



AKADEMIA OBRONY NARODOWEJ

Projekt badawczy 0500A 01923:
MODELOWANIE ZAGROŻEŃ DLA BEZPIECZEŃSTWA INFORMACYJNEGO PAŃSTWA. TEORIA WALKI INFORMACYJNEJ

ZAGROŻENIA DLA BEZPIECZEŃSTWA INFORMACYJNEGO PAŃSTWA

(Identyfikacja, analiza zagrożeń i ryzyka)

Tom I

Raport z badań

Biblioteka Główna
Akademii Obrony Narodowej
S/5838 t.1
05-005838-002-0

WARSZAWA

68716

AKADEMIA OBRONY NARODOWEJ

Projekt badawczy 0500A 01923:
MODELOWANIE ZAGROŻEŃ DLA BEZPIECZEŃSTWA INFORMACYJNEGO PAŃSTWA. TEORIA WALKI INFORMACYJNEJ

BIBLIOTEKA GŁÓWNA - ARCHIWUM
Nr ewid. 68716
Akademii Obrony Narodowej

ZAGROŻENIA DLA BEZPIECZEŃSTWA INFORMACYJNEGO PAŃSTWA

(Identyfikacja, analiza zagrożeń i ryzyka)

Tom I

BIBLIOTEKA GŁÓWNA
Nr ewid.
Akademii Obrony Narodowej

Raport z badań

Warszawa **2004**

Opracował zespół autorski:

Gen. broni prof. dr inż. Tadeusz **JEMIOŁO**	**T.I. roz. 1.2.**
Płk prof. dr hab. inż. Piotr **SIENKIEWICZ**	**T.I. roz. 1.1., 1.9., 1.10., T.II.roz.1.1.**
Płk dr hab. Ryszard **SZPYRA**	**T.I roz.1.3. T.II.roz.2.2., 2.3.**
Mjr dr hab. Henryk **SPUSTEK**	**T.I. roz. 1.8.**
Płk dr inż. Marek **KINASIEWICZ**	**T.I. roz. 1.6. T.II. roz.2.4.**
Płk dr inż. Marian **URBANEK**	**T.I. roz. 1.7.**
Ppłk dr inż. Janusz **WOCIAL**	**T.I. roz. 1.7.**
Ppłk dr inż. Piotr **GÓRNY**	**T.I. roz. 1.4.**
Ppłk dr inż. Wiesław **BŁAŻEJCZYK**	**T.III roz.1.,3.,4.**
Mjr mgr inż. Jan **KUCHARSKI**	**T.I. roz. 1.5. T.III.roz.4.,5.**
Kpt. mgr inż. Jerzy **GRZYB**	**T.III. roz.2.,4.**
Mgr Halina **ŚWIEBODA**	**T.I. roz.1.9. redakcja całości**

Spis treści

1.1. METODOLOGICZNE PODSTAWY BADAŃ NAD BEZPIECZEŃSTWEM INFORMACYJNYM PAŃSTWA 5

1.2. WYZWANIA I ZAGROŻENIA DLA GLOBALNEGO BEZPIECZEŃSTWA INFORMACYJNEGO W PIERWSZYCH DEKADACH XXI WIEKU 18

1.2.1. Ogólne uwarunkowania globalnego bezpieczeństwa informacyjnego 18
1.2.2. Terroryzm informacyjny 23
1.2.3. Rodzaje atakowanych systemów informacyjnych 24
1.2.4. Terroryzm informacyjny i jego wpływ na globalne środowisko bezpieczeństwa 25
Bibliografia 29

1.3. DZIAŁANIA (OPERACJE) INFORMACYJNE: POJĘCIA, POGLĄDY, CECHY 30

1.3.1. Ocena piśmiennictwa 30
1.3.2. Geneza i rozwój poglądów na temat operacji informacyjnych 45
Bibliografia 70

1.4. SPECYFIKACJA TYPÓW I OBIEKTÓW ZAGROŻEŃ INFORMACYJNYCH 74

1.4.1. Internet – atrakcja informacyjna czy zagrożenie 76
1.4.2. Klasyfikacja zagrożeń 81
1.4.3. Zagrożenia informacyjne związane z przestępczością komputerową 85
1.4.4. Ochrona informacji 110
Bibliografia 112

1.5. ZAGROŻENIA DLA INFRASTRUKTURY TELEKOMUNIKACYJNEJ PAŃSTWA 113

1.5.1. Stan infrastruktury komunikacyjnej RP 113
1.5.2. Zagrożenia infrastruktury telekomunikacyjnej w czasie pokoju, kryzysu i wojny 132
Bibliografia 134

1.6. IDENTYFIKACJA ZJAWISKA INFOTERRORYZMU 135
1.6.1. Cyberprzestrzeń – nowe pole konfrontacji..... 138
1.6.2. Charakterystyka działań przestępczych w cyberprzestrzeni..... 143
1.6.3. Przeciwdziałanie zagrożeniom infoterrorystycznym..... 149
Bibliografia..... 158

