi dla systemu teleinformatycznego przetwarzającego informacje niejawne. Stwierdzenie niezgodności z wymogami w którejś z faz zarządzania zabezpieczeniem powinno powodować uruchomienie mechanizmów planowania zabezpieczenia. Na ***Diagramie Nr 24*** przedstawiono zależności między podstawowymi procesami zarządzania zabezpieczeniem systemu teleinformatycznego.

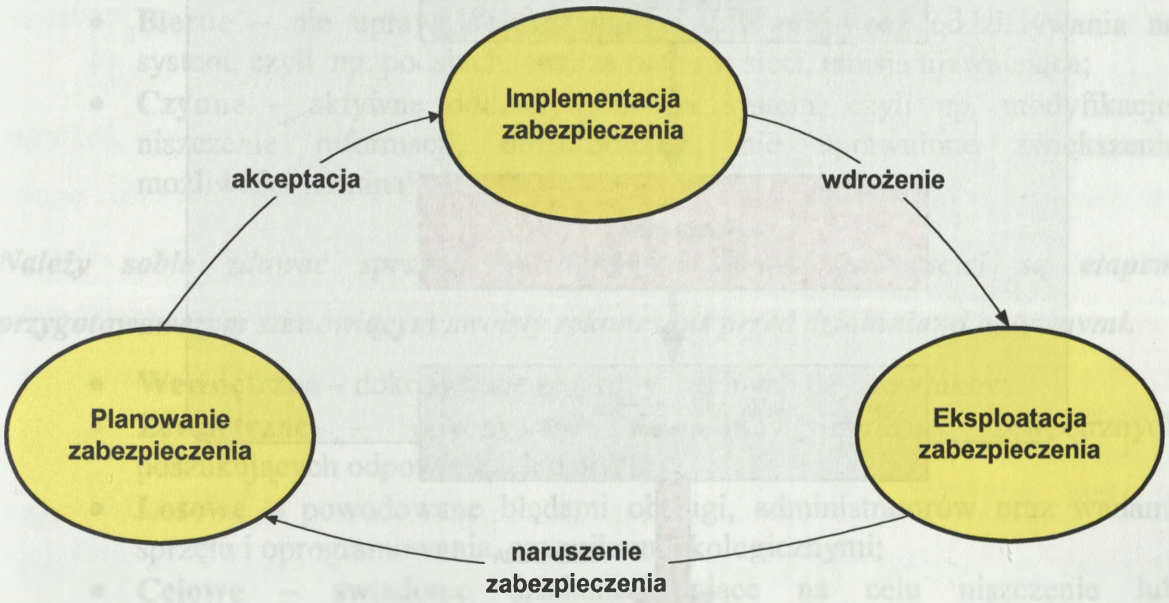


Diagram 24. ***Proces zarządzania zabezpieczeniami***
Źródło: A. Wiśniewski. *Analiza ryzyka. Wytyczne dla administratorów systemów.* AZW Warszawa 2000.

Na ***Diagramie Nr 25*** przedstawiono kolejne fazy procesu planowania zabezpieczenia systemu informacyjnego. W wyniku przeprowadzenia działań zgodnych z przedstawionym tu diagramem powstanie plan zabezpieczenia systemów teleinformatycznego przetwarzającego informacje niejawne. Należy podkreślić, że niezwykle rzadko zdarza się, aby w systemie informacyjnym nie istniały żadne zabezpieczenia. Dlatego planowanie zabezpieczenia polega nie tyle na tworzeniu zabezpieczenia, ale na dokonywaniu jego modyfikacji: wymianie mechanizmów na bardziej skuteczne, wprowadzaniu nowych procedur itp. Kluczowym elementem fazy planowania zabezpieczenia jest zarządzanie ryzykiem.

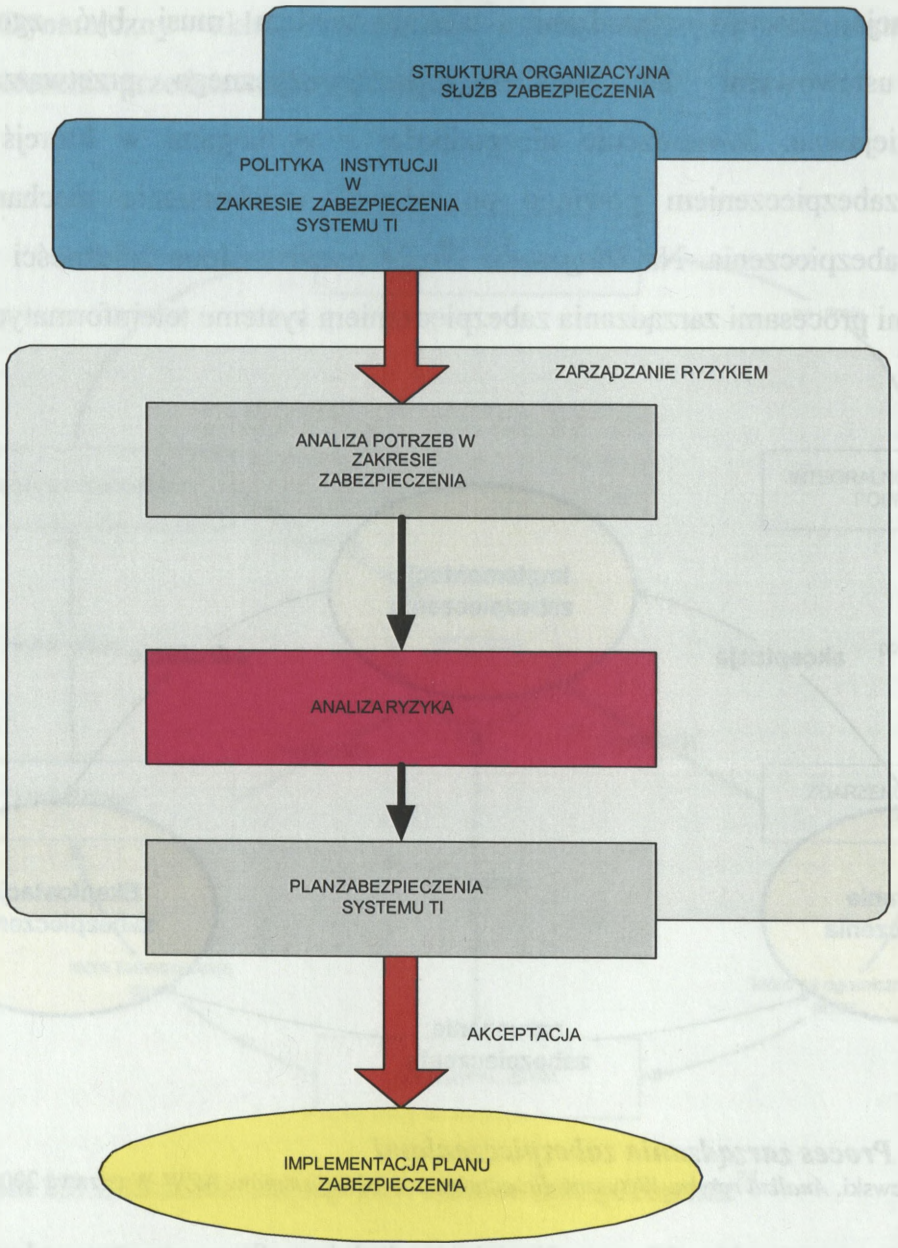


Diagram 25: ***Proces planowania zabezpieczeń***[25]

Według wskazówek wynikających z szeregu nowoczesnych instrumentów zarządzania, bez elementów zarządzania ryzykiem nie da się skonstruować poprawnych *Szczególnych Wymagań Bezpieczeństwa.*

Podstawowym elementem zarządzania ryzykiem - ze szczególnym uwzględnieniem ryzyka zniszczenia, zniekształcenia czy kradzieży informacji - jest przeprowadzenie analizy zagrożeń. Analiza ta wspomagać będzie tworzenie wymagań bezpieczeństwa systemu informacyjnego.

[25] A. Wiśniewski. *Analiza ryzyka. Wytyczne dla administratorów systemów.* AZW Warszawa 2000.

Analiza zagrożeń polega na gromadzeniu informacji o wszystkich możliwych zagrożeniach dla aktywów systemu informacyjnego. Ważne jest, aby nie zostało pominięte żadne istotne zagrożenie, bo może to wpłynąć na niewłaściwy dobór mechanizmów zabezpieczeń. Ważnym elementem analizy jest właściwa klasyfikacja zagrożeń.

Przy dokonywaniu klasyfikacji istotne jest kryterium, które przyjmujemy. Z tego powodu istnieje kilka podziałów dychotomicznych.

Generalna klasyfikacja zagrożeń może być określona w następujących grupach:

- **Bierne** – nie uprawnione ujawnienie informacji bez oddziaływania na system, czyli np. podsłuch, analiza ruchu w sieci, emisja ujawniająca;
- **Czynne** – aktywne oddziaływanie na system, czyli np. modyfikacje, niszczenie informacji, dezinformacja, nie uprawnione zwiększenie możliwości terminala.

Należy sobie zdawać sprawę, że działania bierne najczęściej są etapem przygotowawczym stanowiącym swoisty rekonesans przed działaniami aktywnymi.

- **Wewnętrzne** – dokonywane ze strony legalnych użytkowników
- **Zewnętrzne** – dokonywane ze strony intruzów zewnętrznych poszukujących odpowiednich danych
- **Losowe** – powodowane błędami obsługi, administratorów oraz wadami sprzętu i oprogramowania, czynnikami ekologicznymi;
- **Celowe** – świadome działania mające na celu niszczenie lub unieruchomianie;

Oczywisty jest także podział na:

- **Sprzętowe** – powodowane przez sprzęt;
- **Programowe** – powodowane poprzez oprogramowanie,
- **Osobowe** – powodowane przez ludzi.

Ogólne przedstawione klasyfikacje zagrożeń mogą się wzajemnie przenikać, czyli konkretne zagrożenie może być np. jednocześnie czynne, wewnętrzne, celowe, programowe lub jednocześnie przypadkowe i sprzętowe, mogą występować pojedynczo lub kilka jednocześnie.

Klasyfikacje zagrożeń podsumować można w sposób pokazany na ***Diagramie Nr 26.***



Diagram 26: ***Klasyfikacja zagrożeń.***
Źródło: opracowanie własne

Skuteczny atak na system wymaga przełamania bariery, która stanowią reguły dostępu do systemu. Podkreślić należy, że najbardziej niebezpieczne zagrożenia istnieją ze strony legalnych użytkowników systemu. Zagrożenie wzrasta wraz z liczbą użytkowników i zróżnicowania ich uprawnień.

Źródło zagrożenia zewnętrznego może być całkowicie niezależne od działania ludzkiego (np. żywioły) albo być efektem awarii innych systemów technicznych (np. pożar lub zalanie). Zawsze jednak przyczyna ta leży poza samym systemem informacyjnym. Do kategorii zagrożeń zewnętrznych należy zaliczyć:

- wypadki i katastrofy spowodowane czynnikami naturalnymi np. wodą, ogniem, wyładowaniami atmosferycznymi, trzęsieniem ziemi,
- wpływy środowiskowe, np. zmiany temperatury i wilgotności, zanieczyszczenie powietrza, zapylenie, silne pola magnetyczne, wibracje mechaniczne;
- utrata personelu np. na skutek choroby, wypadku, śmierci lub strajku.

Do zagrożeń przypadkowych zalicza się błędy i awarie. Zagrożenia przypadkowe charakteryzują się losowym rozkładem prawdopodobieństwa

urzeczywistnienia się. W związku z tym często ryzyko związane z tymi zagrożeniami może być zmierzone metodami ilościowymi i być powiązane np. średnią liczbą błędów operatora w roku lub średnim odstępem czasowym miedzy uszkodzeniami.

Zagrożenia rozmyślne dotyczą wyłącznie działań ludzkich. Często w literaturze są one określane jako ataki. Kategoria ta obejmuje zarówno aktywność intruza znajdującego się na zewnątrz, jak i wewnątrz systemu informacyjnego. Cechą charakterystyczną tej kategorii zagrożeń jest intencja wyrządzenia szkody. Do zagrożeń rozmyślnych zalicza się: włamanie, kradzież, przechwycenie, manipulacja, oszustwo, podszycie się (maskarada), uszkodzenie lub zniszczenie.

Każdy istotny element aktywów systemu powinien być analizowany pod kątem zagrożeń, które mogą przyczynić się do jego uszkodzenia lub utraty. Szczególną uwagę należy zwrócić na identyfikację sposobów, jakimi dane zagrożenie może się objawić. Przykładowo, działaniami które mogą prowadzić do uzyskania nieupoważnionego dostępu może być podsłuch i powtórzenie (playback) sesji rejestrowania użytkownika, złamanie hasła, dołączenie nieautoryzowanego wyposażenia do sieci itp.

Dokumentem końcowym tej fazy jest zestawienie aktywów systemu teleinformatycznego z potencjalnymi zagrożeniami prowadzącymi do naruszenia *dostępności, integralności, poufności, rozliczalności, autentyczności, niezawodności.*

Analiza podatności (słabości).

Celem tego podetapu jest określenie, jak dalece poszczególne aktywa systemu informacyjnego są narażone na utratę dostępności, integralności lub poufności, autentyczności, rozliczalności i niezawodności. Wynikiem analizy podatności jest dodatkowa charakterystyka aktywów.

Słabości systemu informacyjnego można rozpatrywać w dwóch kategoriach: słabości zewnętrznych i wewnętrznych. Do kategorii słabości zewnętrznych można zaliczyć:

- niedostatki organizacyjne (np. błędna organizacja pracy, braki w wyszkoleniu personelu, brak fizycznego zabezpieczenia ważnych elementów systemu itp.);
- niedostatki projektowe (np. budynku i jego infrastruktury).

W kategorii słabości wewnętrznych systemu informacyjnego można wyróżnić niedostatki:

- zarządzania (np. kluczami kryptograficznymi, hasłami, dostępem do systemu, braki w organizacji pracy administratora),;
- planowania (np. niedoszacowanie przyszłego wykorzystania zasobów, liczby użytkowników, infrastruktury informatycznej, błędy założeń aplikacji programowych);
- implementacji (np. testowania mechanizmów zabezpieczeń, procedur akredytacji);
- eksploatacji (np. brak mechanizmów monitorowania, braki w dokumentacji systemu, brak separacji miejsc przetwarzania danych i przechowywania kopii bezpieczeństwa).

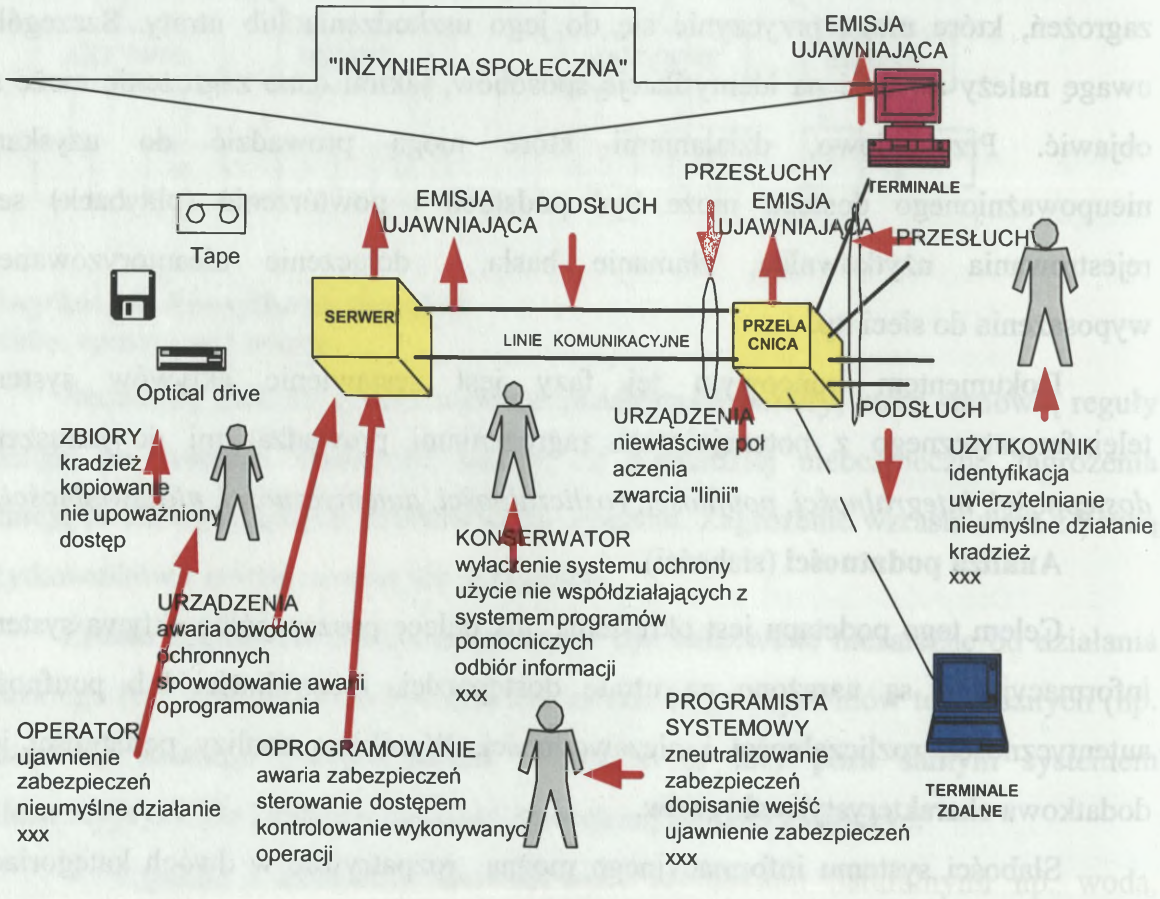


Diagram 27: ***Słabe punkty systemu teleinformatycznego***
Źródło: A. Wiśniewski. *Analiza ryzyka. Wytyczne dla administratorów systemów.* AZW Warszawa 2000.

Materiałem wejściowym analizy jest lista słabości systemu. Istotnym jej elementem jest oszacowanie wagi poszczególnych słabości narażających system na utratę dostępności, integralności, poufności, dostępności, autentyczności i

niezawodności. Skala oszacowania może obejmować np. pięć poziomów: *„maksymalny", „wysoki", „średni", „niski", „pomijalny"*.

W przypadku zarówno zagrożeń zewnętrznych i wewnętrznych konieczne jest uświadomienie sobie dróg, którymi docierają one do systemu, czy też inaczej mówiąc tzw. słabych punktów systemu. Zostały one przedstawione na ***Diagramie Nr 27***, natomiast typowe środki ochrony na tle typowych zagrożeń prezentuje ***Diagramie Nr 28***.

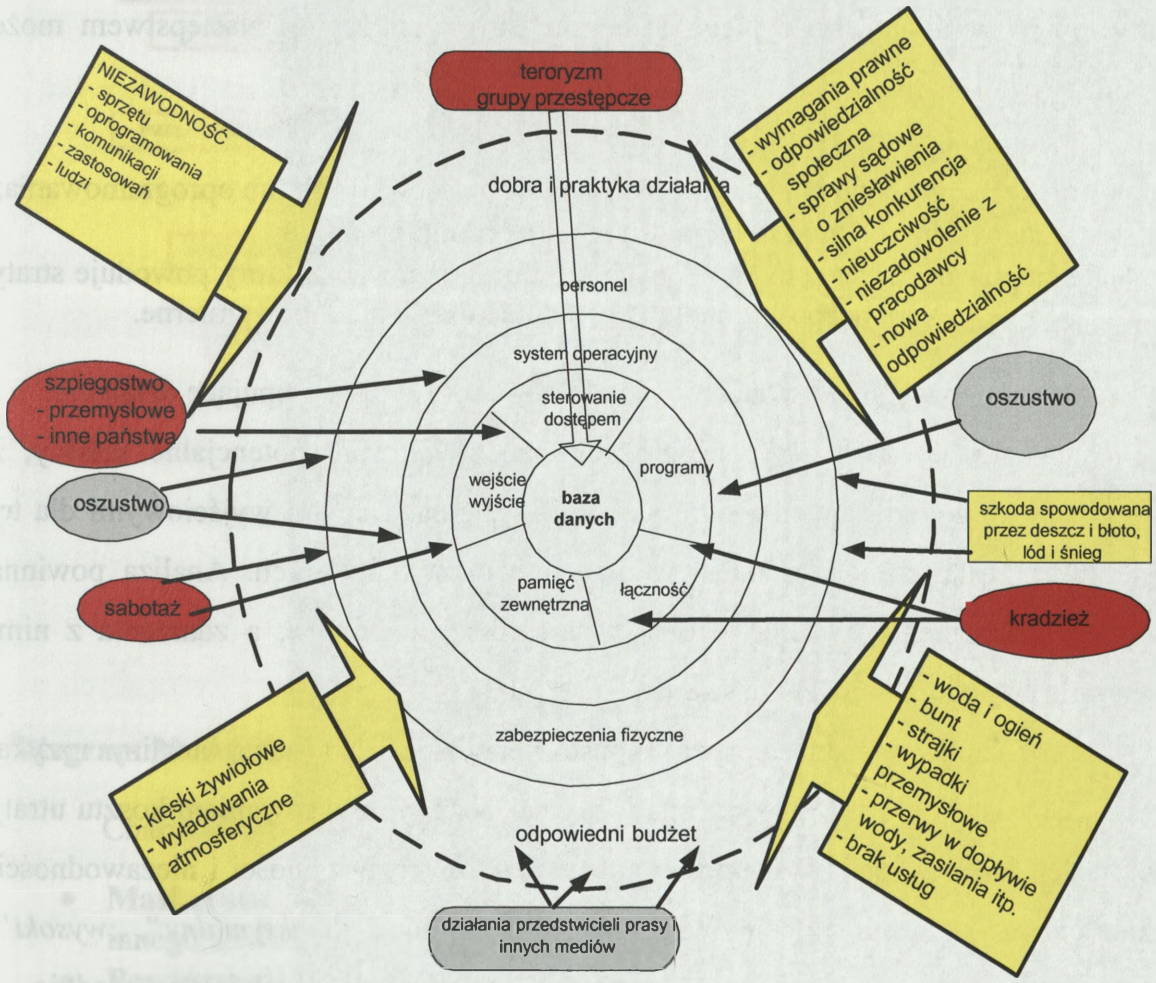


Diagram 28: ***Typowe środki ochrony***[26]

Efektem analizy jest zestawienie aktywów systemu teleinformatycznego, zagrożeń i stopni narażenia dostępności, integralności, poufności, dostępności,

[26] *Ibidem*

autentyczności i niezawodności danego elementu określonych w skali wartościowania:

- brak (pomijalny) 0;
- niski poziom 1-4;
- średni poziom 5-7;
- wysoki poziom 8-9;
- maksymalny poziom 10.

Analiza następstw (zdarzeń)

Efektem przypadkowego lub rozmyślnego działania przynoszącego szkodę aktywom systemu informacyjnego jest następstwo (zdarzenie). Następstwem może być np.:

- ujawnienie informacji wrażliwej;
- niedostępność lub zniszczenie aktywów w postaci danych lub oprogramowania;
- nieupoważniona modyfikacja danych lub oprogramowania;
- nieupoważniony dostęp do danych lub oprogramowania, który powoduje straty wymierne (np. bezpośrednie lub pośrednie koszty) albo niewymierne.

W celu wywołania wymienionych efektów stosuje się następujące działania:

Dla każdej pary aktywa/zagrożenia należy określić potencjalne szkody, z uwzględnieniem związanych z nimi słabości systemu. Danymi wyjściowymi dla tej analizy są zestawienia otrzymane w dwóch poprzednich fazach. Analiza powinna wskazać te elementy systemu, które są najbardziej zagrożone, a zdarzenia z nimi związane powodują największe szkody.

Określenie wagi następstwa (konsekwencji) jest podstawą analizy ryzyka. Waga następstwa może być wyrażona jednym, łącznym oszacowaniem kosztu utraty poufności, integralności, dostępności, autentyczności, rozliczalności i niezawodności. Skala oszacowania może obejmować np. pięć poziomów: *„maksymalny”, „wysoki”, „średni”, „niski”, „pomijalny”*. Wartość skali możemy przyjąć tak jak poprzednio.

Miarę następstwa należy oszacować, uwzględniając następujące kategorie konsekwencji:

- spowodowanie uszczerbku na zdrowiu lub życiu człowieka,
- naruszenie prawa, regulaminu lub kontraktu,
- naruszenie rytmu i realizacji zadań i podziału obowiązków,
- naruszenie stosunków zewnętrznych,
- straty finansowe.

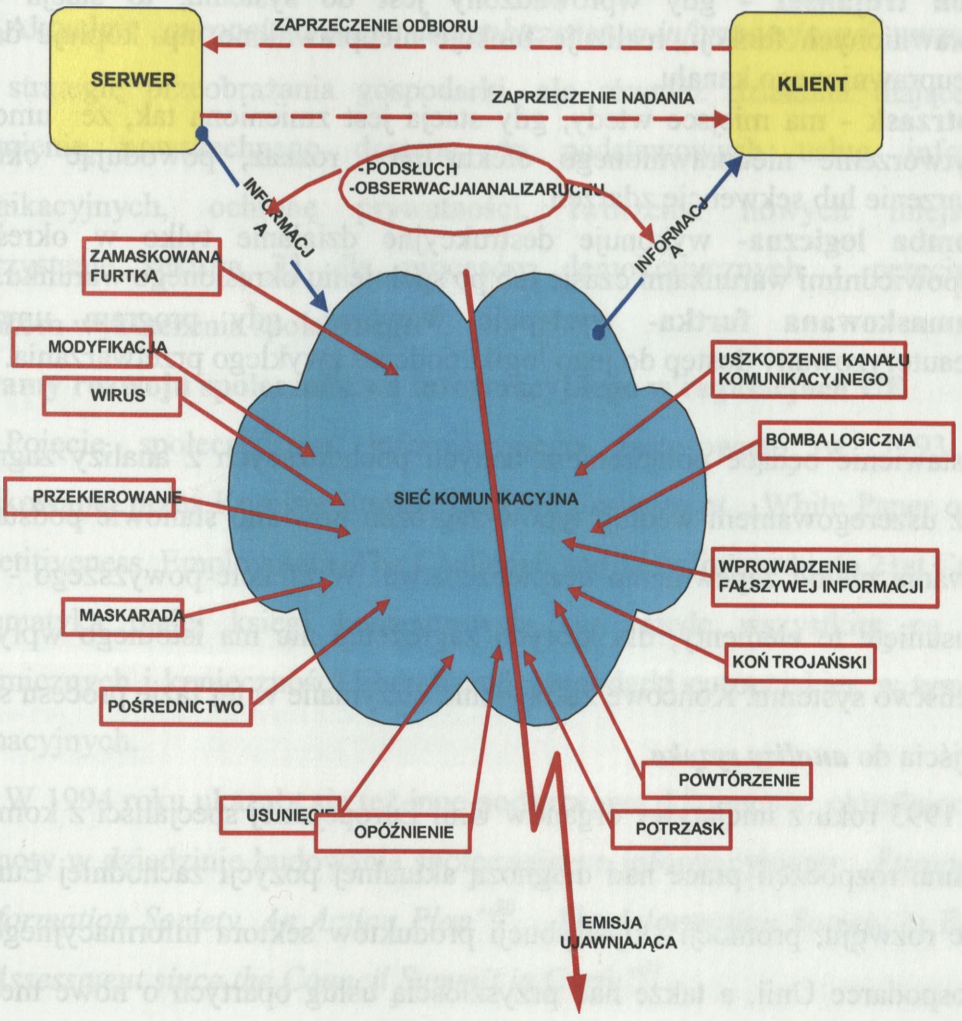


Diagram 29: ***Możliwe ataki na system teleinformatyczny***[27]

Charakterystyka ataków:

- **Maskarada** - ma miejsce wtedy, gdy jeden użytkownik stacji ruchomej udaje innego użytkownika, zazwyczaj stosowana z innymi rodzajami ataków.
- **Powtórzenia** - polegają na ponownym nadaniu informacji, komunikatu lub jego części w celu wytworzenia nieuprawnionego efektu; np. komunikat zawierający informację uprawniającą, powtórzony przez inną stację, może spowodować zwiększenie jej uprawnień.
- **Modyfikacja** - ma miejsce wtedy, gdy zmieniana jest treść przesyłanych danych, przy czym zmiana nie zostaje wykryta. Powszechnie stosowane kodowania nadmiarowe pozwalają wykryć i ewentualnie skorygować błędy powstałe podczas transmisji, ale nie chronią przed celową modyfikacją

[27] *Ibidem*

przesyłanych danych (nawet jeśli są one zaszyfrowane, ale w sposób nie gwarantujący ich integralności).

- **Koń trojański** - gdy wprowadzony jest do systemu, to stacja oprócz uprawnionych funkcji, realizuje funkcje nieuprawnione, np. kopiuje dane do nieuprawnionego kanału.
- **Potrzask** - ma miejsce wtedy, gdy stacja jest zmieniona tak, że umożliwia wytworzenie nieuprawnionego efektu na rozkaz, powodując określone zdarzenie lub sekwencję zdarzeń.
- **Bomba logiczna**- wykonuje destrukcyjne działanie tylko w określonym odpowiednimi warunkami czasie lub po spełnieniu określonego warunku.
- **Zamaskowana furtka**- występuje wówczas, gdy program umożliwia nieautoryzowany dostęp do jego logiki podczas zwykłego przetwarzania.

Zestawienie będące połączeniem danych pochodzących z analizy zagrożeń i słabości z uszeregowaniem według typów zagrożeń powinno stanowić podstawę do wypracowania metod zapewnienia bezpieczeństwa. W efekcie powyższego - z listy zostaną usunięte te elementy, dla których zagrożenie nie ma istotnego wpływu na bezpieczeństwo systemu. Końcowe zestawienie otrzymane w tej fazie procesu stanowi punkt wyjścia do ***analizy ryzyka***.

W 1993 roku z inicjatywy organów Unii Europejskiej specjaliści z komisji M. Bangemanna rozpoczęli prace nad diagnozą aktualnej pozycji zachodniej Europy w dziedzinie rozwoju, promocji i dystrybucji produktów sektora informacyjnego, jego rolą w gospodarce Unii, a także nad przyszłością usług opartych o nowe media. W raporcie M. Bangemanna, wskazano nowy rodzaj zagrożeń, wymuszających na współczesnych państwach wysoko rozwiniętych podjęcie działań koordynujących rozwój TI. Diagnozowano zagrożenia bezpieczeństwa ekonomicznego, mogące powstawać z niedostosowania gospodarek zachodnioeuropejskich do poziomu zaawansowania technologicznego sektora TI. Stwierdzono, że nie można pozwolić na niekontrolowany rozwój technologii, który niesie zagrożenia dla funkcji kontrolnych państwa oraz niektórych wymiarów jego suwerenności ze strony korporacji transnarodowych (*TC - transnational corporations*), jako zjawisk związanych z procesem globalizacji. Zalecenia Komisji miały skłonić władze Unii do przyjęcia kompleksowej strategii operacyjnej. Założono, że powstanie wspólnej polityki w dziedzinie kontroli TI pogłębi procesy integracyjne i zaktywizuje gospodarkę, której

najszybciej rozwijającym się działem jest sektor technologii informatycznych. Miało to wzmocnić i ugruntować unijną infrastrukturę krytyczną.

Aktualnie *„europejska droga do społeczeństwa informacyjnego"* uwzględnia nie tylko strategię przeobrażania gospodarki, ale również działania mające na celu zapewnienie powszechnego dostępu do podstawowych usług informacyjno-komunikacyjnych, ochronę prywatności, tworzenie nowych miejsc pracy, wykorzystanie sektora TI dla procesów demokratycznych i przeciwdziałania zjawiskom wykluczenia społecznego[28].

Programy rozwoju społeczeństwa informacyjnego w regulacjach UE

Pojęcie społeczeństwa informacyjnego zastosowano w 1993 roku w opublikowanej przez Komisję Europejską białej księdze pt. „White Paper on Growth, Competitiveness, Employment. The Challenge and Way forward into 21st Century"29. Problematyka białej księgi koncentrowała się przede wszystkim na kwestiach ekonomicznych i konieczności liberalizacji gospodarki europejskiej, w tym sektorów informacyjnych.

W 1994 roku ukazały się też inne podstawowe dokumenty, określające politykę wspólnoty w dziedzinie budowania społeczeństwa informacyjnego: *„Europe's Way to the Information Society. An Action Plan"*[30], *„The Information Society in Europę: the First Assessment since the Council Summit in Corfu"*[31].

W początkach kształtowania strategii europejskiej zdefiniowano ponadto kategorię *„usług społeczeństwa informacyjnego" (Information Society Services)*, tzn. komercyjnej oferty usług świadczonych za pośrednictwem nowych mediów na życzenie osób zainteresowanych. Również w tej fazie kształtowania zaczęto stosować pojęcie *„cybercywilizacja"*.

W 1996 roku Komisja Europejska opublikowała raport *„Living and Working in Information Society. People First"*[32]. W latach 1994-1995 dostosowano sektor legislacyjny Unii w zakresie europejskiego prawa telekomunikacyjnego i ochrony

[28] *European Way for the Information Society. Information Society* Forum Report,Brussels 2000.
[29] *White Paper on Growth, Competitiveness, Employment. The Challenge and Way forward into 21st Century, COM (93) 700 final.*
[30] *Europe's Way to the Information Society. An Action Plan, COM (94) 347 finat,* 19 lipiec 1994 r.
[31] *The Information Society in Europe: the First Assessment since the Council Summit in Corfu*, Brussels 1994

danych osobowych. W ówczesnych strategiach Unii akcentowano potrzebę liberalizacji rynków usług sieciowych, kształcenia społeczeństw w dziedzinie korzystania z nowych mediów, dofinansowanie badań w sektorze TI, podkreślając stale aktualną konieczność dostosowania prawa.

„Zielona Księga" Komisji Europejskiej, czyli *„Green Paper on the Convergence of the Telecommunications, Media and Information Technology Sectors, and the Implications for Regulation. Towards an Information Society Approach"*[33], przyjęta w 1997 roku, omawiała metody kontroli wspólnoty nad zastosowaniem tych samych środków w sektorach infrastruktury krytycznej. Zdefiniowano tu zjawisko konwergencji TI i stwierdzono, że *„prowadzi to nieuchronnie do wzajemnego przenikania zainteresowań sektorów"*[34]. Zarysowano prognozę wzajemnej ingerencji podmiotów, działających dotąd niezależnie i przyszłych prób hierarchizacji działów gospodarki. Nowe zadanie państwa może polegać na równoważeniu wpływu podmiotów działających w różnych gałęziach gospodarki w celu niedopuszczenia do asymetrycznej zależności jednych dziedzin ekonomiki od innych.

Decyzja Komisji Europejskiej, podjęta w czerwcu 1997 roku, zawiera wytyczne funkcjonowania sieci informacyjnych w Unii[35]. Komisja zaleciła podjęcie konsultacji z prywatnymi i komercyjnymi użytkownikami sieci, co stanowiłoby wypełnienie poprzednio wydanych aktów, oraz prognozowała konsekwencje ustanowienia w 1995 roku, na mocy *Decyzji 2717/95/EC, EUROISDN (European Integrated Services Digital Network),* czyli sieci transeuropejskiej. Decyzja Komisji klasyfikuje europejską sieć informacyjną, jako komponent infrastruktury telekomunikacyjnej. Równocześnie wskazuje użyteczność sieci w innych sektorach gospodarki, podkreślając konstruktywną rolę tego medium w postępie gospodarczym każdego z państw członkowskich. Komisja przejmuje odpowiedzialność za koordynację wdrożenia wytycznych, z czego przedstawiać zamierza co trzy lata zbiorcze raporty.

[33] *Green Paper. Living and Working in the Information Society: People First, COM(96)389 final, 24 lipca 1996r. COM (96) 389 final*

[34] W. Marciński, *Idea Społeczeństwa Informacyjnego jako element globalnej strategii rozwoju Unii Europejskiej*; [URL http://www.agh.edu.pl/agh/dep/WNSS/konferencja/doc/ Marcinski.doc].

[35] *Decision No 1336/97/EC of the Parliament and of the Council of 17 June 1997 on Series of Guidelines for Trans-European Telecommunications Networks, OJ L 183*, 11 lipca 1997r.; http://www.tentelecom.org.

Regulacje prawne związane z ochroną kluczowych obszarów zastosowania TI w Unii Europejskiej

Większość regulacji legislacyjnych, które dotyczą TI, zostało ujętych w postaci dyrektyw Komisji Europejskiej. Dyrektywy, jako dokumenty harmonizujące systemy legislacyjne państw członkowskich, mają charakter wiążący i wskazują zadania, które dane państwo winno zrealizować. Nie zawierają jednak norm prawnych i mogą być zaliczane do *„miękkiego prawa wspólnotowego"*, gdyż sposób ich wdrażania leży w gestii każdego członka. Wyznaczany jest również termin przewidziany na wdrożenie, którego dotrzymanie podlega ocenie *Komisji Europejskiej lub Trybunału Sprawiedliwości.* Mechanizm dyrektyw pozostawia członkom Unii swobodę decyzyjną w zakresie formy implementacji założenia programowego, uwzględnia po części zasadę subsydiarności oraz odmienności gospodarek[36].

Ogólne regulacje w zakresie bezpieczeństwa informacyjnego w Unii Europejskiej

Europejskie rozwiązania w dziedzinie bezpieczeństwa sieci, systemów informacyjnych, danych oraz gospodarki sieciowej przedstawione zostały głównie w dokumentach Komisji i Rady Europejskiej, które definiowały rodzaje zagrożeń informacyjnych i wskazywały środki ochrony sektorów infrastruktury krytycznej. Zaznaczano, że zagrożenia dotyczą funkcjonowania społeczeństwa informacyjnego na obszarze wolności, bezpieczeństwa i prawa. W dokumencie „e-Europe 2002" infrastruktura informacyjna została zdefiniowana jako podstawowe narzędzie komunikacji obywateli w Unii Europejskiej oraz jako główny nośnik jej sukcesu gospodarczego. Ataki na systemy informacyjne uznano za zagrożenie dla społeczeństwa informacyjnego i zalecono wspólną prewencję na poziomie struktur Unii. Raport wymienia najczęściej powtarzające się rodzaje przestępstw cybernetycznych: zakłócenie działania systemów, hakerstwo, rozpowszechnianie wirusów oraz inne formy złośliwego niszczenia danych, manipulacja, fałszowanie informacji itd. Wskazuje również dane liczbowe o atakach: ponad 11% użytkowników

[36] R. Tadeusiewicz. *Internet i prawo*; [URL http://www.agh.edu.pl/agh/dep /WNSS/konferencja/doc/ Tadeusiewicz.doc].

informatyki z państw UE zetknęło się z wirusami w swoich systemach komputerowych.

Podczas szczytu w Lizbonie, w marcu 2000 roku, Rada Unii Europejskiej zaprosiła Komisję do współtworzenia stosownych aktów prawnych, w tym „*eEurope Action Plan*". Plan Działania przygotowany przez obie instytucje wspólnoty, zapowiadał przygotowanie do końca 2002 roku jednolitego stanowiska wobec przestępstw cybernetycznych. Komisja opublikowała także komunikat pt. „*Tworzenie bezpiecznego społeczeństwa informacyjnego poprzez polepszanie bezpieczeństwa struktur informacyjnych i wspólną walkę z przestępstwami cybernetycznymi*"[37]. Autorzy opowiadali się tu za kompleksowym rozwiązaniem zagadnienia, za włączeniem do systemu bezpieczeństwa sieci: grup konsumenckich, operatorów, lobbingi handlowe i przemysłowe, struktury rządowe oraz legislatywy państw. Rodzaje ataków cybernetycznych przedstawiono i zdefiniowano w *komunikacie Komisji Europejskiej* z czerwca 2001 roku[38]. Wskazano w nim: nieautoryzowany dostęp do systemu informacyjnego (hakerstwo), zakłócenia systemów informacyjnych (DoS), dokonywanie celowych zmian lub niszczenia danych (wirusy), przechwytywanie wiadomości (sniffing) oraz zniekształcanie informacji (spoofing). Ataki te wymierzone są przede wszystkim w operatorów sieci, sprzedawców usług internetowych, elektroniczne kompanie handlowe oraz uderzają w funkcjonowanie tradycyjnych gałęzi infrastruktury krytycznej, wyposażonych w narzędzia TI. Komisja podkreślała wyraźny wzrost liczby, skali i stopnia zaawansowania technologicznego ataków, które obserwuje się na przełomie XX i XXI wieku, dostrzegając w nich niebezpieczeństwo dla stabilności struktur państwowych całej Wspólnoty. Raportowano coraz wyraźniejszy udział zorganizowanych grup przestępczych w przeprowadzaniu cyberataków, wymieniając przykłady *Brasilian Silver Lords* czy *Pakistan G-force,* które podejmowały próby przejęcia środków finansowych z kont instytucji działających w europejskiej cyberprzestrzeni. Ten nowy fenomen kryminalny wymaga od państw członkowskich solidarnej polityki zapobiegawczej,

[37] e-Europe 2002, *COM (2000) 890 final*, 26 stycznia 2001 r.

[38] *Communication from the Commission to the Council, of the European Parliament, the European Economic and Social Committee and the Committee of Regions „Network and Information Security: Proposal for European Policy Approach", COM (2001) 298 final*, 6 czerwca 2001r.

w pierwszej kolejności wdrożenia *Planu Działania* przyjętego przez Komisję w lutym 2001 roku[39]. Ponadto, winny być przedsięwzięte środki zapobiegawcze atakom terrorystycznym na strategiczne systemy informacyjne *(vital information systems)* w całej Unii. Postulowano ponadto dostosowanie i ujednolicenie europejskiego prawa ekstradycji i walki z wszelkimi postaciami terroryzmu, oraz współpracy Unii z innymi strukturami regionalnymi[40].

W marcu 2000 roku, podczas szczytu w Lizbonie, Rada Europejska przyjęta proponowany przez Komisję *„eEurope Action Plan"*, który w trzy miesiące później w Santa Maria de Feira, na kolejnym szczycie Rady, uzupełniony został o wstępną strategię ochrony sieci i zaowocował ustanowieniem unijnej polityki zwalczania cyberprzestępstw do końca 2002 roku. W ramach uprawnień uzyskanych w Lizbonie Komisja opublikowała wkrótce komunikat poświęcony stworzeniu zabezpieczeń europejskiego programu Sl, poprzez rozbudowę systemów bezpieczeństwa i informacji oraz zwalczanie przestępstw pochodzenia informatycznego[41]. Komunikat adresowany był do wszelakich grup interesów, mogących wnieść wkład w stworzenie legislacyjnych i technicznych form ochrony TI: prawników, informatyków, operatorów sieci, środowisk konsumenckich itp., oraz zawierał apel o współpracę w kreowaniu prawnych i technicznych środków bezpieczeństwa. Inny problem to ochrona danych — ich autentyczności, poufności, warunków sprzedaży informacji, którą dotąd regulowały Directive 95/46/EC, Directive 97/66/EC i Directive 98/84/EC[42]. Stanowiły one, że operator sieci i dostawca usług oferowanych przez Internet zobowiązuje się zabezpieczyć środki technicznej i organizacyjnej ochrony sieci, poufność danych i podnosić proporcjonalnie do postępu technologicznego poziom stosowanych zabezpieczeń. Kolejne zagadnienie polityki cyberbezpieczeństwa Unii to promocja *netyki*, edukacji informacyjnej i mechanizmów reagowania kryzysowego w sektorze infrastruktury

[39] *Preventing Fraud and Counterfeiting of Noncash Means of Payment. Action Plan, COM (2001) 11 final, 9* lutego 2001 r.
[40] Por. *Proposal for a Council Framework Decision on the European Arrest Warrant and Surrender Procedures between the Members States, COM (2001) 522 final*, 25 września 2001 r.; *Proposal for a Council Framework Decision on Combating Terrorism, COM (2001) 521 final*, 19 września 2001 r.
[41] *Creating a Safer Information Society...*, op.cit.
[42] *OJ L. 281*, 23 listopada 1995 r.; *OJ L. 024*, 30 stycznia 1998 r.

krytycznej. W tym kierunku uruchomiony został w 1998 roku program CORDIS, czyli *„Information Society Technologies Program"*, opisany poniżej.

Rezolucja Rady Unii Europejskiej w sprawie stanowiska Rady Europejskiej, przyjętego na szczycie w Sztokholmie (23-24 marca 2001 roku), w sprawie akcji specjalnych i wspólnej polityce bezpieczeństwa informacyjnego, zawiera strategię ochrony sieci oraz praktyczne wskazówki jej realizacji[43]. Sieć internetowa i inne środki komunikacji uznano za kluczowe czynniki rozwoju społeczeństwa informacyjnego i integracji europejskiej. Wobec wzrastającej roli transakcji elektronicznych, usługi sieciowe stają się coraz ważniejsze dla interesu publicznego. Rezolucja była planem działań na kolejne miesiące rozwoju TI: do końca 2002 roku proponowano zakończenie akcji promocyjnej i szkoleń komputerowych oraz określenie wspólnych standardów zabezpieczeń technicznych (zgodnie z normą *ISO 15408*), w połączeniu z ułatwianiem wzajemnego certyfikowania usług świadczonych przez operatorów z różnych krajów; do połowy 2002 roku przegląd krajowych koncepcji odpowiedzi na ataki komputerowe. Podczas szczytu w Sztokholmie potwierdzono również, że Rada i Komisja podejmą wspólne działania zmierzające do pogłębienia i poszerzenia zakresu bezpieczeństwa sieci informacyjnych w Unii. Nowe propozycje zostały przedstawione podczas szczytu Rady w Goeteborgu. Komisja wywiązała się z zadania, publikując dokument pt. *„Network and Information Security: A European Policy Approach"* [44].

W 2002 roku, na marcowym spotkaniu Rady Europejskiej w Sztokholmie, stanowiącym już drugi szczyt przeglądowy organizowany zgodnie z agendą lizbońską, odświeżono potrzebę wspierania działań w dziedzinie polityki bezpieczeństwa informacyjnego i stwierdzano w dokumentach końcowych, że *„Rada wespół z Komisją rozwijać będą kompleksową strategię bezpieczeństwa sieci, włączając w to procedury działania"*[45]. Warto również odnotować konkretne propozycje penalizacji. Uwzględniając treści *Konwencji Rady Europy o Cyberprzestępczości*, w kwietniu 2002 roku Komisja Europejska wydała oświadczenie,

[43] *Council Resotution on a Common Approach and Specific Actions in the Area of Network and Information Security, 2002/C 43/02*, 28 stycznia 2002 r.
[44] *Network and Information Security: A European Policy Approach, COM/2001*, 6 czerwca 2001 r.
[45] Za: *Proposal for a Council Framework Decision on Asainst Information Systems, COM (2002) 173 final.*

że przestępstwa komputerowe, grożące podmiotom państwowym, będą objęte karą do czterech lat pozbawienia wolności.

Rada Europy wobec problemów cyberprzestępczości

Najważniejszym dokonaniem Rady Europy w dziedzinie walki o ochronę danych, sieci i systemów informacyjnych pozostaje *„Convention on Cybercrime"*[46]. Przyjęta w Budapeszcie 23 listopada 2001 roku weszła w życie w sierpniu 2002 roku. Zdaniem ekspertów, może stanowić modelowe rozwiązanie legislacyjne w państwach wysoko rozwiniętych, ale nie powinna służyć za przykład dla krajów rozwijających się. Do zagadnienia cyberprzestępstwa odnosi się ona bardzo szeroko. Pierwszy obszar konwencji obejmuje przedmiot „zbrodni komputerowych", tzn. infekowanie wirusami komputerowymi, hakerstwo, inne formy ataku na infrastrukturę krytyczną. Drugi poświęcony jest dostępowi rządu do danych komputerowych i systemów komunikacji. Odpowiada na pytania powstające wokół uprawnień rządu do odtajniania danych komputerowych, przeglądu danych, łamania szyfrów i innych typów zabezpieczeń, inwigilacji korespondencji elektronicznej itp. Trzecia część dotyczy współpracy transgranicznej z państwami, które prowadzą cybepolitykę odmienną od unijnej. Celem dokumentu jest uwspólnienie polityki zwalczania i ścigania cyberprzestępstw oraz procedur ekstradycji przestępców czy terrorystów, co jest najistotniejsze w przypadku krajów o bardziej liberalnej, bądź bardziej restrykcyjnej, strategii rządu wobec cyberprzestępstw. Treści konwencji dotyczą walki z przestępczością komputerową, definiując ją na tyle szeroko, by część zaleceń mogła być zastosowana do walki z cyberterroryzmem.

Art. 25 konwencji dotyczy przestępstw komputerowych przeciw komunikacji sieciowej, oraz danym komputerowym czyli *cyberprzestępstw*. Wymienia się zatem: *nielegalny dostęp (art. 2), nielegalne przechwycenie danych (art. 3), zakłócenie przesytem danych (art. 4), zakłócenia systemu (art. 5).*

Konwencja nie narzuca formalnych standardów, od których spełnienia zależałoby prawo do świadczenia usług przez dostawców Internetu. *Art. 20 i 21* konwencji stanowią, że do czasu rzeczywistego wdrożenia jej przepisów przez

systemy prawne państw, wymaga się od kompetentnych władz „wyegzekwowania od dostawców usług internetowych, w granicach ich rzeczywistych technicznych możliwości", gromadzenia lub nagrywania, albo ułatwiania powyższych działań kompetentnym władzom, w zakresie obrotu danymi i treścią przekazu. Konwencja uznaje prawo do anonimowości komunikacji. Komentarz RE podkreśla jasno, że dokument nie narzuca dostawcom Internetu obowiązku rejestrowania treści korespondencji użytkowników. Zatem konwencja nie wymaga, by dostawca Internetu weryfikował tożsamość abonentów lub ograniczał prawo do stosowania pseudonimów *(Art. 181*).

Cyberterroryzm w polityce bezpieczeństwa NATO

Organizacja Traktatu Północnoatlantyckiego przeredagowała swoją doktrynę bezpieczeństwa podczas Szczytu Waszyngtońskiego, zorganizowanego w kwietniu 1999 roku, w 50. rocznicę podpisania Traktatu Północnoatlantyckiego. W dokumencie pt. *„Defence Capabilities Initiative" (DCI)* stwierdzono m.in., że *„skuteczność NATO jest pochodną [...] bezpiecznego, szybkiego i niezawodnego obiegu informacji"*[47]. Dokument ten ukonstytuował pojęcie „bezpieczeństwa teleinformatycznego", które łączy w sobie cechy bezpieczeństwa informacji ze stabilnością jej przepływu. Pełna ochrona przed zagrożeniem cyberterrorystycznym, definiowanym jako *soft terrorism*, możliwa jest poprzez zapewnienie sprawnej realizacji kilku zadań, w tym m.in.:

- określenia wrażliwości i podatności systemu operacyjnego sojuszu na zagrożenia z zewnątrz;
- rozwoju i aktualizacji bezpieczeństwa informacyjnego NATO *(INFOSEC);*
- wygenerowania obszarów dostępu do systemu informacji sojuszu *Infrastruktura Klucza Publicznego* (*PKI*) NATO;
- pogłębienia współpracy z cywilnymi instytucjami monitoringu bezpieczeństwa teleinformatycznego, np. *CERT*;
- stworzenia systemu wielopoziomowych zabezpieczeń i mechanizmów szybkiego reagowania na incydenty komputerowe[48].

[46] *Convention on Cybercrime,* Budapest, 23 listopada 2001 r.; [URL http://corwentions. coe. int/Treaty / EN / CadreListeTraites. htm].
[47] M. Machalski, *Wybrane elementy polityki NATO w walce z cyberterroryzmem*, „Telenet", styczeń 2002.
[48] *Ibidem.*

Do walki z cyberprzestępczością powołano w NATO szereg struktur specjalnych. Istniejące podkomitety i grupy robocze sojuszu w zakresie zapobiegania skutkom cyberataku pokrywają cały obszar bezpieczeństwa teleinformatycznego. Należą do nich m.in.:

- *NATO Computer Incidents Response Capability (NCIRC)* zajmuje się wymianą informacji o zagrożeniach i kieruje akcjami szybkiego reagowania na ataki. Problematyka NCIRC została omówiona w ***Rozdziale 3.2.2***;
- *High Level Steering Group (HLSG)* steruje całym sektorem przedsięwzięć w zakresie polityki bezpieczeństwa teleinformatycznego;
- *Vulnerability Assessment Team (VAT)* analizuje i określa aktualny stopień zagrożenia potencjalnym atakiem, wypracowuje narzędzia analizy zagrożeń i zarządzania ryzykiem. Przykłady tych narzędzi omawia ***Rozdział 4.3***.

Na uwagę zasługuje również polityka sojuszu wobec wykorzystania Internetu. W sieciach publicznych mogą być zatem umieszczane informacje jawne, do których dostęp nie wyrządzi szkody sojuszowi. Sieci publiczne mogą służyć przesyłowi informacji o ograniczonych klauzulach tajności dopiero po ich wcześniejszym zaszyfrowaniu certyfikowanymi narzędziami kryptograficznymi. Dodatkowo przyjmuje się, że Internet służył będzie komunikacji specjalnej tylko w wypadku braku dostępu do innych, profesjonalnych środków łączności specjalnej.

W ekspertyzach NATO, dotyczących terroryzmu, pojawiają się wartościowe definicje i rozróżnienia. *Cyberterroryzmem* określone zostały akty terroryzmu z zastosowaniem informacji albo systemów informacyjnych, jako narzędzi ataku bądź obrony. Zastrzeżono przy tym, że między *cyberprzestępstwem* a *cyberterroryzmem* istnieje różnica co do motywów i celów, zatem nie każdy rodzaj cyberataku uznany będzie za *cyberterrorystyczny*. Celem działań *cyberterorystycznych* będzie wywołanie strachu, paniki wśród ludności cywilnej albo zakłócenie systemów obronności państwa. Komputer może służyć jako narzędzie ułatwiające tę działalność.

Widać wyraźnie, że NATO, jako sojusz polityczno-wojskowy, koncentruje swoją strategię w zakresie bezpieczeństwa informacyjnego wokół kategorii *cyberterroryzmu*. Skupia się również na tworzeniu specjalistycznych grup roboczych,

odpowiedzialnych za wąskie obszary wdrażania zabezpieczeń informacji i systemów ich przetwarzania.

Strategie regionalne w Unii Europejskiej i NATO różnią się zasadniczo od rozwiązań globalnych. Unia Europejska promuje kategorię społeczeństwa informacyjnego, łącząc ochronę technologii nowych mediów, z podniesieniem poziomu życia i wykształcenia obywateli. Zmiany legislacyjne w Unii uwzględniają kategorię *cyberprzestępstw*, ale nie *cyberterroryzmu*, który jest pojęciem rzadko spotykanym w dokumentach wspólnotowych.

Raporty i oceny rozwoju polskiego TI

Dyskusja w środowiskach specjalistycznych na temat zaawansowania technologicznego polskiej gospodarki po transformacji systemowej rozpoczęła się w latach dziewięćdziesiątych. W 1994 roku w Poznaniu odbył się Pierwszy Kongres Informatyki Polskiej, którego raport podsumowywał stan przygotowania do informatyzacji gospodarki i życia publicznego. Autorzy raportu rzetelnie i krytycznie ocenili rozwój TI w Polsce: „*Nasze społeczeństwo ma obojętny stosunek do informatyki i nie jest przekonane do korzyści wynikających z jej powszechnego stosowania. Nie widzi również możliwych zagrożeń*"[49]. Wśród tych ostatnich, autorzy opracowania wyszczególnili przede wszystkim naruszenie poufności danych, szczególnie danych osobowych, i wskazali konieczne legislacyjne środki prewencji. Dostrzeżono również groźbę rozwarstwienia społecznego oraz powstanie w Polsce „*informacyjnej underclass*". Ponadto uznano za niepokojący dystans, który może powstać, gdy program TI znajdzie zastosowanie w administracji publicznej, czemu nie będzie towarzyszył rozwój dostępności nowych mediów. Aby temu zapobiec, postulowano właściwą, szybką procedurę legislacyjną, uzupełnianą przez promocję szkoleń i kształcenia, pozwalającą na opanowanie obsługi komputerów i sieci. Pośrednio wypowiadano się również o niebezpieczeństwach, spowodowanych przejęciem kontroli nad informacją przez zorganizowane grupy o nastawieniu antyspołecznym i antypaństwowym, co w pewien sposób poruszało problematykę

[49] *Strategia Rozwoju Informatyki w Polsce; Stan, Perspektywy, Zalecenia*, Poznań 1994;[URL http://www.kongres.org.pl/online/1szy_Kongres/Raport.html].

cyberterroryzmu. Proponowane działania legislacyjne miały rozwijać się w dwóch kierunkach: ku stworzeniu komputerowej, sieciowej bazy aktów prawnych, stale aktualizowanej i zabezpieczanej przed ingerencją zewnętrzną (*informatyzacja legislacji*) oraz ku zdynamizowaniu prac prawodawczych związanych z TI (*legislacja informatyzacji),* co powinno odbywać się z uwzględnieniem specjalistycznych opinii informatyków.

Drugi Kongres Informatyki Polskiej zorganizowany został po upływie pięciu lat, na przełomie listopada i grudnia 1999 roku. W przyjętym raporcie stwierdzano m.in.: *„Podkreślenie konieczności zmian legislacyjnych wynikających z upowszechniania się nowych technik informatycznych wypływa ze stale zwiększającego się zagrożenia przestępstwami komputerowymi. Włamania do systemów, wprowadzanie niszczących wirusów czy kradzież danych oraz zmiany zapisów księgowych powodują coraz większe szkody finansowe i mogą obecnie dotknąć każdego obywatela nawet nie korzystającego z komputera. Dlatego konieczne jest analizowanie tego rodzaju przestępstw, odpowiednie przeszkolenie policji oraz organów śledczych, a także wprowadzenie do kodeksów karnych i handlowych odpowiednich zapisów umożliwiających skazanie złapanych przestępców komputerowych"*[50]. Uznano, że dla środowiska informatycznego najważniejszymi regulacjami prawnymi, które weszły w życie w minionych kilku latach, są ustawy:

- O łączności z 1990 roku (z późniejszymi nowelizacjami);
- O prawie autorskim i prawach pokrewnych z 1994 roku;
- O zamówieniach publicznych z 1994 roku;
- O ochronie danych osobowych z 1997 roku51.

Do dyskusji włączył się również parlament. Sejm w *uchwale z 14 lipca 2000 roku, w sprawie budowania społeczeństwa informacyjnego*, diagnozował, iż *„system prawny i polityka rządu nie tworzą dostatecznych warunków rozwoju społeczeństwa informacyjnego"*[52]. Delegowano zatem na Radę Ministrów kompetencje w zakresie przygotowania narodowej strategii rozwoju społeczeństwa informacyjnego, czego

[50] *Rozwój informatyki...*, op.cit.
[51] *Ibidem.*
[52] *Uchwała Sejmu Rzeczypospolitej Polskiej* z dnia 14 lipca 2000 r. w *sprawie budowania podstaw społeczeństwa informacyjnego w Polsce, „Monitor Polski"* z 2000 r. nr 22, poz. 448.

efektem stał się raport KBN z listopada 2000 roku. W uchwale sejmowej wyodrębniono następujące zadania strategiczne: powszechny dostęp do Internetu; rozwój *Egovernment, Eeducation;* szybki Internet dla ośrodków naukowo-badawczych; teleinformatyka w systemie finansowym i obronności, transporcie i ochronie zdrowia oraz prewencji kryminalnej; wreszcie zgodna ze standardami międzynarodowymi transformacja aktów prawnych regulujących problemy bezpieczeństwa informacyjnego, kryptografii, podpisu elektronicznego itp.

W listopadzie 2000 roku *Komitet Badań Naukowych* przedstawił raport pt. „*Cele i kierunki rozwoju społeczeństwa informacyjnego w Polsce*". Autorzy tego dokumentu, naukowcy kluczowych ośrodków akademickich w kraju, stwierdzali we wprowadzeniu m.in.: „*Pierwsze kraje, które wkroczą do społeczeństwa informacyjnego, uzyskają największe korzyści. One ustalą porządek rzeczy dla wszystkich, którzy pójdą w ich ślady. Dla kontrastu, kraje, które odkładają decyzje lub preferują rozwiązania częściowe, mogą doświadczyć w najbliższej dekadzie katastrofalnego spadku inwestycji i zmniejszenia liczby miejsc pracy*"[53]. Dostrzeżono zatem zmianę zachodzącą we współczesnych parametrach potęgi i podsumowano umiejętności przystosowania się państwa do zmian w zasadach kreowania przywództwa w systemie międzynarodowym, w nowej epoce powszechnej informatyzacji. Stwierdzano, że mocarstwowość XXI wieku a zwłaszcza hegemonia globalna wymaga kompleksowego dostosowania polityki państwa do najbardziej aktualnych *megatrendów* rozwojowych (np. globalizacji), wymaga też współuczestnictwa w ich kształtowaniu. Wiąże się z nią również potrzeba uchwycenia kluczowych, priorytetowych płaszczyzn stosunków międzynarodowych. Wśród nich główne miejsce zajmuje obecnie *informacja* i *telematyka*.

Raport wyjaśniał różnicę terminologiczną między „*globalnym społeczeństwem informacyjnym*", promowanym przez Unię Europejską, a „*globalną infrastrukturą informacyjną*", rozwijaną przez rząd USA. Wskazywano, że koncepcja unijna skupia się na czynnikach humanistycznych i cywilizacyjnych, które pomijają Amerykanie, badający głównie zaplecze technologiczne współczesnej cywilizacji. Dostrzegano

[53]Raport KBN, *Cele i kierunki rozwoju...*, op. cit., s. 2.

także zagrożenia płynące z rozwoju i upowszechniania techniki informatycznej i cywilizacji informacyjnej. *„Wskazuje się, że rozwój technik informacyjnych i wzrost gospodarczej roli informacji może prowadzić do rozwarstwienia społecznego, w wyniku którego osoby nie posiadające dostępu do informacji będą cywilizacyjnie i ekonomicznie upośledzone. Ułatwiony dostęp do informacji może zagrażać prywatności [...] oraz wywołać pojawienie się nowej grupy przestępstw"*[54]. Określona została równocześnie rola państwa jako podmiotu zapobiegającego zagrożeniom, który to cel realizować należy w postaci skoordynowanego planu obejmującego główne dziedziny strategiczne i działy pomocnicze.

Autorzy raportu podjęli próbę zdefiniowana polityki państwa w zakresie implementacji idei społeczeństwa obywatelskiego jako: *„zespołu działań zmierzających do zapewnienia wszystkim obywatelom dostępu do informacji [...]"*, przy czym stwierdzono, że społeczeństwo informacyjne w Polsce zostanie ukształtowane siłami rynkowymi, z udziałem mechanizmów społecznych. Zadanie rządu sprowadza się do „stworzenia odpowiednich mechanizmów ekonomicznych, prawnych i administracyjnych dla zagwarantowania powszechnego dostępu do informacji, zapewnienia uczciwej konkurencji, umożliwienia zainteresowanym podmiotom korzystania z istniejących i przyszłych możliwości zastosowań teleinformatyki oraz tworzenia nowych rozwiązań, tak w sferze techniki jak i organizacji pracy"[55]. Podkreślono także konieczność szybkiego rozwoju infrastruktury krytycznej w naszym kraju.

Sugerowano, by rozwój telekomunikacji był równocześnie: koordynowany przez stosowne resorty rządowe, skorelowany z procesami integracyjnymi Polski z Unią Europejską i by uwzględniał potrzebę standaryzacji usług, jako niezbędny i minimalny warunek bezpieczeństwa infrastruktury krytycznej państwa. W rozdziale pt. *„Prawo i przestępstwa teleinformatyczne"* jako cel podaje się: *„dostosowanie regulacji prawnych do wymagań szybkiego postępu technicznego i ery społeczeństwa informacyjnego. Zastosowanie technik teleinformatycznych do opracowania nowych aktów prawnych"*[56].

[54] *Ibidem*, s. 3.
[55] *Ibidem*, s. 4.
[56] Raport KBN, *Cele i kierunki rozwoju...*, op. cit., s. 12.

Pojawienie się nowych rodzajów przestępstw interpretowano jako konsekwencję nowych zagrożeń bezpieczeństwa obywateli w zakresie prawa do prywatności i danych osobowych. Równocześnie autorzy raportu sugerowali zmniejszenie do minimum liczby nowych regulacji prawnych, które ze względu na ustawiczną zmienność środków teleinformatycznych, zachowywałyby krótką aktualność. Właściwsza wydaje się technika nowelizacji już istniejących ustaw oraz przepisów wykonawczych na szczeblach resortów. Proponowano też przyjęcie ogólnych zasad *netyki*, opartych na istniejących przepisach prawnych. Na przykład ochrona danych osobowych, a nawet pełna anonimowość użytkowników sieci, winna być zapewniona wszędzie tam, gdzie może być ona zachowana poza siecią. Postulowano również implementację porozumień w sprawie handlowych aspektów ochrony własności intelektualnej, podpisanych przez Polskę w ramach porozumień *Światowej Organizacji Handlu (WTO)* w 1996 roku i uznano, że należy podjąć starania o przystąpienie do traktatu o prawie autorskim *Światowej Organizacji Własności Intelektualnej (WIPO)*[57].

Raport nie zawierał definicji przestępstwa komputerowego ani cyberterroryzmu, kluczowych pojęć badanego przez nas zagadnienia. Dowodził natomiast świadomości zagrożeń, które autorzy dostrzegali w niekontrolowanym rozwoju telemediów. „*Nowym jakościowo zjawiskiem jest pojawienie się w sieciach telekomunikacyjnych treści nielegalnych i szkodliwych, a w tym pornografii, materiałów nacjonalistycznych i terrorystycznych. Należy, podchodząc ze szczególną uwagą do kwestii wolności wypowiedzi, szybko opracować założenia do ustawy o zakazie rozpowszechniania treści nielegalnych i szkodliwych w sieciach teleinformatycznych, przyjmując za punkt wyjścia prace OECD oraz Uchwałę Rady Europy z dnia 17 lutego 1997 roku. Ustawa powinna jasno określać odpowiedzialność osób i instytucji, będących źródłem informacji, jej edytorem oraz jej dostarczycielem w długim nieraz łańcuchu pośredników*"[58]. Powinna również określać formalnoprawne mechanizmy kontroli treści udostępnianych w sieciach, przy zapewnieniu swobodnej wymiany informacji. W celu ochrony nieletnich

[57] A. Bógdał-Brzezińska, M. F. Gawrycki. *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*. FSM Warszawa 2003
[58] *Ibidem.*

przed treściami szkodliwymi należy wprowadzić i upowszechnić system niezależnego, dobrowolnego rankingu i klasyfikacji treści publikowanych w sieciach teleinformatycznych przez organizacje konsumenckie[59].

W raporcie zajęto się także szyfrowaniem informacji przesyłanych w sieciach teleinformatycznych. O ile powszechnie uznaje się szyfrowanie informacji za konieczne dla zapewnienia prywatności i bezpieczeństwa użytkowników sieci oraz poprawnego rozwoju gospodarki elektronicznej, o tyle stopień skomplikowania klucza (jego długość) i algorytmu szyfrującego, oraz dostęp agend rządowych do tego klucza, pozostaje kwestią sporną. Doradzano, by dla zachowania bezpieczeństwa kraju i ochrony przed terroryzmem, rozważyć umożliwienie agendom rządowym dostępu do kluczy szyfrowania wszelkich informacji w sieciach publicznych, co stanowiłoby jednak naruszenie tajemnicy komunikowania się (*por. art. 49 Konstytucji RP*). Proponowano przyjęcie takich rozwiązań prawnych i systemów zarządzania kluczami, by zachowana została równowaga pomiędzy interesami państwa, uzasadnionymi jego bezpieczeństwem, a interesami jego obywateli. Regulacje w tym zakresie powinny być tworzone w uzgodnieniu z Unią Europejską, gdzie proponuje się obecnie powołanie niezależnych instytucji przechowujących klucze szyfrujące i udostępniających je agendom rządowym po okazaniu nakazu prokuratorskiego. Uprawnia on do naruszenia tajemnicy poczty elektronicznej, podobnie jak do założenia podsłuchu. Szyfrowanie informacji może podlegać pewnym ograniczeniom, a jej deszyfrowanie nie powinno być dozwolone bez wiedzy nadawcy (ze wskazanym wcześniej wyjątkiem). Regulacje te powinny uwzględniać wytyczne dla polityki szyfrowania, opracowane przez OECD. Należy również zapewnić warunki techniczne umożliwiające rozkodowywanie informacji pochodzących z innych krajów świata, w tym z Unii Europejskiej, oraz nawiązanie współpracy operacyjnej w tym zakresie. Systemy tworzone na potrzeby zapewnienia bezpieczeństwa państwa, obejmujące administrację, policję, wojsko, służby specjalne i niektóre instytucje komercyjne, powinny wykorzystywać najnowocześniejsze metody zabezpieczeń. Jasne jest, że nie istnieją i być może nigdy nie powstaną zabezpieczenia pewne, których nie da się

[59] *Ibidem.*

złamać. Ogólnie jednak przyjmuje się, że informacja jest dobrze zabezpieczona, gdy koszt złamania zabezpieczenia jest wyższy od wartości tej informacji. Dlatego też stosowane w takich systemach urządzenia i techniki powinny posiadać odpowiedni certyfikat Agencji Bezpieczeństwa Wewnętrznego. Konieczne jest również podjęcie na potrzeby państwa badań nad technicznymi i organizacyjnymi metodami zabezpieczeń systemów teleinformatycznych oraz przetwarzanych w nich danych.

Strategia *ePolska* 2001-2006

Polska podziela stanowisko grupy państw kandydujących do Unii, że należy dostosowywać systemy administracyjne do założeń wspólnej polityki rozwojowej. Strona polska deklarowała w 2001 roku posiadanie 49% osieciowanych jednostek samorządowych, przyznając równocześnie niewystandaryzowanie jakości ich połączeń. Integracja Polski ze strukturami Unii Europejskiej wymagać będzie realizacji idei społeczeństwa informacyjnego, w którym ogromną rolę w gospodarce odgrywają systemy informacyjne. *„Społeczeństwo informacyjne jest narzędziem dla rozwoju państwa. [...] Dążąc do celu, jakim jest rozwój społeczeństwa informacyjnego, państwo musi ograniczyć swe kompetencje do tych dziedzin, gdzie są niezbędne: ustanawianie prawa, dbanie o bezpieczeństwo, tworzenie struktur administracyjnych oraz podejmowania niezbędnych decyzji administracyjnych. Dopiero wówczas możemy mówić o usunięciu przeszkód stających na drodze rozwoju państwa"* opinię tę wygłosił K. Ferenc, prezes spółki CENTRUST, podczas konferencji pt. *„Standardy bezpieczeństwa systemów informatycznych w Unii Europejskiej"*[60]. Została ona zorganizowana w Krakowie w maju 2002 roku i stała się okazją do wzmocnienia rządowego stanowiska w sprawie bezpieczeństwa informatycznego. Minister Danuta Huebner, w wystosowanym na tę okazję liście do uczestników konferencji, stwierdziła m.in.: *„Droga do rozwoju wiedzie przez wiedzę, dlatego naturalne wydaje się realizowanie wizji społeczeństwa informacyjnego i elektronicznego obrotu gospodarczego"*[61]. Nawiązywano w ten sposób do aktywnej postawy Polski w organizowaniu wielostronnych konsultacji związanych z dostosowaniem do standardów TI.

[60] M. Wardaszko, *Bezpieczeństwo a Unia*; [URL http://www.msignet.com.pl/archi wum/51.html].

W maju 2000 roku w Warszawie zorganizowana została konferencja pt. „*Information Society — Accelerations European Integration*", poświęcona zagadnieniom społeczeństwa informacyjnego. W dokumencie końcowym konferencji Polska i inne kraje kandydujące zobowiązały się do współpracy z Komisją Europejską przy opracowaniu wspólnego dokumentu programowego eEurope+ oraz przygotowania krajowego planu działania inicjatywy ePolska. Deklaracja konferencji warszawskiej zakłada, że celami politycznymi, które mają osiągnąć kraje kandydackie poprzez wspólny plan działania eEurope+ są:

- zademonstrowanie opinii publicznej wspólnych wysiłków krajów „*piętnastki*" oraz krajów kandydujących na rzecz realizacji wyzwań nowej ekonomii;
- wskazanie, że proces akcesji to coś znacznie większego niż negocjowanie acquis communautaire;
- polityczne wsparcie dla wysiłków czynionych przez kandydujące kraje w kierunku integracji europejskiej;
- zaprezentowanie komplementarności inicjatywy eEurope oraz planu eEurope+.

Jednocześnie podkreślano, że plan działania eEurope+ jest ofertą fakultatywną i nie będzie krajom tym narzucany, powinien natomiast korelować z narodowymi inicjatywami, do których należy ePolska.

W programie ePolska, autoryzowanym przez Ministerstwo Łączności, przedstawiono w czerwcu 2001 roku plan działań na rzecz rozwoju społeczeństwa informacyjnego w Polsce[62]. Program obejmuje pięcioletni okres zmian, które nastąpią w wielu sektorach gospodarki pod patronatem rządu. Rozdziały dokumentu odpowiadają realizacji proponowanych przez Sejm i *KBN* obszarów implementacji społeczeństwa informacyjnego: rozwojowi infrastruktury telekomunikacyjnej, szybkiej, powszechnej internetyzacji, programom edukacyjnym adresowanym do pracowników, wykorzystaniu Internetu w administracji, sądownictwie i policji, ochronie zdrowia, opiece społecznej, w transporcie.

[61] *Ibidem.*
[62] Ministerstwo Łączności. *ePolska. Plan działań na rzecz rozwoju społeczeństwo informacyjnego w Polsce na lata 20012006*, materiał z 14 czerwca 2001 r.

4.2.7. *Analiza diagnostyczna stanu bezpieczeństwa informacyjnego państwa*

ANALIZA DIAGNOSTYCZNA

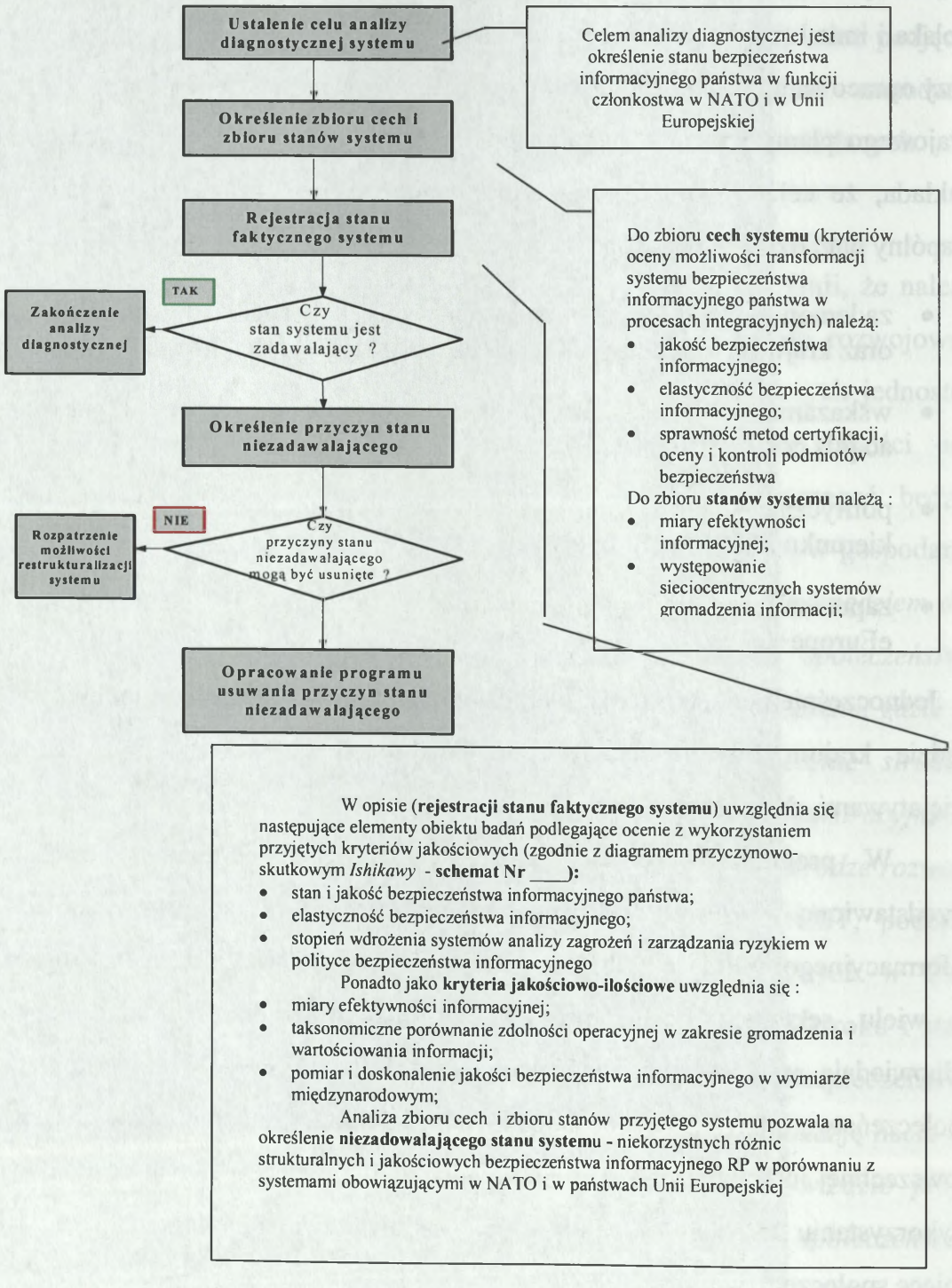


Diagram 30: ***Przebieg analizy diagnostycznej przedmiotowego materiału***
Źródło: opracowanie własne

Określając cel **analizy diagnostycznej** jako ocenę stanu bezpieczeństwa informacyjnego RP jako państwa – członka NATO i w perspektywie integracji z Unią Europejską - zgodnie ze ***Diagramem Nr 30*** stosuje się kolejne kroki analizy parametrów wytypowanych w wyniku zastosowania **analizy problemowej** - ***Rozdział 4.2.5.***

Do **zbioru stanów** systemu należą zgodnie z wytypowanymi parametrami podlegającymi badaniom: miary efektywności informacyjnej, występowanie sieciocentrycznych systemów gromadzenia informacji, stosowanie zautomatyzowanych narzędzi analizy zagrożeń i zarządzania ryzykiem. **Zbiorami cech** systemu pozostaną: jakość bezpieczeństwa informacyjnego, elastyczność bezpieczeństwa informacyjnego, sprawność metod certyfikacji, oceny i kontroli podmiotów bezpieczeństwa.

4.3. Ryzyko jako wymierna kategoria obszaru analizy zagrożeń bezpieczeństwa informacyjnego

Słownik PWN podaje, że ryzyko jest to *możliwość, prawdopodobieństwo, że coś się nie uda, przedsięwzięcie, którego wynik jest nieznany, niepewny, problematyczny...*[63]

Pojęcie ryzyka, a przede wszystkim sama analiza ryzyka zawsze towarzyszyła wszelkim przedsięwzięciom, jednak dopiero od niedawna dziedzina ta stała się przedmiotem dogłębnych badań.

Według W. Tarczyńskiego i M. Mojsiewicz określenie *ryzyko* pochodzi od staro włoskiego słowa *risicare* – czyli *odważyć się*. Jest zatem *ryzyko* raczej wyborem niż nieuchronnym przeznaczeniem. *„Wiążąc ryzyko z wyborem potwierdzamy nierozerwalny związek ryzyka z czasem"*[64].

Analitycy odróżniają *ryzyko* od *niepewności*. Współcześnie definiuje się *niepewność jako stan, w którym przyszłe możliwości i szanse ich wystąpienia nie są znane* (niepewność sensu stricte, niepewność niemierzalna). Pojęcie ryzyka jest natomiast używane wtedy, gdy:

[63] *Słownik Języka Polskiego PWN*, Tom III, Warszawa 1978, s. 155.
[64] W. Tarczyński, M. Mojsiewicz, *Zarządzanie ryzykiem*, Warszawa 2001, s. 11.

- rezultat, jaki będzie osiągnięty w przyszłości, nie jest znany, ale możliwe jest zidentyfikowanie przyszłych sytuacji;
- znane jest prawdopodobieństwo zrealizowania się poszczególnych możliwości w przyszłości[65] (niepewność mierzalna).

Natura ryzyka:

1. *Ryzyko nie jest czymś jednorodnym, a zatem nie jest możliwe podanie jednej uniwersalnej i jednoznacznej definicji tego pojęcia.*
2. *Ryzyko występuje w co najmniej dwóch aspektach:*
   - *obiektywnym;*
   - *subiektywnym.*
3. *Ryzyko może być badane w różnych kontekstach, na przykład jako:*
   - *niebezpieczeństwo;*
   - *hazard;*
   - *niepewność;*
   - *prawdopodobieństwo.*
4. *Ryzyko jest czymś zmiennym i stadialnym, czyli jest raczej procesem niż stanem otoczenia*[66].

Analiza ryzyka obejmuje wszelkie przedsięwzięcia mające na celu określenie źródeł i charakteru zagrożeń, określenie ich i ocenę wpływu zagrożeń na działanie systemu oraz określenie sposobów ich eliminacji lub zmniejszenia ryzyka.

Zarządzanie ryzykiem dotyczy rozpoznawania rodzaju ryzyka, prze założeniu możliwości jego *skwantyfikowania*. W praktyce zarządzanie ryzykiem obejmuje następujące działania:

- *rozpoznanie rodzajów ryzyka*
- *pomiar ryzyka,*
- *kontrola ryzyka,*
- *informacja o ryzyku*[67].

W przypadku bezpieczeństwa systemów informacyjnych, *ryzyko* to *możliwość wystąpienia jakiegoś niepożądanego i niebezpiecznego dla systemu zdarzenia (procesu)*[68]. Za *analizę ryzyka*, zbadanie ryzyka – czyli trafne rozpoznanie

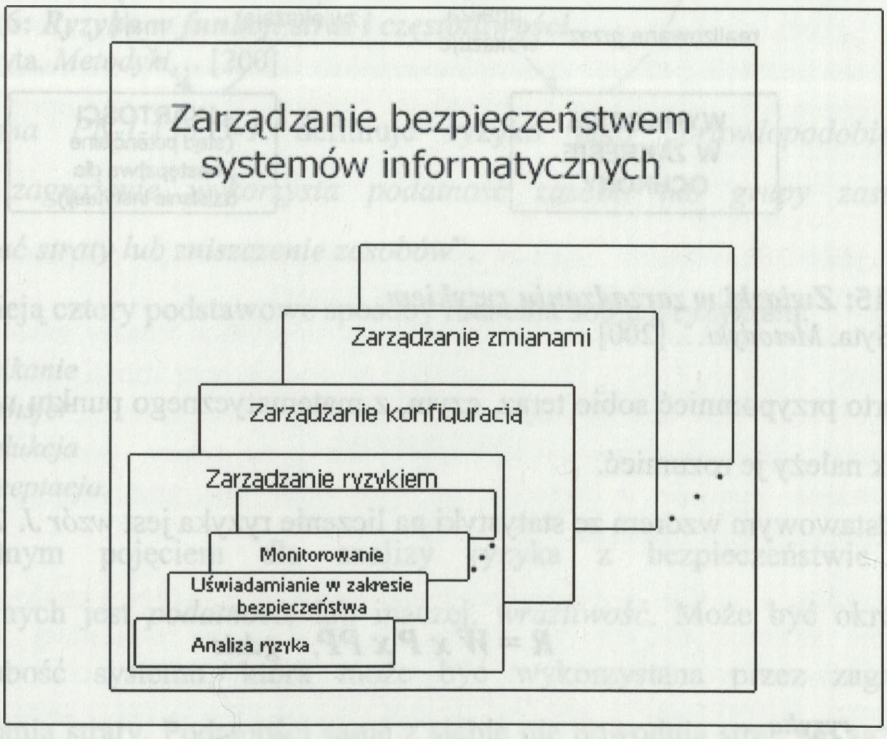
[65] *Ibidem*, s. 12.
[66] *Ibidem*, s. 15.
[67] *Ibidem* 35-37.
[68] *Jeśli analizujemy ryzyko w systemach bezpieczeństwa informacyjnego, to będziemy koncentrować się na zagrożeniach jakie mogą uniemożliwić pożądane funkcjonowanie tego systemu. Pozytywne skutki naszych*

potencjalnych zagrożeń, uważa się pomiar i przygotowanie informacji o charakterze zagrożeń, dającej użyteczny materiał wyjściowy do sporządzenia skutecznej polityki bezpieczeństwa systemu.

Celem *zarządzania ryzykiem* jest:

- *doskonalsze zabezpieczenie systemów teleinformatycznych;*
- *umożliwienie kierownictwu jednostki organizacyjnej podejmowanie decyzji związanych z nakładami finansowymi na zabezpieczenia i ochronę informacji;*
- *uzyskanie dokumentacji ułatwiającej przeprowadzenie procesu certyfikacji lub akredytacji systemów.*

Miejsce *analizy ryzyka* ilustruje poniższy schemat:

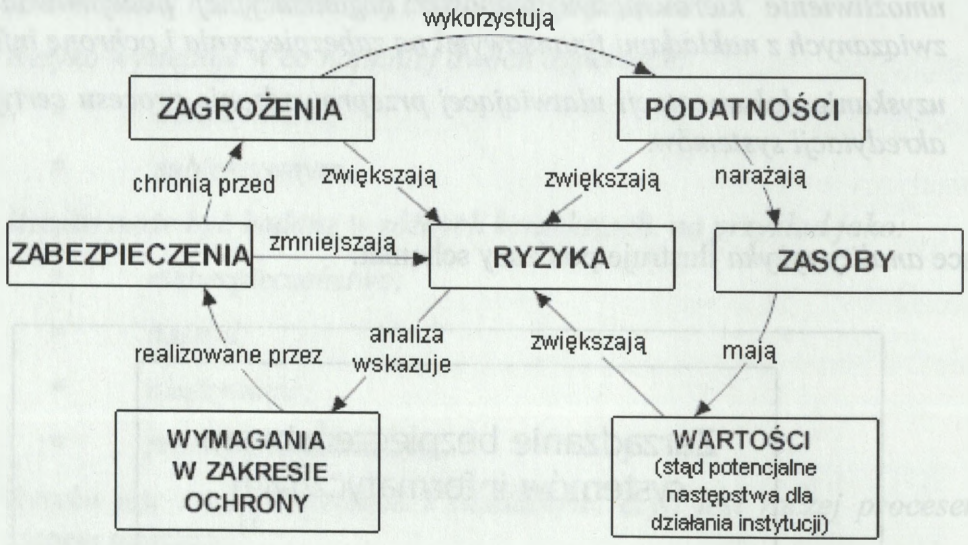


Rysunek 14: ***Miejsce analizy ryzyka w zarządzaniu bezpieczeństwem systemów informatycznych***
Źródło: J. Syta. *Metodyki*... [200]

Ryzyko nie zawsze musi budzić negatywne skojarzenia. Wiele wynalazków powstało właśnie dzięki temu, że ktoś postawił wszystko na jedną kartę i wygrał. Z drugiej strony niejedna tragedia była spowodowana wzięciem na swoje barki za

działań – takie jak podniesienie poziomu bezpieczeństwa, usprawnienie i perspektywiczne zabezpieczenie kanałów przesyłu informacji – będą raczej przedmiotem zainteresowania polityki bezpieczeństwa niż analizy

dużego ryzyka lub niedoszacowaniem. By z pełną świadomością móc podejmować decyzje należy ryzyko najpierw poznać, trzeba wiedzieć jak dużo możemy stracić, jaki to może mieć wpływ na naszą działalność aż wreszcie jak prawdopodobne jest, że coś nieprzyjemnego się nam przytrafi.



Rysunek 15: ***Związki w zarządzaniu ryzykiem***
Źródło: J. Syta. *Metodyki*... [200]

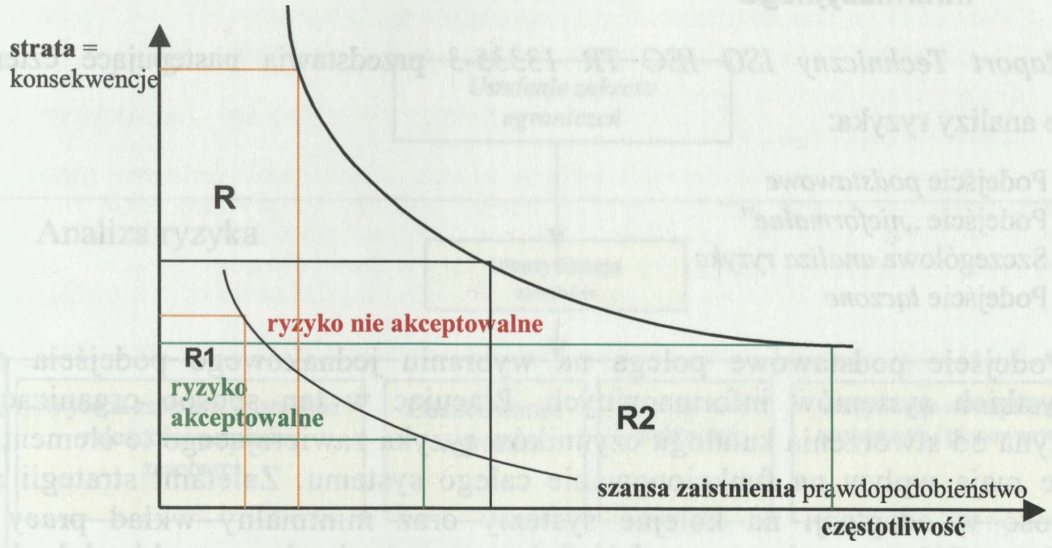
Warto przypomnieć sobie teraz, czym, z matematycznego punktu widzenia jest ryzyko, jak należy je rozumieć.

Podstawowym wzorem ze statystyki na liczenie ryzyka jest *wzór J. Turnera*

$$R = W \times P \times PP, \quad \textit{gdzie}$$

R **-** ***ryzyko***
W - wpływ (konsekwencje - jakie szkody/zyski może przynieść projekt)
P - prawdopodobieństwo wystąpienia określonej sytuacji
PP - publiczna percepcja – czynnik sugerowany przez Turnera, który ma wyrażać wpływ opinii społecznej ocenianie wielkości konsekwencji przez analityków

ryzyka. Analiza ta posłuży jedynie za materiał wyjściowy do stworzenia skutecznej polityki bezpieczeństwa a potem do trafnych jej modyfikacji już w czasie funkcjonowania sytemu.



Rysunek 16: ***Ryzyko w funkcji strat i częstotliwości***
Źródło: J. Syta. *Metodyki*... [200]

Norma PN-I-13335-1 definiuje ryzyko jako „*prawdopodobieństwo, że określone zagrożenie wykorzysta podatność zasobu lub grupy zasobów, aby spowodować straty lub zniszczenie zasobów*".

Istnieją cztery podstawowe sposoby radzenia sobie z ryzykiem:

- *Unikanie*
- *Transfer*
- *Redukcja*
- *Akceptacja*

Istotnym pojęciem dla analizy ryzyka z bezpieczeństwie systemów informacyjnych jest *podatność,* lub inaczej, *wrażliwość*. Może być określana jako pewna słabość systemu, która może być wykorzystana przez zagrożenie do spowodowania straty. Podatności same z siebie nie powodują strat, ale są warunkiem lub zbiorem warunków, które mogą umożliwić zagrożeniu wpłynąć na zasoby. Podatność systemu należy koniecznie rozważać z dwóch perspektyw – wewnętrznej, zależnej od samej organizacji, oraz zewnętrznej. Podatności cały czas ewaluują i z tego też powodu należy je prze cały czas monitorować.

Drugim terminem, który należy znać, a przede wszystkim o którym należy pamiętać, są następstwa, jako zjawiska mogą mieć wpływ na przyszłą pracę systemu informacyjnego.

4.3.1. Metody szacowania ryzyka w analizach zagrożeń bezpieczeństwa informacyjnego

Raport Techniczny ISO IEC TR 13335-3 przedstawia następujące cztery strategie analizy ryzyka:

- Podejście *podstawowe*
- Podejście *„nieformalne"*
- Szczegółowa *analiza ryzyka*
- Podejście *łączone*

1. Podejście podstawowe polega na wybraniu jednakowego podejścia do wszystkich systemów informacyjnych. Pracując w ten sposób organizacja zaczyna od stworzenia katalogu czynników ryzyka zawierającego te elementy, które mają wpływ na funkcjonowanie całego systemu. Zaletami strategii są łatwość w adaptacji na kolejne systemy oraz minimalny wkład pracy i środków. Główną wadą tego podejścia jest zagrożenie zbyt wysokim lub zbyt niskim „postawieniem poprzeczki". Może to spowodować niewspółmiernie wysoki do potrzeb poziom zabezpieczeń, lub też wręcz przeciwnie - braki w zabezpieczeniach oraz duże problemy w sytuacji, gdy w systemie zaczniemy wprowadzać zmiany.
   Podejście podstawowe stosuje *metody kwantytatywne.*

2. Podejście *„nieformalne"* polega na wykorzystaniu wiedzy eksperckiej zarówno specjalistów jak i zwykłych użytkowników systemu.
   Główną zaletą również w tym przypadku są niewielkie koszty zasobów. Wśród wad należy wymienić dużą subiektywność w ocenie oraz możliwość przeoczenia niektórych aspektów. Zabezpieczeniem przed tą sytuacją może być stosowanie formularzy, które dodatkowo będę pomocne przy pracy, ponieważ zapewnią postępowanie zgodnie z określonym sposobem uniemożliwiając przeoczenie pewnych elementów systemu.

3. *Szczegółowa analiza ryzyka* to dogłębna, bardzo szczegółowa analiza wszystkich systemów informatycznych w organizacji. Polega na dokładnej identyfikacji zagrożeń spowodowanych przez określone czynniki, ich wpływu oraz podatności na cały system. Główną zaletą jest fakt, że pozwala na identyfikację całego systemu, a raporty powstałe w wyniku jej przeprowadzenia mogą być używane do zarządzania zmianami zabezpieczeń.
   Głównymi wadami są wysokie koszty przygotowania, długi czas oczekiwania na komplet wyników oraz niebezpieczeństwo, że ze względu konieczność oczekiwania na wszystkie wyniki, może się okazać, że jest już za późno by zapobiec zagrożeniom. Norma zaleca następujący przebieg procesu:

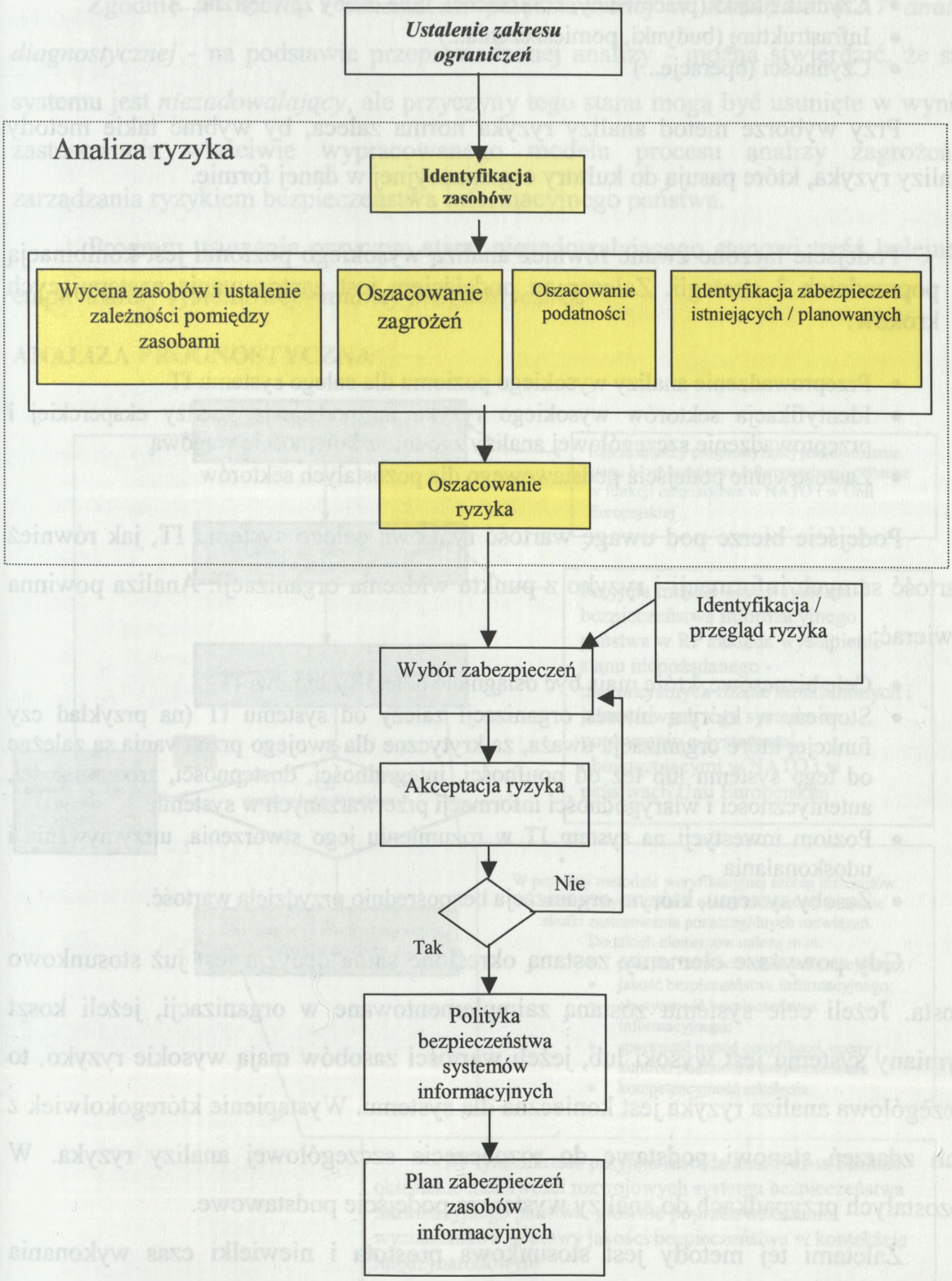


Diagram 31 ***Zarządzanie ryzykiem obejmujące szczegółową analizę ryzyka***
Źródło: J. Syta. *Metodyki*... [200]

Na początku analizy ryzyka należy określić jej ramy. Opis powinien zawierać:

- Czynniki IT (sprzęt komputerowy, oprogramowanie, informacje...)
- Czynnik ludzki (pracownicy, kontrahenci, inne osoby zewnętrzne...)
- Infrastrukturę (budynki, pomieszczenia...)
- Czynności (operacje...)

Przy wyborze metod analizy ryzyka norma zaleca, by wybrać takie metody analizy ryzyka, które pasują do kultury organizacyjnej w danej formie.

4. Podejście łączone zwane również analizą wysokiego poziomu jest kombinacją poprzednich 3 strategii. Zalecanym podejściem jest zastosowanie następujących kroków:

- Przeprowadzenie analizy wysokiego poziomu dla całego systemu IT
- Identyfikacja sektorów wysokiego ryzyka na podstawie wiedzy eksperckiej i przeprowadzenie szczegółowej analizy zgodnie z kolejnością wagową
- Zastosowanie podejścia podstawowego dla pozostałych sektorów

Podejście bierze pod uwagę wartość rynkową całego systemu IT, jak również wartość samych informacji i ryzyko z punktu widzenia organizacji. Analiza powinna zawierać:

- Cele biznesowe, które mają być osiągnięte dzięki systemowi IT
- Stopień, w którym interes organizacji zależy od systemu IT (na przykład czy funkcje, które organizacja uważa, za krytyczne dla swojego przetrwania są zależne od tego systemu lub też od poufności, integralności, dostępności, zrozumiałości, autentyczności i wiarygodności informacji przetwarzanych w systemie
- Poziom inwestycji na system IT w rozumieniu jego stworzenia, utrzymywania i udoskonalania
- Zasoby systemu, którym organizacja bezpośrednio przydziela wartość.

Gdy powyższe elementy zostaną określone sama decyzja jest już stosunkowo prosta. Jeżeli cele systemu zostaną zaimplementowane w organizacji, jeżeli koszt wymiany systemu jest wysoki lub, jeżeli wartości zasobów mają wysokie ryzyko, to szczegółowa analiza ryzyka jest konieczna dla systemu. Wystąpienie któregokolwiek z tych zdarzeń stanowi podstawę do rozpoczęcia szczegółowej analizy ryzyka. W pozostałych przypadkach do analizy wystarcza podejście podstawowe.

Zaletami tej metody jest stosunkowa prostota i niewielki czas wykonania analizy, zagrożeniem jest możliwość niewłaściwej identyfikacji niektórych z systemów wysokiego ryzyka.

4.3.2. Zarządzanie ryzykiem jako instrument realizacji polityki bezpieczeństwa informacyjnego – analiza prognostyczna

Zgodnie z teorią i schematem przedstawionej w ***Rozdziale 4.2.7*** *analizy diagnostycznej* - na podstawie przeprowadzonej analizy - można stwierdzić, że stan systemu jest *niezadowalający*, ale przyczyny tego stanu mogą być usunięte w wyniku zastosowania właściwie wypracowanego modelu procesu analizy zagrożeń i zarządzania ryzykiem bezpieczeństwa informacyjnego państwa.

Program usuwania przyczyn stanu niezadowalającego stanowi treść kolejnego etapu analizy systemowej - *analizy prognostycznej.*

ANALIZA PROGNOSTYCZNA

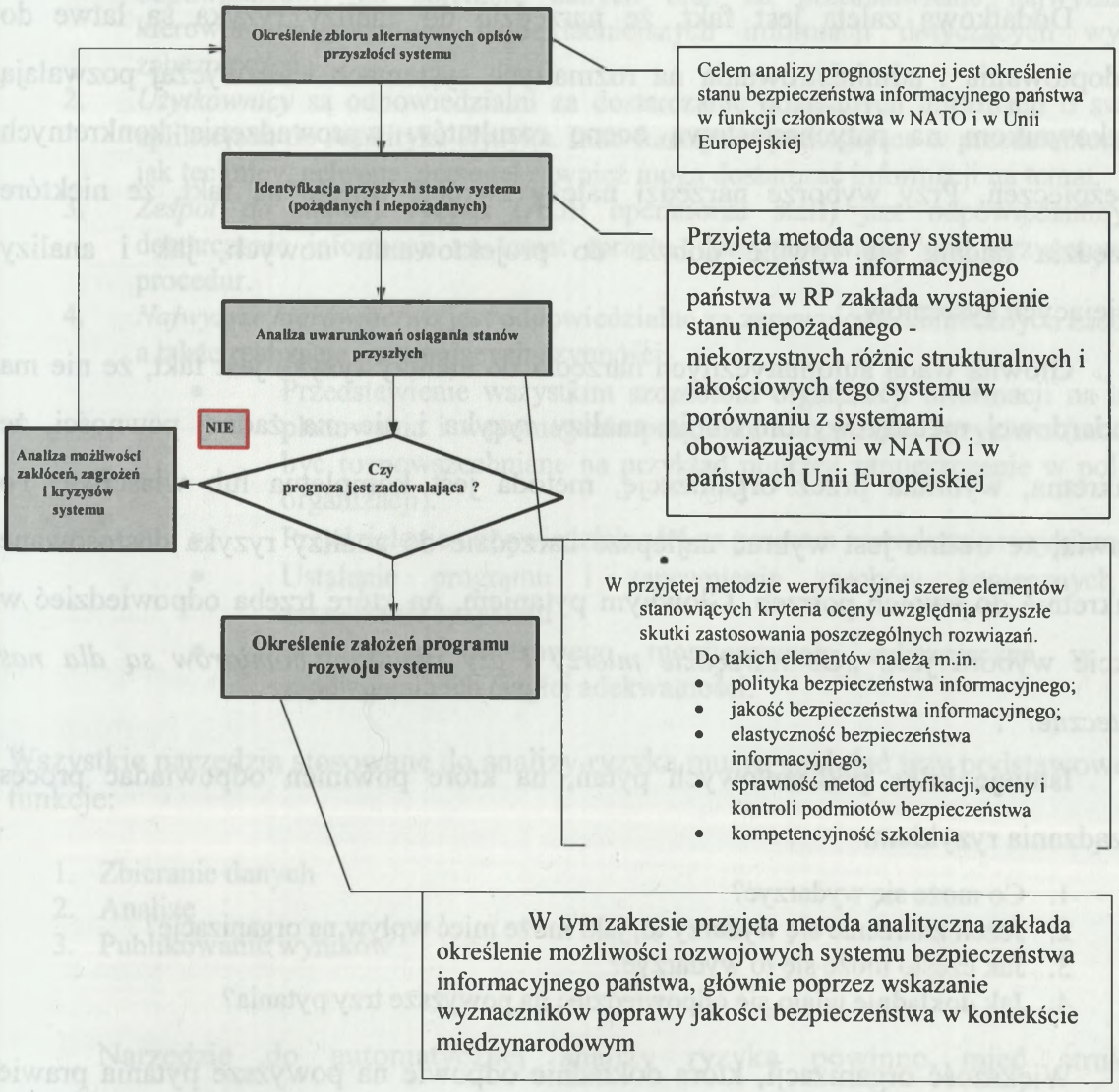


Diagram 32: ***Analiza prognostyczna przedmiotowego materiału***
Źródło: opracowanie własne

Istnieje wiele metod oceny analizy ryzyka. Elementarną częścią metod są matryce. Te matryce, odpowiednio pogrupowane, z przypisanymi określonymi wagami, zakresami wartości i użyte do konkretnych zasobów tworzą metody. Na podstawie takich metod większość dużych firm konsultingowych opracowała, a teraz sprzedaje, własne programy – narzędzia do analizy i zarządzania ryzykiem.

Główną zaletą automatycznych narzędzi jest szybkość. W przeciwieństwie do ręcznej analizy ryzyka, która może nawet trwać miesiącami automatyczne narzędzia są w stanie wykazać słabości systemu w znacznie krótszym czasie. Jest to szczególnie ważne, by nie utracić aktualności danych, gdyż może się okazać, że rezultaty analizy są już nieaktualne ze względu na wprowadzone zmiany w systemie.

Dodatkową zaletą jest fakt, że narzędzia do analizy ryzyka są łatwe do zaadoptowania i administrowania na rozmaitych systemach i zazwyczaj pozwalają użytkownikom na natychmiastową ocenę rezultatów wprowadzenia konkretnych zabezpieczeń. Przy wyborze narzędzi należy zwrócić uwagę na fakt, że niektóre narzędzia nadają się równie dobrze do projektowania nowych, jak i analizy istniejących systemów.

Główną wadą automatycznych narzędzi do analizy ryzyka jest fakt, że nie ma standardowej metody wykonywania analizy ryzyka i nie ma żadnej pewności, że konkretna, wybrana przez organizację, metoda jest kompletna lub właściwa. To sprawia, że trudno jest wybrać najlepsze narzędzie do analizy ryzyka dostosowane konkretnie do swoich potrzeb. Głównym pytaniem, na które trzeba odpowiedzieć w trakcie wyboru jest: „*Co narzędzie mierzy i czy rezultaty pomiarów są dla nas użyteczne?*".

Istnieje kilka podstawowych pytań, na które powinien odpowiadać proces zarządzania ryzykiem:

1. Co może się wydarzyć?
2. Jeżeli zdarzenie się wydarzy to, jaki może mieć wpływ na organizację?
3. Jak często może się to wydarzyć?
4. Jak dokładnie udało się odpowiedzieć na powyższe trzy pytania?

Większość organizacji, która dokładnie odpowie na powyższe pytania prawie na pewno zidentyfikuje takie elementy ryzyka, które uzna za niemożliwe do zaakceptowania. Wtedy musi odpowiedzieć na kolejne trzy pytania:

1. Co można zrobić?
2. Ile to będzie kosztowało?
3. Czy działania będą efektywne?

Proces wyboru narzędzia do analizy ryzyka można podzielić na kilka kroków:

I. Przydzielenie osób, których celem będzie ocena dostępnych narzędzi AR
II. Zdefiniowanie wymaganych kryteriów
III. Przygotowanie kwestionariusza
IV. Prośba o przeprowadzenie demonstracji kandydujących pakietów
V. Analiza możliwości pakietów
VI. Wybór pakietu

Zespół powinien się składać z następujących członków:

1. *Analityk Ryzyka* powołany do przeprowadzania analizy ryzyka. Jest on odpowiedzialny za zbieranie danych oraz za przedstawienie najwyższemu kierownictwu możliwie najdokładniejszych informacji dotyczących wyboru zabezpieczeń.
2. *Użytkownicy* są odpowiedzialni za dostarczanie dokładnych informacji o swoich aplikacjach do Analityka Ryzyka. Inne funkcje wspomagające w przedsiębiorstwie jak technicy, ochrona, personel również mogą dostarczać informacji na temat.
3. *Zespół do analizy ryzyka* (ADP operational staff) jest odpowiedzialny za dostarczanie informacji na temat sprzętu, oprogramowania oraz przygotowanie procedur.
4. *Najwyższe kierownictwo* jest odpowiedzialne za zapewnienie koniecznych zasobów a także realizację następujących czynności:
    - Przedstawienie wszystkim szczeblom organizacji informacji na temat planowania i wspomagania programu zarządzania ryzykiem (może to być rozpowszechniane na przykład poprzez zamieszczenie w polityce organizacji).
    - Przydzielenie odpowiedzialności za program zarządzania ryzykiem
    - Ustalenie programu i zapewnienie zasobów koniecznych do zarządzania ryzykiem
    - Wymaganie okresowego monitorowania zabezpieczeń w celu zapewnienia ich ciągłej adekwatności.

Wszystkie narzędzia stosowane do analizy ryzyka muszą spełniać trzy podstawowe funkcje:

1. Zbieranie danych
2. Analizę
3. Publikowanie wyników

Narzędzie do automatycznej analizy ryzyka powinno mieć strukturę pozwalającą na zbieranie informacji tekstowych lub graficznych na temat zrozumienia systemu. Ta faza jest konieczna do przygotowania opisów zasobów oraz określenia

wagi dla organizacji. Narzędzie powinno również zbierać informacje dotyczące zaistniałych zdarzeń, podatności zasobów oraz stosowanych zabezpieczeń.

Najważniejszą czynnością w trakcie całego procesu analizy ryzyka jest prawidłowa *identyfikacji zasobów*. Jest tak, ponieważ to na ich podstawie dostarczane są kierownictwu dane na temat konieczności wprowadzenia zabezpieczeń. Analiza zasobów może również wykazać, że nie ma w tym momencie niczego, co należałoby szczególnie chronić.

Wiele narzędzi do analizy ryzyka operuje na zasobach materialnych takich jak budynki, materiały. Należy również pamiętać, by analiza obejmowała zasoby niematerialne jak reputacja organizacji, morale pracowników. Narzędzia AR powinny uwzględniać również koszty wprowadzenia i utrzymywania systemu bezpieczeństwa informacji jak na przykład koszty wymiany oprogramowania, danych, dokumentacji, jak również kontrolę efektywności systemu.

Aby ułatwić identyfikację i nie pominąć pewnych elementów zasoby można pogrupować na przykład w takie kategorie:

- Informacje
- Wyposażenie
- Zapasy
- Personel
- Usługi
- Budynki
- Przychód

Kolejną czynnością, jaką należy wykonać w procesie zbierania danych jest *identyfikacja zagrożeń*, które mają wpływ na bezpieczeństwo zasobów. W przeciwieństwie do zasobów, które są wyjątkowe dla każdej organizacji, zagrożenia są bardziej ogólne. Pierwsze próby pogrupowania zagrożeń podjęli Carroll oraz Parker. Obecnie stosuje się następujący podział:

Zagrożenia losowe:

- *Zewnętrzne* (np. zakłócenia w zasilaniu, wyładowania atmosferyczne, pożar, zalania wodą pomieszczeń). Zaistnienie takich zagrożeń może prowadzić na przykład do utraty integralności lub zniszczenia danych, zaś w ekstremalnych sytuacjach, do zniszczenia infrastruktury technicznej systemu. Ciągłość pracy systemu zostaje zakłócona, choć zazwyczaj nie dochodzi do naruszenia poufności informacji.

- *Wewnętrzne* (np. niezamierzone błędy i pomyłki operatorów, administratorów bądź użytkowników systemu, awarie sprzętu lub oprogramowania). Wystąpienia tych zagrożeń może prowadzić do utraty integralności danych, zniszczenia danych albo zakłócenia ciągłości pracy systemu. W wyjątkowych sytuacjach może nastąpić naruszenie poufności informacji.

Zagrożenia zamierzone

Ataki na system podejmowane są najczęściej z niskich (chęć zysku, rewanżu, wandalizm) lub przestępczych pobudek (szpiegostwo gospodarcze lub terroryzm). Jest to najpoważniejszy rodzaj zagrożeń, ponieważ jest nastawiony na naruszenie poufności informacji. Sprawca najczęściej unika uszkadzania infrastruktury technicznej i zakłócania ciągłości pracy systemu, ponieważ zazwyczaj dąży do ukrycia faktu swej ingerencji w systemie.

Przykłady zagrożeń przedstawiono w ***Tabeli Nr 9.***

Przykładowe zagrożenia związane z informacją		
Losowe		**Zamierzone**
Zewnętrzne	**Wewnętrzne**	
Trzęsienie ziemi	Pomyłki i pominięcia	Podsłuch
Piorun	Skasowanie pliku	Modyfikacja informacji
Powódź	Nieprawidłowe skierowanie	Włamania do systemu
Pożar	Zapomnienia hasła	Złośliwy kod
Gradobicie	Wypadki fizyczne	Kradzież

Tabela 9: ***Przykłady zagrożeń***
Źródło: J. Syta. *Metodyki*... [200]

Identyfikacja zagrożeń powinna obejmować następujące strefy:

- Środowisko/Otoczenie fizyczne
- Personel
- Administracja
- Sprzęt i oprogramowanie
- Komunikacja

Kolejnym elementem, na który należy zwrócić uwagę w trakcie fazy zbierania danych jest określenie podatności zasobów. Niektóre narzędzia traktują podatność jako zagrożenie dla bezpieczeństwa całego systemu, które umożliwia zagrożeniom wpływ na poufność, integralność lub dostępność zasobów. Inne traktują podatność jako brak zabezpieczeń lub też wykorzystują ją do kontroli, która pozwala zapobiegać pogwałceniom bezpieczeństwa. Niezależnie od podejścia żadne narzędzie nie może dobrze pracować bez wiedzy jak podatny jest system na potencjalne zagrożenia.

Ostatnim elementem, którego nie może zabraknąć na tym etapie jest efektywność zabezpieczeń. By analizować ryzyko konieczna jest wiedza na temat tego jak organizacja może być pewna bezpieczeństwa swojej pracy, na ile skuteczne są dotychczas stosowane zabezpieczenia lub też o ile wzrośnie poziom bezpieczeństwa w wyniku wykorzystania innych metod. Zabezpieczenia można podzielić na:

- *Bezpieczeństwo administracyjne*
- *Bezpieczeństwo fizyczne*
- *Bezpieczeństwo oprogramowania*
- *Bezpieczeństwo personelu*
- *Bezpieczeństwo otoczenia/środowiska*
- *Bezpieczeństwo komunikacji*

Narzędzia do analizy ryzyka powinny, jeżeli to możliwe zbierać informacje na każdy z powyższych tematów.

Istnieją dwa podstawowe podejścia do procesu analizy ryzyka: *kwantytatywne* i *kwalitatywne*.

Pierwsze z nich kwantytatywne najczęściej oznacza analizę ryzyka i oszacowanie wspomagające matematyczne obliczenia wpływu zagrożenia, częstotliwości i prawdopodobieństwa. Podejście operuje wyłącznie na danych numerycznych, bierze pod uwagę dane historyczne i statystyczne.

Podejście kwalitatywne polega na prowadzeniu rankingu zagrożeń i zasobów. Bazuje na wiedzy i ocenie osób dokonujących analizy. Wynik jest najczęściej opisowy, lecz można dokonać później, w razie potrzeby, przełożenia słów na cyfry. Podejście jest znacznie prostsze do stosowania pod warunkiem ustalenia granic dla kryteriów.

Przy stosowaniu *kwalitatywnych metod analizy ryzyka* nie ma możliwości analizy efektywności kosztowej zabezpieczeń, chyba, że wcześniej skwantyfikowano wartości ryzyka. *Metody kwalitatywne* często zwracają większą uwagę na opisy niż wyliczenia. Z tego też powodu bywają często krytykowane, że opisy nie koniecznie są obiektywne oraz, że interpretacja danych zależy tylko i wyłącznie od ich zrozumienia przez osobę badającą, co wiąże się z dużą subiektywnością rozumienia wyników

Większość narzędzi do analizy ryzyka stasuje albo *metody kwalitatywne*, albo *kwantytatywne*. Stosunkowo niewiele potrafi łączyć obie.

Metody Kwantytatywne

Wartość monetarna

Polega na określeniu elementów ryzyka poprzez kwotę, jaką może to nas kosztować. Można ją stosować dla wszystkich zasobów i zabezpieczeń, dostarcza podstaw dla matematycznych i statystycznych wyliczeń ryzyka. Wadą jest fakt, że nie zawsze można niektóre wyrażenia wyrazić przy pomocy wartości monetarnej (np. bezpieczeństwo publiczne).

Wartość procentowa

Wartość procentowa jest nawet częściej stosowana niż konkretne wartości. Co prawda na przykład wartość zasobów nie może być wyrażona procentowo, lecz można już tak przedstawić procent zasobów utraconych w przypadku pojawienia się zagrożenia. Zaletami jest bardzo proste porównywanie np. prawdopodobieństwa wystąpienia zagrożeń, poziomu zabezpieczeń systemu, efektywności itp. Metoda wspomaga matematyczne i statystyczne obliczenia. Główną wadą jest fakt, że gdy jest używana ręcznie, bez wsparcia systemów eksperckich, obliczanie procentu może wymagać dokładniejszego zrozumienia problemu niż to konieczne oraz może zajmować dużo czasu. Inną wadą jest sytuacja, gdy w przypadku konfliktu nie można jednoznacznie określić, kto ma racją (na przykład, czy ryzyko poważnego pożaru wynosi 30%, czy 70%.

Liczba wystąpień „n", gdzie n > 0

Metoda polega na wyliczaniu wartości na podstawie danych historycznych. Wiemy, ile razy na przestrzeni lat pojawiało się zagrożenie, możemy na tej podstawie wyliczyć średnią, a następnie powiedzieć z dużą dozą prawdopodobieństwa, że w kolejnych latach będzie podobnie. Zaletą jest danie stabilnej podstawy do obliczeń statystycznych oraz łatwość zrozumienia. Wadami są konieczność posiadania odpowiednich danych, brak uwzględniania faktu zmian w systemie.

Prawdopodobieństwo

Jest bardzo popularną techniką opisującą możliwość wystąpienia wydarzenia w skończonej liczbie możliwości. Zaletami jest łatwość zrozumienia, wspomaga graficzne korelacje różnych prawdopodobieństw i rozwiązań

Opis graniczny

Metoda polega na określeniu minimalnych granic (na przykład częstotliwości występowania zjawiska lub wag poszczególnych elementów ryzyka). Pozwala to na operowanie kilkoma wartościami – najlepszą, najgorszą oraz średnią. Metoda wspomaga obliczenia matematyczny i statystyczne, jest intuicyjna i niewiele kosztuje. Wymaga posiadania historycznych danych, niekiedy wymaga również konwersji na wartości liczbowe, gdy do opisu stosowano zarówno kwanty- jak i kwalitatywne metody.

Ocena pozycji konkurencyjnej (benchmarking)

W *normie ISO 9004-4* występuje pod nazwą "*Działania porównawcze*". Benchmarking stosuje się w celu porównania procesu z procesami firm uznanych za wiodące w danej dziedzinie. Przyjęty punkt odniesienia zależy od konkretnej firmy: porównywać można się z przedsiębiorstwem "średnim", najlepszym w grupie albo też uznanym za wiodące na rynku. Im przedsiębiorstwo uznaje swoją organizację i działalność za lepsze, tym przyjmuje sobie wyższy punkt odniesienia.

Należy pamiętać, aby przedsiębiorstwo "*wzorcowe*" w jak największym stopniu organizacyjnym i marketingowym przypominało daną organizację. Muszą to być np. firmy o podobnej skali, produkujące podobny sam wyrób, skierowany do tego samego klienta. Dlatego najlepiej jest porównywać się do bezpośredniego konkurenta. Benchmarking pozwala ustalić cele, które powinny zostać osiągnięte przez organizację. Bardzo istotne jest także wybranie odpowiednich czynników, które będą porównywane.

Można wyróżnić trzy rodzaje benchmarkingu:

- *Wewnętrzny* – porównanie z najlepszymi wewnątrz organizacji
- *Zewnętrzny* – polega na porównywaniu z najlepszymi spoza organizacji
- *Funkcjonalny* – oznacza porównywanie się z najlepszymi pod względem funkcjonalnym – odniesiony jest do różnych rodzajów działalności

Metody Kwalitatywne

Matryce w *metodach kwalitatywnych* potrzebne są do odpowiedniego przełożenia wartości werbalnych na wartości możliwe do przetwarzania zgodnie z zasadami arytmetyki. Dane zasoby organizacji ocenia się na początku pod kątem odpowiedzi na konkretne tematy, a później przy pomocy współczynników wagowych grupuje w zależności od potrzeba analizy.

Najczęściej stosowane matryce w metodach kwalitatywnych są:

Zero, Jeden

Najprostsza z matryc. Albo coś przyjmujemy, albo nie. Zaletą jest prostota wykonania, wadą - sytuacja, gdy nie można jednoznacznie ocenić zagrożeń.

Low, Medium, High

Bardzo łatwa matryca. Użytkownik po prostu przydziela jedno z 3 określeń dla każdego rozpatrywanego elementu ryzyka. Jest tania, szybka, łatwa do zrozumienia i prosta w zastosowaniu. Do wad należy brak uzasadnienia dla podejmowanych na tej podstawie decyzji – szczególnie może to być widoczne w przypadku podejmowania w ten sposób decyzji finansowych. Kolejną wadą jest pewna subiektywność oceny – nie zawsze można wyniki odnieść do innych.

(Vital, Critical, Importand, Convinient, Informational)

Tak zwana *matryca brytyjska lub HSE (Health & Safety Executive*). Matryca daje do wyboru pięć poziomów, wag elementów ryzyka. Kluczem do jej poprawnego używania jest poprawne zdefiniowanie kryteriów poszczególnych poziomów za względu na czas reakcji i wpływ na zasoby Dalsze rozszerzenie np. 1-7; 1-99 daje możliwość dokładniejszej oceny. Zaletami jest łatwa możliwość porównania różnych elementów ryzyka, łatwość zrozumienia, możliwość zastosowania dla wszystkich elementów ryzyka. Może być używana, gdy wartość monetarna nie jest z jakiś przyczyn dokładnie znana. Wadami są subiektywność, ewentualne problemy przy definiowaniu kolejnych poziomów, a także brak możliwości poparcia danymi analiz kosztowych w przypadku, gdy analiza dotyczy kosztów zabezpieczeń lub określania wartości zasobu.

(Skutek Pomijany, Groźny, Krytyczny, Katastrofalny)

Matryca bardzo często stosowana w Ameryce. Jej zaletą jest fakt, że mając do dyspozycji parzystą liczbę odpowiedz nie mamy możliwości wybrania odpowiedzi w środku, która często niewiele nam mówi. W tym przypadku musimy jasno określić, że coś jest przynajmniej odrobiną lepsze, lub odrobinę gorsze. Inne zalety i wady jak powyżej

Opisowa ocena ryzyka (kwestionariusz)

Stosuje się do sprawdzenie dopuszczalności i wykonywalności projektu, ocena jakości posiadanego zbioru możliwości oraz uzupełnienie analizy efektywności o szerszy wymiar ocen. Przykładowymi zastosowaniami poniższych metod są wartość zasobów, ocena częstotliwości zagrożenia, jego wpływu, efektywność zabezpieczeń, koszt zabezpieczeń, ocena niepewności.

Norma ISO 9004-4 wymienia to narzędzie pod nazwą "*Formularz zbierania danych*", który ma zastosowanie przy systematycznym zbieraniu danych w celu uzyskania jasnego obrazu rzeczywistości. Lista zbiorcza jest narzędziem stosunkowo prostym w użyciu, można ją stosować we wszystkich działach przedsiębiorstwa.

Szczególnymi cechami listy zbiorczej są:

- Krótki czas przygotowania
- Niski koszt zastosowania
- Wysoka efektywność
- Duża elastyczność

Warto nadmienić, iż lista zbiorcza powinna być tak skonstruowana, aby wypełnianie odbywało się w jak najprostszy sposób. Procedura zastosowania listy zbiorczej jest następująca:

1. Ustalić cel zbierania danych
   Należy zidentyfikować problem, który lista zbiorcza ma pomóc rozwiązać.

2. Określić dane potrzebne do osiągnięcia celu
   Należy wybrać wyłącznie te informacje, które mogą mieć wpływ na rozwiązanie problemu. Zdarza się, że w trakcie wypełniania karty pojawiają się nowe wady, które dotychczas nie występowały. Należy wobec tego na każdym formularzu zostawić miejsce na problemy dotąd nie zaobserwowane.

3. Określić sposób analizy danych.
   Konieczne jest ustalenie, jak będą grupowane poszczególne czynniki oraz to, jak często te badania należy przeprowadzać.

4. Zaprojektować formularz do zapisywania danych.
   Musi zawierać takie elementy jak przyczyny i rodzaje występujących wad, częstotliwość ich występowania, a także informacje: kto, gdzie i jak zbierał dane.
5. Sprawdzić formularz
   Należy odpowiedzieć sobie na pytanie, czy formularz pozwoli zebrać wszystkie potrzebne informacje.
6. Przegląd i ewentualna korekcja formularza
   Trzeba zapoznać się z wszystkimi pytaniami, sprawdzić czy pozwolą na uzyskanie potrzebnych danych. W razie konieczności należy formularz poprawić.
7. Zbieranie danych
   Konieczne jest wytypowanie osób, które w rzetelny, odpowiedzialny i systematyczny sposób będą zbierać dane. Należy im dodatkowo wyjaśnić, w jakim celu przeprowadza się badanie oraz w jaki sposób dokonywać zapisów.
8. Analiza, wnioski
   Należy wcześniej ustalić metody, jakie będą wykorzystane do analizy danych. Lista zbiorcza ma pomóc w zbieraniu danych, które będą później analizowane w celu rozwiązania konkretnego problemu.

Katalog czynników ryzyka

Służy identyfikacji czynników ryzyka poprzez listę pytań. Dobrze przygotowane lista powinna zawierać wszystkie punkty konieczne do sprawdzenia w procesie analiz ryzyka. Zabezpiecza przed błędem polegającym na przeoczeniu pewnych aspektów. Katalog sprawia, że trzeba porównać sytuację z wcześniej przygotowaną listą.

Analiza portfelowa to wycena mocnych i słabych stron przedsiębiorstwa (np. ***SWOT***). Silne strony służą budowaniu strategii, określenie słabych stanowi identyfikację elementów ryzyka.

Nazwa tej metody pochodzi od następujących angielskich słów: *Strengths – siły, Weaknesses – słabości, Opportunities – szanse, Threats – zagrożenia*. Zasadniczo analiza SWOT jest metodą diagnozy i oceny sytuacji strategicznej. Zastosowanie tej metody daje obraz czynników wewnętrznych organizacji – czyli słabych i silnych stron oraz zewnętrznych – czyli szans i zagrożeń. *SWOT* daje tym samym obraz stanu przedsiębiorstwa i umożliwia określenie strategii przyszłych działań. Należy pamiętać, iż analizę *SWOT* należy oprzeć na niepodważalnych faktach. Trzeba przeprowadzić

rzetelną ocenę wszystkich aspektów funkcjonowania przedsiębiorstwa, aby na tej podstawie móc wysnuć wartościowe wnioski.

Analiza wewnętrzna organizacji może dotyczyć jej zabezpieczeń sprzętowych, organizacji pracy, uprawnień dostępu do danych.

Procedura przeprowadzania analizy *SWOT* jest następująca:

1. Stworzenie zespołu
2. Określenie profilu przedsiębiorstwa
3. Diagnoza – polega na określeniu silnych i słabych stron organizacji
4. Stworzenie i weryfikacja listy
5. Prognoza – określa szanse i zagrożenia dla rozwoju organizacji
6. Stworzenie i weryfikacja listy
7. Skonsultowanie list
8. Konsolidacja – opracowanie strategii działania na podstawie diagnozy i prognozy

Zalety analizy *SWOT* to:

- Krótki czas przygotowania
- Syntetyczna forma
- Wykorzystanie doświadczenia i wiedzy zespołu
- Ułatwienie wyboru strategii działania
- Określenie obszarów organizacji wymagających udoskonalenia

Ograniczeniami w zastosowaniu tej metody są:

- Pracochłonność przygotowania analizy
- Trudność w określeniu najważniejszych składników

Należy pamiętać, aby analizę *SWOT* wykonywać okresowo, np. raz do roku. Pozwoli to na prześledzenie, czy działania podjęte przez organizację były właściwe i w jakim stopniu wpłynęły na działalność przedsiębiorstwa.

Metoda delficka

Połączenie opinii zaproszonych ekspertów przy wyeliminowaniu niepożądanych efektów, które powstają, gdy eksperci pracują razem w grupie. Składa się z 3 kroków:

a) Doboru uczestników panelu zarówno z organizacji jak i spoza niej. Poszczególni eksperci nie mają ze sobą kontaktu i nie wiedzą nawet, kto uczestniczy.
b) Prośba skierowana do każdego z uczestników o sporządzenie anonimowej predykcji dotyczącej danego zagadnienia
c) Przekazanie każdemu z uczestników opracowania powstałego na podstawie ich wcześniejszych odpowiedzi i prośba o nową predykcję uwzględniającą wyniki pochodzące z opracowania.

Słabe strony: bardzo ogólna – powinna być stosowana, gdy nieosiągalne są informacje niezbędne do wykorzystania technik ilościowych lub, gdy nie ma żadnego doświadczenia w projektach tego typu. Możliwość nadmiernego zaufania umiejętnościom poszczególnych osób oceniających ryzyko projektu, brak odpowiedniego wyczucia problemu przez te osoby, silne oddziaływanie na jakość formułowanych odpowiedzi takich czynników jak motywacja poszczególnych osób, czas, jakim dysponują, powiązania z innymi ekspertami mogące wpłynąć na weryfikację własnych poglądów.

Metoda nominalnego procesu grupowego

Metoda w odróżnieniu od metody delfickiej dopuszcza kontakt ekspertów i ich bezpośrednią komunikację. Obejmuje 3 kroki:

a) Zgromadzenie ekspertów i prośba o generowanie odpowiedzi w formie pisemnej
b) Sporządzenie listy wszystkich uzyskanych odpowiedzi a następnie przeprowadzenie przez ekspertów dyskusji nad każdą z odpowiedzi.
c) Nadanie przez poszczególnych uczestników panelu rangi każdej z odpowiedzi następnie sporządzenie za pomocą metod matematycznych ich rankingu.

Słabe strony: możliwość nadmiernego zaufania umiejętnościom poszczególnych osób oceniających ryzyko projektu, brak odpowiedniego wyczucia problemu przez te osoby, silne oddziaływanie na jakość formułowanych odpowiedzi takich czynników jak motywacja poszczególnych osób, czas jakim dysponują, powiązania z innymi ekspertami mogące wpłynąć na weryfikację własnych poglądów.

Burza mózgów

Sprzyja kreatywności, praca grupowa ludzi zróżnicowanych zawodowo. Zalety: możliwość oceny projektu przez ludzi o różnym doświadczeniu, więc szeroka perspektywa. Wady: możliwość wygenerowania zbyt wielu źródeł ryzyka.

Jest stosowania w celu określenia możliwych rozwiązań problemów oraz potencjalnych sposobów doskonalenia działań.

Burza mózgów służy głównie stworzeniu i zebraniu w dość krótkim czasie dużej liczby pomysłów, które mogą pomóc przy rozwiązaniu problemu. Rozwiązania powstają na skutek wszystkich skojarzeń (także takich, które mogą wydawać się niezwiązane ze sprawą) dotyczących badanego tematu. Narzędzie to wykorzystuje twórcze myślenie zespołu do kreowania pomysłów służących rozwiązaniu problemu.

Każda zgłoszona propozycja na ogół motywuje wszystkich uczestników burzy mózgów do dalszej pracy nad tworzeniem nowych pomysłów.

Procedura przeprowadzenia burzy mózgów jest następująca:

1. Wyznaczenie prowadzącego spotkanie
2. Określenie celu sesji burzy mózgów
3. Każdy członek zespołu po kolei wypowiada swoją myśl
4. O ile to możliwe przyjęcie zasady, że każdy członek zespołu rozwija pomysły wcześniej zgłoszone
5. Przestrzeganie zasady o nie dyskutowaniu i nie komentowaniu na tym etapie żadnych zgłoszonych pomysłów
6. Zapisywanie pomysłów miejscu widzianym przez wszystkich członków zespołu
7. Burzę mózgów kontynuuje się aż do momentu wyczerpania pomysłów
8. Dokonanie przeglądu wszystkich zgłoszonych pomysłów

Zaletami tej metody są pobudzenie kreatywności i działania zespołowego pracowników, stworzenie wielu możliwości rozwiązań oraz podejście do problemu z wielu stron.

Istotnymi ograniczeniami w stosowaniu burzy mózgów mogą być trudności w zachęceniu członków zespołu do udziału w burzy mózgów i do kreatywnego myślenia.

Metoda synektyczna (Gordona)

Sprzyja kreatywności, coraz rzadziej stosowana. Opiera się na grupowej dyskusji, członkowie są starannie dobrani, tak żeby mogli rozwiązywać problemy dotyczące całej organizacji. Obejmuje 2 etapy:

a) Uczynienie rzeczy obcych znanymi poprzez ich zdefiniowanie, analizę oraz ponowne sformułowanie – wymaga dobrego zrozumienia problemu
b) Rzeczy znane czyni się obcymi – zniekształca się, odwraca i przestawia problem – sprawia to, że na problem należy spojrzeć z nieznanej perspektywy.

Zalety: możliwość oceny projektu przez ludzi o różnym doświadczeniu, więc szeroka perspektywa. Wady: możliwość wygenerowania zbyt wielu źródeł ryzyka.

Debata publiczna

W sytuacji bardzo dużych projektów (elektrownia atomowa). Debata publiczna jest prowadzona z udziałem 3 stron – tej za, przeciw oraz neutralnego mediatora. Bardzo duża liczba argumentów, które mogą się pojawić w takiej debacie może przypominać burzę mózgów.

Plany alternatywne/analiza scenariuszy

Wielowarstwowe spojrzenie w przyszłość, wizja ewolucji. Może stanowić nie tylko narzędzie do wczesnego wykrywania potencjalnych źródeł zagrożeń, jak również może służyć wskazaniu sposobu reagowania na poszczególne rodzaje ryzyka.

Lepsza od analizy wrażliwości, ponieważ oprócz wrażliwości NPV uwzględnia również prawdopodobny zakres wartości zmiennych. Wadą jest fakt, że tworzy się tylko kilka możliwych scenariuszy.

Kolejne czynności:

- Rozpoznanie zmiennych zależnych
- Identyfikacja zmiennych
- Określenie stanu wejściowego systemu i jego otoczenia
- Wykrycie tendencji rozwojowych
- Sporządzenie prescenariuszy
- Projekcja przyszłych decyzji systemu
- Identyfikacja czynników zagrażających
- Konstrukcja scenariusza

Analiza pełnego rysunku *(rich picture analysis)*

Charakterystycznym podejściem w metodach holistycznych jest tzw. „*miękka*" analiza systemowa. Uwzględnia ona nie tylko namacalne „*twarde*" informacje dotyczące analizowanego projektu (fakty, liczby) ale również tak zwaną „*miękką złożoność*" (*soft complexity*). Polega to na tym, że z każdym projektem związani są w danym czasie określeni ludzie, którzy mają własne odczucia, podejście do projektu, sposób postrzegania go. To może spowodować konflikty

Analiza pełnego rysunku polega na sporządzeniu rysunku prezentującego w sposób holistyczny sytuację projektu przez jego analityków: struktura projektu (elementy, powiązania, procesy) oraz elementy miękkie.

Rysunek powinien umożliwiać identyfikację obszarów konfliktowych, będących potencjalnym źródłem ryzyka.

Mapa systemu

Diagram z wyszczególnionymi elementami systemu oraz jego środowisko widziane przez analityków. Pomocna w określaniu zasięgu projektu – wskazuje na uczestników, źródła pochodzenia dóbr, obszar, gdzie mogą się pojawiać zagrożenia.

Diagram oddziaływań

Inną nazwą tego narzędzia jest diagram relacji. Diagram relacji został zaprojektowany dla ukazania logicznych powiązań i zależności zespołu czynników wpływających na analizowane zagadnienie. Pozwala na znalezienie logicznych powiązań i zależności między czynnikami, które określone mogą być we wcześniej opracowanym diagramie pokrewieństwa. Celem stosowania diagramu zależności jest daleko idące uporządkowanie informacji. Z diagramu relacji korzysta się, gdy:

- Występują trudności związane z określeniem współzależności skutku i przyczyny w analizowanym obszarze,
- Wskazane wcześniej zależności pomiędzy czynnikami są bez zastanowienia odrzucane,
- Występują symptomy pojawienia się podobnych problemów w przyszłości,
- Istnieje wymóg, co do poddania analizie danego procesu.

Procedura postępowania przy tworzeniu diagramu zależności jest następująca:

1. Zdefiniować problem w zrozumiały sposób
2. Zapisać jak największą liczbę czynników związanych z rozpatrywanym problemem
3. Połączyć liniami powiązane ze sobą czynniki
4. Określić kierunek linii strzałkami
5. Przeanalizować przebieg strzałek związanych z każdym czynnikiem
6. Znaleźć główne przyczyny występowania problemu poprzez porównanie liczby linii podporządkowanych danej kategorii czynnika lub przyczyny

Analiza diagramu polega na prześledzeniu kierunku strzałek, oznaczających zależności między poszczególnymi czynnikami. Do dalszej analizy należy wybrać ten czynnik, w którym skoncentrowana jest największa liczba strzałek.

Przy tworzeniu diagramu zależności należy przestrzegać tych samych zasad, co w przypadku diagramu pokrewieństwa. Ważne jest również, by etap łączenia poszczególnych czynników strzałkami poprzedzony został dyskusją na temat ich powiązań, oraz by ustalić właściwą kolejność czynników.

Służy zbadaniu oddziaływań pomiędzy komponentami projektu, pomiędzy całym systemem projektu a otoczeniem. Powinien zawierać różne rodzaje oddziaływań (finansowe, prawne, geologiczne...). Dla pełnej wyrazistości należy konsekwentnie stosować różne symbole graficzne. Diagram oddziaływań może sugerować zjawiska takie jak:

a) Istnienie zjawisk nie połączonych z innymi
b) Ujawnianie oddziaływań obejmujących kilka zjawisk

Techniki sieciowe

Najbardziej znaną techniką sieciową jest *Sieć Petriego*. Polega ona na stworzeniu modelu obrazującego kolejne czynności. Schemat w kształcie sieci może zawierać różne informacje jak na przykład czas, zasoby finansowe, ludzkie...

Pomocne w rozwiązywaniu problemów zarządzania procesami inwestycyjnymi, badawczymi, produkcyjnymi. Wykorzystywane przede wszystkim w planowaniu, ale również w procesie kwantyfikacji ryzyka (w szczególności w badaniu ryzyka przekroczenia czasu i kosztów projektu)

Field sales assessment

Metoda polega na poproszeniu grupy sprzedawców o określenie jak będzie wyglądała sprzedaż konkretnych produktów w przyszłości. Następnie po zebraniu danych badacze mają się zastanowić jak zmodyfikować produkty, które charakteryzują się nadmiernym optymizmem lub też pesymizmem sprzedawców. Po drobnej modyfikacji metodę można stosować do określenia możliwych zagrożeń związanych z konkretnymi zasobami

Subiektywne określanie prawdopodobieństwa

Metoda polega na przydzielanie wartości prawdopodobieństwa, że coś się wydarzy na podstawie wiedzy badacza (na przykład projekt ma 75% szans na powodzenie). W przypadku, gdy istnieje kilka różnych wartości są one uśredniane.

Diagram drzewa

W *normie ISO 9004-4* występuje pod nazwą "*wykres drzewa*" jako narzędzie dla danych nieliczbowych. Inne nazwy to diagram systematyki i drzewo decyzyjne. To narzędzie ma zastosowanie do ukazywania związków pomiędzy danym zagadnieniem a jego elementami składowymi. Czynniki mogą zostać przedstawione w formie drzewa w celu pokazania logiki i kolejności powiązań jako ciąg zdarzeń i prawdopodobieństw ich wystąpienia. Diagram drzewa jest graficzną prezentacją następujących po sobie czynności, których wykonanie prowadzi do określonego celu.

Diagram drzewa wykorzystywany jest najczęściej wtedy, gdy:

- Zagadnienie wymaga przełożenia na czynności operacyjne,
- Konieczne jest określenie działań, które wymagają kontroli,

- Trzeba zidentyfikować czynniki najistotniejsze dla podjęcia decyzji,
- Określony skutek wymaga znalezienia wszystkich możliwych przyczyn,
- Konieczna jest koordynacja działań,
- Istotnie jest zachowanie kierunku wykonywanych zadań dla osiągnięcia przyjętych celów.

Procedura tworzenia drzewa decyzyjnego jest następująca:

- Jasno określić zagadnienie, które będzie badane
- Określić za pomocą burzy mózgów główne kategorie zagadnienia
- Stworzyć wykres poprzez umieszczenie rozpatrywanego zagadnienia w ramkach po lewej stronie, natomiast odgałęzienia z prawej strony, jedno pod drugim
- Dla każdej głównej kategorii znaleźć i umieścić z prawej strony elementy składowe i elementy podrzędne
- Przejrzeć wykres w celu zapewnienia, że nie ma żadnych luk ani w kolejności postępowania, ani w logice

Rozwiązywanie określonego problemu należy rozpocząć od najbardziej szczegółowych czynników.

Diagram jest narzędziem, które ze względu na czytelność zawartych informacji może w dużym stopniu pomóc przy podjęciu decyzji.

Wykres Ishikawy (*technika rybiego szkieletu*)

W normie *ISO 9004-4* to narzędzie nazwano wykresem przyczynowo-skutkowym. Inne popularne nazwy to "*wykres Ishikawy*" oraz "technika rybiego szkieletu". Jest stosowany do analizy przedsiębiorstwa, przedstawiania związków przyczynowo-skutkowych (między poszczególnymi czynnikami a wywołanym przez nie efektem) oraz do ułatwienia rozwiązywania problemów organizacji. Jest narzędziem, które pozwala systemowo identyfikować i grupować czynniki wpływające na badane zjawisko. Czynniki, które należy rozpatrzyć przy tworzeniu diagramu można zgrupować w "*6M*", czyli:

- *Man* - człowiek
- *Machine* - maszyna
- *Method* - metoda
- *Material* - materiał
- *Management* - kierowanie
- *Measurment* - pomiary

Obszar analizy można powiększyć również o takie czynniki jak: otoczenie, środowisko, systemy danych i informacji.

Procedura postępowania przy budowie diagramu przyczynowo - skutkowego jest następująca:

1. Ustalić skutek w sposób jasny i logiczny
2. Określić główne kategorie możliwych przyczyn

Trzeba wybrać te czynniki, które prawdopodobnie wywierają największy wpływ na skutek. To, czy tak jest naprawdę, okaże się podczas kolejnych etapów badania.

3. Zacząć budować wykres

Należy określić skutek w ramce z prawej strony i umieszczając główne kategorie jako "*dopływy*" do osi, która zmierza do ramki "*rynek*"

4. Budować wykres

Należy przemyśleć i zapisać przyczyny występujące na wszystkich kolejnych poziomach (aż do przyczyn elementarnych). Może się także okazać, że istnieją kolejne, nie zidentyfikowane wcześniej czynniki, których nie można podłączyć do żadnej z kategorii. Należy wówczas zostawić je na najwyższym poziomie. Na tym etapie warto jest wykorzystać inne techniki (wspomagające), np. burzę mózgów.

5. Wybrać i zidentyfikować główne przyczyn

Należy wybrać 3-5 przyczyn należących do najwyższego poziomu, które mają największy wpływ na skutek oraz wymagają dalszych działań.

Szczególnymi charakterystykami diagramu przyczynowo – skutkowego są:

- Całościowe ujęcie badanego zagadnienia
- Czytelne i przejrzyste dokonywanie zapisów
- Łatwość analizy wyników
- Prosta budowa

Przy budowie diagramu należy pamiętać, że zbyt duża liczba uwzględnionych kategorii może spowodować nieczytelność informacji. Powyższy diagram zastosowano w ***Rozdziale 2.4.4*** rozprawy.

Analiza Pareto-Lorenza

W *normie ISO 9004-4* narzędzie to nosi nazwę *wykres Pareto.* Stosuje się tę metodę do przedstawienia według ważności udziału każdego składnika w całkowitym skutku oraz do uszeregowania sposobów doskonalenia. V. Pareto na podstawie obserwacji dotyczących dochodu społeczeństwa wysnuł tezę, że *80 %*

wszystkich zdarzeń jest powodowanych przez zaledwie 20 % przyczyn (oczywiście należy przyjąć pewną tolerancję dla tych wartości).

Technika ta służy do uszeregowania poszczególnych czynników od najczęstszych do najrzadszych, lub – z drugiej strony – wywołujących od największych do najmniejszych skutków. Analiza pokazuje udział każdego składnika w końcowym efekcie.

Procedura tworzenia *analizy Pareto-Lorenza* jest następująca:

- Wybrać czynniki, które będą poddane analizie.
- Wybrać jednostkę miary używaną podczas analizy.
- Określić przedział czasu, w którym dane będą analizowane.
- Wypisać składniki od strony lewej do prawej w porządku malejącej wartości miary.
- Narysować dwie pionowe osie, po jednej na każdym końcu osi poziomej.

Lewa oś powinna być wyskalowana w jednostce miary. Jej wysokość musi być równa sumie wartości wszystkich składników. Prawa oś musi mieć taką samą wysokość i być identycznie wyskalowana.

- Nad każdym składnikiem narysować prostokąt, którego wysokość oznacza wartość jego jednostki miary.
- Narysować linię sumarycznej częstotliwości poprzez zsumowanie wartości każdego składnika od lewej do prawej.
- Wykorzystać wykres Pareto w celu zidentyfikowania najważniejszych składników prowadzących do doskonalenia jakości.

Do wykorzystania tego narzędzia konieczne jest posiadanie rzetelnych danych liczbowych. *Diagram Pareto-Lorenza* umożliwia zidentyfikowanie najważniejszych czynników, którymi trzeba się zająć. Mogą to być takie składniki jak rodzaj usterek czy struktura kosztów. Przedstawienie wyników analizy umożliwia ustalenie priorytetów i koncentrację wysiłków na rozwiązywaniu tych przyczyn, które powodują większość problemów.

QFD (*Quality Function Deployment*)

Inne nazwy tego narzędzia to "*dom jakości*", „*diagram tablicowy*". Jest to odmiana diagramu matrycowego, który przedstawia połączenia i zależności pomiędzy zmiennymi. Według *American Supplier Institute QFD* jest to system dla przełożenia wymagań klienta na odpowiednie wymagania przedsiębiorstwa na każdym etapie,

począwszy od badań i rozwoju poprzez projektowanie i produkcję aż po marketing, sprzedaż i dystrybucję.

Natomiast *Danish Technological Institute* określa QFD jako narzędzie – system, który angażuje wszystkie funkcje przedsiębiorstwa, stosowany w celu zapewnienia – przez wszystkie fazy rozwoju wyrobu od idei po dostawy – iż potrzeby klienta zostaną zaspokojone.

Procedura tworzenia domu jakości jest następująca:

- zidentyfikować wszystkie wymagania klienta;
- dokonać analizy konkurencji z punktu widzenia klienta;
- ustalić wszystkie cechy wyrobu;
- wykazać związki pomiędzy życzeniami klienta a cechami wyrobu;
- dokonać analizy konkurencji z punktu widzenia producenta;
- ustalenie wartości najważniejszych z punktu widzenia klienta cech;
- ustalenie związków między parametrami;
- ustalenie sparametryzowanych celów.

Najczęściej diagram tablicowy opracowuje wyznaczony i wspierany przez kierownictwo zespół, którego zadaniem jest określenie specyfiki i potrzeb rynku. W skład zespołu powinni wchodzić fachowi, doświadczeni pracownicy (także produkcyjni).

W tworzeniu diagramu tablicowego należy udzielić odpowiedzi na pytania zgodne z zasadą "*5W+H*" oznaczającą:

- *Who* - kto jest klientem?
- *What* - co jest wymaganiem klienta?
- *When* - kiedy badać i zaspokajać potrzeby odbiorcy?
- *Where* - gdzie występują najważniejsze etapy realizacji wymagań klienta?
- *Why* - dlaczego należy identyfikować i spełniać potrzeby klienta?
- *How* - jak zaspokoić potrzeby odbiorcy?

Zastosowanie tej zasady w praktyce ułatwia określenie klienta i lepsze zidentyfikowanie jego wymagań, co zaowocuje wzrostem konkurencyjności.

Podstawowe korzyści z zastosowania diagramu tablicowego to:

- wzrost zadowolenia klienta;
- krótszy czas projektowania wyrobu;
- niższe koszty;
- mniejsze straty;
- mniejsza liczba zmian konstrukcyjnych;
- lepsza komunikacja międzywydziałowa;
- większa konkurencyjność produktu.

Niemniej jednak do zasadniczych ograniczeń zastosowania tej metody należy zaliczyć wysoki koszt opracowania "*domu jakości*" a także mały stopień uwzględnienia wpływu środowiska zewnętrznego na przedsiębiorstwo.

Tablicowa analiza danych

Ta metoda zwana jest też "*matrycową analizą danych*". To narzędzie służy do graficznego przedstawienia relacji między dwoma parametrami o charakterze jakościowym. Jej celem jest ustalenie związku między wybranymi cechami produktu. Dane do tworzenia tablicowej analizy danych pochodzą przede wszystkim z badań marketingowych, których przeprowadzenie może dodatkowo doprowadzić do znalezienia niszy rynkowej.

Procedura tworzenia tablicowej analizy danych jest następująca:

- zebrać dane;
- stworzyć oś współrzędnych dla określonych parametrów;
- narysować oś;
- nanieść wartości parametrów;
- przeanalizować rozmieszczenie otrzymanych wartości.

Do zalet tej metody można zaliczyć wykazanie relacji pomiędzy poszczególnymi cechami produktu, możliwość zastosowania przy określaniu strategii przedsiębiorstwa, a także czytelną formę.

Metoda ta ma również wady, takie jak długi proces opracowania danych oraz możliwość ustalenia na jednym wykresie relacji tylko pomiędzy dwoma parametrami

Sieć PERT

Sieć PERT stosuje się zazwyczaj dla procesów niepowtarzalnych, w których okres realizacji i czas zakończenia przedsięwzięcia są oszacowane jedynie w przybliżeniu. Zawiera wyłącznie przyjęte z pewną tolerancją czasy trwania poszczególnych etapów.

Procedura tworzenia diagramu sieciowego jest następująca:

- sporządzenie graficznego obrazu procesu, łącznie z parametrami, które będą wywierały ważny wpływ na analizę czynności;
- obliczenie terminów rozpoczęcia, zakończenia oraz nakładów potrzebnych do realizacji wszystkich etapów;
- analiza modelu pod kątem ograniczenia wykorzystania zasobów;
- kontrola i śledzenie wykonywania przedsięwzięcia.

Zalety diagramów sieciowych to:

- możliwość pokazania zależności między czynnościami;
- pozwalają na poprawę procesu planowania wykonywania zadań;
- identyfikują "kamienie milowe" – punkty krytyczne w procesie realizacji przedsięwzięcia;
- umożliwiają tworzenie i wybór wariantu wykonywania zadań dla osiągnięcia zaplanowanego celu;
- ułatwiają tworzenie harmonogramu przedsięwzięcia.

Do wad tej metody zaliczyć można pracochłonność tworzenia diagramu i jedynie przybliżone oszacowanie czasu poszczególnych etapów.

PDPC

PDPC jest bardzo pomocnym narzędziem w doborze najbardziej optymalnej drogi osiągnięcia zamierzonego celu. Dokonuje się tego poprzez symulację możliwego rozwoju zdarzeń. *Diagram PDPC* oprócz chronologicznego porządku postępowania ukazuje także alternatywne rozwiązania, które mogą być zastosowane w przypadku wystąpienia hipotetycznych problemów w przedsiębiorstwie. Ułatwia określenie aspektów, które wcześniej nie były brane pod uwagę w analizie funkcjonalnej.

Procedura tworzenia *diagramu PDPC* jest następująca:

- Zbudować drzewo decyzyjne dla danego zagadnienia
- Wybrać jedną gałąź drzewa
- Ustalić, jakie nieprzewidziane dotychczas wydarzenia mogą wystąpić
- Zaznaczyć na wykresie przewidywane zdarzenia
- Dla każdego wydarzenia wyznaczyć metody zapobiegawcze
- Powyższe czynności należy powtórzyć dla każdej z gałęzi drzewa decyzyjnego

Zaletami tej metody są:

- Zgromadzenie wszystkich możliwych problemów przedsiębiorstwa,
- Możliwość zaplanowania działań zapobiegawczych przed tymi problemami.

Wśród wad *diagramu PDPC* wymienić należy:

- Teoretyczne podejście do badanej kwestii,
- Możliwość wystąpienia zupełnie nowych zdarzeń, na które organizacja nie będzie przygotowana.

Celem porównania jakości wybranych narzędzi analizy ryzyka – przeprowadza się, zgodnie z teorią analizy systemowej – *analizę porównawczą*.

4.3.3. Stan zaawansowania i rozwoju systemów zarządzania ryzykiem w wybranych państwach NATO i Unii Europejskiej – ANALIZA PORÓWNAWCZA

Specyficzne, wykorzystywane w państwach NATO i Unii Europejskiej, metody analizy ryzyka stanowią połączenie ogólnych metod. Poprzez umiejętne dobranie *kwalitatywnych* i *kwantytatywnych* matryc można przeprowadzić bardziej szczegółowe analizy ryzyka.

ANALIZA PORÓWNAWCZA

Metod analizy zagrożeń i zarządzania ryzykiem jest dużo. Większość z dużych firm, które zajmują się konsultingiem cały czas pracuje nad kolejnymi narzędziami. Pewnym wyznacznikiem skuteczności metod jest pozytywna ocena *NISC/NCSC Risk Management Laboratory*. Poniżej porównane metody w większości mają taką ocenę.

ALGORITHMISC

Algorithmisc jest pakietem do analizy ryzyka stworzonym przez bazującą na własnych sprawdzonych komponentach. Pakiet składa się z następujących elementów69:

- *Algo Market*
- *Algo Reporting database*
- *RiskWatch*
- *HistoRisk*
- *Algo RiskEngine*
- *Algo Portfolio Credit RiskEngine*

Pakiet daje dostęp do tworzenia scenariuszy dla oceny ryzyka wielu rynków używając do tego kombinacji statystycznych narzędzi do mierzenia ryzyka oraz podejść testujących wrażliwość zasobów. Spełnia standardy kwantytatywne opracowane przez BIS.

Jego moduł *Risk Watch* jest narzędziem, które przy pomocy teoretycznych modeli jest w stanie obliczyć przyszłe wartości scenariuszy. *Algorithmisc* używa szerokiej gamy metodologii jak parametryczny lub bazowany na scenariuszach *VaR (Value-at-Risk), EaR (earnings-at-risk), stress testing, analiza wrażliwości oraz analizę porównawczą.*

[69] Dane z witryny internetowej www.algorithmisc.com

Wyniki analiz potrafi porównać obecne dane do danych otrzymanych na podstawie analizy scenariuszy przy pomocy techniki Benchmarkingu.

Program oferuje pełny zestaw instrumentów finansowych zawierający ponad 400 typów obligacji, papierów dłużnych, walut obcych i szeroką gamę instrumentów pochodnych -ponad 20 różnych rynków a także możliwość dodawania własnych modeli przy pomocy *Application Programming Interface (API).*

Kolejnym modułem pakietu ***Algorithmisc jest Algo Reporting Database***. Jest to relacyjna baza danych przechowująca dane historyczne. Daje dostęp do wyświetlania danych na wiele różnych sposobów.

HistoRisk to serwer scenariuszy, który generuje scenariusze na podstawie danych statystycznych, historycznych a także przygotowuje analizy typu: „*Co się stanie jeżeli*". *HistoRisk* używa wielu technik generowania scenariuszy włączając w to techniki zawierająca *Monte-Carlo* oraz *quasi-Monte Carlo.*

Producenci oferują szeroką integrację z modelami dostarczanymi przez *FEA, APT, RiskCare, Intex oraz Andrew Davidson.*

Assessing a value for the frequency and the possible damage of risk70

Ta metoda kładzie nacisk na wpływ niechcianych zdarzeń i na określeniu, którym z systemów należy się pierwszeństwo, które są dla nas najważniejsze.

Robi się to poprzez połączenie każdego z zasobów z dwoma wartościami, które następnie określą wartość zasobu.

Gdy zsumuje się wszystkie wartości zasobów w systemie zostanie określona wartość ryzyka systemu IT.

Metoda postępowania jest następująca:

- Na początku każdemu z zasobów przyporządkowuje się wagę. Określa ona potencjalne zniszczenie, które może się pojawić w przypadku zagrożenia zasobu. Wartości należy przydzielić do wszystkich możliwych zagrożeń zasobów.
- Następnie przydziela się wartość określającą częstotliwość. Tę wartość ustala się na podstawie kombinacji prawdopodobieństwa wystąpienia i podatności na system.
- Następną czynnością jest ustalenie wartości zasobu/zagrożenia. Robi się to poprzez znalezienie liczby znajdującej się na przecięciu wartości zasobu oraz wartości częstotliwości. Wartości zasobu/zagrożenia, są sumowane by dać całkowitą wartość zasobu. Ten schemat może być używany do rozróżnienia zasobów będących częścią systemu IT.

[70] *ISO IEC TR 13335-3 / 1998 Annex E, Example 3*

Ostatnim krokiem jest zsumowanie wszystkich wartości zasobów/zagrożeń dla całego systemu. W ten sposób powstaje suma całego systemu, które może być następnie użyta do rozróżnienia pomiędzy systemami oraz do określenia, któremu z systemów należy się priorytet zabezpieczeń.

BUDDY SYSTEM

Buddy System używa w pełni automatycznego podejścia do zbierania informacji na temat stacji roboczych, serwerów, aplikacji, wolno stojących komputerów, dla których należy przeprowadzić analizę ryzyka[71].

Centralnie zlokalizowany moduł służący do analizy przeprowadza analizę podatności, pomiary zażaleń, scenariusze „*Co się stanie, jeżeli*", analizę ryzyka oraz zarządza ryzykiem. Moduł generuje raporty – zawiera przygotowane ponad 50 własnych wzorów zawierających informacje, które można zastosować w wielu różnych sytuacjach, jak również pozwala tworzyć własne raporty dostosowane do konkretnych potrzeb przedsiębiorstw.

System zawiera analizę kosztów, spodziewanych strat używając przede wszystkim metodę *ROI (Return on Investments*).

Od 1987 roku jest stosowany do oceny ryzyka w sieciach komputerowych, systemach oraz projektach najrozmaitszej skali złożoności.

Użytkownicy są w stanie zidentyfikować trudności, zagrożenia, zasoby i ich podatności a następnie zanalizować i skwantyfikować ryzyko. Zakończone pomiary są wprowadzane do systemu, gdzie analityk najpierw przetwarza ich podatności w danym momencie (*as-is*), a następnie analityk może je dowolnie modelować przeprowadzając analizę „*co się stanie, jeżeli...*" dla stref o dużej podatności.

Buddy System charakteryzuje się umiejętnością mierzenia efektów kaskadowych pośród logicznie połączonych pomiarów. Analityk może szybko i łatwo połączyć kilka pomiarów przeprowadzając analizę wpływu, jaki ma jeden z elementów na inne. Wyniki są następnie pokazywane graficznie albo jako średnie, albo jako najgorszy z możliwych scenariuszy.

[71] Dane z witryny http://www.buddysystem.net/html/details.shtml

Efekt kaskadowy jest szczególnie przydatny szczególnie w takich sytuacjach, gdy któryś z zasobów jest postrzegany jako globalny. Wtedy wszystkie inne zasoby w mniejszym lub większym stopniu oddziałują na niego, a wskaźnik korelacji może być ustalony przez analityka.

CORA

Cora jest akronimem od *Cost-of-Risk-Analysis System*. Jest systemem opracowanym ponad 30 lat temu przez *International Security Technology Inc.*

Cora współpracuje ze stosowanymi w organizacjach systemami zarządzania ryzyka (*RIMS Risk Information Management System*) importując z nich informacje.

Fachowcy od ryzyka definiują i przechowują parametry ryzyka jako pliki z zasadami ryzyka (*risk rules*). Te zasady stanowią później podstawę pracy dla personelu operacyjnego (poziom ryzyka w środowisku, poziom aktywności). Sprawia to, że oszczędza się czas ekspertów oraz dodatkowo sprawia, że analiza jest przeprowadzana dokładnie według zasad ustalonych przez ekspertów. W praktyce wygląda to tak, że eksperci identyfikują zagrożenie (jak na przykład powódź) jako potencjalnie niebezpieczne dla jednego lub więcej oddziałów. Zbierają informacje historyczne na ten temat i starają się oszacować częstość wystąpienia tego zagrożenia w przyszłości. *Cora* dostarcza strukturę umożliwiającą przechowywanie tych informacji. Oddzielnie przygotowuje się oszacowania potencjalnej straty dla wszystkich elementów organizacji oraz używa się *Cora* do oszacowań. Eksperci używają *Cora* do wykrycia i przechowywania danych na temat podatności dla wszystkich zagrożeń.

Dzięki tym bazom danych nie trzeba na przykład osobno określać zagrożeń i podatności dla wielu oddziałów, lecz można podzielić wszystko na standardowe typy (na przykład hurtownie, biura regionalne, sklepy, centrale), eksperci przeanalizują ryzyko, a potem samemu będzie można określić ryzyko dla poszczególnych oddziałów jedynie zmieniając wartości parametrów.

Dla wszystkich oddziałów *Cora* osobno przeprowadza analizę rocznej spodziewanej straty (*ALE),* Straty wynikającej z pojedynczego wystąpienia zdarzenia (*SOL*) oraz stopę zwrotu (*ROI*) nakładów na zabezpieczenia, ubezpieczenia oraz plany awaryjne.

Osobny moduł *CORA Financial Simulator* służy do zbierania, analizy i przeprowadzania analiz spodziewanych strat, których udało się uniknąć oraz kosztów projektu a następnie umożliwia obliczenie ogólnego finansowego wpływu ryzyka dla każdej ze zdefiniowanych strategii bezpieczeństwa. Menedżer ryzyka jest w stanie skonstruować, nagrać oraz odtworzyć alternatywne ustawienia analizy

Cora definiuje organizacją jako grupę pojedynczych oddziałów oraz innych „*dyskretnych*" elementów traktując je jak obiekty niezależnie czy są do hurtownie, statki, czy też rury – wszystko jest dostosowane do indywidualnych potrzeb organizacji. Każdy z zasobów, wierzytelności czy funkcji przedsiębiorstwa ma określone własne prawdopodobieństwo straty (*loss potential*). Jest to definiowane jako najgorsze w skutkach wystąpienie najniebezpieczniejszego z zagrożeń.

Cora sporządza przejrzyste tabelkowe raporty, które można swobodnie eksportować do takich arkuszy kalkulacyjnych jak na przykład *Excel* w celu dodatkowego przetwarzania. Wszystkie dokumenty tworzone przy pomocy *Cora* mają standardowy nagłówek zawierający między innymi dane osoby wprowadzającej dane oraz dokładną datę

CRAMM

CRAMM, czyli *CCTA Risk Analysis & Management Metodology* to pakiet służący do analizy i zarządzania ryzykiem, którego podstawową metodą działania jest metoda kwalifikacyjna[72]. Pakiet składa się z 3 części, a dodatkowo jest wspierany dużą biblioteką ankiet, kwestionariuszy i zaleceń.

Część pierwsza polega na przeprowadzeniu:

- identyfikacji zasobów (aktywów) i zagrożeń;
- oceny podatności na poszczególne rodzaje zagrożeń.

Oceny prowadzi się według skali punktowej 1-10.

Część druga polega na oszacowaniu ryzyka powodowanego zagrożeniami.. Zasoby i zagrożenia, których wystąpienie mogłoby spowodować utratę ich wartości grupuje się stosując skalę punktową 1-5.

[72] B. Kusina - Bonair S.A. *Analiza ryzyka wstępem do projektowania bezpieczeństwa teleinformacyjnego firmy.* Konferencja *Enigma*, 13 maja 1999

Część trzecia zawiera zbiór rozwiązań mogących mieć zastosowanie w procesie zarządzania ryzykiem. Pakiet udostępnia dużą liczbę raportów, które mogą mieć zastosowanie przy implementacji systemów *ITSec.*

Pakiet powstał przy współpracy brytyjskich specjalistów rządowych i firmy *BIS Applied System Limited. J*est zabezpieczony przed nieuprawnionym dostępem oraz utratę poufności baz danych, które są tworzone w trakcie realizacji zadań.

FMEA

Analiza rodzajów i skutków potencjalnych uszkodzeń *FMEA* jest zazwyczaj stosowane do analizy uszkodzeń obiektów technicznych. Jednak można je równie dobrze zastosować przy analizie bezpieczeństwa systemów informatycznych.

Metoda składa się z prostego podejścia identyfikacji:

- sposobów powstawania usterek;
- tego, jakie skutki będą wynikiem uszkodzenia;
- działań wymaganych do zminimalizowania konsekwencji.

Metoda może być stosowana zarówno na etapie projektowania nowego systemu, jak i w trakcie jego eksploatacji. Polega na określeniu dla każdego, wcześniej sprecyzowanego lub zaobserwowanego błędu funkcjonowania lub uszkodzenia fizycznego elementu systemu, postaci uszkodzenia. Tak określona jest metodą jakościową. Jednak, gdy poszerzymy analizę o ilościową ocenę istotności postaci uszkodzenia, czyli o takie kryteria jak częstotliwość występowania, dotkliwość skutku i wykrywalność dostaniemy metodę ilościową. Formularz analizy *FMEA* oprócz zasadniczych dla metody informacji, powinien zawierać także nazwę zespołu i datę.

Procedura analizy powinna zawierać następujące elementy:

- Podział systemu na analizowane podsystemy. Zgromadzenie dokumentacji, wykresów, schematów funkcjonowania. Opracowanie wzajemnych zależności konstrukcyjnych, funkcyjnych, niezawodnościowych.
- Określenie dla podsystemów listy elementów o najniższym poziomie dekompozycji i przypisanie im ewentualnych wpływów środowiska mogących zwrotnie wpływać na system.
- Określenie dla każdego elementu i spełnianej przez niego funkcji, postaci awarii(uszkodzenia).
- Wyznaczenie dla każdej postaci uszkodzenia wskaźników częstotliwości, dotkliwości skutku i wykrywalności.
- Opisania działania mającego na celu usunięcie uszkodzenia i przywrócenie stanu zdolności do pracy.

Do określenia krytyczności poszczególnych uszkodzeń i ich kwantyfikacji używa się techniki *RPN (Risk Priority Number)*. Wskaźnik ten jest wyznaczany jako iloczyn liczb ze skali częstotliwości, uciążliwości skutku i wykrywalności. Trudno jest dokładnie określić skalę, ponieważ w literaturze przyjmuje ona bardzo różne wartości. Norma amerykańska *STD-169 w* metodzie *102* zalecają obliczenie wartości Cm (*Failure Mode Criticality Nember*) – odpowiednik RPN, dla każdej postaci uszkodzenia powodujące utratę funkcji, lub nie wykonanie zadania według wzoru:

$$C_m = b \times a \times l_p \times t$$

gdzie:
b – warunkowe prawdopodobieństwo utraty funkcji lub zadania
a – udział danej postaci uszkodzenia w zbiorze wszystkich uszkodzeń
l_p *– intensywność uszkodzeń dal obiektów naprawialnych*
t - czas pracy lub narażenia

Dla danego elementu liczba krytyczna C_r jest dumą wszystkich wartości C_m:

$$C_r = \Sigma C_{mi}$$

Niekiedy można spotkać uzupełnienie wartości wskaźnika *RPN* w zależności od analizowanego obiektu i celu analizy o czynnik wykrywalności lub prawdopodobieństwa wywołania uszkodzeń wtórnych.

$$RPN = P \times S \times D$$

gdzie:
P– liczba określająca prawdopodobieństwo zaistnienia zdarzenia (częstotliwość)
S – liczba określająca istotność skutku dla danej postaci uszkodzenia
D – liczba określająca możliwość wykrycia danej postaci uszkodzenia

Najczęściej stosowaną skalą jest skala 10 punktowa, przy czym rangi pogrupowane są w 5 przedziałach. Tabela zawiera propozycje kryteriów podziału czynnika z odpowiadającymi im rankingami i wartościami bezwzględnymi prawdopodobieństw dla pojawiania się postaci uszkodzenia i możliwościami ich detekcji.

Formularze

Metoda polega na porównywaniu metodą każdy z każdym wszystkich kryteriów. Jeżeli jedno z kryteriów jest ważniejsze od drugiego, to w tym miejscu wpisujemy 1, w przeciwnym wypadku 0. Następnym krokiem jest sumowanie wierszami liczby wag oraz dzielenie przez łączną sumę wszystkich wartości wierszy. Następnie wynik uśredniamy (na przykład po odrzuceniu skrajnych wartości).

Ocena ryzyka kwantyfikowalnego jest dwustronna:

1. Eksperci oceniają rzeczowe, terminowe i finansowe trudności oraz wypowiadają się na temat konieczności przeprowadzenia analizy ryzyka
2. W drugiej ankiecie zbiera się stanowiska dotyczące pakietów roboczych uznanych za szczególnie krytyczne, przy czym układ formularza dopasowuje się do aktualnego zaawansowania projektu

Pakiet roboczy		Możliwe trudności	Dodatkowe nakłady na pokonanie problemów w przypadku		
Nr	Opis		najkorzystniejszym	prawdopodobnym	najmniej korzystnym

Tabela 10: ***Formularz do ujęcia i kwantyfikacji ryzyka FTA***
Źródło: J. Syta. *Metodyki*... [200]

Analiza bezpieczeństwa metodą drzewa błędów *FTA* jest również nazywana drzewem uszkodzeń lub drzewem porażeń. Metodę stosuje się przede wszystkim w analizie ryzyka i niezawodności złożonych systemów. Obejmuje ona związki pomiędzy zdarzeniami szczytowymi, od których rozpoczyna się analizę, a zdarzeniami bazowymi uważanymi za pierwotne przyczyny uszkodzeń systemów. Metoda pozwala na szeroką analizę obejmującą środowisko, zdarzenia naturalne, błędy człowieka...

Idea budowy drzewa błędów polega na wykorzystaniu bramek łączących zdarzenia relacjami logicznymi. Wymaga to jednak doskonałej znajomości następstw zdarzeń, ich interakcji i związków przyczynowo-skutkowych. Dla złożonych struktur wymagane jest stosowanie skomplikowanych bramek logicznych, co może powodować znaczne trudności w analizie całego drzewa.

Budowa drzewa rozpoczyna się od precyzyjnego określenia wydarzenia szczytowego i analizie przyczynowej warunków wystąpienia zdarzenia. Postawienie pytań: *co?, gdzie?,* kiedy znacznie ułatwia procedurę. W trakcie pracy należy

przestrzegać złożonego obszaru analizy zarówno w odniesieniu do procesu i czynników wymuszających, jak i fizycznych granic systemu. Najniższy poziom analizy dotyczy zdarzeń podstawowych uznawanych w danym schemacie za zdarzenia pierwotne, dla których nie ma już potrzeby wyznaczania przyczyn ich powstania.

HAZOP

Analiza zagrożeń i funkcjonowania – *HAZOP* może być używana do identyfikacji zagrożeń w fazie prowadzenia procesu. Jest to metoda zespołowa, w której 4-6 osobowy zespół generuje potencjalne zagrożenia wynikające z nieprawidłowego przebiegu procesu. Metoda opiera się na drobiazgowej analizie wcześniej zidentyfikowanych procesów. Źródłem wiedzy jest wspólna dyskusja sterowana przez prowadzącego. Wyczerpywanie możliwości w dyskusji zapewnia stosowanie zastawu słów wiodących dal poszczególnych elementów procesu. Na powodzenie analizy wpływa także jakość zgromadzonej dokumentacji, skład zespołu i jego zdolności intelektualne oraz umiejętność kreowania nowych scenariuszy wydarzeń. W formularzu analitycznym powinno się pojawić pięć punktów:

- *Zamierzenia* – cele funkcjonowania systemu określone w dokumentacji techniczno-ruchowej, opisane w procedurach, na schematach i wykresach
- *Odchylenia* – błędy w działaniu systemu w odniesieniu do elementarnych składników procesu opisanych wyżej wymienionymi parametrami
- *Przyczyny* – realne przyczyny odchyleń w procesie ustalone w toku dyskusji specjalistów
- *Skutki* – konsekwencje błędnego funkcjonowania procesu
- *Słowa wiodące* – słowne określenia potencjalnych odchyleń wartości parametrów od założeń projektowych

Parametrami mogą być na przykład czas, informacji, koszt...
Złożenie słowa kluczowego z parametrem pozwala na tworzenie odchyleń np.:
Brak + informacja = zła informacja
Więcej + koszt = większe koszty

Wydajność analizy *HAZOP* jest uzależniona od kilku czynników organizacyjnych i proceduralnych. Nie należy uważać *HAZOP* za narzędzie weryfikacji projektu i forum dyskusyjne pomiędzy projektantem a użytkownikiem. Koncepcje zmiany projektu, należy opracować po analizie, jako wynik przeprowadzonych prac. Końcową czynnością po zakończeniu sesji zespołowych powinno być opracowanie i wydanie raportu dokumentującego przebieg prac i sposoby realizacji zaleceń.

IST/RAMP

IST/RAMP jest skrótem od *International Security Technology/Risk Analysis Management Program.*

Pakiet wykorzystuje *metodę kwantytatywną*. W trakcie działania program generuje zestawy potrzebnych ankiet i kwestionariuszy. Po ich uzyskaniu grupowane są w pięciu kategoriach aktywów i zagrożeń[73].

Pakiet dysponuje bardzo dużą biblioteką incydentów i ma możliwość prowadzenia analizy porównawczej. Wymaga sprzętu *mainframe*, komputery klasy PC wykorzystuje do zobrazowania wyników.

Matrix of Predefined Values[74]

W tej metodzie aktualne lub proponowane wartości fizyczne są wartościowane według kosztów wymiany lub rekonstrukcji (*pomiary kwantytatywne*). Koszty te przekształca się w tej samej skali, którą później będziemy używać dla wartościowania zasobów danych. Aktualne lub proponowane oprogramowanie są wartościowane tak samo, jak zasoby fizyczne ze zidentyfikowanymi kosztami zakupu lub unowocześnienia na tę samą *skalę kwalitatywną*, którą używamy dla zasobów danych. Dodatkowo, jeżeli się okaże, że jakakolwiek aplikacja ma własne wymagania ze względu na poufność lub integralność, to jest wartościowane w taki sam sposób jak zasoby danych.

Wartości dla zasobów danych są określane poprzez przeprowadzanie wywiadów z różnymi członkami personelu (*data owners*), którzy są w stanie wyrażać się autorytatywnie w celu określenia wartości i wrażliwości danych będących aktualnie w użyciu, przechowywanych, przetwarzanych lub otrzymywanych.

Wywiady określają przybliżone wartości i wrażliwości danych z punktu widzenia najgorszych możliwych scenariuszy zaistniałych ze względu na nieautoryzowany dostęp, modyfikacje, brak dostępu przez niemożliwy do określenia okres czasu lub zniszczenia.

Oszacowanie jest realizowane przy pomocy ramowych oszacowań zasobów danych zawierających takie tematy jak:

---

[73] R. Jacobson. *IST/RAMP and CRITI-CALC: Risk Management Tools, Proceedings, Computer Security Risk Management Model Builder's Workshop*, Denver, CO., May 1988.
[74] *ISO IEC TR 13335-3 / 1998 Annex E, Example 1*

- Bezpieczeństwo osobiste
- Informacje osobiste
- Przepisy prawne, normy
- Udziały ekonomiczne i komercjalne
- Straty finansowe, przerwanie pracy
- Porządek publiczny
- Polityka biznesowa i operacyjna
- Straty dobrej woli

Oszacowania wykonuje się na skali numerycznej jak na przykład 1-4 pokazanej w tabeli 1. Należy ją stosować tam, gdzie tylko jest to możliwe i logiczne (na przykład w sytuacji, gdy rozpatrujemy zagrożenia ludzkiego życia należy stosować *skalę kwalitatywną).*

Kolejną czynnością jest połączenia par wszystkich zasobów, których dotyczy zagrożenie, dla wszystkich zagrożeń z odpowiednim poziomem zagrożenia (prawdopodobieństwem wystąpienia) i poziomem podatności. Każda odpowiedź na pytania ma swoją wartość, która to jest określana na podstawie bazy wiedzy. Dzięki temu możemy zidentyfikować zagrożenia na skali niskie-wysokie zagrożenia, a podatności określamy podobnie do przykładowej matrycy. Informacje potrzebne do wypełnienia tabeli powinny być zebrane na podstawie rozmów z odpowiednim personelem. Typy zagrożeń mogą być rozpatrywane jako odpowiednio określone grupy na podstawie przyczyn powstania (ludzie, siły natury, ludzkie pomyłki, błędy oprogramowania lub wyposażenia).

Wartości zasobów oraz poziomy zagrożeń i podatności odpowiednie to każdego typu wpływu są łączone w tabeli tak, jak pokazane poniżej. By zidentyfikować każdą kombinację wprowadza się dodatkową skalę ryzyka 1-8

Dla każdego zasobu bierze się pod uwagę odpowiednie podatności oraz odpowiadające im zagrożenia. Jeżeli okaże się, że istnieje podatność bez przypisanego zagrożenia lub zagrożenia bez podatności, oznacza to, że w tym momencie nie ma ryzyka (trzeba pamiętać, że może się pojawić praktycznie w każdej chwili). Odpowiednie wiersze z tabeli są teraz identyfikowane poprzez wartość zasobu, a kolumny poprzez poziom zagrożeń i podatności.

MAGERIT

Nazwa *MAGERIT* pochodzi od *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las AdminisTraciones Públicas*

Metoda jest zalecana przede wszystkim dla administracji publicznej[75]. Zajmuje się 3 dziedzinami:

- Opisem metodologii analizy i zarządzania ryzykiem
- Przygotowaniem jak najbardziej pełniej informacji i pogrupowanie jej w bazie danych stanowiącej produkt wyjściowy do właściwej oceny ryzyka
- Oprogramowaniem narzędziowym wspierającym implementację metody

Magerit jest przygotowane do uwzględniania technik elektronicznych i informatycznych. Ma dwa główne cele:

- Analizować elementy ryzyka, które oddziaływają na system informacyjny organizacji
- Określić prawdopodobieństwo wystąpienia ryzyka oraz potencjalne zagrożenia, które może spowodować

Analiza ryzyka przeprowadzana przez *Magerit* pozwala zidentyfikować zagrożenia oraz obserwować, w jaki sposób różne ich komponenty oddziaływają na zasoby. Na tej podstawie określa się podatność systemu oraz wpływ, jaki mogą mieć na organizację. Z tego też powodu można powiedzieć, że analiza ryzyka napędza cały system organizacji. Na jej podstawie określa się, którymi obszarami należy się zająć w pierwszej kolejności, a również, bazując na tej analizie organizacja może wybierać i wprowadzać zabezpieczenia w celu minimalizacji możliwych strat.

Produkt obejmuje wszystkie fazy przetwarzania, przesyłania i przetwarzania informacji w systemach *EDP*.

Macierz ryzyka w metodzie PHA					
Stopień skutku	Prawdopodobieństwo				
	5	4	3	2	1
5	25	20	15	10	5
4	20	16	12	8	4
3	15	12	9	6	3
2	10	8	6	4	2
1	5	4	3	2	1

[75] *La Guida de Aproximacion de los Sistemas do Informacion.* Consejo Superior de Informatica, Madryt, Hiszpania

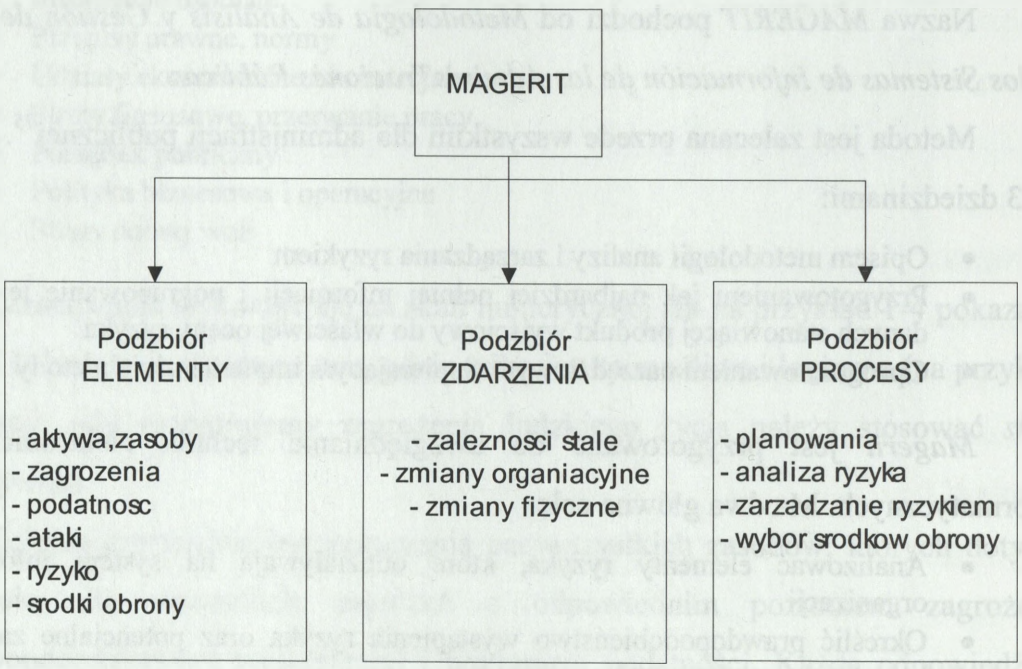


Diagram 33: ***Schemat działania MAGERIT***
Źródło: J. Syta. *Metodyki*... [200]

Podzbiór ELEMENTY dostarcza komponentów, podzbiór ZDARZENIA łączy komponenty między sobą nawzajem w trakcie wydarzeń i po czasie, podzbiór PROCESY dostarcza zasadniczych opisów dla projektu bezpieczeństwa

MASSIA

MASSIA to skrót od *Methode d'Audit de la Securite des Systemes d'Information de l'Armement.* Produkt ten łącznie z oprogramowaniem narzędziowym oferuje:

- Pełne zbadanie podatności systemu informatycznego
- Zbadane operacyjnych procedur ochrony (*SecOPs*)

W trakcie badań dokonuje się przeglądu stałej organizacji systemu, podsystemu działań zapobiegawczych, wewnętrznych i zewnętrznych kontroli itd.

MASSIA stosuje przede wszystkim metody kwalifikacyjne prowadzące do uzyskania pełnych danych dla opracowania *SSRS*. Metoda jest stosowana głównie do prowadzenia procedur kontrolnych *ITSec*.

Producentem jest francuska firma *MARTA & SYSTEM*.

PHA

Wstępna analiza zagrożeń *PHA* jest metodą służącą do identyfikacji zagrożeń stosowaną najczęściej w fazie koncepcyjnej systemu. Jest to metoda od lat stosowana w transporcie oraz przemyśle, ale z powodzeniem może być również zastosowana do bezpieczeństwa systemów informatycznych. Analiza może być stosowana w odniesieniu do materiałów, aparatury i urządzeń, styku systemu z otoczeniem, wpływu otoczenia, procedur, terytorialnego układu systemu oraz środków i sprzętu bezpieczeństwa.

Główne etapy analizy to:

- Spis spodziewanych niebezpieczeństw (zagrożeń)
- Ustalenie stopienia dotkliwości ewentualnego skutku (w skali 4-6 stopniowej)
- Ustalenie wskaźnika częstości wystąpienia zagrożenia w porównywalnej skali
- Oszacowanie ryzyka jako iloczynu wskaźników stopnia skutku i częstotliwości
- Ocena ryzyka przez porównanie z wartościami akceptowanymi (położenia wskaźnika ryzyka w macierzy bezpieczeństwa)

W metodzie *PHA* ocena ryzyka może być dokonywana na podstawie macierzy ryzyka w układnie skali pięciostopniowej. W macierzy wyróżnia się 3 obszary zróżnicowane pod względem ryzyka. Najjaśniejsze określają poziom ryzyka akceptowany na tym etapie analizy i nie wymagający dodatkowych badań analitycznych. Szare elementy o skali ryzyka 4-9 wymagają dodatkowych analiz i ewentualnych działań korygujących. Obszary 10-25 pokazują niedopuszczalny poziom ryzyka dyskwalifikują analizowany element systemu. Warto zwrócić uwagę na pole w prawym górnym rogu. Mimo, że wartość wynosi zaledwie 5 zostało uznane za niedopuszczalne, ponieważ a analizie zwraca się szczególną uwagę na zdarzenia o znacznych skutkach, nawet, jeżeli prawdopodobieństwo ich wystąpienia jest niewielkie.

Ranking the Threats by Measures of Risk

Ta metoda daje możliwość ustalenia rankingu zagrożeń poprzez mierzenie ryzyka. Dokonuje się tego poprzez sporządzenie tabeli, która będzie łączyła wagę (wpływ) zasobu i prawdopodobieństwo wystąpienia zagrożenia. Kolejnymi czynnościami są:

- Ocenienie wpływu zasobu według wcześniej ustalonej skali (na przykład 1-5) i umieszczenie danych w kolumnie (b) tabeli.
- Określenie prawdopodobieństwa wystąpienia zagrożenia według wcześniej ustalonej skali (na przykład 1-5) i umieszczenie danych w kolumnie (c) tabeli.
- Wyliczenie ryzyka poprzez pomnożenie kolumn b i c (b)*(c)
- Ustalenie rankingu ryzyka w kolejności ich wag (na przykład 1-najmniejszy wpływ i prawdopodobieństwo wystąpienia)

Przykład zastosowania metody Ranking the Threats by Measures of Risk				
Opis ryzyka	Wpływ zasobu	Prawdopodobieństwo wystąpienia	Ryzyko	Ranking ryzyka
(a)	(b)	(c)	(d)	(e)
Zagrożenie A	5	2	10	2
Zagrożenie B	2	4	8	3
Zagrożenie C	3	5	15	1

Tabela 11: ***Przykład zastosowania metody Ranking the Threats by Measures of Risk***
Źródło: J. Syta. *Metodyki*... [200]

Tak ustalony ranking pokazuje w prosty i zrozumiały sposób, które z zasobów są dla nas najważniejsze. Niekiedy trzeba stosować modyfikację polegającą połączeniu tych empirycznych danych z wartościami pieniężnymi

RISKPACK

RISKPACK to pakiet przeznaczony do analizy ryzyka w agencjach rządowych. Stosuje metodę kwalitatywno-kwantytatywną. Zestawy ankiet i scenariuszy są pogrupowane w czterech kategoriach, z których każda tworzy oddzielny, osobno oceniany, zbiór aktywów i zagrożeń. Również osobno są przedstawiane i raportowane poziomy ryzyka.

System zawiera moduł korekcji, który na podstawie przeprowadzonej analizy podpowiada zalecenia dla poprawy stany bezpieczeństwa.

Pakiet zawiera również osobny moduł kwantytatywny: *ALE Calculator*. Istnieje również możliwość modyfikacji baz danych i kwestionariuszy.

RISKWATCH

RISKWATCH jest systemem zalecanym do stosowania w agencjach rządowych w USA. W pakiecie zastosowano metodologię kwalitatywno-kwantytatywną.

RiskWatch składa się z 7 modułów:

1. Analizy ryzyka
2. Planowania zarządzania ryzykiem
3. Pomocy przy tworzeniu planu wprowadzania elementów zabezpieczeń
4. Pomocy przy tworzeniu planów awaryjnych

5. Testów bezpieczeństwa systemu
6. Zobrazowania graficznego
7. Reprogramowania i modyfikacji pakietu

Pakiet oferuje rozbudowaną bibliotekę incydentów, duże możliwości raportowania – zarówno numerycznego jak i graficznego. Oddzielnie program umożliwia modyfikację zawartości ankiet i kwestionariuszy. Ankiety mogą być zarówno elektroniczne jak i papierowe, można je zarówno rozsyłać po sieci, jak i kopiować na dyskietki[76].

Działalność całego pakietu można monitorować przez specjalnie przygotowany system kontroli. Dodatkowo istnieje możliwość sprawdzania „ci się stanie, jeżeli".

ROZETA MARION

MARION jest pakietem służącym głównie do analizy ryzyka w organizacjach biznesu.

Stosuje metodę *kwalitatywno-kwantytatywną* oraz bardzo dużą bibliotekę aktualnych incydentów. Pakiet zawiera wiele ankiet i kwestionariuszy stosowanych do oceny rozwiązań w zakresie bezpieczeństwa.

Oprogramowanie wylicza wyniki analizy dla 27 kategorii zasobów i zagrożeń, jest również możliwe uzyskiwanie wyników zarówno w formie numerycznej jak i graficznej.

MARION umożliwia prowadzenie analizy porównawczej wyników oraz utworzenie tzw. cenowej bazy danych dla elementów zabezpieczeń. Daje to możliwość programowego oszacowania kosztów ponoszonych w związku z poprawą systemu zabezpieczeń.

[76] witryna internetowa http://www.riskwatch.com/products/is/index.html

Rozeta Marion – układ według Sekretariatu Generalnego Komisji Bankowej

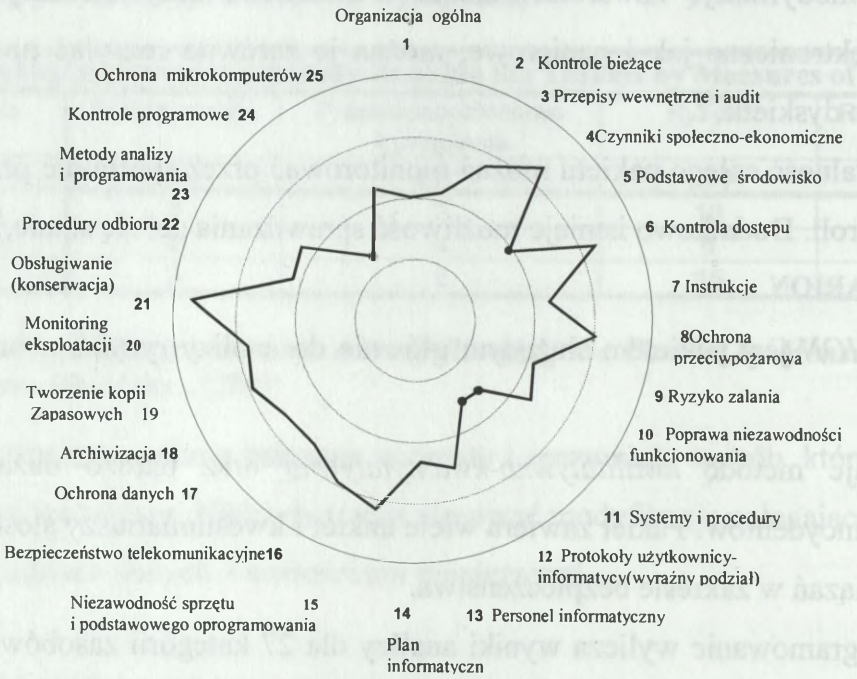


Diagram 34: ***Zarządzanie ryzykiem w metodzie Rozeta Marion***
Źródło: J. Syta. *Metodyki*... [200]

VIR'94

VIR'94, czyli *Voorschrft Informatiebeveiliging Rijkdienst* może być stosowana na wszystkich szczeblach zarządzania. Jest zalecana przez oficjalne służby ochrony informacji jako dyrektywa działania.

Pakiet składa się z 6 części:

1. Słownictwo i terminologia
2. Przewodnik po zakresie działania i cele
3. Polityka informacyjna i zasady obiegu dokumentacji
4. Środki ochrony informacji
5. Realizacja ITSec
6. Uwagi i zadania końcowe

VIR'94 stosuje metodę *D&V* podzielenia ryzyka na

- D - Dependency – 5 etapową analizę uzależnienia organizacji od systemów IT
- V - Vulnerability – 3 etapową analizę podatności

(w holenderskich analizach nie żywa się określenia *ryzyko,* lecz *zależność*)

W dyrektywie wprowadza się jako narzędzie automatycznej analizy oprogramowanie typu *CRAMM,* które z swych 2 pierwszych częściach odpowiada metodzie *D&V.*

Koncepcja stosowania rozmaitych metod analizy ryzyka w bezpieczeństwie systemów informatycznych jest stosunkowo nowa. Do tej pory bardzo często osoba odpowiedzialna za projekt sama decydowała, na podstawie własnych doświadczeń, co i jak należy robić. Często nie miało to żadnego uzasadnienia poza sformułowaniem, że tak chyba będzie najlepiej. Jeżeli organizacji uda się opracować dobry system analizy ryzyka, to przynajmniej ten problem zniknie. Jednolity system *ITSec* sprawi, że wszyscy zaczną wreszcie mówić tym samym językiem, będą rozumieć, czego tak naprawdę się od nich wymaga i co należy do ich obowiązków.

Danych na temat *roli analizy ryzyka* z systemach bezpieczeństwa informacji nie można jeszcze znaleźć. Powoli są ustanawiane kolejne normy regulujące tę sferę działania organizacji, coraz częściej pojawiają się artykuły i opracowania na ten temat, ale ciągle jeszcze bardzo dużo zależy od inwencji osób wprowadzających system[77].

Zebrane w rozprawie metody zawierają większość stosowanych obecnie technik zarządzania ryzykiem w tym obszarze. Cały czas pojawiają się nowe, coraz więcej firm opracowuje własne metody, lecz wszystkie z nich bazują na opisanych w pracy matrycach. To na ich podstawie tworzy się metody dostosowane do konkretnych organizacji czy też rodzaju przedsiębiorstw. Ustala się sposób badania określonych zasobów, określa, jakie zmiany wprowadzą określone typy zabezpieczeń oraz określa sposób interpretacji uzyskanych danych.

Ponieważ ta dziedzina nauki dopiero się rozwija, bardzo trudno jest uzyskać jakiekolwiek bliższe informacje na temat tego, jak naprawdę działają opisywane w rozprawie komercyjne systemy analizy ryzyka. Większość opisów ogranicza się jedynie do sformułowania, jakich metody używa system (*kwanty-* czy *kwalitatywnych*) oraz ewentualnie do określenia gałęzi przemysłu lub funkcji działalności organizacji, w których należy stosować produkt. Inne informacje na temat tego jak działa produkt, jak interpretuje dane kwalitatywne, których metod używa - są niejawne.

[77] J. Syta. *Metodyki analizy ryzyka za szczególnym uwzględnieniem bezpieczeństwa systemów informatycznych.* Politechnika Warszawska 2001

Rozdział 5

5. Model procesu analizy zagrożeń i zarządzania ryzykiem bezpieczeństwa informacyjnego państwa

„Jeśli nie zaatakujesz aktywnie czynników ryzyka, one aktywnie zaatakują Ciebie!"
T. Gilb: "Principles of Software Engineering Management"

W kontekście metodologicznym **modelowanie**, to proces formalnego wykorzystywania metod systemowych dla poznania obiektów badawczych na podstawie rezultatów otrzymanych w toku badania. Modelowanie może przybierać dwie formy: modelowania *„miękkiego"*, tj. opisowego, scenariuszowego oraz modelowania *„twardego"*, w którym dominują równania matematyczne[1]. W *inżynierii systemów*, subdyscyplinie naukowej zajmującej się optymalizacją działania systemów złożonych, modelowania dokonuje się według jednego z dwóch najczęściej stosowanych podejść:

- układowego, tj. polegającego na tworzeniu modelu obiektu według założonych charakterystyk wewnętrznych, modelu zamkniętego na wpływ otoczenia;
- systemowego, uwzględniającego warunki środowiska, w którym funkcjonuje przedmiot (obiekt) badań oraz wielostronne relacje między otoczeniem i obiektem.

Przeprowadzona w ***Rozdziale 4*** główna część analizy systemowej potwierdza zasadność przyjęcia podejścia systemowego do tworzenia modelu procesów analizy zagrożeń i zarządzania ryzykiem bezpieczeństwa informacyjnego państwa. Według K. Duraj-Nowakowej *„Użyteczność modelowania wynika z uniwersalności tej metody. W rezultacie modelowania otrzymuje się opis wyższego poziomu działalności w postaci systemu i następstw celowych działań prowadzących do efektywnego rozwiązywania zadań. Proces modelowania jest jedną z najważniejszych metod podejścia systemowego, pozwalającą uzyskać niezbędne dane o obiekcie i wyłonić jego własności (obserwacja i eksperyment). Przyglądając się modelowaniu w kontekście jego użyteczności warto zaznaczyć, że metoda ta może być stosowana zarówno na poziomie badań empirycznych, jak i teoretycznych; na poziomie empirycznym w przeprowadzaniu pomiaru, opisu i w innych funkcjach, na poziomie*

[1] K. Duraj-Nowakowa. *Teoria systemów a pedagogika.* Wydawnictwo Naukowe WSP. Kraków 1992.

teoretycznym w interpretacjach, funkcji eksplanatywnej i predyktywnej oraz podczas eksperymentu tzw. myślowego; natomiast na obu poziomach może pełnić funkcję kryterium w czynnościach porównawczych."[2]

Jak wynika z powyższych rozważań prowadzenie analizy systemowej i modelowanie obiektu (systemu) stanowią metody wzajemnie się uzupełniające.

Modelem, w rozumieniu niniejszej pracy *modelem nominalnym,* określa się *układ założeń przyjmowanych w danej nauce w celu ułatwienia lub umożliwienia rozwiązania danego problemu badawczego*[3].

Przy tworzeniu modelu procesów analizy zagrożeń i zarządzania ryzykiem bezpieczeństwa informacyjnego państwa posłużono się koncepcją, polegającą na:

1. **Wyborze elementów i cech systemu;**
2. **Wyborze i ocenie elementów otoczenia systemu;**
3. **Wskazaniu istotnych sprzężeń między elementami systemu oraz między systemem i jego otoczeniem;**
4. **Graficznej prezentacji systemu;**
5. **Opisowej prezentacji systemu;**
6. **Ocenie jakości systemu - weryfikacji hipotez badawczych**[4]**.**

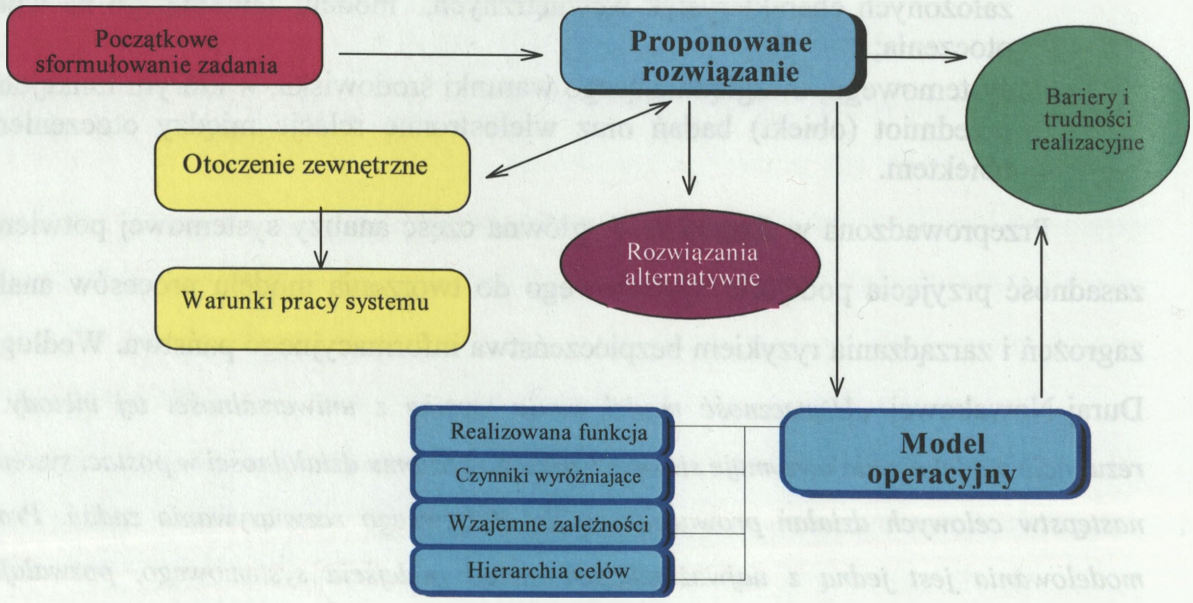


Diagram 35: ***Koncepcja modelu procesów analizy zagrożeń i zarządzania ryzykiem***
Źródło: opracowanie własne

[2] *Ibidem* str. 220
[3] *Nowa Encyklopedia Powszechna PWN*. Warszawa 1996 tom IV, s. 258
[4] J. Habr, J. Veprek. *Systemowa analiza i synteza*. PWE. Warszawa 1976, s. 178-179

Jak definiuje C. Cempel: *„**Model** to uproszczona wersja rzeczywistego systemu w określonym czasie i przestrzeni prowadząca do lepszego zrozumienia rzeczywistości (jedna z definicji). **Symulacja** to manipulacja modelem ze zmianą skali czasu i przestrzeni umożliwiająca zrozumienie oddziaływań i zachowania jako całości, co bez tego byłoby niemożliwe"*[5].

W ***Rozdziale 2.3*** posłużono się modelowaniem matematycznym w zakresie miar efektywności informacyjnej w oparciu o sieciocentryczną architekturę systemów informacyjnych pola walki. W załącznikach zamieszczono elementy symulacji przebiegu działań bojowych z wykorzystaniem zmiennych dotyczących efektywności informacyjnej. Powyższe zrealizowano w oparciu o schemat modelowania matematycznego, zamieszczony na ***Diagramie Nr 36.***

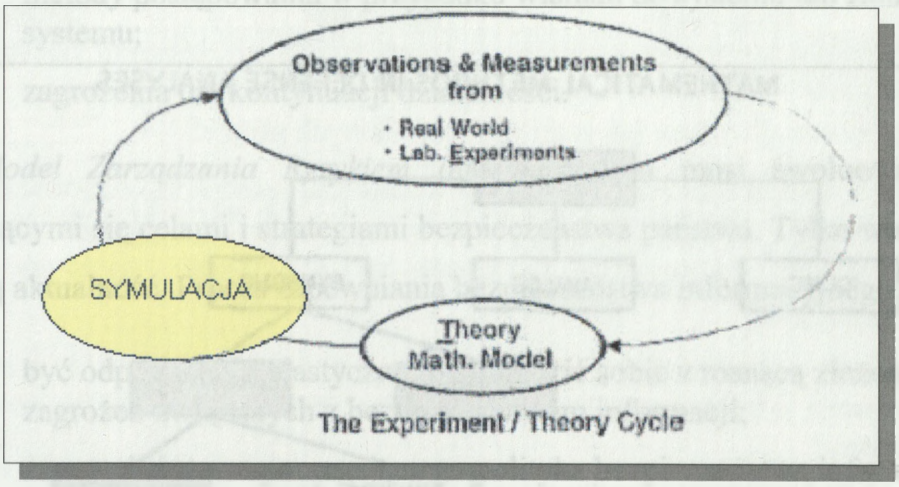


Diagram 36: ***Modelowanie i symulacja matematyczna***
Źródło: Przemieniecki J. S. *Mathematical Methods in Defense Analyses. AFT Ohio USA 2003*

Zgodnie z poglądami amerykańskich analityków zajmujących się matematycznym modelowaniem pola walki: ***"Warfare Can Be Calculated.*** *Combat Modeling (CM) is calculating of combat outcomes based on mathematical models. CM is rather a kind of practical tool for support to military decision makers. CM may be based on different types of mathematical models, traditionally deterministic models of the Lanchester type homogeneous and heterogeneous combat situations. Unfortunately*

[5] C. Cempel. *Teoria i inżynieria systemów- skrypt.* IMS Politechnika Poznańska 2002

the generalization requires an approximation, but it seems to be tolerable. During the cold war combat modeling became a major tool to support NATO military decision makers" – (Wojnę można policzyć. Modelowanie walki jest obliczaniem jej wyniku, opartym na modelach matematycznych. Jest rodzajem narzędzia wspierającego pracę wojskowych decydentów. Modelowanie walki oparte może być na różnych odwzorowaniach matematycznych, najczęściej na deterministycznych modelach Lanchestera, w odniesieniu do operacji połączonych jak i jednowymiarowych. Niestety, uogólnianie wymaga aproksymacji, lecz wydaje się to być do przyjęcia. W czasach zimnej wojny modelowanie walki stało się głównym narzędziem, wspierającym procesy decyzyjne NATO – [tłum. autora] [6].

Klasyfikację zastosowań modeli matematycznych w analizach dotyczących sektora obrony przedstawia zaczerpnięty z podanego niżej źródła diagram.

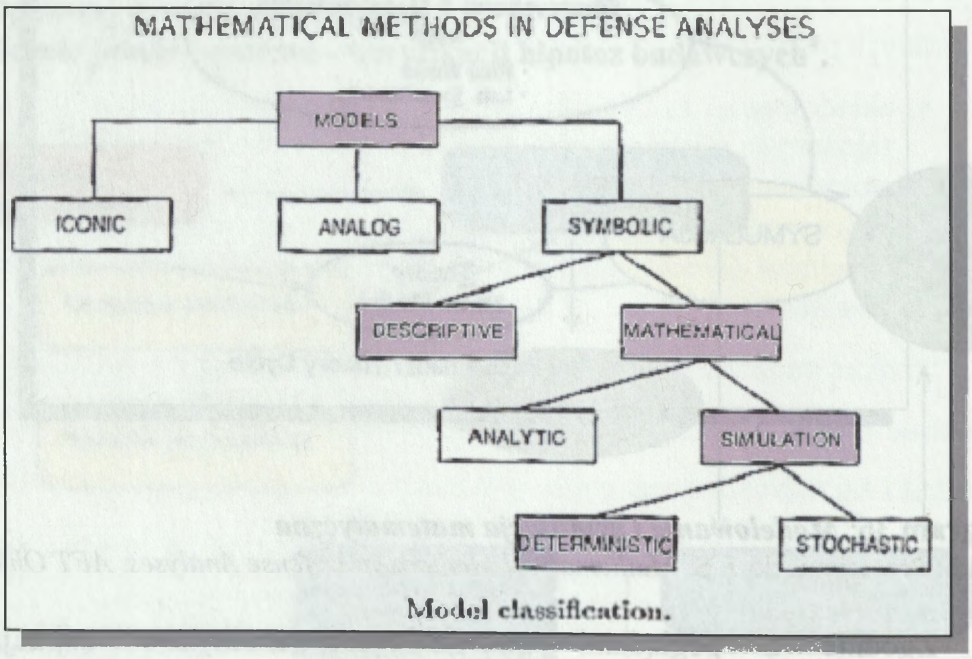


Diagram 37: ***Modelowanie i symulacja matematyczna***
Źródło: Przemieniecki J. S. *Mathematical Methods in Defense Analyses. AFT Ohio USA 2003*

[6] Booss-Bavnbek B., Hoeyrup J. Birkheauser. *Mathematics and War*. Verlag Berlin 2003

Bezpieczeństwo informacji, jej integralność oraz autentyczność to tylko niektóre podmioty procesu zarządzania ryzykiem informacyjnym. Dlatego też należy wyjść poza koncepcję samego tylko bezpieczeństwa informacji. Aby w przyszłości efektywnie zarządzać ryzykiem związanym z systemami informatycznymi, musi zostać opracowany całościowy ***Model Zarządzania Ryzykiem Informacyjnym*** uwzględniający następujące obszary:

- skuteczne i integralne metody zarządzania projektami oraz infrastrukturą informatyczną;
- wydajne i sprawne środowisko kontrolne;
- mechanizmy zapewniające bezpieczeństwo i dostępność informacji;
- metody zarządzania uprawnieniami w systemach i kontrolą dostępu do systemów;
- metody postępowania w przypadku włamań do systemu lub zainfekowania systemu;
- zagrożenia dla kontynuacji działalności.

Model Zarządzania Ryzykiem Informatycznym musi ewoluować wraz ze zmieniającymi się celami i strategiami bezpieczeństwa państwa. Tylko wtedy zachowa on swoją aktualność. Proces zapewniania bezpieczeństwa informacyjnego powinien:

- być odpowiednio elastyczny, by poradzić sobie z rosnącą złożonością i skalą zagrożeń związanych z bezpieczeństwem informacji;
- zapewniać, że wspomagająca go polityka bezpieczeństwa informacji zostanie dobrze zdefiniowana, a zasady i reguły w niej zawarte będą możliwe do wyegzekwowania;
- odzwierciedlać przekonanie, że ludzie oraz procesy mają kluczowe znaczenie, a technologia stanowi jedynie część całościowego modelu zarządzania ryzykiem informatycznym;
- ewoluować wraz ze zmieniającym się ustawodawstwem, zagrożeniami oraz mechanizmami kontrolnymi;
- zapewniać możliwość szybkiego reagowania na zagrożenia oraz umożliwiać przewidywanie nowych zagrożeń, trendów oraz okazji do wprowadzenia ulepszeń.

Weryfikację spełniania powyższych cech przez zautomatyzowane systemy analizy ryzyka zawiera ***analiza efektywności.***

5.1. Analiza efektywności stosowania wyselekcjonowanych narzędzi analizy zagrożeń i zarządzania ryzykiem w zakresie bezpieczeństwa informacyjnego – pomiar efektywności z wykorzystaniem wybranych narzędzi badawczych

ANALIZA EFEKTYWNOŚCI

Pojęcie *efektywności* nie jest w dostępnej literaturze jednoznacznie definiowane. Efektywność systemu jest *„relacją systemową między potrzebami (bieżącymi lub przyszłymi) osiągania zamierzonych celów działania, funkcjonowania zgodnie z przeznaczeniem i wymaganiami a potencjałem systemu (użytym lub przewidywanym do użycia). W dosłownym znaczeniu system jest efektywny, jeżeli wywołuje (lub może wywoływać) określony (zamierzony) efekt. Efekty zaś mogą być dodatnie i mogą być ujemne"*[7].

Do **kryteriów** oceny efektywności należą:

- **kryteria operacyjne** związane z organizacją i przebiegiem podstawowych procesów działania i wyrażające ich powodzenie, czyli fakt osiągania zamierzonych celów lub realizacji określonych potrzeb;
- **kryteria ekonomiczne** związane z wielkością (wartością) efektów dodatnich (korzyści) i ujemnych (nakładów) i wyrażające korzystność działalności podstawowej (wytwórczej, usługowej itp.) w systemie - są to ***stymulanty*** i ***destymulanty***;
- **kryteria informacyjne** związane z organizacją systemu i przebiegiem procesów informacyjnych, wyrażające wpływ tych procesów na powodzenie systemu;
- **kryteria techniczne** związane ze sprawnością elementów systemu, a w szczególności środków technicznych i wyrażające wpływ techniki na powodzenie systemu;
- **kryteria eksploatacyjne** związane z funkcjonowaniem środków działania i wyrażające wpływ ich funkcjonowania na zdolność systemu do sprawnego działania w określonym czasie.

[7] P. Sienkiewicz. *Analiza systemowa. Podstawy i zastosowania*. Bellona 1994. s. 188

Przebieg analizy efektywności ukazuje poniższy schemat:

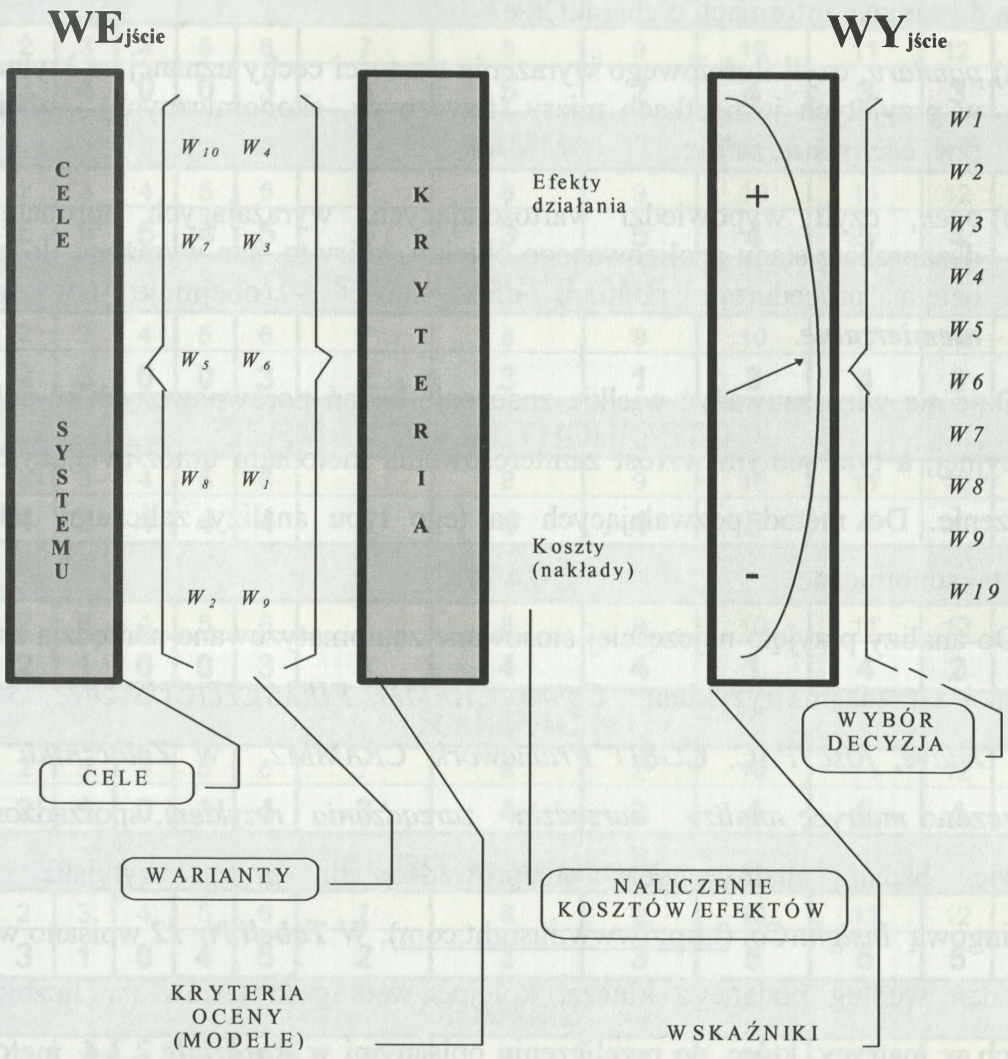


Diagram 38: ***Analiza efektywności***

Źródło: P. Sienkiewicz. *Analiza systemowa. Podstawy i zastosowania*. Bellona 1994

W analizie efektywności obiektów (systemów) szczególne znaczenie przypisać należy następującym przedsięwzięciom:

- określenie *przestrzeni cech obiektu* (systemu) istotnych z punktu widzenia zidentyfikowanych potrzeb i celów;
- wybór *kryteriów oceny efektywności*;
- określenie *wskaźników efektywności*, czyli funkcji pozwalających na ilościowe wyrażenie wartości kryteriów;
- opracowanie *metod* (algorytmów) *wyznaczania wartości efektywności* obiektów (systemów);
- określenie *reguł wnioskowania*: formułowania sądów ocenowych, sądów porównawczych itp.

Praktyczna realizacja sformułowanej zasady w procesie analizy systemowej powinna dostarczyć informacji o charakterze:

a) *pomiaru*, czyli ilościowego wyrażenia wartości cechy uznanej za kryterialną w przyjętych jednostkach miary (fizycznych, ekonomicznych) - obejmuje tzw. ***cechy mierzalne***;

b) *ocen*, czyli wypowiedzi wartościujących, wyrażających aprobatę lub dezaprobatę stanu analizowanego obiektu, który to stan wyrażono ilościowo dzięki procedurom pomiaru efektywności - obejmuje tzw. ***cechy niemierzalne***.

Daje się więc zauważyć wielkie znaczenie badań porównawczych w polityce integracyjnej, a tym samym wzrost zainteresowania metodami umożliwiającymi ich prowadzenie. Do metod pozwalających na tego typu analizy zaliczamy właśnie metody taksonomiczne.

Do analizy przyjęto najczęściej stosowane zautomatyzowane narzędzia analizy zagrożeń i zarządzania ryzykiem: *Cobra, CRAMM, FIRM/CITICUS ONE, BSI/GS TOOL, Octave, Risc PAC, COBIT Framework, CRAMM2.* W ***Załączniku Nr 4*** zamieszczono *matrycę analizy narzędzia zarządzania ryzykiem*, sporządzoną na podstawie badań analitycznych przeprowadzonych przez brytyjską firmę konsultingową *Insight Co.* (http://www.insight.com). W ***Tabeli Nr 12*** wpisano wyniki tych badań według podanego klucza, kolejno według kryteriów (w liczbie 13) podanych w matrycy, które, po przeliczeniu opisanymi w ***Rozdziale 2.3.4*** metodami taksonomicznymi - zobrazowano na ***Wykresach Nr 11*** i ***12***. Wynik wyróżnia produkt *CRAMM*, zarówno pod względem dysponowania najlepszymi cechami jakościowymi (niska miara dystansu w stosunku do wzorca), jak i pod względem właściwych proporcji wyróżników charakteryzujących sprawność narzędzia (wysoka miara podobieństwa z wzorcem).

W 2003 roku *zautomatyzowany system analizy zagrożeń CRAMM* został wybrany przez organa bezpieczeństwa NATO jako główne narzędzie analityczne (pod nazwą *CRAMM NATO profile)* w procesach monitorowania zagrożeń bezpieczeństwa informacyjnego.

W ***Załączniku Nr 4*** zamieszczono odwzorowania graficzne głównych badanych narzędzi analizy ryzyka.

COBRA												
1	2	3	4	5	6	7	8	9	10	11	12	13
4	3	4	0	0	3	3	5	2	4	3	3	4
CRAMM												
1	2	3	4	5	6	7	8	9	10	11	12	13
5	5	5	5	4	5	5	3	5	4	5	4	4
FIRM/CITICUS ONE												
1	2	3	4	5	6	7	8	9	10	11	12	13
2	2	3	0	0	3	2	3	1	3	4	3	3
GERMAN BSI METHOD/GSTOOL												
1	2	3	4	5	6	7	8	9	10	11	12	13
4	4	3	4	4	4	5	4	4	5	4	4	4
OCTAVE												
1	2	3	4	5	6	7	8	9	10	11	12	13
3	2	1	0	0	3	3	4	4	1	4	2	3
Risk PAC												
1	2	3	4	5	6	7	8	9	10	11	12	13
4	2	1	0	0	4	3	4	3	4	2	4	3
COBIT Framework												
1	2	3	4	5	6	7	8	9	10	11	12	13
3	3	1	0	4	5	2	3	3	5	5	5	5
CRAMM2												
1	2	3	4	5	6	7	8	9	10	11	12	13
1	1	1	1	1	1	1	1	1	1	1	1	1

OVERAL	1	2	3	4	5
COBRA			√		
CRAMM				√	
FIRM/CITICUS ONE		√			
GERMAN BSI METHOD/GSTOOL				√	
OCTAVE		√			
Risk PAC			√		
COBIT Framework			√		
CRAMM2	√				

***KLUCZ*: 1=słabe, 2=dostateczne, 3=średnie, 4=silne, 5=bardzo silne**

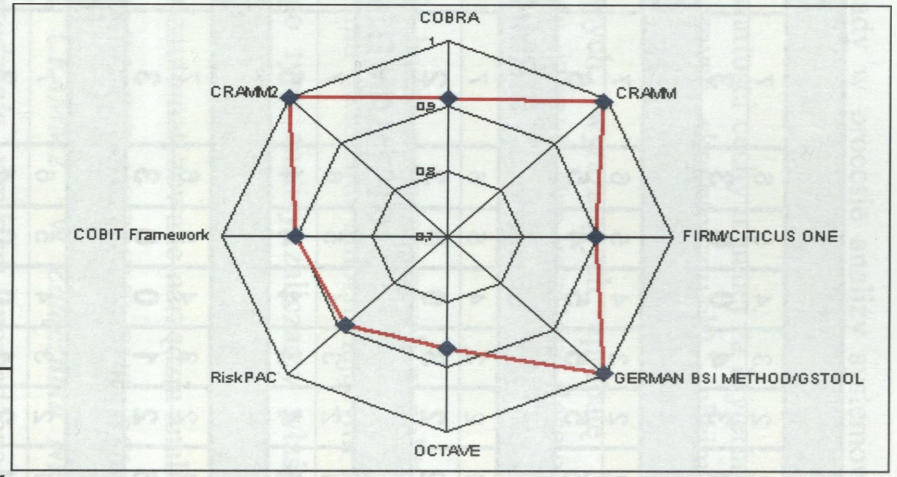
Tabela 12: ***Analiza ocenowa wybranych narzędzi analizy zagrożeń i zarządzania ryzykiem***

Miary taksonomiczne zautomatyzowanych systemów analizy ryzyka

Miary podobieństw

System/Kryteria	1	2	3	4	5	6	7	8	9	10	11	12	13
COBRA	4	3	4	0	0	3	3	5	2	4	3	3	4
CRAMM	5	5	5	5	4	5	5	3	5	4	5	4	4
FIRM/CITICUS ONE	2	2	3	0	0	3	2	3	1	3	4	3	3
GERMAN BSI METHOD/GSTOOL	4	4	3	4	4	4	5	4	4	5	4	4	4
OCTAVE	3	2	1	0	0	3	3	4	4	1	4	2	3
Risk PAC	4	2	1	0	0	4	3	4	3	4	2	4	3
COBIT Framework	3	3	1	0	4	5	2	3	3	5	5	5	5
CRAMM2	1	1	1	1	1	1	1	1	1	1	1	1	1
MAX	5	5	5	5	4	5	5	5	5	5	5	5	5

COBRA	0,909852
CRAMM	0,990759
FIRM/CITICUS ONE	0,895335
GERMAN BSI METHOD/GSTOOL	0,992144
OCTAVE	0,87033
Risk PAC	0,887925
COBIT Framework	0,900688
CRAMM2	0,998538

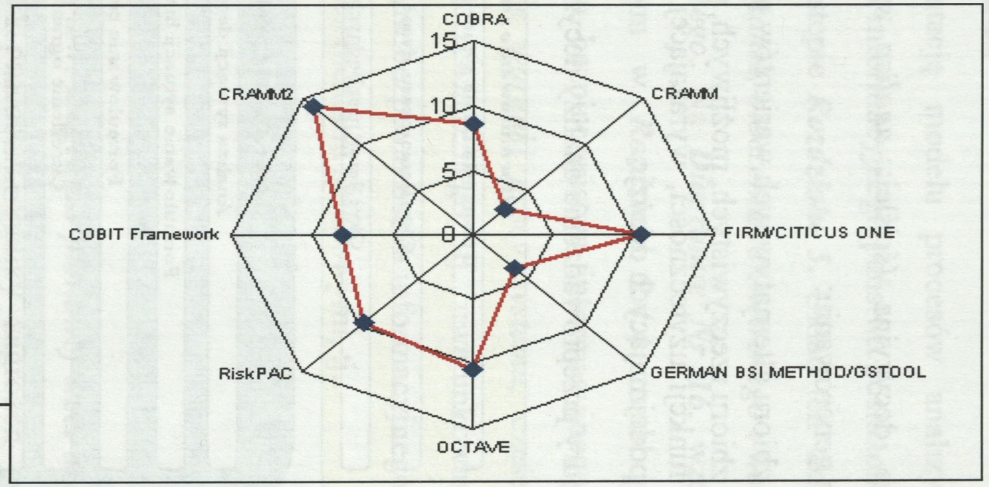


Wykres 11: ***Miary podobieństw wybranych narzędzi analizy ryzyka***

Miary dystansów

System/Kryteria	1	2	3	4	5	6	7	8	9	10	11	12	13
COBRA	4	3	4	0	0	3	3	5	2	4	3	3	4
CRAMM	5	5	5	5	4	5	5	3	5	4	5	4	4
FIRM/CITICUS ONE	2	2	3	0	0	3	2	3	1	3	4	3	3
GERMAN BSI METHOD/GSTOOL	4	4	3	4	4	4	5	4	4	5	4	4	4
OCTAVE	3	2	1	0	0	3	3	4	4	1	4	2	3
Risk PAC	4	2	1	0	0	4	3	4	3	4	2	4	3
COBIT Framework	3	3	1	0	4	5	2	3	3	5	5	5	5
CRAMM2	1	1	1	1	1	1	1	1	1	1	1	1	1
MAX	5	5	5	5	4	5	5	5	5	5	5	5	5

COBRA	8,602325
CRAMM	2,645751
FIRM/CITICUS ONE	10,44031
GERMAN BSI METHOD/GSTOOL	3,605551
OCTAVE	10,48809
Risk PAC	9,591663
COBIT Framework	8,124038
CRAMM2	14,17745



Wykres 12: ***Miary dystansów wybranych narzędzi analizy ryzyka***

5.2. Modelowanie narzędzi systemowych w procesie analizy zagrożeń i zarządzania ryzykiem informacyjnym

ANALIZA DECYZYJNA

... wszystko sprowadza się do czynności decyzyjnych. Można wykorzystywać najlepsze w świecie komputery i zebrać wszelkie wykresy i liczby, ale w końcu trzeba jednak uzyskane informacje poddać syntezie i ustalić plan działań.
L. Iaccoca. *Autobiografia*

Analiza decyzyjna (ściślej: *analiza sytuacji decyzyjnych*) polega przede wszystkim na generowaniu:

- zbioru alternatywnych wariantów projektów decyzji;
- zbioru rzeczywistych, możliwych, prawdopodobnych stanów rzeczy;
- funkcji użyteczności, wyrażającej ocenę wariantów z punktu widzenia podejmujących decyzję.

Procedury przeprowadzenia analizy decyzyjnej obrazuje ***Diagram Nr* 38.**

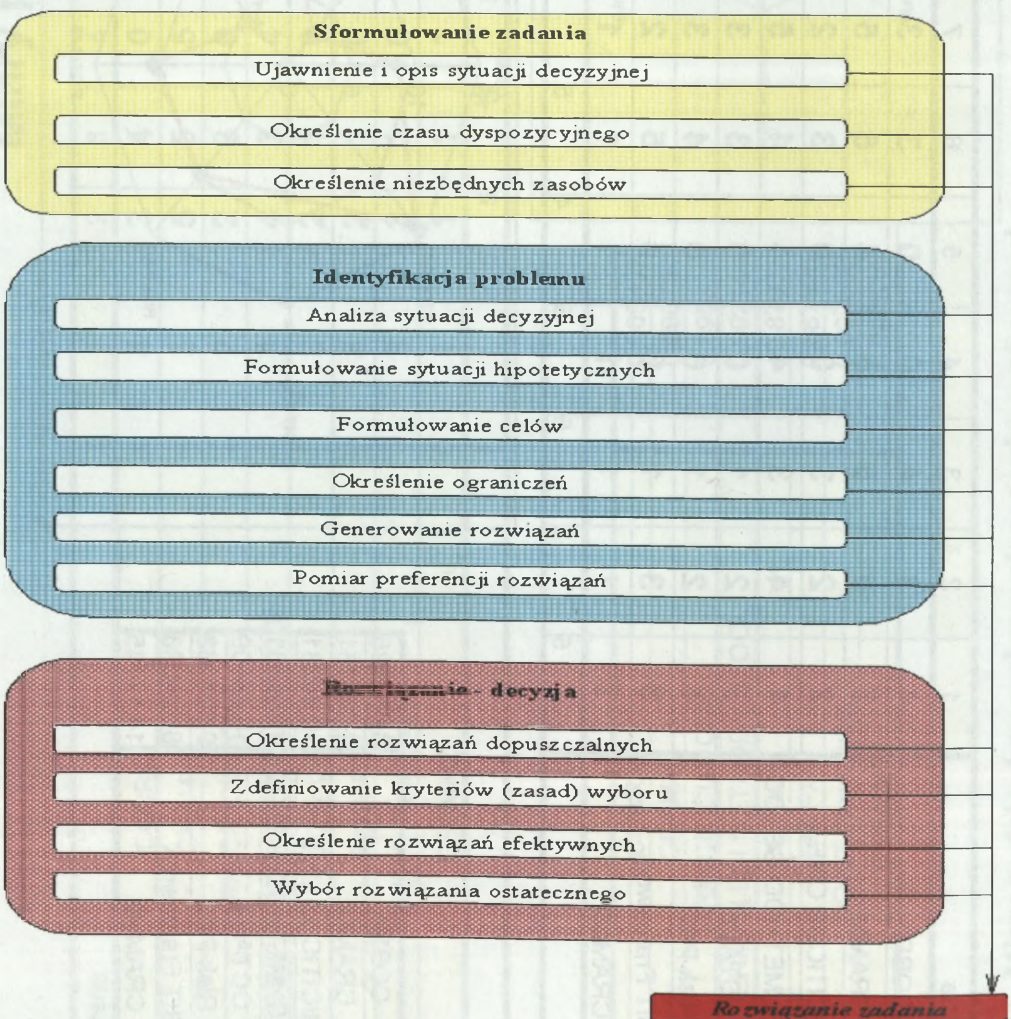


Diagram 39: ***Schemat analizy decyzyjnej***[8]

[8] L.G. Jewłanow. *Tieorija i praktika priniatija rieszenij.* Moskwa 1984

Z wykorzystaniem analizy decyzyjnej dokonuje się wyboru rozwiązania ostatecznego (wypracowanie *modelu procesów analizy zagrożeń i zarządzania ryzykiem bezpieczeństwa informacyjnego państwa*) poprzez **syntezę** wyników uzyskanych na podstawie badań i analiz.

Podejmując graficzną prezentację modelu procesów analizy zagrożeń i zarządzania ryzykiem bezpieczeństwa informacyjnego państwa posłużono się układem modelowania przedstawionym na wstępie ***Rozdziału 5.*** Układ ten określa potrzebę zilustrowania *proponowanego rozwiązania, otoczenia zewnętrznego* i *warunków pracy systemu,* a także *modelu operacyjnego.* Na ***Diagramie Nr 16***, wzorowanym na *wykresie Ishikawy*, zaprezentowanym w ***Rozdziale 2.4.4*** został przedstawiony graficznie układ procedur z zakresu bezpieczeństwa informacyjnego państwa. W części centralnej schemat prezentuje *warunki pracy systemu,* części skrzydłowe schematu zawierają opis *otoczenia zewnętrznego*, tj. uwarunkowań środowiska zewnętrznego i wewnętrznego procesów bezpieczeństwa informacyjnego w Polsce.

Model operacyjny wraz z jego elementami składowymi, tj.:

- realizowaną funkcją;
- czynnikami wyróżniającymi;
- wzajemnymi zależnościami;
- hierarchizacją celów.

przedstawiony jest poniżej w postaci tzw. ***diagramu pionowej sieci działań*** (jedno z narzędzi *TQM*). Sieć zawiera układ procesów analizy zagrożeń bezpieczeństwa informacyjnego i pokazuje kolejne kroki celem jego zapewnienia.

Rozwinięciem *modelu procesu zarządzania ryzykiem* w systemie bezpieczeństwa informacyjnego państwa jest, przedstawiony jako *proponowane rozwiązanie,* układ założeń dostosowawczych[9].

[9] zgodnie z encyklopedyczną definicją zawartą na wstępie ***Rozdziału 5***

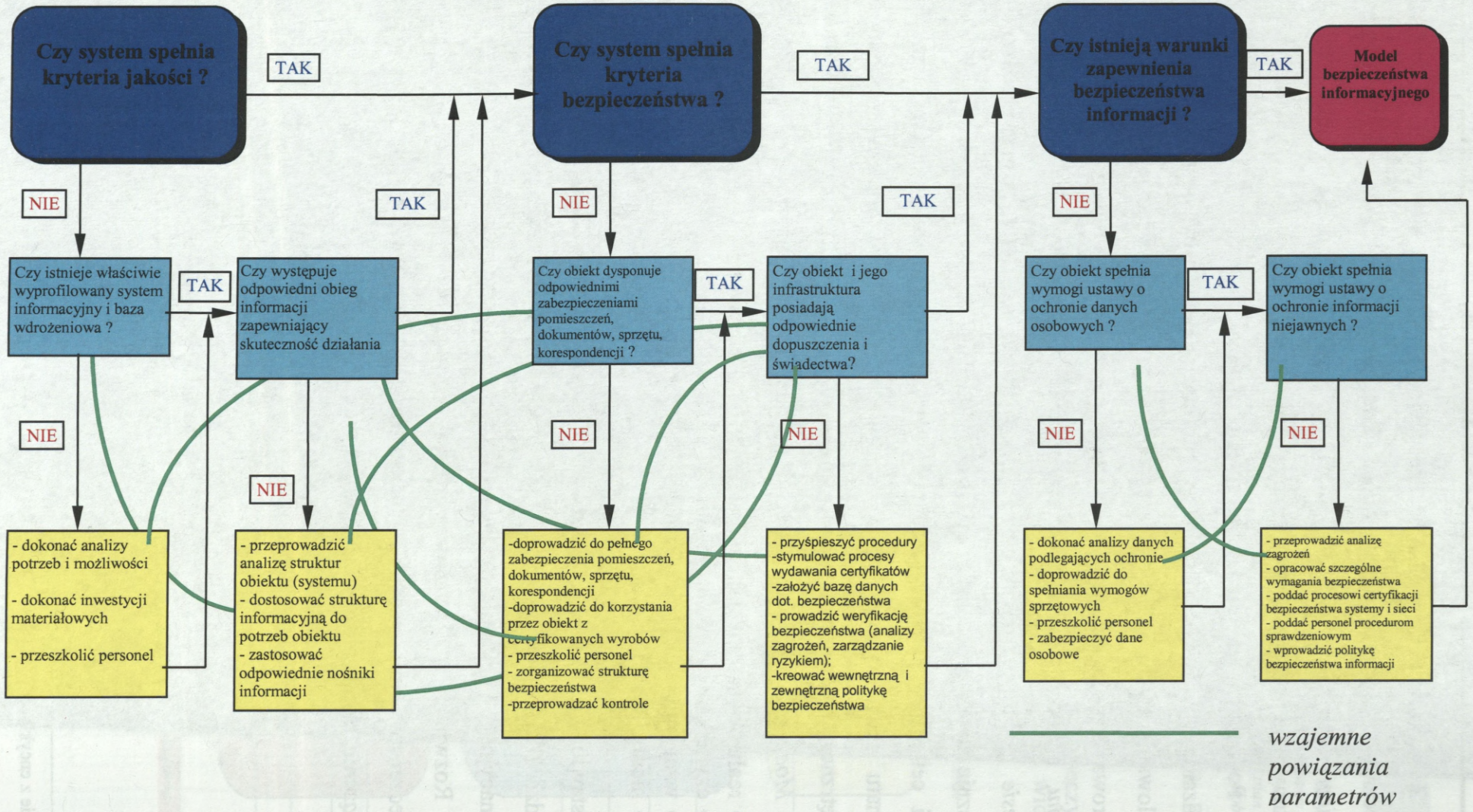


Diagram 40: ***Pionowa sieć działań w zakresie bezpieczeństwa informacyjnego państwa***

Wymagania dotyczące zarządzania ryzykiem

Cel

Opracowanie polityki zarządzania ryzykiem w systemie bezpieczeństwa informacyjnego i mechanizmów jej wsparcia jest niezbędne do zapewnienia realizacji bardziej szczegółowych programów zarządzania ryzykiem na poziomie poszczególnych przedsięwzięć lub na niższych szczeblach systemu.

Polityka zarządzania ryzykiem

Organ kierowniczy (*służby ochrony państwa*) określa oraz dokumentuje swą politykę zarządzania ryzykiem. Polityka zarządzania ryzykiem musi być powiązana ze strategicznym kontekstem systemu oraz celami, zadaniami i charakterem prowadzonej działalności. Ma ona na celu

- inicjowanie działań w celu zapobieżenia lub zredukowania ujemnych skutków ryzyka;
- kontrolowanie dalszego postępowania wobec ryzyka do momentu gdy poziom ryzyka będzie do przyjęcia;
- identyfikacja oraz rejestrowanie wszelkich problemów dotyczących zarządzania ryzykiem;
- inicjowanie, zalecanie lub zapewnianie rozwiązań przez przeznaczone do tego kanały;
- weryfikacja implementacji rozwiązań oraz komunikowanie oraz wewnętrzne i zewnętrzne konsultacje;
- szkolenie.

Zasoby

Organizacja ustala wymagania dotyczące zasobów i zapewnia odpowiednie zasoby, w tym wyznacza przeszkolony personel do zarządzania, wykonywania pracy, i weryfikacji czynności obejmującej również wewnętrzne inspekcje.

Proces zarządzania ryzykiem

Szczegóły procesu zarządzania ryzykiem przedstawiono na ***Diagramie Nr 40***. Proces zarządzania należy określić w celu zdefiniowania podstawowych parametrów, w kontekście których należy zarządzać ryzykiem, oraz w celu zapewnienia płynności decyzji podejmowanych w ramach bardziej

szczegółowych analiz ryzyka. Kontekst określa zakres pozostałej części procesu zarządzania ryzykiem.

Proces należy rozpocząć z pełną świadomością potrzeby wyważenia kosztów, korzyści i możliwości. Należy też określić wymagane zasoby i dokumentację którą należy prowadzić.

Określenie zakresu i granic zastosowania procesu zarządzania ryzykiem obejmuje:

- określenie przedsięwzięcia lub czynności oraz ustanowienie jej celów i zadań;
- określenie rozciągłości przedsięwzięcia w czasie oraz lokalizacji;
- ustalenie wszelkich wymaganych szczegółowych analiz oraz ich zakresu, zadań i wymaganych zasobów. Typowe źródła ryzyka i obszary jego oddziaływania mogą posłużyć jako wskazówka.
- określenie zakresu oraz wszechstronności czynności związanych z zarządzaniem ryzykiem które należy wykonać.

Opracowanie kryteriów oceny ryzyka

Decyzje dotyczące dopuszczalności ryzyka i postępowania wobec ryzyka mogą opierać się na kryteriach operacyjnych, technicznych, finansowych, prawnych, społecznych i innych. Kryteria mogą być zależne od wewnętrznej i zewnętrznej percepcji zagrożeń oraz od wymogów legislacyjnych. Jest ważne, aby odpowiednie kryteria zostały wyznaczone na początku.

Jakkolwiek kryteria ryzyka są wstępnie opracowywane w ramach określania kontekstu zarządzania ryzykiem, można je dalej rozrywać i doprecyzowywać w miarę identyfikacji określonych rodzajów ryzyka i wyboru technik analizy ryzyka, tzn. kryteria ryzyka muszą odpowiadać rodzajom ryzyka i sposobowi wyrażania jego poziomów.

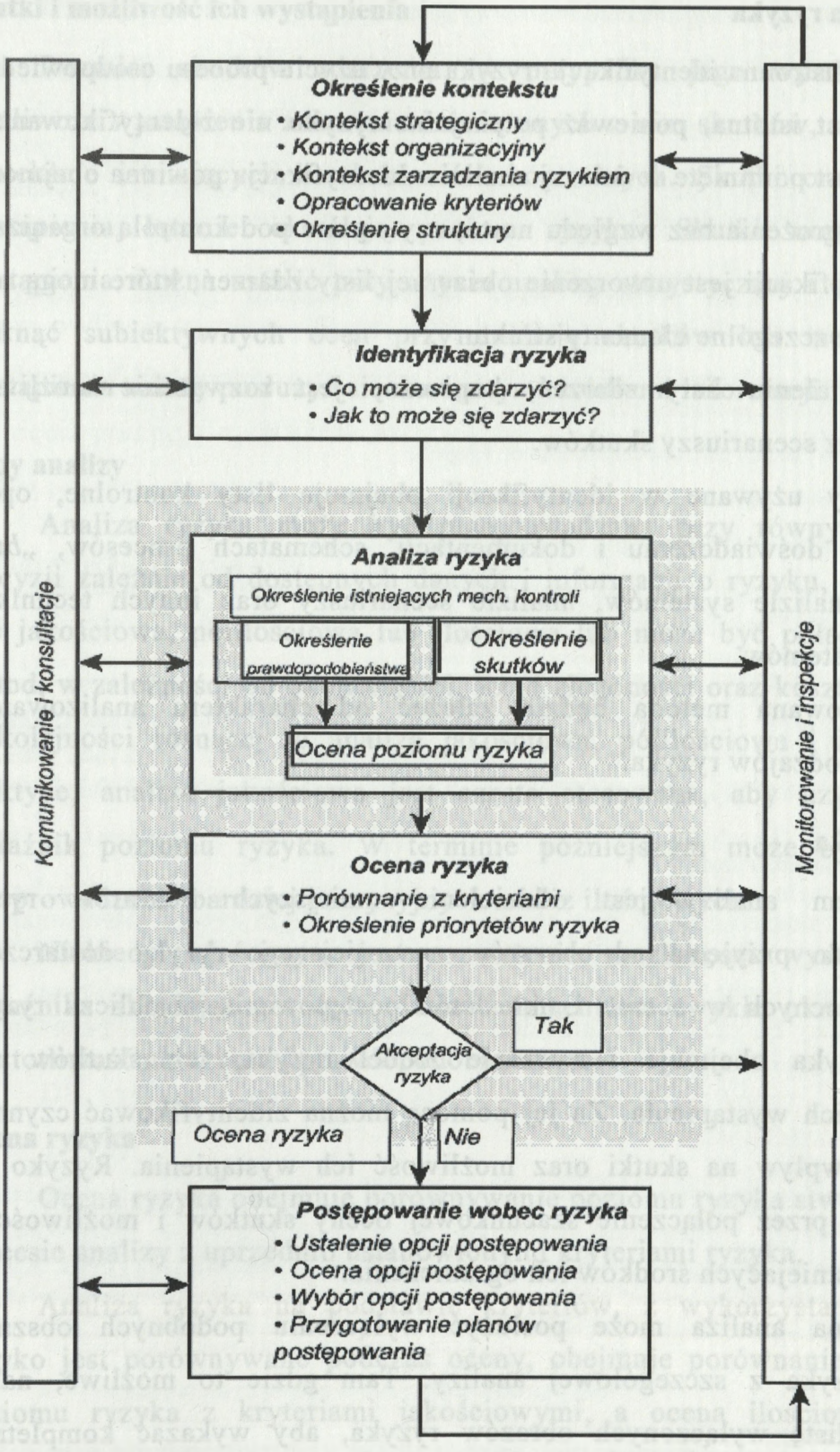


Diagram 41: ***Proces zarządzania ryzykiem***

Źródło: Wiśniewski A. *Analiza ryzyka. Wytyczne dla administratorów systemów.* AZW Warszawa 2000

Identyfikacja ryzyka

Wszechstronna identyfikacja ryzyka przy użyciu procesu o odpowiedniej strukturze jest istotna, ponieważ potencjalne ryzyko nie zidentyfikowane na tym etapie jest pominięte w dalszej analizie. Identyfikacja powinna obejmować wszystkie zagrożenia bez względu na to, czy są one pod kontrolą organizacji. Celem identyfikacji jest utworzenie obszernej listy zdarzeń, które mogą mieć wpływ na poszczególne elementy struktury.

Po ustaleniu listy zdarzeń, konieczne jest rozważenie możliwych przyczyn oraz scenariuszy skutków.

Metody używane w identyfikacji obejmują listy kontrolne, opinie bazujące na doświadczeniu i dokumentacji, schematach procesów, *„burzy mózgów"*, analizie systemów, analizie scenariuszy oraz innych technikach inżynierii systemów.

Zastosowana metoda będzie zależeć od charakteru analizowanych czynności i rodzajów ryzyka.

Analiza ryzyka

Zdaniem analizy jest oddzielenie mniejszych obszarów ryzyka możliwego do przyjęcia od obszarów znaczniejszego ryzyka dostarczenie danych pomocnych w ocenie i określeniu postępowania w obliczu ryzyka. Analiza ryzyka obejmuje rozważenie źródeł ryzyka, ich skutków oraz możliwości ich wystąpienia. Za jej pomocą można zidentyfikować czynniki, które mają wpływ na skutki oraz możliwość ich wystąpienia. Ryzyko jest analizowane przez połączenie szacunkowej oceny skutków i możliwości w kontekście istniejących środków ich ograniczenia.

Wstępna analiza może posłużyć wyłączeniu podobnych obszarów niskiego ryzyka z szczegółowej analizy. Tam gdzie to możliwe, należy sporządzić listę wyłączonych obrazów ryzyka, aby wykazać kompletność analizy ryzyka.

Skutki i możliwość ich wystąpienia

Rozmiar skutków zdarzenia, w przypadku jego wystąpienia, oraz możliwość wystąpienia zdarzenia i związanych z nim skutków, są oceniane w kontekście istniejących mechanizmów kontrolnych. Skutki oraz możliwość wystąpienia łącznie określają poziom ryzyka. Skutki oraz możliwość wystąpienia można ustalić przy użyciu analizy statystycznej i obliczeń. Aby uniknąć subiektywnych ocen przy analizie skutków lub możliwości ich wystąpienia należy posłużyć się dostępnymi źródłami informacji i technikami.

Typy analizy

Analiza ryzyka może być przeprowadzana przy równych stopniach precyzji zależnie od dostępnych danych i informacji o ryzyku, analiza może być jakościowa, półilościowa lub ilościowa lub może być połączeniem tych metod, w zależności od okoliczności. Rząd złożoności oraz koszty tych analiz w kolejności rosnącej to analiza jakościowa, półilościowa i ilościowa. W praktyce, analiza jakościowa jest często stosowana, aby uzyskać ogólny wskaźnik poziomu ryzyka. W terminie późniejszym może być konieczne przeprowadzenie bardziej precyzyjnych analiz ilościowych.

Niekiedy właściwym jest rozważenie możliwości wystąpienia jako wskaźnika składającego się z dwóch elementów, zwykle określanych jako częstotliwość narażenia i prawdopodobieństwo.

Ocena ryzyka

Ocena ryzyka obejmuje porównywanie poziomu ryzyka stwierdzonego w procesie analizy z uprzednio ustanowionymi kryteriami ryzyka.

Analiza ryzyka na podstawie kryteriów, z wykorzystaniem których ryzyko jest porównywane podczas oceny, obejmuje porównanie ilościowego poziomu ryzyka z kryteriami jakościowymi, a ocena ilościowa obejmuje porównanie liczbowego poziomu ryzyka z kryteriami, które mogą być wyrażane jako konkretną liczbą.

Wynik oceny ryzyka jest spriorytetyzowaną listą obszarów ryzyka, wobec których należy podjąć dalsze działania.

Identyfikacja opcji postępowania wobec ryzyka

Diagram Nr 41 ilustruje proces postępowania wobec ryzyka. Obejmuje on następujące możliwości:

- *Unikanie ryzyka* przez postanowienie nie podejmowania czynności (działań, decyzji), które mogą nieść ze sobą ryzyko

Unikanie ryzyka może podnieść wagę innych rodzajów ryzyka. Niechęć do podejmowania ryzyka skutkuje:

- decyzją o unikaniu lub ignorowaniu ryzyka niezależnie od dostępnych informacji i ponoszonych kosztów;
- niepodjęciem postępowania wobec ryzyka;
- pozostawianiem istotnych wyborów lub decyzji innym stronom;
- odkładaniem istotnych dla dalszego działania decyzji;
- wyborem opcji, ponieważ oznacza ona potencjalnie niższe ryzyko niezależnie od korzyści.

- *Ograniczenie skutków*

Obniżenie skutków i możliwości wystąpienia można określać nazwą *„kontrola ryzyka"*. Kontrola ryzyka obejmuje określenie względnych korzyści nowych mechanizmów kontrolnych w świetle skuteczności istniejących mechanizmów.

- *Przeniesienie ryzyka*

Obejmuje to ponoszenie przez inną stronę całości lub części ryzyka. Mechanizmy te obejmują zastosowanie kontraktów, ubezpieczeń i in. Przeniesienie ryzyka na inne strony, redukuje ryzyko, ale może nie zmniejszać poziomu ryzyka ogólnego, gdyż podmiot, na który ryzyko zostało przeniesione może nie poradzić sobie ze skutecznym zarządzaniem ryzykiem.

- *Zachowanie ryzyka*

Po obniżeniu lub przeniesieniu ryzyka, mogą istnieć ryzyka szczątkowe, które zostają zachowane. Należy wprowadzić plany zarządzania następstwami tych obszarów ryzyka jeśli one wystąpią, w tym identyfikacji środków finansowania ryzyka. Ryzyko nadmiarowe może także zostać zachowane na skutek braku prawidłowego działania, tzn. gdy nie zidentyfikowano lub nie przyjęto innego sposobu postępowania wobec ryzyka.

Ocena opcji postępowania wobec ryzyka

Wybór najbardziej odpowiedniej opcji obejmuje wyważenie kosztu implementacji pod względem uzyskanych korzyści. Ogólnie, koszt zarządzania ryzykiem musi być proporcjonalny do uzyskanych korzyści.

Decyzje powinny uwzględniać potrzebę uważnego rozważenia rzadkich, lecz poważnych rodzajów ryzyka, co może uzasadniać środki będące nie do uzasadnienia na zasadach ściśle ekonomicznych.

Na ogół negatywny wpływ ryzyka powinien być obniżony w możliwie jak najwyższym stopniu, niezależnie od wszelkich absolutnych kryteriów.

Jeśli poziom ryzyka jest wysoki, ale znaczne możliwości mogą powstać dzięki podjęciu ryzyka, jak np. wykorzystanie nowej technologii, akceptacja ryzyka musi być oparta na ocenie kosztu postępowania wobec ryzyka i kosztu usunięcia potencjalnych skutków w porównaniu z możliwościami zyskiwanymi dzięki podjęciu ryzyka.

Monitorowanie i inspekcje

Ciągłe sprawdzanie ryzyka ma zasadnicze znaczenie dla zagwarantowania aktualności planu zarządzania. Czynniki, które mogą wpływać na możliwość wystąpienia i skutki mogą się zmieniać, to samo dotyczy czynników, które dotyczą przydatności, czy kosztu poszczególnych opcji postępowania. Dlatego jest konieczne, aby regularnie powtarzać cykl zarządzania ryzykiem. Inspekcja jest integralną częścią planu zarządzania ryzykiem.

Rejestr ryzyka

Dla każdego zidentyfikowanego ryzyka, rejestr powinien zawierać:

- źródło;
- charakter;
- istniejące mechanizmy kontrolne;
- skutki i możliwość wystąpienia;
- wstępną klasyfikację ryzyka; i
- podatność na czynniki zewnętrzne/wewnętrzne.

Harmonogram postępowania wobec ryzyka plan działania

Dokument postępowania wobec ryzyka i plan działania dokumentuje przyjmowane mechanizmy kontrolne i wyszczególnia następujące informacje:

- kto jest odpowiedzialny za implementację planu;

- jakie zasoby będą wykorzystane;
- alokację środków;
- harmonogram implementacji;
- szczegóły mechanizmu i częstotliwość kontroli jego zgodności z planem postępowania.

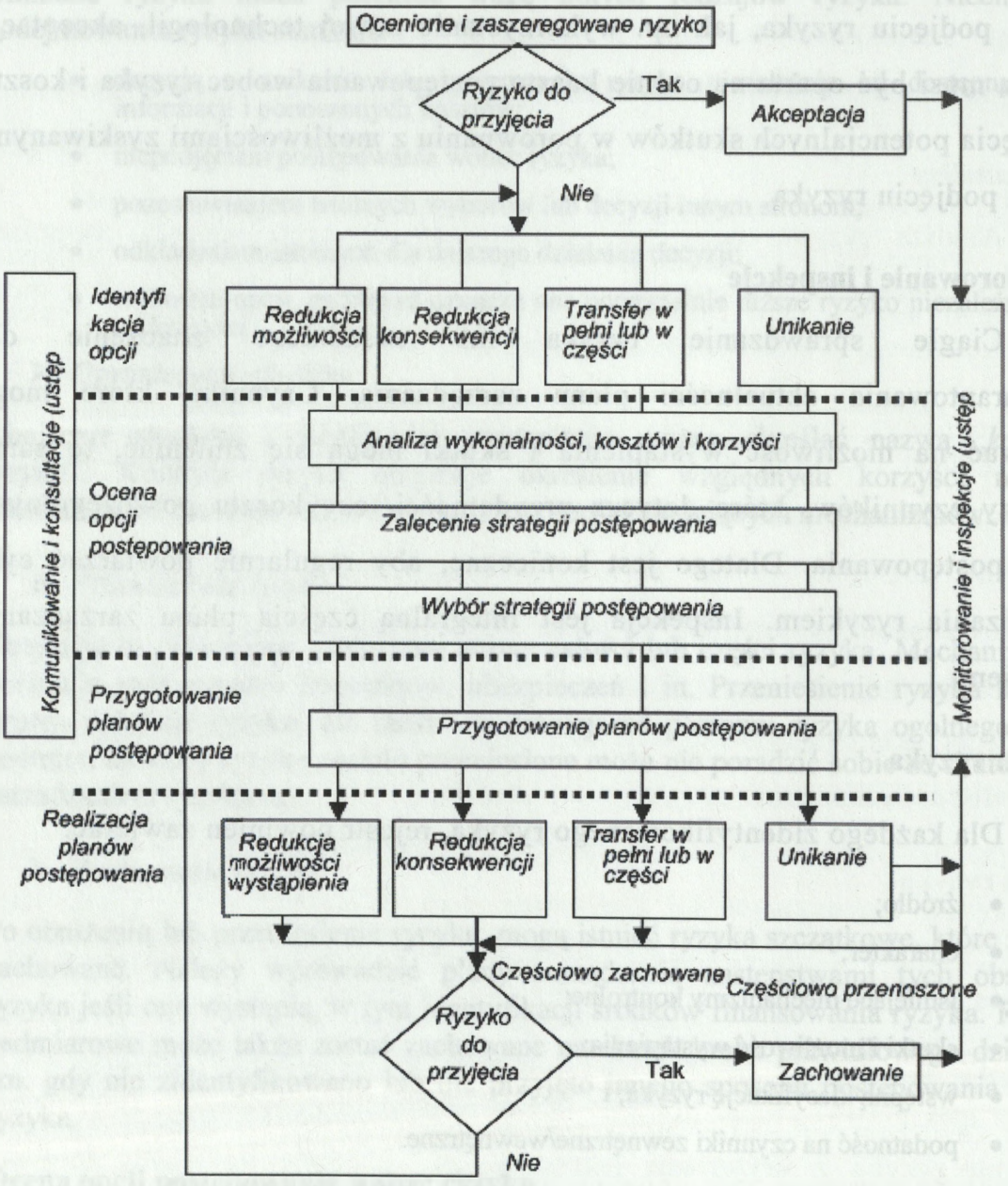


Diagram 42: ***Proces postępowania wobec ryzyka***

Źródło: Wiśniewski A. *Analiza ryzyka. Wytyczne dla administratorów systemów.* AZW Warszawa 2000

Wszyscy zdajemy sobie sprawę, że efektywne działania w dziedzinie zabezpieczenia i ochrony informacji wymagają znalezienia z jednej strony równowagi pomiędzy kosztem zabezpieczeń a osiągniętym poziomem bezpieczeństwa, a z drugiej strony skutecznością tych działań. Skuteczne działania zależną od osiągnięcia i utrzymywania wysokiego poziomu fachowości i świadomości osób funkcyjnych. Aby to osiągnąć należy bezwzględnie stworzyć program działań uświadamiających, szkoleniowych, motywujących i dyscyplinujących. Program, odpowiadający założeniom wynikającym z profesjonalnie realizowanej analizie zagrożeń powinien obejmować wszystkie szczeble organizacyjne i musi być jednocześnie dostosowany do ich specyfiki.

Bezpieczeństwo informacji nie jest stanem stałym i jednorazowym, musi być ono podtrzymywane i permanentnie monitorowane. Należy kontrolować wpływ zmian otoczenia na bezpieczeństwo, rozliczać je i sprawdzać. Tylko takie konsekwentne działania są właściwe i mogą przynieść pożądany skutek.

Diagram 42. Proces postępowania wobec ryzyka

Źródło: Wiśniewski A., *Analiza ryzyka. Wytyczne dla administratorów systemów*, AZW Warszawa 2000

6. Zakończenie - wnioski

W celu uzyskania pełnego obrazu oczekiwań XXI wieku niezbędna jest refleksja dotycząca kilku kwestii zasadniczych, wobec których Europa i poszczególne kraje mają własną strategię, w tym dążenie do poprawy bezpieczeństwa i stabilizacji *„starego kontynentu"* . Wśród wielu wyzwań, za najważniejsze dla Europy i Polski należy uznać:

- *globalną presję demograficzną, wynikającą z wydłużenia przeciętnego czasu życia i szybkiego przyrostu naturalnego; przewiduje się, ze liczba ludności krajów rozwiniętych nie wzrośnie znacznie w ciągu najbliższego stulecia, ale ludność krajów rozwijających się może w tym czasie zwiększyć się trzykrotnie;*
- *eskalację nacjonalizmu i fundamentalizmu religijnego, zjawiska szczególnie niepokojące w krajach o wysokim odsetku ludności pochodzenia islamskiego;*
- *nasilający się* ***terroryzm międzynarodowy*** *o nieobliczalnych skutkach, wpływający bezpośrednio i pośrednio na kształt stosunków międzynarodowych i spójność sojuszniczą;*
- *wzrost przestępczości „wirtualnej", przeradzającej się w* ***cyberterroryzm****, przełamujący dotychczasowe „tradycyjne" incydenty komputerowe w kierunku* ***zsynchronizowanych uderzeń na systemy i sieci teleinformatyczne*** *przy jednoczesnym zróżnicowaniu źródeł pochodzenia ataków, miejsca pobytu sprawcy i lokalizacji obiektów ataku;*
- *zagrożenie środowiska naturalnego, wywołane przez presję demograficzną i przez zrozumiałe dążenie ludności krajów rozwijających się do poprawy standardu życia, często z powtórzeniem modelu konsumpcji i stylu życia w krajach rozwiniętych - co wywołuje zwiększone potrzeby energetyczne, powodujące niszczenie terenów zielonych, zanieczyszczanie atmosfery itp.;*
- ***zwiększającą się rolę technologii informacyjnych i telekomunikacyjnych, globalizację systemów informacyjnych, która sprawia, ze informacja staje się jednym z zasadniczych zasobów produkcyjnych, a jej właściwe wykorzystanie niesie szansę rozwiązania niektórych dylematów zarysowanych wyżej;***
- *globalizację rynków towarów i usług, która z jednej strony ułatwia rozwiązanie części wskazanych problemów, z drugiej strony jednak silniej akcentuje pojawiające się nierówności rozwojowe, wzmagając m.in. tendencje i presje migracyjne.*

Powyższe wyzwania nie mogą być traktowane jako jednoznaczne zagrożenia, ale wpływają one na strategie rozwojowe wszystkich krajów i regionów świata.

Każda rewolucja techniczna wywołuje unowocześnienie instytucji społecznych, politycznych i gospodarczych, a także militarnych. *Informacja* stała się zasobem strategicznym i musi być przedmiotem szczególnej ochrony, zwłaszcza, że liczba rzeczywistych i potencjalnych zagrożeń, jak wykazano w rozprawie, jest znaczna.

Przedstawione w niniejszej pracy uwarunkowania dotyczące ochrony informacji niejawnych przedstawiają obecny stan bezpieczeństwa informacyjnego. Niewątpliwie członkostwo w NATO i w Unii Europejskiej będzie powodowało ewolucję i dostosowywanie polskiego prawa w zakresie ochrony informacji niejawnych do międzynarodowych standardów. Jednym z elementów polityki informacyjnej powinno się stać wymuszanie zmian w systemie regulacji prawnych, zgodnie z ideą *Kompleksowego Zarządzania Jakością TQM,* zmian sprzyjających skutecznym zabezpieczeniom „*infosfery*" przed różnymi zagrożeniami, tak aby przestępstwa komputerowe były traktowane podobnie jak pozostałe przestępstwa skierowane przeciw państwu, przeciw obronności kraju i przeciw własności. Wzrost liczby przestępstw komputerowych - połączonych z coraz szerszą inwigilacją różnych dziedzin życia społecznego - wynika z gwałtownego rozwoju sieci teleinformatycznych i powszechności komputerów domowych, spełniających funkcje terminali. Istotną cechą zjawiska przestępczości komputerowej jest to, że dla sprawcy nie istnieją granice geograficzne ani polityczne, łatwiej jest zachować anonimowość i zatrzeć ślady działalności.

Rozwój systemów teleinformatycznych i telekomunikacyjnych przyniósł wiele niekwestionowanych korzyści społecznych. Stworzył techniczne i organizacyjne przesłanki nowej fazy rozwoju cywilizacji - społeczeństwa informacyjnego, czyli społeczeństwa bogatego w informację (*wiedzę*) i czerpiącego z niej swój dobrobyt. Z chwilą kiedy informacja stała się dobrem podlegającym powszechnemu obrotowi, nadającym się do szybkiego, automatycznego przetwarzania oraz różnorodnego wykorzystania (zwłaszcza komercjalnego), jej znaczenie gospodarcze i społeczne gwałtownie wzrosło. Wraz ze wzrostem technicznych możliwości dostępu do zasobów informacyjnych i wymiany informacji zrodziło się nieznane dotychczas zagrożenie jej

bezprawnym i nieuczciwym wykorzystaniem. Występuje zatem potrzeba ograniczenia wolności informacji ze względu na ochronę interesów jej wytwórców, dysponentów oraz osób których informacja dotyczy. Ustawodawcy tworzący przepisy prawa, normujące określone kategorie stosunków społecznych, nie mogli w tej sytuacji pozostać obojętni. Zarówno informację, jak i sposoby jej zabezpieczenia, objęto regulacjami prawnymi. Właśnie te rozwiązania prawne starano się pokazać w niniejszej rozprawie, dodatkowo je rozszerzając o aspekty prawa unijnego.

Tak, jak wielkie są szanse rozwoju *„infosfery"* i różne nadzieje ludzkości w tej dziedzinie, tak wielkie też wydają się i zagrożenia. Te z nich, które można z dużym prawdopodobieństwem przewidzieć, scharakteryzowano w niniejszej pracy. Najważniejsze jest wdrożenie metod i środków zabezpieczenia, które mogą zwiększyć stopień bezpieczeństwa systemów teleinformatycznych i sieci zapewniających integrację usług telekomunikacyjnych. Należy unikać szablonowego podejścia do wdrażania architektury bezpieczeństwa, przewidywać nieznane obecnie możliwości uzyskiwania dostępu do informacji podlegających ochronie. Skuteczność nawet najlepiej zaprojektowanych zabezpieczeń zależy od ludzi. Potrzeba ochrony informacji w państwie demokratycznym opartym na konstytucyjnych swobodach obywateli jest uzasadniona żywotnymi interesami państwa. Dotyczy to przede wszystkim informacji dotyczących najważniejszych dziedzin działalności państwa, takich jak: rozpoznawanie zagrożeń dla bezpieczeństwa państwa, funkcjonowanie jego systemu kierowania, systemu obronnego i organizacji sił zbrojnych - elementów stanowiących tajemnicę państwową. Ochroną tych informacji zajmują się wyspecjalizowane służby.

Nadal, pomimo różnych, przewidzianych stosownymi przepisami zabezpieczeń dla informacji niejawnych, najważniejszym czynnikiem pozostaje człowiek, jako wytwórca, użytkownik i odbiorca informacji niejawnych. To ze strony człowieka istnieje największe zagrożenie dla właściwej ochrony informacji, zarówno stanowiących tajemnicę państwową jak i służbową. Również od czynnika ludzkiego zależy właściwa realizacja procedur analizy zagrożeń i zarządzania ryzykiem informacyjnym.

W niniejszej rozprawie, w ***Rozdziale 1.3.2*** sformułowano hipotezy dotyczące stanu i perspektyw bezpieczeństwa informacyjnego państwa. Podzielono je na grupy problemowe:

1. ***Hipotezy dotyczące słabych stron polskiego systemu bezpieczeństwa informacyjnego.***
2. ***Hipotezy dotyczące możliwości wdrożenia narzędzi wspomagających politykę bezpieczeństwa informacyjnego państwa.***
3. ***Hipotezy dotyczące zakresu i sposobu realizacji przedsięwzięć zapewniających bezpieczeństwo informacyjne państwa.***

Celem weryfikacji przyjętych założeń autor rozprawy przeanalizował przyjęte w ***Rozdziale 1.1*** zmienne, mające wpływ na potwierdzenie lub podważenie hipotez:

- ***zmienne zależne:*** wartość informacji pola walki, jakość narzędzi analiz i pomiarów bezpieczeństwa informacyjnego, jakość programów i metod nauczania i szkolenia w zakresie bezpieczeństwa informacyjnego, nakłady na bezpieczeństwo informacyjne;
- ***zmienne niezależne:*** stan prawny w zakresie bezpieczeństwa informacyjnego, narodowe normy i kryteria bezpieczeństwa, elementy wzorcowe NATO i państw Unii Europejskiej, dostosowanie standardów bezpieczeństwa do wymogów NATO i UE;
- ***zmienne pośredniczące:*** metody analizy zagrożeń i zarządzania ryzykiem, problematyka certyfikacji i akredytacji, zapewnienie elastyczności rozwiązań wobec wymogów współczesnych operacji informacyjnych.

Analizując zmienne zależne można wykazać, że w rozprawie przeprowadzono, oparty na modelowaniu matematycznym, wywód o determinującej roli informacji na współczesnym polu walki, zarówno pod kątem doboru środków (sensorów) *walki informacyjnej*, jak i miar efektywności informacji w przebiegu działań bojowych w oparciu o przykładowe operacje (***Rozdział 2.3***). Jednocześnie zweryfikowano pozytywnie hipotezę o wpływie wykorzystywania własnych, sojuszniczych i europejskich narzędzi bezpieczeństwa informacyjnego na realizację zasady uzyskiwania przewagi informacyjnej (*dominacji*), przy spełnieniu warunku zapewnienia wysokiej jakości wykorzystywanym narzędziom analitycznym i nadaniu wysokiej rangi procesom szkolenia w zakresie bezpieczeństwa informacyjnego. Mniej miejsca poświęcono sprawie nakładów na szeroko pojęte *bezpieczeństwo informacyjne*, ograniczając się do stwierdzenia (wykazano w analizie narzędzi

zarządzania ryzykiem) o wpływie odpowiednio dobranych narzędzi analizy zagrożeń na optymalizację kosztów zabezpieczeń. Tym samym potwierdzono hipotezę o potrzebie upowszechnienia nowoczesnych ***metod i narzędzi*** *pomiaru i analizy zagrożeń bezpieczeństwa informacyjnego* jako warunku zapewnienia bezpieczeństwa informacyjnego państwa.

Biorąc pod uwagę przyjęte *zmienne niezależne* wykazano, że legislacyjna baza bezpieczeństwa informacyjnego państwa wymaga dalszego dostosowania do wymogów NATO i Unii Europejskiej, zarówno w odniesieniu do zasadniczych aktów prawnych, jak i do unormowań niższego rzędu, m.in. w zakresie *Wspólnych Kryteriów Oceny* (***Rozdział 3.1)***. Uzupełniając aspekt prawny bezpieczeństwa informacyjnego o informacje dotyczące naruszeń bezpieczeństwa i występujących zagrożeń dla systemów i sieci teleinformatycznych (***Rozdział 3*** i ***4.1)*** potwierdzono hipotezy grupy drugiej.

Intensywny rozwój technik informatycznych, dający coraz większe możliwości w zakresie wytwarzania, przetwarzania, przesyłania i przechowywania informacji – dokumentów niejawnych, nie może się odbywać bez równoległego poszukiwania nowych i bezpiecznych form ochrony systemów informatycznych. Analizowane przy weryfikacji hipotez *zmienne pośredniczące*, mające wpływ na model procesu analizy zagrożeń i zarządzania ryzykiem bezpieczeństwa informacyjnego (***Rozdział 4.2*** i ***4.3)***, potwierdzają potrzebę korelowania ***rozwoju narzędzi przetwarzania informacji*** z procesami ***zapewniania jej bezpieczeństwa,*** co stanowi przesłankę interoperacyjnego związania narodowego systemu bezpieczeństwa informacyjnego z sojuszniczym i unijnym. Ujęcie tej problematyki w ramy procesów *Kompleksowego Zarządzania Jakością TQM* (***Rozdział 5***) pozwoliłoby na połączenie jakości wypracowanych narzędzi analizy zagrożeń i zarządzania ryzykiem bezpieczeństwa informacyjnego z możliwością ich ciągłego doskonalenia. Stanowi to potwierdzenie trzeciej grupy hipotez badawczych.

Formułując ***wnioski*** z przeprowadzonych badań i zamieszczonych w niniejszej, objętej *grantem KBN jako projekt badawczy Nr O T00A 012 23* rozprawy, należy stwierdzić, że analiza zagrożeń i zarządzanie ryzykiem stanowią istotne elementy w tworzeniu szczególnych wymagań bezpieczeństwa systemu informacyjnego. Otrzymana w

wyniku przeprowadzenia tego procesu wiedza umożliwia dobór koniecznych środków ochrony, optymalny zarówno ze względu na wymagania bezpieczeństwa dla informacji niejawnych przetwarzanych w systemie, jak i ze względu na konieczne nakłady finansowe.

Przeprowadzona w sposób właściwy ***analiza zagrożeń*** da pewność, że wszystkie prawdopodobne ryzyka zostały zidentyfikowane, a dobrane w wyniku procesu ***zarządzania ryzykiem*** środki ochrony zabezpieczą w stopniu wystarczającym informacje niejawne.

Należy jednak mieć świadomość, że ryzyko można oszacować i zredukować, ale nie da się go wyeliminować całkowicie.

Biorąc pod uwagę wszelkie możliwe zagrożenia dla bezpieczeństwa informacyjnego państwa można przyjąć, że osiągnięcie całkowitego bezpieczeństwa nie jest możliwe, lecz analiza przewidywanych zagrożeń, prowadzona jako część procesu zarządzania ryzykiem, pozwala przedstawić w sposób kompleksowy zagrożenia dla informacji i określić czynności związane z ich neutralizacją.

Większość potencjalnych zagrożeń pochodzi z niezamierzonych lub celowych działań wewnętrznych, jest wynikiem braku wiedzy i praktyki lub braku świadomości zagrożeń na poziomie użytkownika lub administratora systemu.

Korzyścią z zastosowania *procesu zarządzania ryzykiem* jest wzrost świadomości zagrożeń na wszystkich poziomach jednostki organizacyjnej, od kierownictwa odpowiedzialnego za zarządzanie do użytkowników i personelu pomocniczego. Wzrost świadomości zagrożeń wzmacnia bezpieczeństwo informacyjne obiektu, systemu, organizacji i państwa.

Wysiłek i wiedza ekspercka zaangażowane w wykonanie analizy zagrożeń i w zarządzanie ryzykiem informacyjnym powinny być postrzegane równolegle i równoważnie z procesami tworzenia infrastruktury informacyjnej.

Jeżeli niniejsza rozprawa przyczyni się do wzrostu świadomości roli informacji w systemie bezpieczeństwa państwa i poszerzy wiedzę o metodach zarządzania ryzykiem w procedurach bezpieczeństwa informacyjnego – jej cel zostanie osiągnięty.

BIBLIOGRAFIA

Literatura przedmiotu

1. Abrams M.D., Bailey D. *Abstraction and Refinement of Layered Security Policy* [w:] Abrams M. D., Jajodia S., Podell H.J. *Information Security - an Integrated Collection of Essays*, IEEE Computer Society Press, Los Alamos, California 2001.
2. Abrams M.D., Podell H.J. *Supporting Policy and Functions* [w:] Abrams M. D., Jajodia S., Podell H.J. *Information Security - an Integrated Collection of Essays.* IEEE Computer Society Press, Los Alamos, California.
3. Adamski A. *Prawo karne komputerowe.* Warszawa 2000.
4. Ahuja V. *Bezpieczeństwo w sieciach.* ZNI *MIKOM,* Warszawa 1997.
5. Ajdukiewicz K. *Logika pragmatyczna.* PWN, Warszawa 1965.
6. Alcove D., Seger K., Von Storch W. *Computer Crime: A Crimefighter's Handbook,* Sebastopol 1995.
7. Alexander C., Pal L., *Digital Democracy: Policy and Politics in the Wired World.* Oxford 1998.
8. Amoroso E. G. *Fundamentals of Computer Security Technology.* Upper Saddle.
9. Andrukiewicz E. *Rola polityki bezpieczeństwa w systemach i sieciach teleinformatycznych przetwarzających informacje niejawne.* IT Security Magazine Nr 1, 1999.
10. Andrukiewicz E. *Wybór strategii zarządzania ryzykiem w procesie planowania zabezpieczeń.* Instytut Łączności, Warszawa 2000.
11. Andrukiewicz E. *Dostęp kontrolowany.* PCkurier, marzec 1999.
12. Arquilla J., Ronfeldt D. (red.). *Countering the New Terrorism*, Santa Monica 1999.
13. Arquilla J., Ronfeldt D. (red.). *In Athena's Camp.* Santa Monica 1997.
14. Balcerowicz B. *Wybrane problemy obronności państwa.* AON, Warszawa 2001.
15. Balcerowicz B. *Czy grozi nam wojna światowa? Cel: wola wroga.* Polityka Nr 4, 2000.
16. Banaszak B., Wygoda K. *Regulacja prawna ochrony danych osobowych w Polsce w świetle Ustawy z dn. 29 sierpnia 1997 r. i standardów europejskich.* [w:] Wyrzykowski M. (red.): *Ochrona danych osobowych.* Instytut Spraw Publicznych, Warszawa 1999.
17. Barczak A. *Komputerowe gry wojenne.* Warszawa 1996.
18. Bauman Z. *Globalizacja i co z tego dla ludzi wynika.* Warszawa 2000.

19. Białas A. *Wprowadzenie do problematyki certyfikacji środków sprzętowych i programowych zapewniających bezpieczeństwo informacji.* IT Security Magazine Nr 10, 2000.

20. Białas A. *Budowa zaufania do zabezpieczeń teleinformatycznych poprzez ich ocenę i certyfikację;* [w:] Grzywak A. [red]: *Internet w społeczeństwie informacyjnym.* Wyd. WSB, Dąbrowa Górnicza 2003.

21. Bierć A. *Ochrona prawna danych osobowych w sferze działalności gospodarczej w Polsce.* [w:] Wyrzykowski M. (red.): *Ochrona danych osobowych.* Instytut Spraw Publicznych, Warszawa 1999.

22. Bógdał-Brzezińska A., Gawrycki M. F. *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie.* FSM Warszawa 2003.

23. Bolter J. D. *Człowiek Turinga.* Warszawa 1990.

24. Bosh L. *Netherlands Annual Review of Military Studies.* Mollema 1999.

25. Brancato J. D. & Ferris M. *The Net.* USA 1995.

26. Brieskorn N. *Ochrona danych osobowych a zagrożenia prywatności.* [w:] Wyrzykowski M. (red.): *Ochrona danych osobowych.* ISP, Warszawa 1999.

27. Brinkley D.L., Schell R.R. *What is there to Worry About?* [w:] Abrams M. D., Jajodia S., Podell H.J. *Information Security - an Integrated Collection of Essays*, IEEE Computer Society Press, Los Alamos, California 1995).

28. Buchała K. *Reforma polskiego prawa karnego materialnego. Przestępstwa przeciwko ochronie informacji i oszustwo komputerowe.* Warszawa 1999.

29. Buchała K., Szewczyk M., Ćwąkalski Z., Zoll A. *Komentarz do kodeksu karnego. Część ogólna.*, Warszawa 1990.

30. Buchan G. *Information Warfare and the Air Force: Wave of Future?* USA 1995.

31. Caelli W., Longley D., Shain M.. *Information Security Handbook.* Macmillan Publishers Ltd. 1991.

32. Castells M. *The Information Age: Economy, Society and Culture.* London 1996

33. Castells M. *The Power of Identity.* Malden 1997.

34. Castells M. *The Rise of the Network Society.* Oxford 1996.

35. Cendrowski J. *Tajemnice prawnie chronione i informacje niejawne.* IT Security Magazine Nr 1, 1999.

36. Cendrowski J. *Wybrane aspekty zmian w przepisach o chronione informacji niejawnych.* IT Security Magazine Nr 20, 2001.

37. Cendrowski J., Kośla R. *Rola kryteriów oceny zabezpieczeń teleinformatyki dla bezpieczeństwa teleinformatycznego polskiej administracji publicznej XXI w.* IT Security Magazine Nr 6-7, 2001.

38. Cendrowski J., Owsiejczyk W. *Ochrona informacji niejawnych – uzupełnienie*. IT Security Magazine, Nr 5-6, 2000.

39. Cendrowski J., Owsiejczyk W. *Ochrona informacji niejawnych cz. 4. Ochrona elektromagnetyczna*. IT Security Magazine Nr 3, 2000.

40. Cendrowski J. *Polityka bezpieczeństwa a ochrona danych osobowych*. IT Security Magazine Nr 5-6, 2000.

41. Cendrowski J. *Ochrona informacji niejawnych w systemach i sieciach teleinformatycznych*. IT Security Magazine Nr 1- 2, 2000.

42. Chapman, C.B. (1991). *Risk in investment, procurement and performance in construction*. E&F Spon.

43. Charette R. *Software Engineering Risk Analysis and Management*. Paris 1998.

44. Cheswick W. R. Bellovin S. M. *Firewalls and Internet Security*. London 1997.

45. Ciborowski L. *Walka informacyjna*. ECE, Wyd. Adam Marszałek, Toruń 1999.

46. Ciborowski L. *Zautomatyzowane systemy dowodzenia taktycznymi wojsk lądowych: analiza rozwiązań światowych*. Warszawa 1996.

47. Clark D., David & David Wilson. *Proceedings*. IEEE USA1987.

48. Clausewitz K. von. *O wojnie*. Warszawa 1958.

49. Cleaver H. *The Chiapas Uprising and the Future of Class Struggle*. USA 1992.

50. Czaputowicz J. *System czy nieład? Bezpieczeństwo europejskie u progu XXI wieku*. Warszawa 1998.

51. Czechowski R., Sienkiewicz P. *Przestępcze oblicza komputerów*. Wydawnictwo Naukowe PWN, Warszawa 1993.

52. Darilek R. , Perry W., Bracken J., Gordon J., Nichiporuk B. *Measures of Effectivness for the Information - Miary Efektywności Dla Armii Wieku Informacyjnego* – RAND Corp. Santa Monica 2000.

53. Denning D. *Wojna informacyjna i bezpieczeństwo informacji*, Warszawa 2002.

54. Deyson E. *Przepis na życie w epoce cyfrowej*. Warszawa 1999.

55. Dobosz I. *Tajemnica korespondencji jako dobro osobiste i jego ochrona w prawie*. Warszawa 2000.

56. Dobosz M. *Wspomagana komputerowo statystyczna analiza wyników badań*. Warszawa 2001

57. Dordic H., Wang G. *The Information Society. A Retrospective View*. London 1995.

58. Doroziński D. *Hakerzy. Technoanarchiści cyberprzestrzeni*. Gliwice 2001.

59. Drucker P. F. *The Age of Discontinuity*. New York 1968.

60. Drzewiecki Z. *Ustawa o ochronie danych osobowych w pigułce.* [w:] *Praktyczne konsekwencje obowiązywania ustawy o ochronie danych osobowych.* Seminarium Stowarzyszenia Marketingu Bezpośredniego, Warszawa 1999.

61. Dutton, W. (red.). *Society on the Line: Information Politics in the Digital Age.* Oxford 1999.

62. Eco U. *Diariusz najmniejszy.* Kraków 1995.

63. Elin N. (red.). *Architecture of Fear.* New York 1997.

64. Ellul J. *La technique ou l'enjeu du siecle.* Paris 1954.

65. Estabrooks M. *Electronic Technology, Corporate Strategy and World Transformation.* Westport 1995.

66. Fajgielski P. *Polityka w zakresie praw człowieka na przykładzie ochrony danych osobowych* (Wrocław, 18 - 19 czerwca 1999 r.) [w:] *Państwo i Prawo* Nr 9/1999.

67. Fajgielski P. *Przetwarzanie i ochrona danych* (Ustroń, 2 - 4 grudnia 1998 r.). [w:] *Państwo i Prawo* Nr 4/1999.

68. Finne T. *Analyzing Information Security: Knowledge-Based DSS Approach.* Abo Akademie University, Institute for Advanced Management Systems Research. Finland 1996.

69. Fiołny Z. *Organizacja taktycznych sieci łączności.* Materiały z sympozjum naukowego. Warszawa 2001.

70. Flakiewicz W. *Systemy informacyjne przedsiębiorstw i instytucji.* PWE Warszawa 1987.

71. Forystek M. *Analiza ryzyka infrastruktury IT.* Warszawa 2000.

72. Franklin J. (red.). *The Politics of Risk Society.* Cambridge 1998.

73. Fukuyama F. *Koniec historii.* Warszawa 1991.

74. Fukuyama F *Wielki wstrząs.* Warszawa 2000.

75. GAO V. *United State General Accounting Office, Executive Guide: Information Security Management* 1998.

76. Garfinkel S., Spafford G. *Bezpieczeństwo w Unix'ie i Internecie.* Warszawa 1997.

77. Garstka A., Hayes R., Signori D. *Understanding Information Age Warfare.* Materiały z sympozjum . Warszawa, czerwiec 2002.

78. Gattiker U. E. *Uniting Efforts for Protecting Critical IT Infrastructure.* Kopenhaga 2002.

79. Giddens A. *Trzecia droga. Odnowa socjaldemokracji*, Warszawa 1999.

80. Gilbert I.E. *Guide for selecting automated risk analysis tools.* NIST, USA 1989.

81. *Global Networks and Local Values. A Comparative Look at German and the United States*. New York 2002.

82. Goban-Klas T. *Media i komunikowanie masowe*. Warszawa 1999.

83. Goban-Klas T., Sienkiewicz P. *Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania*. Wydaw. Fundacji Postępu Telekomunikacji. Kraków 1993.

84. Godzić W. (red.). *Humanista w cyberprzestrzeni*. Kraków 1999.

85. Goodell J., *Hacker i samuraj*. Gdańsk 1996.

86. Grzywak A. *Bezpieczeństwo Systemów Komputerowych* – praca zbiorowa. Politechnika Śląska 2001.

87. Guehenno, J. M. *The End of the NationState*. Minneapolis 1995.

88. Hager N., *Secret Power*: *New Zealand's Role in the International Spy Network*. Nelson 1996.

89. Haliżak E., Parzymies S. (red.). *Unia Europejska. Nowy typ wspólnoty międzynarodowej*. Warszawa 2002.

90. Haliżak E., Popiuk-Rysińska L. (red.., *Państwo we współczesnych stosunkach międzynarodowych*. Warszawa 1995.

91. Hamm R. *Ochrona danych a prawo karne*.[w:] Wyrzykowski M. (red.): *Ochrona danych osobowych*. Instytut Spraw Publicznych, Warszawa 1999.

92. Handy Ch. *Wiek paradoksu. W poszukiwaniu sensu przyszłości*. Warszawa 1996.

93. Harvey R. *The Return of the Strong*. London 1995.

94. Heldrich A. *Ochrona osobowości a wolność prasy*.[w:] Wyrzykowski M. (red.): *Ochrona danych osobowych*. Instytut Spraw Publicznych. Warszawa 1999.

95. Herman A, Swiss T. *The World Wide Web and Contemporary Cultural Theory*. Routledge, New York 2000.

96. Hirst P., Thomson G. *Globalization in Question*. Cambridge 1996.

97. Hoffman B. *Oblicza terroryzmu*. Warszawa 1999.

98. Howard J. D., Longstaff T.A. *A Common Language for Computer Security Incidents*. Część I. Springfield 1998.

99. Howard J. D., Longstaff T.A. *A Common Language for Computer Security Incidents*. Część II. Springfield 1998.

100. Huntington S. *Trzecia fala demokratyzacji*. Warszawa 1996.

101. Huntington S. *Zderzenie cywilizacji*. Warszawa 1997.

102. Icove D., Seger K., VonStoch W. *Computer Crime – A Crimefighter's Handbook*. O'Reilly & Associates, Inc, USA 1995.

103. Janczak J. *Zakłócanie informacyjne*. Warszawa 2001.

104. Jedynak A. *Conference Roadshow - newest Microsoft technologies: Microsoft Solution Framework.* Warsaw 2000.

105. Jemioło T. *Globalizacja. Szanse i zagrożenia.* AON 5215/2000, Warszawa 2000

106. Jemioło T. Malak K. (red.) *Bezpieczeństwo zewnętrzne Rzeczypospolitej.* AON 2000.

107. Jonscher C. *Życie okablowane.* Warszawa 2001.

108. Kerberos. *Ocena poziomu bezpieczeństwa systemu informatycznego.* Warszawa 2000.

109. Kilian W. *Ochrona danych w przedsiębiorstwach.* [w:] Wyrzykowski M. (red.): *Ochrona danych osobowych.* Instytut Spraw Publicznych, Warszawa 1999.

110. Kisielnicki J., Sroka H. *Metody projektowania i wdrażania systemow.* Placet, Warszawa 1999.

111. Kleer J. (red.). *Globalizacja.* Łódź 2000.

112. Kleinrock L. *Communication Nets: Stochastic Message Flow and Delay.* New York 1964.

113. Kleinrock L. *Queuing Systems: Vol II, Computer Applications.* New York 1976.

114. Konarski X. *Ustawa o ochronie danych osobowych a doświadczenia państw Unii Europejskiej.* [w:] *Praktyczne konsekwencje obowiązywania ustawy o ochronie danych osobowych.* Seminarium Stowarzyszenia Marketingu Bezpośredniego, Warszawa 1999.

115. Konieczny J. *Inżynieria systemów.* WNT. Warszawa 1983.

116. Konieczny K., Rabiej B. *Radiodostęp w taktycznej sieci telekomunikacyjnej.* Warszawa 1998.

117. Kostyra T. *Ustawa o ochronie danych osobowych a działalność instytucji finansowych.* [w:] *Praktyczne konsekwencje obowiązywania ustawy o ochronie danych osobowych.* Seminarium Stowarzyszenia Marketingu Bezpośredniego, Warszawa 1999.

118. Koziej S. *Koncepcja wspólnego bezpieczeństwa w Europie a obronność Polski.* [w]: *Wystarczalność Obronna*, Warszawa 1996.

119. Koziej S. *Rajdy bojowe.* Warszawa 1987.

120. Koziej S. *Teoria sztuki wojennej.* Warszawa 1993.

121. Krause M., Tipton H.F. *Handbook of Information SecurityManagement.* CRC Press LLC 1999.

122. Kuczyński R. W. *Społeczeństwo informacyjne. Cyberkultura. Sztuka multimediów.* Kraków 2001.

123. Kulesza E. *Ochrona danych osobowych a nowa kodyfikacja prawa karnego w Polsce.* [w:] Wyrzykowski M. (red.): *Ochrona danych osobowych. Instytut Spraw Publicznych*, Warszawa 1999.

124. Kulesza E. *Pozycja i uprawnienia Generalnego Inspektora Ochrony Danych Osobowych w świetle Ustawy o ochronie danych osobowych. Uwagi de lege lata i de lege ferenda.* [w:] Przegląd Sejmowy Nr 6 (35) /1999.

125. Kunicka-Michalska B. *Nowe przepisy o ochronie tajemnicy państwowej i służbowej*. PiP, Nr 11/1983.

126. Kunicka-Michalska B. *Ochrona tajemnicy w kodeksie karnym, Akta Universitatis Nicolai Copernici* 1978; tejże - *Ochrona tajemnicy zawodowej w polskim prawie karny.*, Warszawa 1972.

127. Kurzępa B. *Przestępstwa z ustawy o ochronie danych osobowych.* [w:] *Prokuratura i Prawo* Nr 6/1999.

128. Kushner H. W. (red.). *The Future of Terrorism: Violence in the New Millennium*. Thousand Oaks 1998.

129. Kusina B. *Pakiety dokumentacyjne polityki bezpieczeństwa teleinformatycznego ze szczególnym uwzględnieniem operacyjnych (wykonawczych) procedur bezpieczeństwa oraz wybranych elementow kontroli ITSec.* Enigma 2001; www.bezpieczenstwoIT.pl

130. Kwećka R. *Informacja w walce zbrojnej.* Warszawa 2001.

131. Kyas O. *Internet Security - Risk Analysis, Strategies and Firewalls.* International Thompson Computer Press Milfors, USA 1997.

132. Le Bot Y. *Subcomandante Marcos: El Sueno Zapatista*, Mexico 1997.

133. Lem S. *Bomba megabitowa*. Kraków 1999.

134. Levinson P. *Miękkie ostrze. Naturalna historia i przyszłość rewolucji informacyjnej.* Warszawa 1999.

135. Liang Q., Xiangsu W. *Unrestricted Warfare: Assumption on War and Tactics in the Age of Globalization*. Beijing 1999.

136. Libicki M. *What is Information Warfare*? Washington 1995.

137. Liderman K. *Analiza ryzyka*. WinSecurity Magazine nr 12, 2001 r

138. Liderman K.: *Bezpieczeństwo teleinformatyczne*. BEL. Warszawa 2001.

139. ŁośNowak T. *Stosunki międzynarodowe. Teorie systemy uczestnicy.* Wrocław 2000.

140. Lubacz J. (red.). W *drodze do społeczeństwa informacyjnego*. Warszawa 1999.

141. M. Łobocki. *Metody badań pedagogicznych*. PWN, Warszawa 1978.

142. M. Szewczyk. *Prawnokarna ochrona tajemnicy zawodowej lekarza.* Czasopismo Prawa Karnego i Nauk Penalnych, z. 1/2000.

143. Madej A *Rynek e-commerce wart będzie 5 bin USD*. Computerworld/IDG 25.05.2001.

144. Mąka D. *Elementy analizy zagrożeń i zarządzania ryzykiem w świetle polityki bezpieczeństwa informacyjnego*. IT Security Magazine nr 8-9, 2001.

145. Margolis M., D. Resnick. *Politics As Usual. The Cyberspace „Revolution"*, London 2000.

146. Masuda Y. *Information Society or Postlndustrial Society*. Tokio 1969.

147. Mazurkiewicz W.J. *Projektowanie i ocena wojskowych systemów łączności*. Warszawa 1994.

148. McCaffrey B. R. *The Drug Scourge as a Hemispheric Problem*. Carlisle 2001.

149. McCue B. *Combat Analysis – Lanchester and the Battle of Trafalgar*. Pergamon Press 1999.

150. McLuhan M. *Wybór tekstów*. Poznań 2001.

151. McRae H. *Świat w roku 2020*. Warszawa 1996.

152. Mediamark Research. *Internet Access and Usage fall 2000 –Cybe rStats Report*, www.mediamark.com.

153. Mednis A. *Ochrona danych osobowych a zagrożenia prywatności - rozwiązania polskie*. [w:] Wyrzykowski M. (red.): *Ochrona danych osobowych*. Instytut Spraw Publicznych, Warszawa 1999.

154. Mednis A. *Ustawa o ochronie danych osobowych*. Wydawnictwo Prawnicze PWN, Warszawa 1999.

155. Michniak J. Dokum*enty dowodzenia i łączności materiały z sympozjum naukowego*. Warszawa 2001.

156. Michniak J. *Teoria wojskowych systemów łączności - konspekt wykładów*. Warszawa 1996.

157. Minc A. *Le nouveau moyen age*. Paris 1993.

158. Mitnick K., Simon W. *Sztuka podstępu*. Gliwice 2003.

159. Molander R. C., Riddile A. S., S. A. Wilson. *Strategie Information Warfare: A New Face of Wa.,* Santa Monica 1996.

160. Mrózek A. *Ustawowe prawo ochrony danych*. Wyd. UMK, Toruń 1981.

161. Muszyński A. *Związki struktury gospodarki narodowej z systemem obronnym i jego potencjałem*. *„Materiały i studia WAP"*, Warszawa 1980.

162. Naisbitt J., Megatrendy. *Dziewięć nowych kierunków zmieniających nasze życie*. Poznań 1997.

163. Neumann J. von. *Collected Work , t. IVII*. Oxford 1961-1963.

164. Nowacki G. *Walka informacyjna próby kategoryzacji*. Warszawa 1999.

165. Nowacki T. *Metodologia Pedagogiki Pracy*. WSiP, Warszawa. 1978.

166. Ogryczak W. *Wielokryterialna optymalizacja liniowa i dyskretna*. Wyd. UW, 1997.

167. Ohimae K. *The End of the Nation State: the Rise of National Economies.* 1998.

168. Piotrowski M. *Totalne Zarządzanie Jakością.* ITE-EiP, Radom-Warszawa 1997.

169. Poleski W. *Teoria wojskowych systemów łączności - konspekt wkładu.* Warszawa 1995.

170. Postman N.. *Triumf techniki nad kulturą.* Technopol , Warszawa 1995.

171. Power R. *Tangled Web – Tales of Digital Crime from the Shadows of Cyberspace.* Pergamon Press 1998.

172. *Protecting the Homeland. Report of the Defense Science Board Task Force on Defensive Information Operations.* http://www.dod.us.

173. Raftery J. (). *Risk Analysis in Project Management*, E&FN SPOT 1994.

174. *Rent-a-hacker.* http://www.rent-a-hacker.com/2001

175. Restell P. *BSI-DISC News-sheet BS 7799 - Information security anagement.* BSI. www.bsi-qlobal.com.

176. Rifkin J. *Koniec Galaktyki Internetu.* Poznań 2003.

177. Rogowski S. *Ochrona danych o stanie zdrowia w ubezpieczeniach osobowych.* [w:] *Przegląd Ubezpieczeń Społeczno - Gospodarczych.*Nr 5/1999.

178. Rugała R. *Elementy Koncepcji Operacji Sieciocentrycznych (NCO) w aspekcie Architektury Systemów Dowodzenia.* OBR CTM Gdynia 2003.

179. Safjan M. *Ochrona danych osobowych - granice autonomii informacyjnej.* [w:] Wyrzykowski M. (red.): *Ochrona danych osobowych.* Instytut Spraw Publicznych, Warszawa 1999.

180. Schell R.R., Brinkley D.L. *Evaluation Criteria for Trusted Systems"* [w:] Abrams M., Jajodia S., Podell H. *Information Security an Integrated Collection of Essays*, IEEE Computer Society Press, Los Alamos, California 1995.

181. Senn J.A. *Information Systems in Management.* Wadswort CA 1990.

182. Sibiga G. *Zgłoszenie zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych.* [w:] *Monitor Prawniczy* Nr 8/1999.

183. Sienkiewicz P. *Dowodzenie z Komputerem.* Wyd. MON, Warszawa 1984.

184. Sienkiewicz P. *Inżynieria systemów : wybrane zastosowania wojskowe.* Wyd. MON 1983.

185. Sienkiewicz P. *Teoria efektywności systemów* . Wyd. ZN im. Ossolińskich, Wrocław 1983.

186. Sienkiewicz Piotr. *Człowiek i technika w nowoczesnych systemach dowodzenia.* Zeszyty naukowe AON Nr 3/1992.

187. Sienkiewicz Piotr : *Decyzje i komputery* . Magazyn *Militaria* Nr 2/1995.

188. Sienkiewicz. P. *Analiza systemowa. Podstawy i zastosowania*. Wyd. Bellona, Warszawa 1994.

189. Śmiałek W., Tymanowski J. *Bezpieczeństwo państw i narodów w procesie integracji europejskiej. Systemy Rozpoznania i Walki Radioelektronicznej*. Warszawa 2000.

190. Smith M. R. *Commonsense computer security*, McGraw-Hill Companies 1993.

191. Sobieska L., Czublun P. *Ochrona danych osobowych*. [w:] *Prawo Asekuracyjne* Nr 1/1999.

192. Sovis F. *Security and Auditing of Information Systems*, BIALTEC vol. VI, Bialtec conference 1998, http://www.nbs.sk/

193. Stallings W. *Ochrona danych w sieci i intersieci w teorii i praktyce*. WNT 1997.

194. Starzyk J. *Wspólna Polityka Zagraniczna i Bezpieczeństwa Unii Europejskiej* . Warszawa 2002.

195. Stefanowicz B. *Informacyjne systemy zarządzania*, SGH, Warszawa 1997.

196. Stonebumer G., Goguen A., Feringa A. *Risk Management Guide for Information Technology Systems*. Berlin Verlag 1999.

197. Stoner J., Wankel Ch. *Kierowanie*. PWE, Warszawa 1992.

198. Sułek M. *Podstawy potęgonomii i potęgometrii*. WSEiA, Kielce 2001.

199. Sułek M. *Potencjał gospodarczo-obronny – pojęcie, pomiar, decyzje*. AON Warszawa 1993.

200. Syta J. *Metodyki analizy ryzyka za szczególnym uwzględnieniem bezpieczeństwa systemów informatycznych*. Politechnika Warszawska 2001.

201. Syta J. Projekt Systemu Bezpieczeństwa Informacji opartego na przepisach ISO 17799 dla AVET INS. Lund-Warszawa 2001.

202. Szaliłow M. *Organizacyjno prawne aspekty ochrony systemów łączności i przesyłanej w nich informacji*. AON Warszawa 2001.

203. Szałowski R. *Prawna ochrona informacji niejawnych i danych osobowych*. Warszawa 2000.

204. Szewc A. *Z problematyki ochrony danych osobowych*. Cz. I. [w:] *Radca Prawny*. Czasopismo Samorządu Radców Prawnych Nr 3/1999.

205. Szewc A. *Z problematyki ochrony danych osobowych*. Cz. II. [w:] *Radca Prawny*. Czasopismo Samorządu Radców Prawnych Nr 4/1999.

206. Szewc A.: *Z problematyki ochrony danych osobowych*. Cz. III. *Radca Prawny*. Czasopismo Samorządu Radców Prawnych Nr 5/1999.

207. Szomański B. *Integracja systemu zarządzania bezpieczeństwem informacji zgodnie z BS7799 z zintegrowanymi systemami zarządzania (ISO 9001, ISO 14001, PN 18000)*, Enigma 2001, www.bezpieczenstwoIT.pl.

208. Szpor G. *Publicznoprawna ochrona danych osobowych.* [w:] *Przegląd Ustawodawstwa Gospodarczego* Nr 12/1999.

209. Szpyra R. *Operacje informacyjne państwa w działaniach sił powietrznych* – rozprawa habilitacyjna. AON Warszawa 2003.

210. Taradejna R. i M. *Tajemnica państwowa i inne tajemnice chroniące interesy państwa i obywateli. Wybrane zagadnienia prawnej ochrony informacji dotyczących działalności gospodarczej, społecznej i zawodowej oraz życia prywatnego.* Warszawa 1999.

211. Tarczyński W., Mojsiewicz M. *Zarządzanie ryzykiem.* Warszawa 2001.

212. Tinnefeld M. - Th. *Ochrona danych - kamień węgielny budowy Europy.* [w:] Wyrzykowski M. (red.): *Ochrona danych osobowych.* Instytut Spraw Publicznych, Warszawa 1999.

213. Toffler A., Toffler H. *Budowa nowej cywilizacji.* Warszawa 1998. Toffler A., Toffler H., Verton D. *Wojna i antywojna.* Warszawa 1998. Tzu S. *Sztuka wojny.* Warszawa 1994.

214. Toffler A. *Trzecia fala.* Warszawa 1986.

215. Vigilinx A. *White Paper: Security Assessment Methodology*; www.vigilinx.com/2001.

216. Waltz E. *Information Warfare – Principles and Operations.* ARTECH House MA 1998.

217. Webster R. *Theories of the Information Society..* [w:] White K. C. *CyberTerrorism: Modem Mayhem,* Carlisle 1998.

218. Wiener N. *Cybernetyka, czyli sterowanie i komunikacja w zwierzęciu i maszynie*, PWN, Warszawa 1971.

219. Wiener N. *Cybernetyka i społeczeństwo.* Warszawa 1960.

220. Wiśniewski A. *Analiza ryzyka. Wytyczne dla administratorów systemów.* AZW Warszawa 2000.

221. Wiśniewski M. *Emisja elektromagnetyczna – analiza zagrożeń dla poufności danych.* Praca magisterska. Politechnika Poznańska 2000.

222. Wolfenstetter K. - D. *Przyjazne techniki ochrony danych.* [w:] Wyrzykowski M. (red.): *Ochrona danych osobowych.* Instytut Spraw Publicznych, Warszawa 1999.

223. Wróbel W. *Prawnokarna ochrona tajemnicy państwowej.* Czasopismo Prawa Karnego i Nauk Penalnych, z.1/2000.

224. Wyrzykowski M. (red.): *Ochrona danych osobowych.* Instytut Spraw Publicznych, Warszawa 1999.

225. Wyrzykowski M. *Ochrona danych - zagadnienia konstytucyjne.* [w:] Wyrzykowski M. (red.): *Ochrona danych osobowych.* Instytut Spraw Publicznych, Warszawa 1999.

226. Zacher L. W. (red.). *Problemy społeczeństwa informacyjnego*. Warszawa 2000.

227. Zacher L. W. (red.). *Rewolucja informacyjna i społeczeństwo*. Transformacje, Warszawa 1997.

228. Zalmay Khalilzhad M., White J. P. (red.). *The Changing Role of Information*. Pergamon Press 1999.

229. Zaskórski P. *Automatyzacja procesów dowodzenia*. Toruń 2001.

230. Zeszyty Naukowe AON. Współczesne Siły Powietrzne – Misje, Zadania, Tendencje Rozwoju – Numer Specjalny 2003.

Dzienniki urzędowe

1. USTAWA z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych. (Dz.U.99.11.95 z późn. zm.).

2. USTAWA z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu. (Dz.U.02.74.676).

3. ROZPORZĄDZENIE PREZESA RADY MINISTRÓW z dnia 25 lutego 1999 r. w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych. (Dz.U.99.18.162).

4. ROZPORZĄDZENIE PREZESA RADY MINISTRÓW z dnia 25 lutego 1999 r. w sprawie szczegółowego trybu prowadzenia przez służby ochrony państwa kontroli w zakresie ochrony informacji niejawnych stanowiących tajemnicę państwową. (Dz.U.99.18.160).

5. ROZPORZĄDZENIE PREZESA RADY MINISTRÓW z dnia 16 lipca 2001 r. w sprawie wysokości opłat za przeprowadzenie przez służbę ochrony państwa czynności warunkujących wydanie certyfikatu dla systemu lub sieci teleinformatycznej, urządzenia lub narzędzia kryptograficznego oraz za wydanie tych certyfikatów. (Dz.U.01.77.820).

6. ZARZĄDZENIE Nr 73 PREZESA RADY MINISTRÓW z dnia 26 czerwca 2002 r. w sprawie nadania statutu Agencji Bezpieczeństwa Wewnętrznego. (M.P.02.26.432).

7. DECYZJA Nr 181/MON MINISTRA OBRONY NARODOWEJ z dnia 06 października 2000 r. w sprawie organizacji szczególnej ochrony systemów i sieci teleinformatycznych w resorcie obrony narodowej.

8. DECYZJA Nr 16/MON MINISTRA OBRONY NARODOWEJ z dnia 25 stycznia 2001 r. w sprawie szkolenia w zakresie ochrony informacji niejawnych. (Dz.Urz.MON.01.1.9).

9. DECYZJA Nr 100/MON MINISTRA OBRONY NARODOWEJ z dnia 6 czerwca 2000 r. w sprawie jednostki certyfikującej właściwej w Ministerstwie Obrony Narodowej do certyfikacji wyrobów o przeznaczeniu specjalnym, służących do ochrony informacji niejawnych. (Dz.Urz.MON. 00.55).

10. DECYZJA Nr 29/MON MINISTRA OBRONY NARODOWEJ z dnia 22 lutego 2001 r. w sprawie trybu certyfikacji kontroli kancelarii zagranicznych kancelarii, środków i materiałów kryptograficznych, punktów obsługi dokumentów zagranicznych, stacji

łączności kryptograficznej oraz pomieszczeń wydzielonych (terminali) teleinformatycznych w jednostkach organizacyjnych resortu Obrony Narodowej.

11. Umowa między Stronami Traktatu Północnoatlantyckiego o ochronie informacji. (Dz.U.00.64.740).
12. ROZPORZĄDZENIE PREZESA RADY MINISTRÓW z dnia 16 lipca 2001 r. w sprawie wysokości opłat za przeprowadzenie przez służbę ochrony państwa czynności warunkujących wydanie certyfikatu dla systemu lub sieci teleinformatycznej, urządzenia lub narzędzia kryptograficznego oraz za wydanie tych certyfikatów. (Dz.U.01.77.820).
13. ROZPORZĄDZENIA PREZESA RADY MINISTRÓW z dnia 21 czerwca 1994 r. w sprawie zakresu i trybu stosowania przepisów ustawy o badaniach i certyfikacji wyrobów produkowanych w kraju i importowanych wyłącznie na potrzeby obronności i bezpieczeństwa państwa, a także właściwość organów w tych sprawach (Dz. U. 94.80.370).
14. ROZPORZĄDZENIE MINISTRA OBRONY NARODOWEJ z dnia 6 kwietnia 2001 r. w sprawie wyrobów, które nie mogą być nabywane bez certyfikatu (Dz.U. 01.43.483 z póź. zm).
15. USTAWA z dnia 14 grudnia 1995 r. o urzędzie Ministra Obrony Narodowej. (Dz.U. 96.10.56 z późn. zmianami).
16. ROZPORZĄDZENIE RADY MINISTRÓW z dnia 9 lipca 1996 r. w sprawie szczegółowego zakresu działania Ministra Obrony Narodowej (Dz.U.96.94.426).
17. USTAWA z dnia 03.04.1993 r. o badaniach i certyfikacji (Dz.U. Nr 55, poz. 250 ze zm.).
18. ROZPORZĄDZENIA PREZESA RADY MINISTRÓW z dnia 21 czerwca 1994 r. w sprawie zakresu i trybu stosowania przepisów ustawy o badaniach i certyfikacji wyrobów produkowanych w kraju i importowanych wyłącznie na potrzeby obronności i bezpieczeństwa państwa, a także właściwość organów w tych sprawach (Dz. U. Nr 80 poz. 370).
19. DECYZJA Nr 191/MON MINISTRA OBRONY NARODOWEJ z dnia 12 października 1999 r. w sprawie działalności kontrolnej w resorcie obrony narodowej (Dz.Rozk. MON 1999 poz. 89).

Normy

1. PN-I-13335-1: „*Wytyczne do zarządzania bezpieczeństwem systemów informatycznych. Pojęcia i modele bezpieczeństwa systemów informatycznych*".
2. PrPN-ISO/IEC 17799: „Technika informatyczna. Praktyczne zasady zarządzania bezpieczeństwem informacji".
3. Norma BS 7799 cz.1 / 1999.
4. Norma BS 7799 cz.2 / 1999.
5. Norma FIPS65 Guidelines for Automatic Data Processing Risk Analysis; National Bureau of Standards; August 1969.
6. Norma ISO IEC 10118 1/ 1994.

7. Norma ISO IEC 10118 2/ 1994.
8. Norma ISO IEC 10118 3/ 1998.
9. Norma ISO IEC 10118 4/ 1998.
10. Norma PN-I-13335-1 / 1999.
11. Norma PN-ISO 9004-4 / 1996 .
12. ITSEC, (28 Jun 1991). *Information Technology Security Evaluation Criteria, Commission of European Communities.*
13. ISO 9004-4 /1993, *Quality Management and quality system elements - Part 4: Guidelines for quality improvement*, www.iso.ch.
14. ISO Bulletin, (December 2000). *Finding a language to address information security management*, www.iso.ch.
15. ISO IEC TR 13335-1/1996, *Information technology - Guidelines for the management of IT Security: Part 1: Concepts and models for IT Security*, www.iso.ch.
16. ISO I EC TR 13335-3/1998, *Information technology - Guidelines for the management of IT Security: Part 3: Techniques for the management of IT Security,* www.iso.ch.
17. ISO 17799-1/2000 *Information security management - Part 1: Code of practice for information security management.*
18. BS7799-2/2000 *Information security management - Part 2: Specification for Information security management*, BSI.

ZAŁĄCZNIKI

Załącznik 1 – Tabele taksonomiczne sprzętu walki informacyjnej

Tabela specjalnego sprzętu walki informacyjnej wybranych państw NATO wg źródeł dostępnych (Jane's C4I Systems2001 - 2002, SIPRI Yearbook 2002, Military Balance 2002-2003)

Nazwa	Ilość	Kraj	Ludność w mln	Nasycenie na 1 mln	
Systemy Wczesnego Ostrzegania i Naprowadzania					
TRS 22XX long-range 3-D radar	14	Francja	58	0,24137931	92
MARTHA air defence command and control network	78	Francja	58	1,344827586	
IRS-20MP/L monopulse secondary surveillance radar	54	Hiszpania	39	1,384615385	68
IRS-M IFF/secondary radar	14	Hiszpania	39	0,358974359	
AN/FPS-117 air defence radar	125	USA	285	0,438596491	454
AN/FPS-118 Over-The-Horizon Backscatter (OTH-B) radar	6	USA	285	0,021052632	
AN/MPQ-64 mobile air defence radar	200	USA	285	0,701754386	
Low-Altitude Aircraft Detection System (LAADS)	12	USA	285	0,042105263	
Relocatable Over-The-Horizon Radar (ROTHR)	3	USA	285	0,010526316	
Series 320 3-D air defence radar	20	USA	285	0,070175439	
HADR Air Defence Radar	16	USA	285	0,056140351	
AIR DEFENSE RADAR	72	USA	285	0,252631579	
AR-320 3-D air defence radar	6	Wlk.Bryt.	58	0,103448276	28
AR327 E/F-band 3-D tactical air defence radar	6	Wlk.Bryt.	58	0,103448276	
S70x Martello 3-D surveillance radar	16	Wlk.Bryt.	58	0,275862069	
RAT-31 DL solid-state 3-D radar	4	Włochy	57,1	0,070052539	9
RAT-31 SL 3-D long-range radar	5	Włochy	57,1	0,087565674	
Systemy Dowodzenia i Kierowania Ogniem					
TACTIC C2 System	800	Francja	58	13,79310345	1600
MESREG message handling system	800	Francja	58	13,79310345	
AN/VPS-2 Modified (Fire control radar)	2	Hiszpania	39	0,051282051	2
ARES rocket artillery employment system	227	Niemcy	82	2,768292683	227
EL/M-2032 (Combat ac radar)	10	Turcja	60	0,166666667	10
SECURE INTELLIGENCE RADIO	260	USA	285	0,912280702	2750
ATCCS MCS CHS	2490	USA	285	8,736842105	
SEPA Artillery Fire-Control System (AFCS)	600	Włochy	57,1	10,50788091	600
Systemy Łączności					

TXM series voice communication control systems	300	Francja	58	5,172413793	1000
THOMPAC 2G ATM Switching Equipment	700	Francja	58	12,06896552	
TACTICAL COMMS	750	Hiszpania	39	19,23076923	750
SCRA/RAP+MST	453	Holandia	15,5	29,22580645	453
SCRA/RAP+MST	2718	Niemcy	82	33,14634146	2718
TACT COMMS	2840	Turcja	60	47,33333333	2840
MMRT	85	USA	285	0,298245614	10666
VARIOUS AIRCRAFT	7400	USA	285	25,96491228	
MULTIBAND MULTIMODE RADIO	3181	USA	285	11,16140351	
Systemy Walki Radioelektronicznej					
BOEING 767-200ER	2	NATO	59	0,033898305	2
E-2C Hawkeye Airborne Early Warning aircraft (AEW)	245	USA	285	0,859649123	338
Prophet	7	USA	285	0,024561404	
TROJAN SPIRIT special purpose integrated remote intelligence terminal	41	USA	285	0,143859649	
E-8C	10	USA	285	0,035087719	
AEW (US DOD)	35	USA	285	0,122807018	
BOEING 767-200ER	1	Wlk.Bryt.	58	0,017241379	331
MIR-2 EMS equipment	330	Wlk.Bryt.	58	5,689655172	
Morskie Systemy Walki Informacyjnej					
System SINBADS	20	Holandia	15,5	1,290322581	24
Gipsy submarine data handling and weapon control system	4	Holandia	15,5	0,258064516	
SHipboard INtegrated Processing And Display System (SHINPADS)	12	Kanada	31	0,387096774	12
Seaspray-3000 (MP aircraft radar)	2	Niemcy	82	0,024390244	2
FALCON series surveillance radar	45	USA	285	0,157894737	153
NAVAL MILSTAR TERMINALS	100	USA	285	0,350877193	
E-6A BLOCK II UPGRADE	8	USA	285	0,028070175	
ICS4 (AN/URC-109) integrated communication system	46	Wlk.Bryt.	58	0,793103448	85
LPD/MCMV	39	Wlk.Bryt.	58	0,672413793	
Igunae/Varan (MP aircraft radar)	14	Włochy	57,1	0,245183888	14
Systemy identyfikacji obiektów pola walki					
FF	1	Grecja	10,3	0,097087379	1
DD/FF/MCMV	4	Holandia	15,5	0,258064516	4
DD/FF	7	Kanada	31	0,225806452	7
DD	4	Niemcy	82	0,048780488	4
FF	2	Portugalia	9,8	0,204081633	2
FF/FFL	18	Turcja	60	0,3	18
AN/ALR-73 Passive Detection System (PDS)	174	USA	285	0,610526316	624
AN/TPX-42 PIDP IFF equipment	320	USA	285	1,122807018	
AN/TPX-46(V) IFF interrogator	130	USA	285	0,456140351	

Systemy Rozpoznania Pola Walki					
DD	3	Francja	58	0,051724138	8
FFL CENTRALIZED C3I	5	Francja	58	0,086206897	
DA-08 (Surveillance radar)	1	Hiszpania	39	0,025641026	2
RAN-12L/X (Surveillance radar)	1	Hiszpania	39	0,025641026	
C3	1700	NATO	59	28,81355932	1700
HARD (Surveillance radar)	4	Niemcy	82	0,048780488	4
AN/FPS-130 fixed station 3-D radar	44	USA	285	0,154385965	4257
AN/TPS-59 3-D tactical radar	16	USA	285	0,056140351	
AN/TPS-63 tactical surveillance radar	154	USA	285	0,540350877	
JSTARS + C2	79	USA	285	0,277192982	
Guardrail Common Sensor (GR/CS) SIGINT System	3	USA	285	0,010526316	
EPLRS EGRU+ NTDR	335	USA	285	1,175438596	
F/A-18D/F-14	66	USA	285	0,231578947	
C2	2850	USA	285	10	
IMAGERY PROCESSING	710	USA	285	2,49122807	
BATTLEFIELD SURVEILLANCE	9	Wlk.Bryt.	58	0,155172414	128
DD	9	Wlk.Bryt.	58	0,155172414	
BATTLEFIELD SURVEILLANCE	110	Wlk.Bryt.	58	1,896551724	
DD	5	Włochy	57,1	0,087565674	5
Satelitarne Systemy Walki Informacyjnej					
Station Portable Autonome de Raccordements TACtiques Utilisant un Satellite (SPARTACUS)	20	Francja	58	0,344827586	22
SYRACUSE III	2	Francja	58	0,034482759	
NATO IV	2	NATO	59	0,033898305	2
BLOCK 5D-3 SATELLITE	2	USA	285	0,007017544	53
DSCS III	1	USA	285	0,003508772	
SATELLITE SYSTEM	4	USA	285	0,014035088	
COMMUNICATION SATELLITE	6	USA	285	0,021052632	
BLOCK IIR SATELLITE	12	USA	285	0,042105263	
BALLISTIC MISSILE DEFENSE	28	USA	285	0,098245614	
SKYNET 4	3	Wlk.Bryt.	58	0,051724138	13
SSBN/SSN	10	Wlk.Bryt.	58	0,172413793	
Page Europa Rapid Acquisition Satellite Terminal (PE-RAST 4.8T)	6	Włochy	57,1	0,105078809	6

Tabela 12: ***Tabela specjalnego sprzętu walki informacyjnej wybranych państw NATO wg źródeł dostępnych (Jane's C4I Systems2001 - 2002, SIPRI Yearbook 2002, Military Balance 2002-2003)***

Źródło: opracowanie własne

Nazwa	Ilość	Kraj	Ludność w mln	Nasycenie na 1 mln	Moduł logarytm	Moduł logarytm nat
Systemy WOiN	92	Francja	58	1,586206897	3,200359834	6,461345567
	68	Hiszpania	39	1,743589744	3,241444306	6,555946059
	454	USA	285	1,592982456	3,202210993	6,465608018
	28	Wlk.Bryt.	58	0,482758621	2,683730038	5,2717615
	9	Włochy	57,1	0,157618214	2,197606401	4,152420461
Systemy Dow i Kier	1600	Francja	58	27,58620690	4,440691989	9,317315898
	2	Hiszpania	39	0,051282051	1,709965389	3,029585534
	227	Niemcy	82	2,768292683	3,442212005	7,01823077
	10	Turcja	60	0,166666667	2,221848754	4,208240531
	2750	USA	285	9,649122807	3,984487834	8,26686701
	600	Włochy	57,1	10,50788091	4,021515142	8,352125539
Specj systemy łączn	1000	Francja	58	17,24137931	4,236572006	8,847312268
	750	Hiszpania	39	19,23076923	4,283996656	8,95651156
	453	Holandia	15,5	29,22580645	4,465766504	9,375052102
	2718	Niemcy	82	33,14634146	4,52043569	9,500932347
	2840	Turcja	60	47,33333333	4,675167099	9,857214769
	10666	USA	285	37,42456140	4,573156719	9,622327211
Systemy WRE	2	NATO	59	0,033898305	1,530177984	2,615609737
	338	USA	285	1,185964912	3,074071846	6,170556715
	331	Wlk.Bryt.	58	5,706896552	3,7564	7,741675365
Systemy WI Morskie	24	Holandia	15,5	1,548387097	3,189879544	6,437213806
	12	Kanada	31	0,387096774	2,587819552	5,050919445
	2	Niemcy	82	0,024390244	1,387216143	2,286427933
	153	USA	285	0,536842105	2,729846571	5,377948741
	85	Wlk.Bryt.	58	1,465517241	3,165990932	6,382208246
	14	Włochy	57,1	0,245183888	2,389491927	4,594253213
Systemy identyf	1	Grecja	10,3	0,097087379	1,987162775	3,667856105
	4	Holandia	15,5	0,258064516	2,411728293	4,645454337
	7	Kanada	31	0,225806452	2,353736346	4,511922945
	4	Niemcy	82	0,048780488	1,688246139	2,979575114
	2	Portugalia	9,8	0,204081633	2,309803924	4,410764795
	18	Turcja	60	0,3	2,477121255	4,796027196
	624	USA	285	2,189473684	3,340339736	6,783661188
Specj systemy rozp	8	Francja	58	0,137931034	2,139661993	4,018998531
	1700	NATO	59	28,81355932	4,459596919	9,360846086
	4	Niemcy	82	0,048780488	1,688246139	2,979575114
	4257	USA	285	14,93684211	4,174258798	8,703830786
	128	Wlk.Bryt.	58	2,206896552	3,343781976	6,791587253
	5	Włochy	57,1	0,087565674	1,942333896	3,564633796
Satelitarne Syst WI	22	Francja	58	0,379310345	2,578994687	5,030599443
	2	NATO	59	0,033898305	1,530177984	2,615609737
	53	USA	285	0,185964912	2,269431014	4,317802733
	13	Wlk.Bryt.	58	0,224137931	2,350515359	4,504506347
	6	Włochy	57,1	0,105078809	2,021515142	3,746955353

Nasycenie specjalnym sprzętem walki informacyjnej wybranych państw NATO

Tabela 13: ***Nasycenie specjalnym sprzętem walki informacyjnej państw NATO;*** Źródło: opracowanie własne

Załącznik 2 – Modele matematyczne walki informacyjnej

Rozwiązanie układu równań różniczkowych Lanchestera

Rozważmy układ równań różniczkowych liniowych:

$$\begin{cases} \frac{dx}{dt} &= -\alpha x - ky + g, \\ \frac{dy}{dt} &= -lx - \beta y + h, \end{cases} \tag{1}$$

gdzie $k, l, \alpha, \beta, g, h > 0$, z warunkiem początkowym

$$\begin{cases} x(0) &= 0, \\ y(0) &= 0. \end{cases} \tag{2}$$

Układ ten można zapisać w postaci:

$$\frac{dU}{dt} = AU + F,$$

gdzie

$$U = \begin{bmatrix} x \\ y \end{bmatrix}, \quad F = \begin{bmatrix} g \\ h \end{bmatrix}, \quad A = \begin{bmatrix} -\alpha & -k \\ -l & -\beta \end{bmatrix}.$$

Układ (1) jest układem niejednorodnym, zatem jego rozwiązanie jest postaci:

$$U = U_0 + U_s,$$

gdzie U_0 stanowi rozwiązanie ogólne układu jednorodnego, zaś U_s - rozwiązanie szczególne układu niejednorodnego. Rozważmy dwa przypadki:

I. $\det A = \alpha\beta - kl \neq 0.$

Na początek wyznaczymy rozwiązanie U_0 układu jednorodnego:

$$\frac{dU}{dt} = AU. \tag{3}$$

Wartości własne macierzy A wyznaczymy z równania:

$$\det(A - \lambda I) = 0,$$

lub równoważnie:

$$\begin{vmatrix} -\alpha - \lambda & -k \\ -l & -\beta - \lambda \end{vmatrix} = \lambda^2 + (\alpha + \beta)\lambda + \alpha\beta - kl = 0. \tag{4}$$

Dla zadanych wartości α, β, k, l wyróżnik Δ równania (4) $\Delta = (\alpha - \beta)^2 + 4kl > 0$, zatem równanie (4) ma dwa różne pierwiastki rzeczywiste:

$$\lambda_{1,2} = -\frac{1}{2}\left[(\alpha+\beta) \pm \sqrt{\Delta}\right] = -\frac{1}{2}\left[(\alpha+\beta) \pm \sqrt{(\alpha-\beta)^2+4kl}\right]. \tag{5}$$

Niech

$$\overline{u_1} = \begin{bmatrix} u_1^1 \\ u_1^2 \end{bmatrix}, \quad \overline{u_2} = \begin{bmatrix} u_2^1 \\ u_2^2 \end{bmatrix}$$

oznaczają wektory własne macierzy A odpowiadające wyliczonym wartościom własny
Wtedy zachodzą równości:

$$(A - \lambda I)\overline{u_1} = 0, \quad (A - \lambda I)\overline{u_2} = 0,$$

równoważnie:

$$\begin{bmatrix} -\frac{1}{2}[\alpha - \beta - \sqrt{\Delta}] & -k \\ -l & -\frac{1}{2}[\beta - \alpha - \sqrt{\Delta}] \end{bmatrix} \begin{bmatrix} u_1^1 \\ u_1^2 \end{bmatrix} = 0,$$

$$\begin{bmatrix} -\frac{1}{2}[\alpha - \beta + \sqrt{\Delta}] & -k \\ -l & -\frac{1}{2}[\beta - \alpha + \sqrt{\Delta}] \end{bmatrix} \begin{bmatrix} u_2^1 \\ u_2^2 \end{bmatrix} = 0,$$

bądź w postaci układów równań:

$$\begin{cases} -\frac{1}{2}[\alpha - \beta - \sqrt{\Delta}]u_1^1 - ku_1^2 = 0, \\ -lu_1^1 - \frac{1}{2}[\beta - \alpha - \sqrt{\Delta}]u_1^2 = 0, \end{cases}$$

$$\begin{cases} -\frac{1}{2}[\alpha - \beta + \sqrt{\Delta}]u_2^1 - ku_2^2 = 0, \\ -lu_2^1 - \frac{1}{2}[\beta - \alpha + \sqrt{\Delta}]u_2^2 = 0, \end{cases}$$

z których wyznaczone $\overline{u_1}, \overline{u_2}$ są postaci:

$$\overline{u_1} = \begin{bmatrix} -2k \\ \alpha - \beta - \sqrt{\Delta} \end{bmatrix}, \quad \overline{u_2} = \begin{bmatrix} -2k \\ \alpha - \beta + \sqrt{\Delta} \end{bmatrix}. \tag{6}$$

Oznaczmy przez Q macierz wektorów własnych, czyli macierz:

$$Q = \begin{bmatrix} -2k & -2k \\ \alpha - \beta - \sqrt{\Delta} & \alpha - \beta + \sqrt{\Delta} \end{bmatrix}.$$

Macierz Q jest macierzą nieosobliwą ($\det Q = -4k\sqrt{\Delta} \neq 0$), oraz $\lambda_1 \neq \lambda_2$ więc układ (1) można sprowadzić do postaci diagonalnej. Zastosujemy podstawienie $U = QV$. Wtedy

$$Q\frac{dV}{dt} = AQV + F,$$

a stąd

$$\frac{dV}{dt} = Q^{-1}AQV + Q^{-1}F := \Lambda V + Q^{-1}F. \tag{7}$$

Niech

$$V = \begin{bmatrix} v_1 \\ v_2 \end{bmatrix}.$$

Wtedy rozwiązanie układu jednorodnego, czyli $dV/dt = \Lambda V$, lub w postaci rozwiniętej

$$\begin{cases} \frac{dv_1}{dt} &= \lambda_1 v_1, \\ \frac{dv_2}{dt} &= \lambda_2 v_2, \end{cases}$$

jest postaci:

$$\begin{cases} v_1 &= C_1 e^{\lambda_1 t}, \\ v_2 &= C_2 e^{\lambda_2 t}, \end{cases} \quad C_1, C_2 \in \mathbb{R}.$$

Stąd i z podstawienia $U = QV$ wyznaczamy macierz U_0

$$U_0 = \begin{bmatrix} x_0(t) \\ y_0(t) \end{bmatrix} = \begin{bmatrix} -2k & -2k \\ \alpha - \beta - \sqrt{\Delta} & \alpha - \beta + \sqrt{\Delta} \end{bmatrix} \begin{bmatrix} C_1 e^{\lambda_1 t} \\ C_2 e^{\lambda_2 t} \end{bmatrix},$$

czyli rozwiązanie ogólne równania jednorodnego (3):

$$\begin{cases} x_0(t) &= -2kC_1 e^{\lambda_1 t} - 2kC_2 e^{\lambda_2 t}, \\ y_0(t) &= (\alpha - \beta - \sqrt{\Delta})C_1 e^{\lambda_1 t} + (\alpha - \beta + \sqrt{\Delta})C_2 e^{\lambda_2 t}, \end{cases} \tag{8}$$

gdzie $C_1, C_2 \in \mathbb{R}$, natomiast λ_1, λ_2 dane są wzorem (5).

Mamy ponadto

$$\begin{aligned} Q^{-1}F &= \frac{-1}{4k\sqrt{\Delta}} \begin{bmatrix} \alpha - \beta + \sqrt{\Delta} & 2k \\ \beta - \alpha + \sqrt{\Delta} & -2k \end{bmatrix} \begin{bmatrix} g \\ h \end{bmatrix} \\ &= \frac{-1}{4k\sqrt{\Delta}} \begin{bmatrix} (\alpha - \beta + \sqrt{\Delta})g + 2kh \\ (\beta - \alpha + \sqrt{\Delta})g - 2kh \end{bmatrix}. \end{aligned}$$

Rozwiązanie szczególne układu (7) wyznaczamy metodą uzmienniania stałych. Niech v_{1s}, v_{2s} oznaczają całki szczególne uładu niejednorodnego (7). Zachodzą zatem związki:

$$\begin{cases} \frac{dv_{1s}}{dt} &= \lambda_1 v_{1s}(t) - \frac{1}{4k\sqrt{\Delta}} \left[(\alpha - \beta + \sqrt{\Delta})g + 2kh\right], \\ \frac{dv_{2s}}{dt} &= \lambda_2 v_{2s}(t) - \frac{1}{4k\sqrt{\Delta}} \left[(\beta - \alpha + \sqrt{\Delta})g - 2kh\right], \end{cases}$$

z których metodą wariacji stałych wyznaczamy rozwiązania szczególne w postaci:

$$\begin{cases} v_{1s}(t) &= \frac{1}{4k\lambda_1\sqrt{\Delta}}\left[(\alpha-\beta+\sqrt{\Delta})g+2kh\right], \\ v_{2s}(t) &= \frac{1}{4k\lambda_2\sqrt{\Delta}}\left[(\beta-\alpha+\sqrt{\Delta})g-2kh\right]. \end{cases}$$

Zatem

$$U_s = Q\begin{bmatrix} v_{1s} \\ v_{2s} \end{bmatrix},$$

a stąd mamy

$$\begin{cases} x_s(t) &= \frac{1}{\alpha\beta-kl}(\beta g-hk), \\ y_s(t) &= \frac{1}{\alpha\beta-kl}(\alpha h-gl). \end{cases} \tag{9}$$

Korzystając z (8) i (9) otrzymujemy rozwiązanie ogólne układu niejednorodnego w postaci:

$$\begin{cases} x(t) &= -2kC_1e^{\lambda_1 t}-2kC_2e^{\lambda_2 t}+\dfrac{\beta g-kh}{\alpha\beta-kl}, \\ y(t) &= (\alpha-\beta-\sqrt{\Delta})C_1e^{\lambda_1 t}+(\alpha-\beta+\sqrt{\Delta})C_2e^{\lambda_2 t}+\dfrac{\alpha h-gl}{\alpha\beta-kl}, \end{cases} \tag{10}$$

gdzie $C_1, C_2 \in \mathbb{R}$, oraz λ_1, λ_2 dane są wzorem (5) .

Uwzględniając warunek początkowy (2) w rozwiązaniu (10), otrzymujemy:

$$\begin{cases} 0 &= -2kC_1-2kC_2+\dfrac{\beta g-kh}{\alpha\beta-kl}, \\ 0 &= (\alpha-\beta-\sqrt{\Delta})C_1+(\alpha-\beta+\sqrt{\Delta})C_2+\dfrac{\alpha h-gl}{\alpha\beta-kl}, \end{cases}$$

lub równoważnie

$$\begin{cases} 2kC_1 + 2kC_2 &= \dfrac{\beta g-kh}{\alpha\beta-kl}, \\ -(\alpha-\beta-\sqrt{\Delta})C_1 - (\alpha-\beta+\sqrt{\Delta})C_2 &= \dfrac{\alpha h-gl}{\alpha\beta-kl}. \end{cases}$$

Powyższy układ równań jest układem równań liniowych, z niewiadomymi C_1, C_2, którego wyznacznik główny

$$W = \begin{vmatrix} 2k & 2k \\ -\alpha+\beta+\sqrt{\Delta} & -\alpha+\beta-\sqrt{\Delta} \end{vmatrix} = -4k\sqrt{\Delta} \neq 0.$$

Zatem układ ten posiada dokładnie jedno rozwiązanie postaci:

$$\begin{cases} C_1 = \dfrac{-1}{4k\sqrt{\Delta}}\left[\dfrac{k(gl-\alpha h)+(\beta-\sqrt{\Delta})(\beta g-hk)}{\alpha\beta-kl}-g\right], \\ C_2 = \dfrac{-1}{4k\sqrt{\Delta}}\left[\dfrac{k(\alpha h-gl)-(\beta+\sqrt{\Delta})(\beta g-hk)}{\alpha\beta-kl}+g\right]. \end{cases}$$

Wstawiając wyznaczone stałe C_1, C_2 do rozwiązania (10), otrzymujemy rozwiązanie układu (1) z zadanym warunkiem początkowym (2):

$$\begin{cases} x(t) = \dfrac{1}{2\sqrt{\Delta}}\left[\dfrac{k(gl-\alpha h)+(\beta-\sqrt{\Delta})(\beta g-hk)}{\alpha\beta-kl}-g\right]e^{\lambda_1 t} \\ \quad + \dfrac{1}{2\sqrt{\Delta}}\left[\dfrac{k(\alpha h-gl)-(\beta+\sqrt{\Delta})(\beta g-hk)}{\alpha\beta-kl}+g\right]e^{\lambda_2 t} \\ \quad + \dfrac{\beta g-kh}{\alpha\beta-kl}, \\ y(t) = \dfrac{\beta-\alpha+\sqrt{\Delta}}{4k\sqrt{\Delta}}\left[\dfrac{k(gl-\alpha h)+(\beta-\sqrt{\Delta})(\beta g-hk)}{\alpha\beta-kl}-g\right]e^{\lambda_1 t} \\ \quad + \dfrac{\beta-\alpha-\sqrt{\Delta}}{4k\sqrt{\Delta}}\left[\dfrac{k(\alpha h-gl)-(\beta+\sqrt{\Delta})(\beta g-hk)}{\alpha\beta-kl}+g\right]e^{\lambda_2 t} \\ \quad + \dfrac{\alpha h-gl}{\alpha\beta-kl}. \end{cases} \tag{11}$$

W przypadku szczególnym, gdy $\alpha = 0, \beta = 0$, układ (1) sprowadza się do układu:

$$\begin{cases} \dfrac{dx}{dt} = -ky+g, \\ \dfrac{dy}{dt} = -lx+h. \end{cases} \tag{12}$$

Korzystając z rozwiązania (10), dla tak dobranych wartości α i β otrzymujemy rozwiązanie ogólne:

$$\begin{cases} x(t) = -2k\left(C_1 e^{-t\sqrt{kl}}+C_2 e^{t\sqrt{kl}}\right)+\dfrac{h}{l}, \\ y(t) = -2\sqrt{kl}\left(C_1 e^{-t\sqrt{kl}}-C_2 e^{t\sqrt{kl}}\right)+\dfrac{g}{k}, \end{cases} \tag{13}$$

natomiast po uwzględnieniu warunku początkowego (2) otrzymujemy z (11)

$$\begin{cases} x(t) = -\dfrac{1}{2l\sqrt{kl}}\left[(gl+h\sqrt{kl})e^{-t\sqrt{kl}}-(gl-h\sqrt{kl})e^{t\sqrt{kl}}\right]+\dfrac{h}{l}, \\ y(t) = -\dfrac{1}{2kl}\left[(gl+h\sqrt{kl})e^{-t\sqrt{kl}}+(gl-h\sqrt{kl})e^{t\sqrt{kl}}\right]+\dfrac{g}{k}. \end{cases} \tag{14}$$

Jeśli ponadto $g = 0, h = 0$, układ (12) ma postać:

$$\begin{cases} \dfrac{dx}{dt} &= -ky, \\ \dfrac{dy}{dt} &= -lx. \end{cases} \tag{15}$$

którego rozwiązanie ogólne otrzymujemy z (13) (wstawiając $g = 0, h = 0$)

$$\begin{cases} x(t) &= -2k\left(C_1 e^{-t\sqrt{kl}} + C_2 e^{t\sqrt{kl}}\right), \\ y(t) &= 2\sqrt{kl}\left(C_1 e^{-t\sqrt{kl}} - C_2 e^{t\sqrt{kl}}\right). \end{cases} \quad C_1, C_2 \in \mathbb{R}. \tag{16}$$

Uwzględniając warunek początkowy otrzymujemy z (14) rozwiązanie trywialne:

$$\begin{cases} x(t) &= 0, \\ y(t) &= 0. \end{cases}$$

II. $\det A = \alpha\beta - kl = 0$.

Jeśli $\alpha\beta - kl = 0$, to

$$\det(A - \lambda I) = \lambda^2 + (\alpha + \beta)\lambda.$$

Z równości $\det(A - \lambda I) = 0$ otrzymujemy następujące wartości własne macierzy A:

$$\lambda_1 = -(\alpha + \beta), \qquad \lambda_2 = 0. \tag{17}$$

Dla takich wartości własnych wyznaczamy wektory własne z układów:

$$\begin{bmatrix} \beta & -k \\ -l & \alpha \end{bmatrix} \begin{bmatrix} u_1^1 \\ u_1^2 \end{bmatrix} = 0,$$

$$\begin{bmatrix} -\alpha & -k \\ -l & -\beta \end{bmatrix} \begin{bmatrix} u_2^1 \\ u_2^2 \end{bmatrix} = 0.$$

Otrzymujemy:

$$\overline{u_1} = \begin{bmatrix} -2k \\ -2\beta \end{bmatrix}, \; \overline{u_2} = \begin{bmatrix} -2k \\ 2\alpha \end{bmatrix}. \tag{18}$$

Zatem macierz wektorów własnych Q ma postać:

$$Q = \begin{bmatrix} -2k & -2k \\ -2\beta & 2\alpha \end{bmatrix}.$$

Stąd $\det Q = -4k(\alpha+\beta)$, oraz

$$Q^{-1} = \frac{-1}{4k(\alpha+\beta)} \begin{bmatrix} 2\alpha & 2k \\ 2\beta & -2k \end{bmatrix}.$$

Równanie jednorodne po diagonalizacji ma więc postać:

$$\begin{cases} \dfrac{dv_1}{dt} &= \lambda_1 v_1, \\ \dfrac{dv_2}{dt} &= 0, \end{cases}$$

skąd otrzymujemy jego rozwiązanie ogólne:

$$\begin{cases} v_1 &= C_1 e^{\lambda_1 t}, \\ v_2 &= C_2, \end{cases} \qquad C_1, C_2 \in \mathbb{R}.$$

Postępując podobnie jak w przypadku $\det A \neq 0$ otrzymujemy kolejno:

$$Q^{-1}F = \frac{-1}{4k(\alpha+\beta)} \begin{bmatrix} 2\alpha & 2k \\ 2\beta & -2k \end{bmatrix} \begin{bmatrix} g \\ h \end{bmatrix} = \frac{-1}{2k(\alpha+\beta)} \begin{bmatrix} \alpha g + kh \\ \beta g - kh \end{bmatrix},$$

oraz

$$\begin{cases} \dfrac{dv_{1s}}{dt} &= \lambda_1 v_{1s} - \dfrac{\alpha g + kh}{2k(\alpha+\beta)}, \\ \dfrac{dv_{2s}}{dt} &= -\dfrac{\beta g - kh}{2k(\alpha+\beta)}, \end{cases}$$

a stąd metodą wariacji stałych wyznaczamy całki szczególne:

$$\begin{cases} v_{1s}(t) &= \dfrac{\alpha g + kh}{2k\lambda_1(\alpha+\beta)}, \\ v_{2s}(t) &= \dfrac{kh - \beta g}{2k(\alpha+\beta)} t. \end{cases}$$

Zatem

$$\begin{cases} v_1(t) &= C_1 e^{\lambda_1 t} + \dfrac{\alpha g + kh}{2k\lambda_1(\alpha+\beta)}, \\ v_2(t) &= C_2 + \dfrac{kh - \beta g}{2k(\alpha+\beta)} t, \end{cases}$$

gdzie λ_1 dane wzorem (17). Z zależności $U = QV$ wyznaczamy

$$U = Q \begin{bmatrix} v_1(t) \\ v_2(t) \end{bmatrix},$$

czyli

$$\begin{cases} x(t) &= -2kC_1e^{\lambda_1 t} - 2kC_2 - \dfrac{\alpha g + kh}{\lambda_1(\alpha+\beta)} + \dfrac{\beta g - kh}{\alpha+\beta}t, \\ y(t) &= -2\beta C_1 e^{\lambda_1 t} + 2\alpha C_2 - \dfrac{\beta(\alpha g + kh)}{k\lambda_1(\alpha+\beta)} + \dfrac{\alpha(kh - \beta g)}{k(\alpha+\beta)}t, \end{cases}$$

gdzie $\lambda_1 = -(\alpha+\beta)$, lub

$$\begin{cases} x(t) &= -2kC_1e^{-(\alpha+\beta)t} - 2kC_2 + \dfrac{\alpha g + kh}{(\alpha+\beta)^2} + \dfrac{\beta g - kh}{\alpha+\beta}t, \\ y(t) &= -2\beta C_1 e^{-(\alpha+\beta)t} + 2\alpha C_2 + \dfrac{\beta(\alpha g + kh)}{k(\alpha+\beta)^2} + \dfrac{\alpha(kh - \beta g)}{k(\alpha+\beta)}t. \end{cases} \quad (19$$

Stałe C_1, C_2 wyznaczymy korzystając z warunku początkowego (2) i rozwiązania (19). Otrzymujemy:

$$\begin{cases} 0 &= -2kC_1 - 2kC_2 + \dfrac{\alpha g + kh}{(\alpha+\beta)^2}, \\ 0 &= -2\beta C_1 + 2\alpha C_2 + \dfrac{\beta(\alpha g + kh)}{k(\alpha+\beta)^2}, \end{cases}$$

lub równoważnie:

$$\begin{cases} 2kC_1 + 2kC_2 &= \dfrac{\alpha g + kh}{(\alpha+\beta)^2}, \\ 2\beta C_1 - 2\alpha C_2 &= \dfrac{\beta(\alpha g + kh)}{k(\alpha+\beta)^2}. \end{cases}$$

Wyznacznik główny tego układu jest równy:

$$W = \begin{vmatrix} 2k & 2k \\ 2\beta & -2\alpha \end{vmatrix} = -4k(\alpha+\beta) \neq 0.$$

Układ posiada więc jednoznaczne rozwiązanie:

$$\begin{cases} C_1 &= \dfrac{\alpha g + kh}{2k(\alpha+\beta)^2}, \\ C_2 &= 0. \end{cases}$$

Zatem rozwiązanie układu równań różniczkowych dla przypadku II, po uwzględnieniu warunku początkowego (2) ma postać:

$$\begin{cases} x(t) &= -\dfrac{\alpha g + hk}{(\alpha+\beta)^2}e^{-(\alpha+\beta)t} + \dfrac{\alpha g + hk}{(\alpha+\beta)^2} + \dfrac{\beta g - kh}{\alpha+\beta}t, \\ y(t) &= -\dfrac{\beta(\alpha g + hk)}{k(\alpha+\beta)^2}e^{-(\alpha+\beta)t} + \dfrac{\beta(\alpha g + kh)}{k(\alpha+\beta)^2} + \dfrac{\alpha(kh - \beta g)}{k(\alpha+\beta)}t. \end{cases} \quad (20)$$

Stabilność rozwiązań.

Zauważmy, że w przypadku **I** otrzymane rozwiązanie będzie stabilne (nieznacznie odbiegające od stanu początkowego) jeśli $\lambda_1 < 0, \lambda_2 < 0$ (punkt równowagi będzie wtedy tak zwanym węzłem asymptotycznie stabilnym). Wartość $\lambda_1 = -[(\alpha + \beta) + \sqrt{\Delta}]/2 < 0$ dla dowolnych wartości α, β, k, l dodatnich (założenie początkowe), natomiast $\lambda_2 = -[(\alpha + \beta) - \sqrt{\Delta}]/2 < 0$ wtedy i tylko wtedy, gdy $\alpha\beta - kl > 0$. Ostatni warunek nie jest spełniony gdy $\alpha = \beta = 0$, gdyż w tym przypadku mamy $\lambda_1 = -\sqrt{kl} < 0$, natomiast $\lambda_2 = \sqrt{kl} > 0$. Zatem rozwiązanie (14) układu (12) jest niestabilne (tzw. siodło niestabilne).

W przypadku **II** otrzymane rozwiązanie jest niestabilne, niezależnie od doboru parametrów wejściowych α, β, k, l.

Rozwiązanie układu równań różniczkowych wykorzystano w ***Rozdziale 2.3.6*** przy założonych parametrach. Obliczeń dokonano z wykorzystaniem arkusza *EXCEL*. Uwzględniono warunek stabilności, którego naruszenie sygnalizuje ukazanie się w górnej części tabeli odpowiedniej adnotacji oznaczonej na czerwono (przykładem – zawarta w załączniku ***Symulacja 2*** przy ***Wykresie Nr 14***, pokazująca w wyniku braku stabilności załamanie krzywej *Koalicji*).

Przyjęto oznaczenie czasu w odcinkach 10-dniowych w przedziale 0 – 100 dni (celem zobrazowania realnego przebiegu działań bojowych) jako liczbową reprezentację 10/365 (w stosunku rocznym).

W ***Symulacji 2*** uzyskany wynik t = 0,059432 x 365 = 21,7 = 22 dni (rzeczywisty przebieg działań w operacji *Iraqi Freedom*), co potwierdza zasadność przyjęcia miar efektywności: *0* dla *Iraku*, *10* dla *Koalicji*).

Załącznik 3 – Elementy symulacji przebiegu działań bojowych z wykorzystaniem równań Lanchestera

Zestaw danych do równań F. W. Lanchestera

Układ sił wg źródła *Cordesman*		IRAK	USA	sojusznicy	Koalicja
		Stany osobowe			
		390000	231000	48180	279 180
Sprzęt					
1.	czołgi	2 600	850	116	966
2.	bwp i transp. opanc.	3 700	556	290	846
3.	środki artylerii lufowej	2 400	150	75	225
4.	środki artylerii rakietowej	675	500		500
6.	śmigłowce	375	383	89	472
7.	samoloty bojowe	355	1673	138	1 811
8.	okręty	14	112	9	121

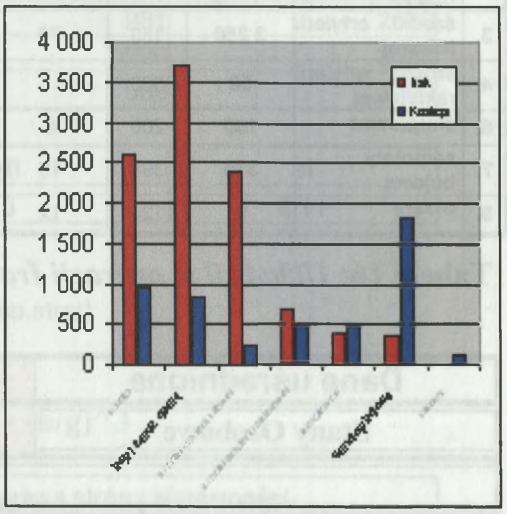


Tabela 14: *Układ sił w operacji Iraqi Freedom (raport Cordesman'a)*

Układ sił - wg źródła "Myśl Wojskowa"		IRAK	USA	sojusznicy	Koalicja
		Stany osobowe			
		400000	231000	47000	278 000
Sprzęt					
1.	czołgi	2 600	850	116	966
2.	bwp i transp. opanc.	3 700	150	300	450
3.	środki artylerii lufowej	2 400		210	210
4.	środki artylerii rakietowej	415			0
6.	śmigłowce	375	700		700
7.	samoloty bojowe	501	1230	117	1 347
8.	okręty	14	112	9	121

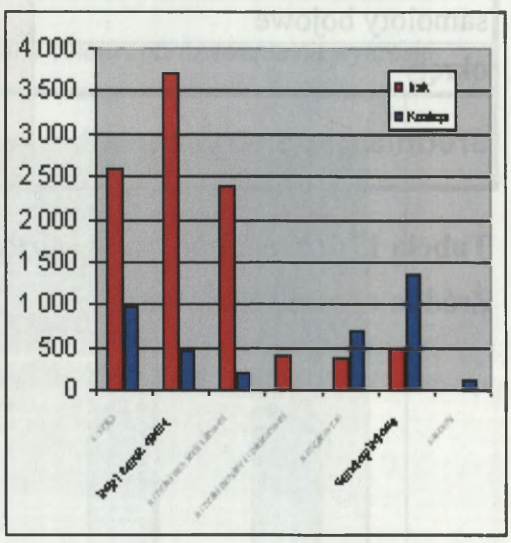


Tabela 15: *Układ sił w operacji Iraqi Freedom („Myśl Wojskowa")*

Układ sił - wg źródła *Konf. Naukowa AON*		IRAK	USA	sojusznicy	Koalicja
		Stany osobowe			
		600000	250000	28000	278 000
Sprzęt					
1.	czołgi	2 600	900	110	1 010
2.	bwp i transp. opanc.	3 700	600	170	770
3.	środki artylerii lufowej	3 250	150	75	225
4.	środki artylerii rakietowej	56	500		500
6.	śmigłowce	150	200	6	206
7.	samoloty bojowe	316	398	16	414
8.	okręty	9	128	12	140

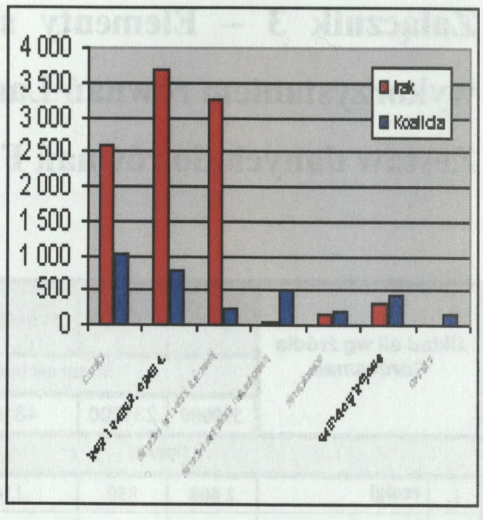


Tabela 16: ***Układ sił w operacji Iraqi Freedom (Konferencja Naukowa AON)***

Dane uśrednione	Irak	Koalicja
Stany Osobowe	463333	278393
Sprzęt		
czołgi	2600	981
bwp i transportery opanc.	3700	689
środki artylerii lufowej	2683	220
środki artylerii rakietowej	382	333
śmigłowce	300	459
samoloty bojowe	391	1191
okręty	12	127
średnia geometryczna sił	**1266**	**995**

Tabela 17: ***Uśrednione dane wartości bojowych Iraku I Koalicji***

Źródło: opracowanie własne

Tabela 18: ***Kwadratowe prawo Lanchestera***

Kwadratowe prawo Lanchestera
ujęcie statyczne

Stany liczbowe	K=dk*ek	I=di*ei	Koalicja (g)	Irak (h)
Liczebność wojsk	5	0,33	278393	463333
Okręty SM	5	0,33	127	14
Samoloty SP	5	0,33	1191	391
Czołgi	5	0,33	981	2600
Artyleria polowa	5	0,33	220	2683
Transportery opanc.	5	0,33	689	3700

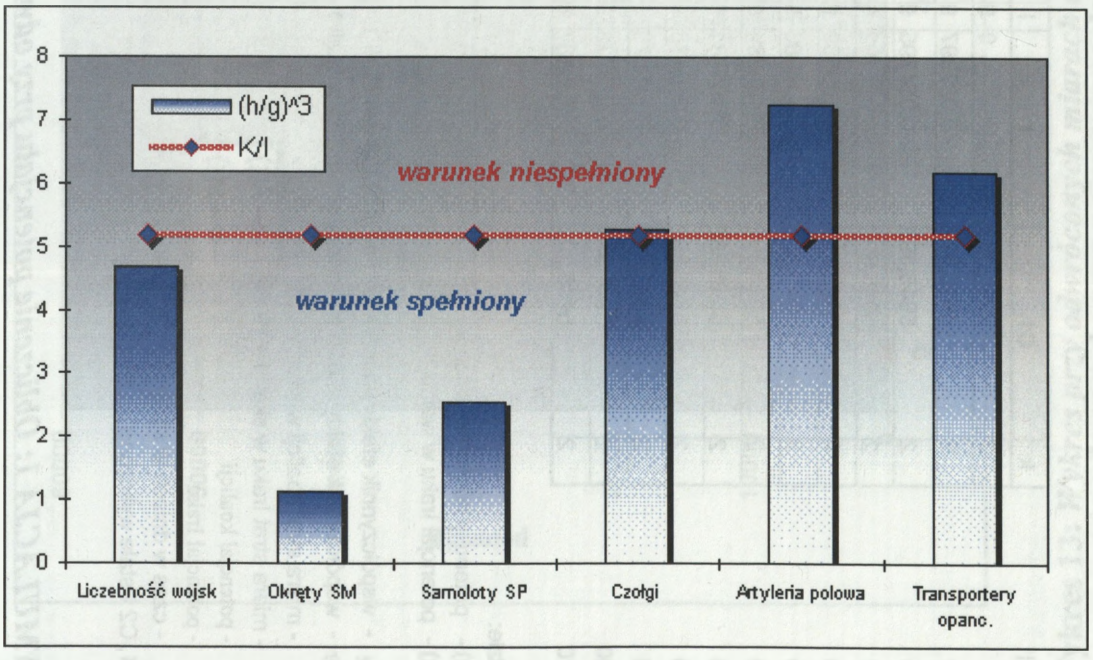
	dk	ek	di	ei
założenia:	10	0,50	3	0,11

dk, di, - współczynniki efektywności informacyjnej
ek, ei - współczynniki skuteczności bojowej (odwrotności wsp.strat)
K, I - efektywność wojsk = iloczyn d *e

warunek powodzenia koalicji : $d_k e_k / d_i e_i > (h/g)^3$

lewa strona nierówności		prawa strona nierówności	
K/I	lg(I/K)+4	(h/g)^3	lg(h/g)^3+4
15	**5,1761**	4,6100	**4,6637**
15	**5,1761**	0,0013	**1,1270**
15	**5,1761**	0,0354	**2,5488**
15	**5,1761**	18,6171	**5,2699**
15	**5,1761**	1813,8191	**7,2586**
15	**5,1761**	154,8629	**6,1899**

parametry nierówności zlogarytmizowane celem zobrazowania na wykresie



Źródło: opracowanie własne

Potencjał koalicji i Iraku w działaniach bojowych z uwzględnieniem miar efektywności informacyjnej

dni	k	C1	t	l	C2	h	g	α	β	x(t)	y(t)
0	2	5945,392	0	9	-8167,61	400000	240000	9	3	0	0
10	2	5945,392	0,027397	9	-8167,61	400000	240000	9	3	5570,519	9814,6629
20	2	5945,392	0,054795	9	-8167,61	400000	240000	9	3	9497,037	17743,54
30	2	5945,392	0,082192	9	-8167,61	400000	240000	9	3	12217,59	24269,385
40	2	5945,392	0,109589	9	-8167,61	400000	240000	9	3	14054,43	29747,763
50	2	5945,392	0,136986	9	-8167,61	400000	240000	9	3	15244,58	34440,64
60	2	5945,392	0,164384	9	-8167,61	400000	240000	9	3	15962,41	38541,101
70	2	5945,392	0,191781	9	-8167,61	400000	240000	9	3	16336,11	42191,541
80	2	5945,392	0,219178	9	-8167,61	400000	240000	9	3	16459,95	45497,046
90	2	5945,392	0,246575	9	-8167,61	400000	240000	9	3	16403,24	48535,242
100	2	5945,392	0,273973	9	-8167,61	400000	240000	9	3	16216,88	51363,546
110	2	5945,392	0,30137	9	-8167,61	400000	240000	9	3	15938,28	54024,492

gdzie:
x(t) - potencjał koalicji w walce
y(t) - potencjał Iraku w walce

α - współczynnik efektywności informacyjnej Iraku w skali 1-10
β - współczynnik efektywności informacyjnej koalicji w skali 1-10
k - miara strat koalicji w skali 1 - 10
l - miara strat Iraku w skali 1 - 10
g - potencjał koalicji
h - potencjał Iraku
t - czas w dniach w stosunku rocznym
C1, C2 - stałe wyliczone z t = 0

układ równań

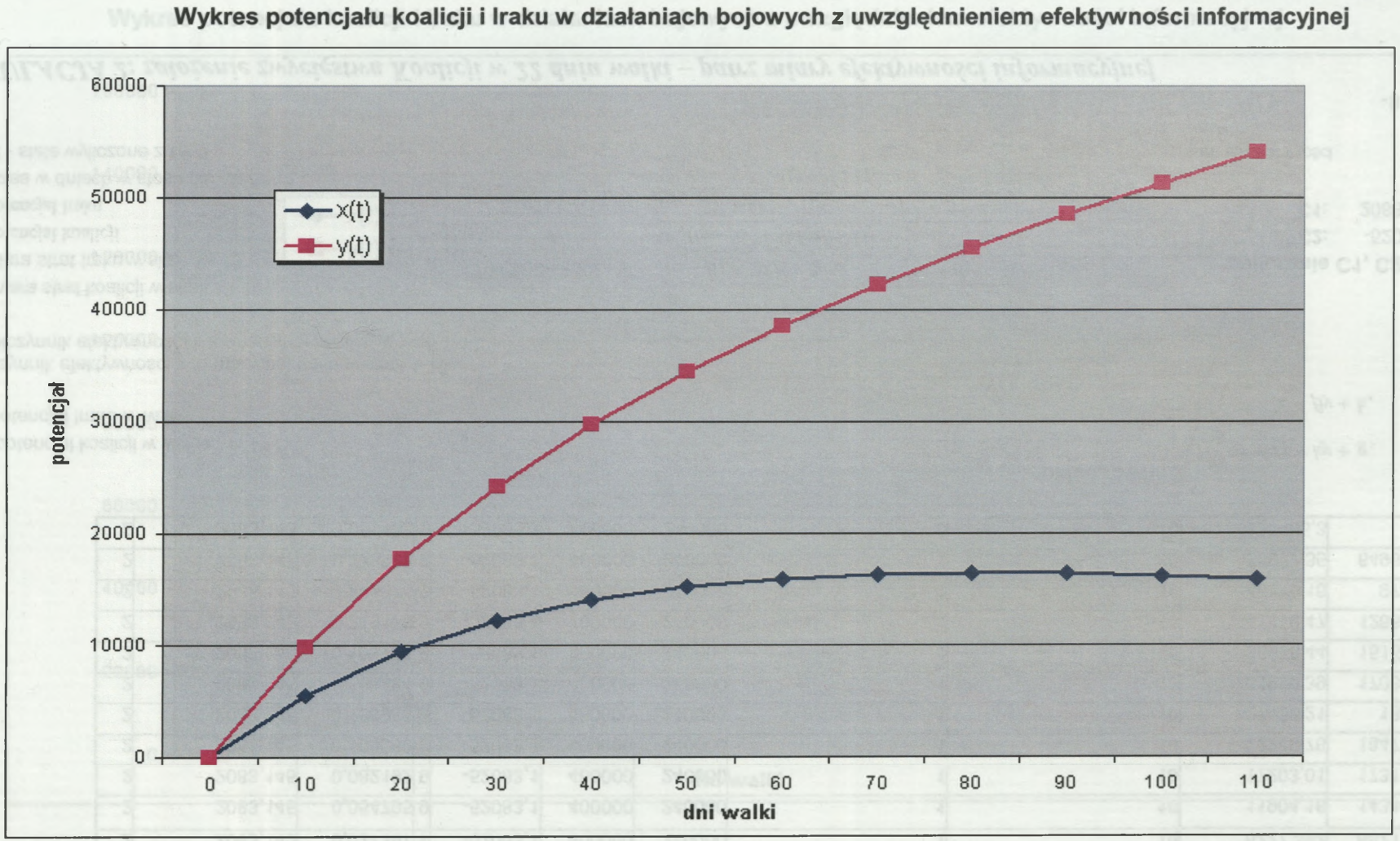
$$\begin{cases} \frac{dx}{dt} = -\alpha x - ky + g, \\ \frac{dy}{dt} = -lx - \beta y + h, \end{cases}$$

$$\begin{cases} C_1 = \frac{-2kgl + kh(\alpha + \beta - \sqrt{(\alpha-\beta)^2 + 4kl}) + \beta g(\alpha - \beta + \sqrt{(\alpha-\beta)^2 + 4kl})}{4k\sqrt{(\alpha-\beta)^2 + 4kl}(\alpha\beta - kl)} \\ C_2 = \frac{2kgl - kh(\alpha + \beta + \sqrt{(\alpha-\beta)^2 + 4kl}) - \beta g(\alpha - \beta - \sqrt{(\alpha-\beta)^2 + 4kl})}{4k\sqrt{(\alpha-\beta)^2 + 4kl}(\alpha\beta - kl)} \end{cases}$$

wyliczenie C1, C2:
C2: -8167,614
C1: 5945,3922

warunek stabilności
$\alpha\ \beta$
$-kl =$ 9

SYMULACJA 1: Obliczenie potencjału przy odwróconych proporcjach efektywności informacyjnej



Wykres 13: ***Wykres przy odwróconych miarach efektywności informacyjnej (zwycięstwo Iraku)***

Potencjał koalicji i Iraku w działaniach bojowych z uwzględnieniem miar efektywności informacyjnej

ab-kl<=0 - układ niestabilny

dni	k	C1	t	l	C2	h	g	α	β	x(t)	y(t)
0	2	2083,145	0	9	-52083,1	400000	240000	1	10	0	0
10	2	2083,145	0,027397	9	-52083,1	400000	240000	1	10	6227,392	8871,9396
20	2	2083,145	0,054795	9	-52083,1	400000	240000	1	10	11904,16	14340,301
30	2	2083,145	0,082192	9	-52083,1	400000	240000	1	10	17203,01	17319,047
40	2	2083,145	0,109589	9	-52083,1	400000	240000	1	10	22249,78	18471,416
50	2	2083,145	0,136986	9	-52083,1	400000	240000	1	10	27136,21	18278,6
60	2	2083,145	0,164384	9	-52083,1	400000	240000	1	10	31929,39	17089,612
70	2	2083,145	0,191781	9	-52083,1	400000	240000	1	10	36678,44	15157,484
80	2	2083,145	0,219178	9	-52083,1	400000	240000	1	10	41419,47	12665,556
90	2	2083,145	0,246575	9	-52083,1	400000	240000	1	10	46179,16	9746,56
100	2	2083,145	0,273973	9	-52083,1	400000	240000	1	10	50977,35	6496,4758
110	2	2083,145	0,059432	9	-52083,1	400000	240000	0	10	135455,3	0

gdzie:

x(t) - potencjał koalicji w walce

y(t) - potencjał Iraku w walce

-

α - współczynnik efektywności informacyjnej Iraku w skali 1-10

β - współczynnik efektywności informacyjnej koalicji w skali 1-10

k - miara strat koalicji w skali 1 - 10

l - miara strat Iraku w skali 1 - 10

g - potencjał koalicji

h - potencjał Iraku

t - czas w dniach w stosunku rocznym

C1, C2 - stałe wyliczone z t = 0

układ równań

$$\begin{cases} \frac{dx}{dt} = -\alpha x - ky + g, \\ \frac{dy}{dt} = -lx - \beta y + h, \end{cases}$$

$$\begin{cases} C_1 = \frac{-2kgl + kh(\alpha + \beta - \sqrt{(\alpha-\beta)^2 + 4kl}) + \beta g(\alpha - \beta + \sqrt{(\alpha-\beta)^2 + 4kl})}{4k\sqrt{(\alpha-\beta)^2 + 4kl}(\alpha\beta - kl)} \\ C_2 = \frac{2kgl - kh(\alpha + \beta + \sqrt{(\alpha-\beta)^2 + 4kl}) - \beta g(\alpha - \beta - \sqrt{(\alpha-\beta)^2 + 4kl})}{4k\sqrt{(\alpha-\beta)^2 + 4kl}(\alpha\beta - kl)} \end{cases}$$

wyliczenie C1, C2:

C2: -52083,14

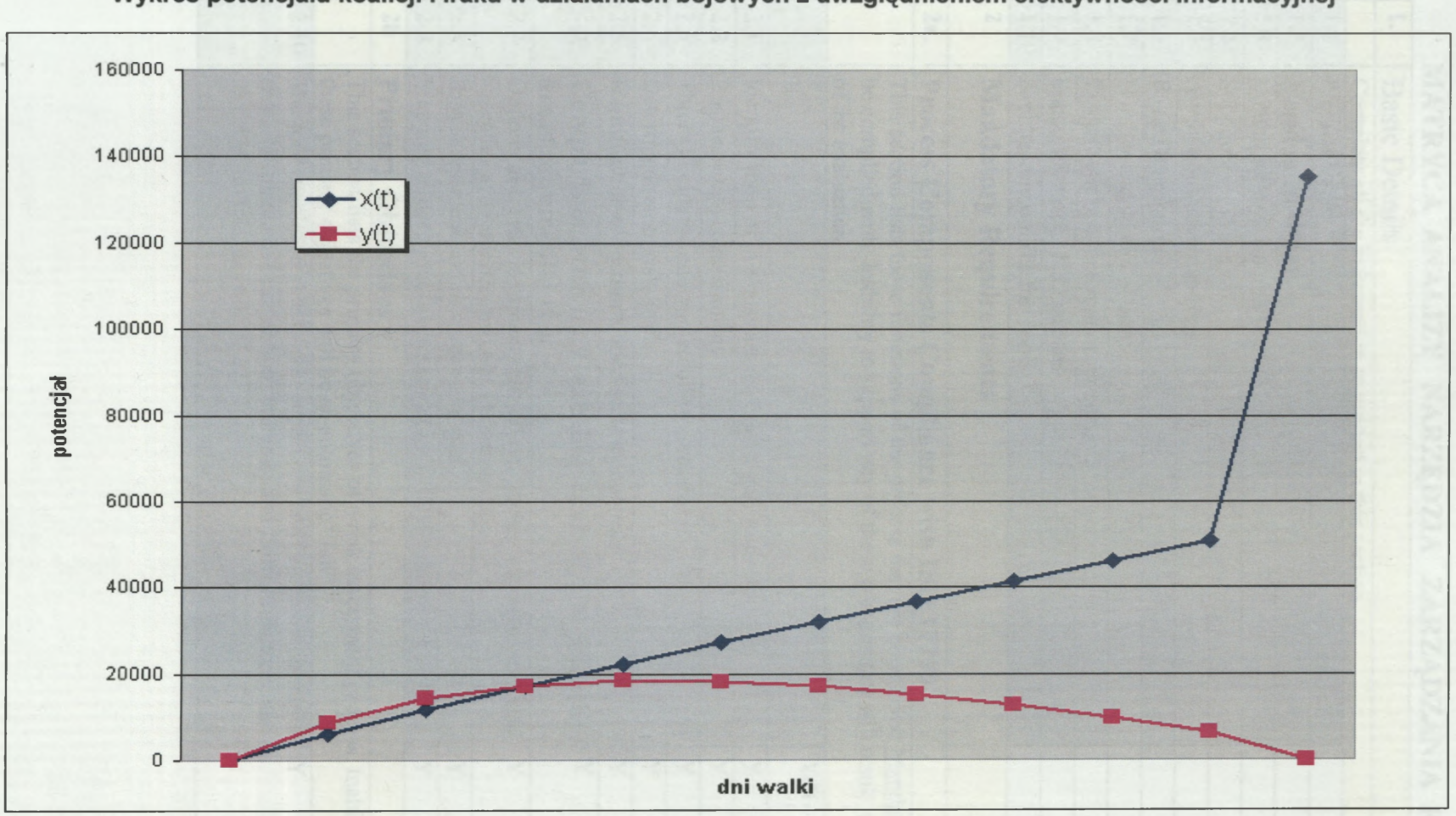
C1: 2083,1448

warunek stabilności

α β

-kl = -8

SYMULACJA 2: założenie zwycięstwa Koalicji w 22 dniu walki – patrz miary efektywności informacyjnej



Wykres 14: ***Wykres symulacji zwycięstwa Koalicji w 22-gim dniu walki (miary efektywności muszą być 0 – Irak, 10 – Koalicja)***

Załącznik 4 – Prezentacja wybranych narzędzi analizy ryzyka

MATRYCA ANALIZY NARZĘDZIA ZARZĄDZANIA RYZYKIEM

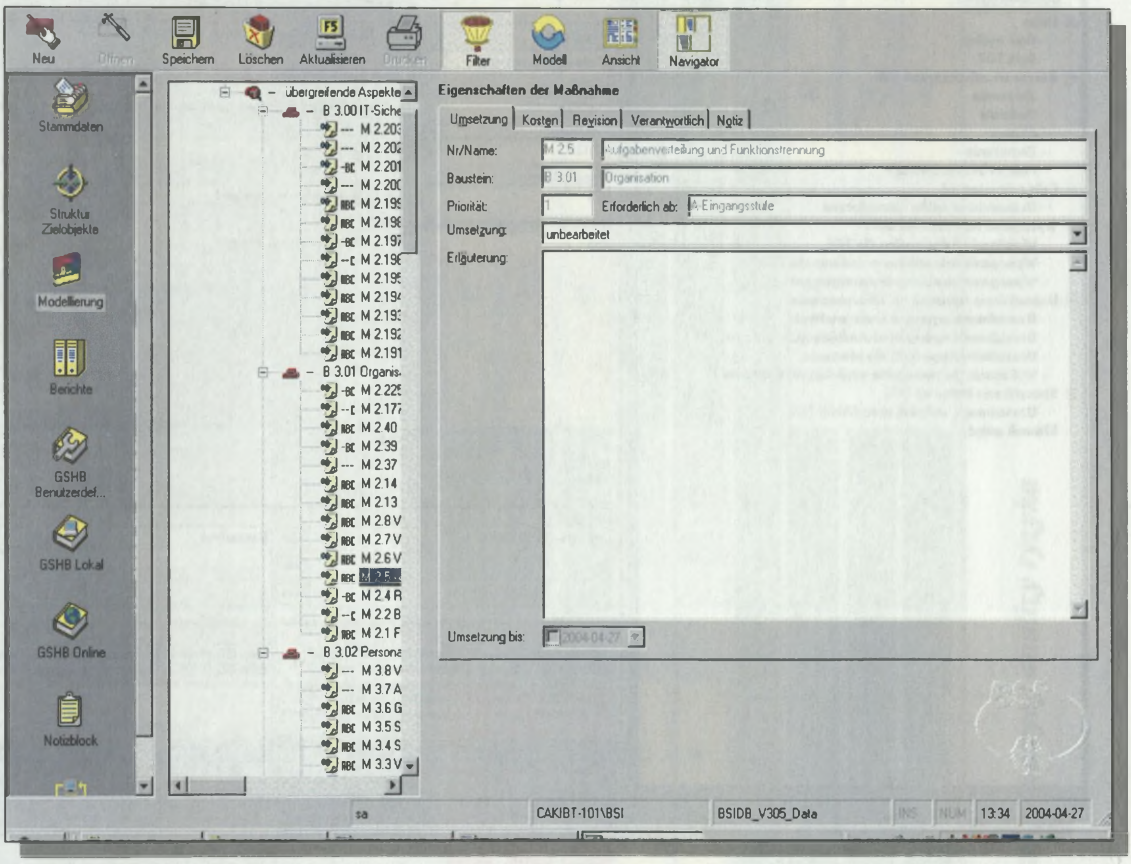
1.	Basic Details		
	Complete all the information requested in this section.		
1.1	Product Name		
1.2	**Version number**		
1.3	Date of Release (month/year)		
1.4	Supplier		
1.5	Attributions/accreditations		
1.6	Basic Description		
1.7	Number and spread of users		
1.8	Costs (Supply & per annum support)		
1.9	Support Services & Locations		
1.10	Architecture outline for Tools		
2	**Mandatory Requirements**		
2a.	**Process Components Compliance with ISO 17799**		
	This section lists those functions of the process that are considered Mandatory and which must be complied with. Inability to support any of these components will result in an automatic "fail" of the evaluation.		
		Y/N	**Optional comment**
2.1	Identification of business assets, threats and vulnerabilities	Y	
2.2	Business impact assessment	Y	
2.3	Threat likelihood and vulnerability assessment	Y	
2.4	Determination of risk levels	Y	
2.5	Identification of recommended security controls	Y	
2.6	**Comparison with any existing controls, to identify areas of remedial risk**	Y	
2.7	Options for risk treatment, including: direct management, risk acceptance, avoidance, managed transference.	Y	
2.8	Risk assessment and risk treatment plan	Y	
2.9	Mapping of decisions taken against ISO 17799 control	Y	
2b	**Primary Objectives**		
	This section lists the primary objectives of a risk assessment process. Inability to deliver and of these primary objectives will be an automatic "fail"		
2.10	The tool should be able to assess security and business continuity risks to planned information systems and infrastructures, and identify suitable controls	Y	

3.	2. Key Method Attributes					
	For each attribute rank the degree of support by graying out the relevant box and add comments. (See appendix for guidance)					
3.1	Consistent approach to risk assessment for information security and business continuity	W	FW	M	S	**VS**
3.2	Able to identify justified risk reduction and recovery measures	W	FW	M	S	**VS**
3.3	Consistent with ISO 17799	W	FW	M	S	**VS**
3.4	Consistent with DCAG Information Security Strategy and standards	W	FW	M	S	**VS**
3.5	Consistent with DCAG corporate risk management approach	W	FW	M	**S**	VS
3.6	Repeatable and highly-supported process to generate consistent results across DCAG	W	FW	M	S	**VS**
3.7	Able to address the range of processes and risk within scope.	W	FW	M	S	**VS**
3.8	Easy to use by the range of potential users	W	FW	**M**	S	VS
3.9	Flexible to support both brief high-level assessments and longer more detailed assessments	W	FW	M	S	**VS**
3.10	Openness of method	W	FW	M	S	**VS**
3.11	Auditable & Interrogatable	W	FW	M	**S**	VS
3.12	Globally available	W	FW	M	**S**	VS
3.13	Support tool with data repository for repetitive tasks, to ensure consistency and to provide supplementary expert knowledge	W	FW	M	**S**	VS

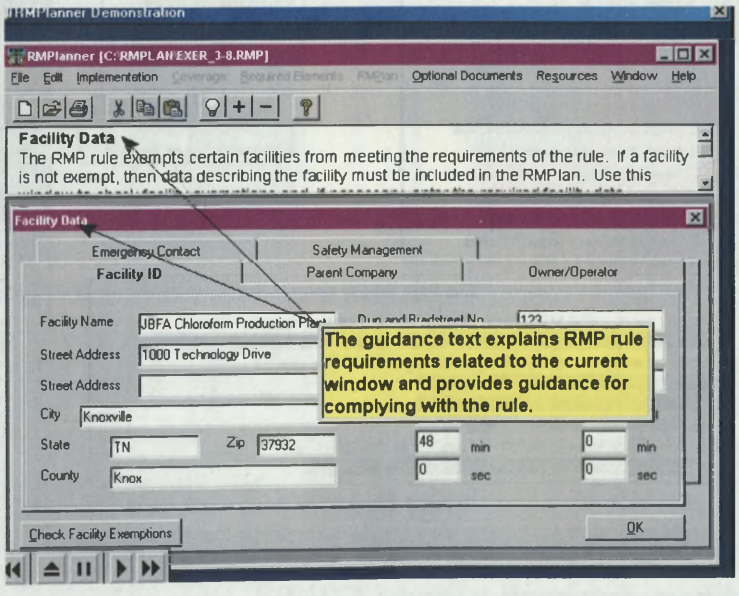
Tabela 19: ***Matryca analizy narzędzia zarządzania ryzykiem***

Źródło : *Insight Co. – badanie narzędzi analizy ryzyka;* http://www.insight.com

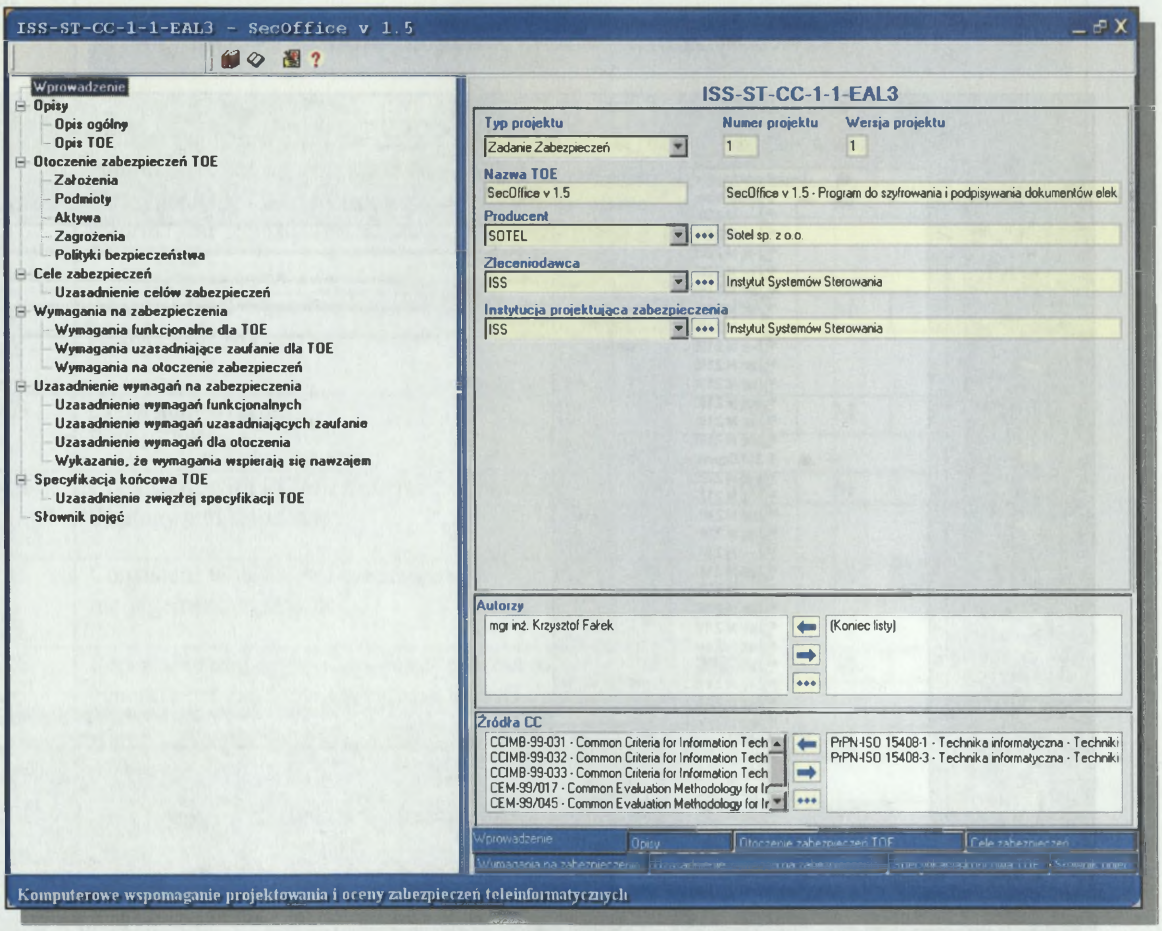
Przykłady zobrazowania narzędzi analizy ryzyka



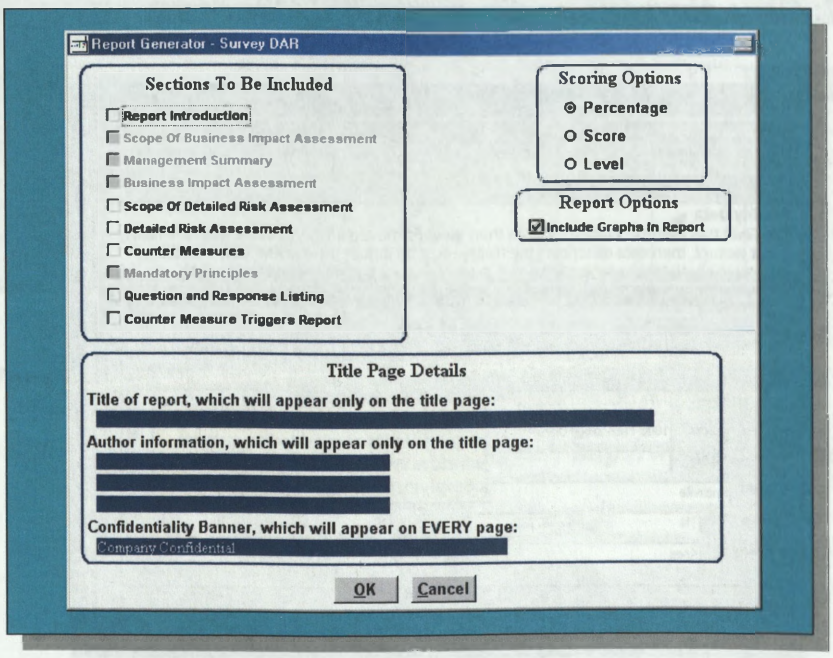
Rysunek 17: ***Okno narzędzia analizy ryzyka BSI (Niemcy)***



Rysunek 18: ***Okno narzędzia analizy ryzyka BUDDY Risk Management Planner***



Rysunek 19: ***Okno narzędzia analizy ryzyka z wykorzystaniem pakietu Common Criteria (A. Białas – firma SOTEL-IBS, Chorzów)***



Rysunek 20: ***Okno narzędzia analizy ryzyka COBRA***

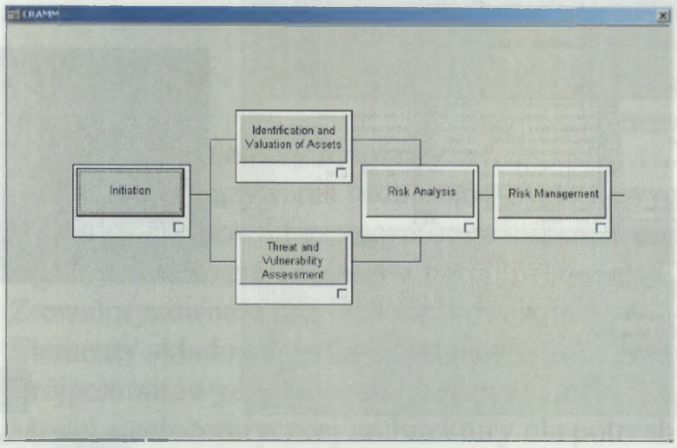
Szacowanie ryzyka		Poufność		Integralność			Dostępność		Rozliczalność	Autentyczność	
		kradzież	podsłuch	wirusy	błędy	złośliwość współużytkownika	awaria	brak zasilania	nieprawidłowy audit	Ominięcie zabezpieczeń	Logowanie się na inne konto
Dane osobowe	Skutki	4	10	1	15	20	2	1	22	12	12
	Podatność	6	1	1	1	1	10	15	1	4	2
	Ryzyko	24	10	1	15	20	20	15	22	28	24
Bezpieczeństwo haseł	Skutki	40	40	12	40	100	2	1	45	40	40
	Podatność	0,5	2	3	5	1	2	1	1	1	2
	Ryzyko	20	80	36	200	100	4	1	45	40	80
Oprogramowanie użytkowe	Skutki	10	10	14	12	12	2	2	1	12	10
	Podatność	20	1	5	3	4	2	15	1	2	1
	Ryzyko	200	10	60	36	48	4	15	1	24	10
Informacje niejawne	Skutki	30	15	3	5	3	4	4	15	40	20
	Podatność	5	6	1	2	2	2	2	1	1	2
	Ryzyko	150	90	3	10	6	8	8	15	40	40

Przykład odwzorowania matrycy analizy ryzyka

CRAMM Front Screen

CRAMM V
Risk Assessment

To use this interactive walkthrough, hover the mouse pointer over a button and click.



Insight Consulting
www.insight.co.uk

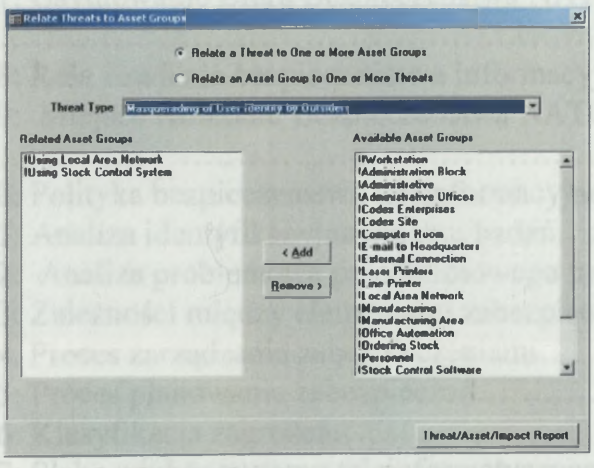
All screen shots are interactive, click on the buttons to take you through to the next screen. Within CRAMM itself the screens have been designed to promote intuitive process flow. To continue with this walkthrough select any of the buttons above.

backwards
to introduction

backwards
to BS 7799

Relate Threats to Asset Groups

CRAMM V
Risk Assessment

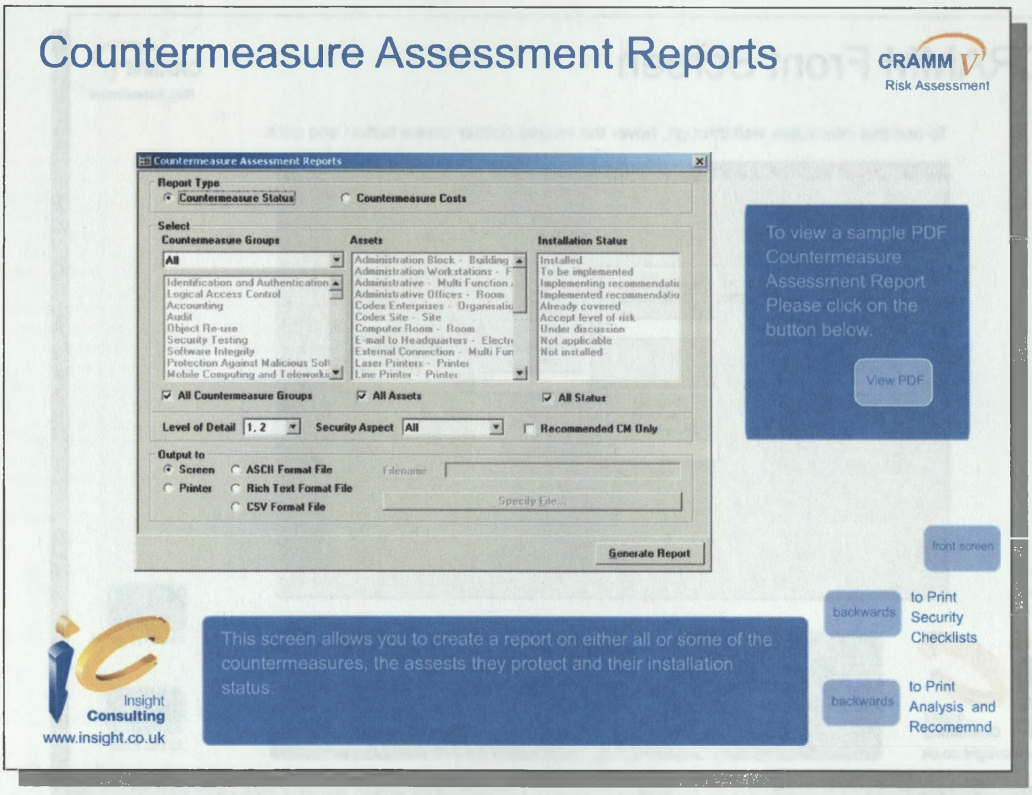


Insight Consulting
www.insight.co.uk

Threats addressed by the review are investigated against selected asset groups. The scope of the review indicates the threats and assets considered. Each threat should be linked with the appropriate asset groups, e.g. threat of fire in server rooms. CRAMM provides comprehensive guidance on associating threats to assets.

front screen

backwards



Rysunek 21: ***Zobrazowanie narzędzia analizy ryzyka CRAMM (Wlk. Brytania)***

Źródło : *Insight Co.;* http://www.insight.com

SPIS ILUSTRACJI

Diagramy

Diagram 1: Obszar przedmiotowy rozprawy....11
Diagram 2: Schemat rozwiązywania problemów systemowych....31
Diagram 3: Analiza systemowa bezpieczeństwa informacyjnego – procedury....35
Diagram 4: Ogólny układ bezpieczeństwa narodowego....43
Diagram 5: Zrewaloryzowanie roli walki informacyjnej....64
Diagram 6: Elementy składowe walki informacyjnej....70
Diagram 7: Trójpoziomowy model walki informacyjnej....71
Diagram 8: Model sieciocentrycznej architektury dla potrzeb *NCO*....73
Diagram 9: Siatki sensorów i środków walki rozpięte na siatce informacyjnej....75
Diagram 10: Model informacji *C.E. Shannona*....79
Diagram 11: Efekt wiedzy....91
Diagram 12: Zobrazowanie przewagi/dominacji informacyjnej....94
Diagram 13: Schemat organizacji ochrony informacji niejawnych w Rzeczypospolitej Polskiej....123
Diagram 14: Odpowiedzialność za bezpieczeństwo informacji niejawnych w jednostce organizacyjnej....125
Diagram 15: *Cykl Deminga*....131
Diagram 16: Diagram przyczynowo-skutkowy Ishikawy typu „rybi szkielet" dot. systemu bezpieczeństwa informacyjnego....133
Diagram 17: Usytuowanie Biura Bezpieczeństwa NATO (*NOS*) w strukturze sojuszu....153
Diagram 18: Rola i zadania bezpieczeństwa informacyjnego (*INFOSEC*) NATO...153
Diagram 19: Miejsce Komitetu Bezpieczeństwa NATO w strukturze władz sojuszu....155
Diagram 20: Polityka bezpieczeństwa teleinformacyjnego....178
Diagram 21: Analiza identyfikacyjna obiektu badań....197
Diagram 22: Analiza problemowa przedmiotowego materiału....199
Diagram 23: Zależności między elementami zabezpieczenia....202
Diagram 24. Proces zarządzania zabezpieczeniami....203
Diagram 25: Proces planowania zabezpieczeń....204
Diagram 26: Klasyfikacja zagrożeń....206
Diagram 27: Słabe punkty systemu teleinformatycznego....208
Diagram 28: Typowe środki ochrony....209
Diagram 29: Możliwe ataki na system teleinformatyczny....211
Diagram 30: Przebieg analizy diagnostycznej przedmiotowego materiału....230
Diagram 31 Zarządzanie ryzykiem obejmujące szczegółową analizę ryzyka....237
Diagram 32: Analiza prognostyczna przedmiotowego materiału....239
Diagram 33: Schemat działania *MAGERIT*....274

Diagram 34: Zarządzanie ryzykiem w metodzie *Rozeta Marion*.....*278*
Diagram 35: Koncepcja modelu procesów analizy zagrożeń i zarządzania ryzykiem.....*282*
Diagram 36: Modelowanie i symulacja matematyczna.....*283*
Diagram 37: Modelowanie i symulacja matematyczna.....*284*
Diagram 38: Analiza efektywności.....*287*
Diagram 39: Schemat analizy decyzyjnej.....*292*
Diagram 40: Pionowa sieć działań w zakresie bezpieczeństwa informacyjnego państwa.....*294*
Diagram 41: Proces zarządzania ryzykiem.....*297*
Diagram 42: Proces postępowania wobec ryzyka.....*302*

Rysunki

Rysunek 1: Mapa działań bojowych operacji *Iraqi Freedom* z 31 .03. 2003 r.....*102*
Rysunek 2: Mapa działań bojowych operacji *Iraqi Freedom* z 8 .04. 2003 r.....*102*
Rysunek 3: Mapa sytuacji bojowej w operacji *Iraqi Freedom* z 10 .04. 2003 r.....*104*
Rysunek 4: Sieciocentryczna architektura pola walki uwypuklająca znaczenie czynnika informacyjnego.....*108*
Rysunek 5: Współzależność różnych rodzajów operacji informacyjnych.....*110*
Rysunek 6: Cykle procesu bezpieczeństwa teleinformacyjnego.....*111*
Rysunek 7: Rodzaje specyfikacji wymagań.....*145*
Rysunek 8: Wykorzystywanie rezultatów ocen.....*147*
Rysunek 9: Wykorzystanie rezultatów oceny *TOE*.....*148*
Rysunek 10: Organizacja procesu oceny i certyfikacji wg *PCA*.....*149*
Rysunek 11: Proces certyfikacji.....*150*
Rysunek 12: Diagram przedstawiający strukturę organizacyjną *CIRC*.....*161*
Rysunek 13: Interpretacja graficzna zjawiska globalizacji.....*190*
Rysunek 14: Miejsce analizy ryzyka w zarządzaniu bezpieczeństwem systemów informatycznych.....*233*
Rysunek 15: Związki w zarządzaniu ryzykiem.....*234*
Rysunek 16: Ryzyko w funkcji strat i częstotliwości.....*235*
Rysunek 21: Zobrazowanie narzędzia analizy ryzyka *CRAMM* (Wlk. Brytania).....*348*
Rysunek 20: Okno narzędzia analizy ryzyka *COBRA*.....*347*
Rysunek 19: Okno narzędzia analizy ryzyka z wykorzystaniem pakietu *Common Criteria* (*A. Białas* – firma *SOTEL-ISS*, Chorzów).....*346*
Rysunek 18: Okno narzędzia analizy ryzyka *BUDDY Risk Management Planner*...*345*
Rysunek 17: Okno narzędzia analizy ryzyka *BSI* (Niemcy).....*345*

Tabele

Tabela 1: Wskaźniki potęgi obliczone metodą *Fucksa*.....*49*
Tabela 2: Dane wyjściowe dla państw NATO (1999 r.).....*52*
Tabela 3: Naliczona potęga państw NATO (1999 r.) w kategorii dochodu narodowego i w kategorii wydatków wojskowych.....*53*
Tabela 4: Nasycenie sprzętem walki informacyjnej w wybranych państwach NATO.*86*
Tabela 5: Obliczenie wskaźników taksonomicznych obiektu-wzorca.....*87*

Tabela 6: Prawa Informacji *Lanchestera*.....96
Tabela 7: Uśrednione dane wartości bojowych Iraku I Koalicji.....101
Tabela 8: Potencjał Koalicji i Iraku w działaniach bojowych z uwzględnieniem miar efektywności informacyjnej.....102
Tabela 9: Przykłady zagrożeń.....243
Tabela 10: Formularz do ujęcia i kwantyfikacji ryzyka *FTA*.....269
Tabela 11: Przykład zastosowania metody *Ranking the Threats by Measures of Risk*.....276
Tabela 12: Analiza ocenowa wybranych narzędzi analizy zagrożeń i zarządzania ryzykiem.....289
Tabela 19: Matryca analizy narzędzia zarządzania ryzykiem.....344
Tabela 18: Kwadratowe prawo *Lanchestera*.....329
Tabela 17: Uśrednione dane wartości bojowych Iraku I Koalicji.....328
Tabela 16: Układ sił w operacji *Iraqi Freedom* (Konferencja Naukowa AON).....328
Tabela 15: Układ sił w operacji *Iraqi Freedom* („*Myśl Wojskowa*").....327
Tabela 14: Układ sił w operacji *Iraqi Freedom* (raport *Cordesman'a*).....327
Tabela 13: Nasycenie specjalnym sprzętem walki informacyjnej państw NATO 326
Tabela 12: Tabela specjalnego sprzętu walki informacyjnej wybranych państw NATO.....325

Wykresy

Wykres 1: Wskaźniki potęgi obliczone metodą *Fucksa* za okres zimnej wojny.....50
Wykres 2: Wykres potęg państw NATO (1999 r.) w kategorii dochodu narodowego i w kategorii wydatków wojskowych (logarytmiczny).....54
Wykres 3: Miary podobieństw nasycenia sprzętem walki informacyjnej.....88
Wykres 4: Miary dystansów nasycenia sprzętem walki informacyjnej.....88
Wykres 5: Wykres przewagi sprzętowej strony irackiej.....101
Wykres 6: Wykres potencjału koalicji i Iraku w działaniach bojowych z uwzględnieniem efektywności informacyjnej (stany liczebne wojsk).....101
Wykres 7: Wykres potencjału Koalicji i Iraku w działaniach bojowych z uwzględnieniem zmaksymalizowanej efektywności informacyjnej Koalicji.....103
Wykres 8: Wykres potencjału koalicji i Iraku w działaniach bojowych z uśrednionymi danymi całości sił.....105
Wykres 9: Spełnianie warunków powodzenia Koalicji w operacji *Iraqi Freedom*...106
Wykres 10: Przyczyny braku skuteczności we wdrażaniu zabezpieczeń informacji..177
Wykres 11: Miary podobieństw wybranych narzędzi analizy ryzyka.....290
Wykres 12: Miary dystansów wybranych narzędzi analizy ryzyka.....291
Wykres 14: Wykres symulacji zwycięstwa Koalicji w 22-gim dniu walki.....341
Wykres 13: Wykres przy odwróconych miarach efektywności informacyjnej.....339

BIBLIOTEKA GŁÓWNA – ARCHIWUM
Nr ewid. 57161
Akademii Obrony Narodowej