1.7. WARTOŚĆ INFORMACJI W SYTUACJACH KRYZYSOWYCH I KONFLIKTOWYCH 159
1.7.1. Informacja i jej właściwości..... 161
1.7.2. Badania ilościowe informacji..... 167
1.7.3. Użyteczność informacji..... 168
1.7.4. Jakość informacji..... 173
1.7.5. Wartość informacji..... 180
1.7.6. Degradacja wartości informacji..... 184
Bibliografia..... 188

1.8. MODELOWANIE WALKI INFORMACYJNEJ 189
1.8.1. O entropii i prawie wzrostu entropii..... 189
1.8.2. Model prawdopodobieństwa wiedzy..... 192
1.8.3. Metoda Monte Carlo w probabistycznym modelu przewagi..... 193
1.8.4. Entropowy model przewagi..... 196
1.8.5. Teoria gier w zastosowaniach militarnych..... 203
1.8.6. Stochastyczne równanie logistyczne..... 207
Bibliografia..... 210

1.9. METODYKA OCENY ZAGROŻEŃ INFORMACYJNYCH..... 211
1.9.1. Analiza możliwych i dopuszczalnych zagrożeń informacyjnych... 211
1.9.2. Analiza ryzyka a analiza zagrożeń..... 216
1.9.3. Zarządzanie ryzykiem..... 220
1.9.4. Zautomatyzowane systemy analizy ryzyka..... 232
1.9.5. Ekonomiczne aspekty bezpieczeństwa informacyjnego..... 242
1.9.6. Standardy normalizacyjne oraz akty prawne w zakresie bezpieczeństwa systemów informatycznych..... 278
1.9.7 Stan prawny w Europie..... 289
1.9.8. Uregulowania prawne w Polsce..... 291
Bibliografia..... 300

1.10. WNIOSKI..... 303

1.1. METODOLOGICZNE PODSTAWY BADAŃ NAD BEZPIECZEŃSTWEM INFORMACYJNYM PAŃSTWA

Przełom wieków przyniósł zjawisko o dwóch obliczach: **globalizację** i **społeczeństwo globalnej informacji**. Jest to w istocie proces dynamiczny i wieloliniowy w swojej naturze, wieloaspektowy i wielowymiarowy (zarówno w sensie przyczyn, jak i skutków). Przyczyną była kumulacja wielu procesów społeczno-politycznych, ekonomicznych i naukowo-technicznych. Wśród nich szczególną wagę ma dynamiczny postęp w sferze **technologii informacyjnych**, w obszarze tzw. MIRT (Mikroelektronika – Informatyka – Robotyka – Telekomunikacja). Przyniósł on m.in. *„kompresje przestrzeni" i „kompresje czasu".*

Skutkiem globalizacji i rozwoju społeczeństwa informacyjnego są nowe wyzwania cywilizacyjne i nowe szanse rozwojowe (zarówno dla krajów wysoko rozwiniętych, jak i dla krajów modernizujących się), ale i nowe zagrożenia. Szczególnym zagrożeniem stał się cyberterroryzm (inforterroryzm). Wyzwaniem natomiast stała się potrzeba stworzenia nowej polityki bezpieczeństwa informacyjnego oraz budowa efektywnego systemu bezpieczeństwa informacyjnego zapewniającego pożądany poziom bezpieczeństwa przede wszystkim tzw. **krytycznej infrastruktury państwa**.

Prezydent G.W. Bush stwierdził (2001) i *„Stany Zjednoczone i ich alianci będą z całą mocą dążyć do utrzymania równowagi sił światowych zapewniającej ludzką wolność. Wymaga to nowej strategii ogólnej, która wyjdzie poza doktryny zimnej wojny i będzie dotyczyła głównie zagrożeń nowego stulecia – takich jak cyberterroryzm, stosowanie broni masowego rażenia, rakiet - znajdujących się w rękach tych, dla których stosowanie terroryzmu i szantaże jest sposobem na życie. Są to groźby, które mogą zagrozić wolności i postępowi, na co nie możemy pozwolić. (...) Cyberterroryzm jest zagrożeniem, które zwalczać musimy wspólnie".* Z kolei, były dyrektor FBI L.Frech ostrzegał mówiąc o cyberterroryźmie *„Jest to nowa groźba, która zmusza nas do stworzenia specjalnego systemu obrony, odstraszania i odpowiadania na ataki. (...) Nasze narodowe infrastruktury krytyczne – cyberstruktury i struktury fizyczne – stanowią dla terrorystów, hakerów, kryminalistów i obcych agentów cel ataków, które mogą mieć katastrofalne konsekwencje".*

W 2002 roku podczas przygotowań do Olimpiady Zimowej w Utah przeprowadzono symulacje wzajemnych zależności infrastrukturalnych, w kontekście możliwych i prawdopodobnych ataków terrorystycznych (w tym cyberterrorystycznych na systemy teleinformatyczne), zgodnie ze scenariuszem p.k. BLACK ICE. Wnioski uzyskane w wyniku przeprowadzenia tego ćwiczenia dotyczyły przede wszystkim konieczności holistyczno-systemowego badania zjawiska cyberterroryzmu, analizy systemowej zagrożeń informacyjnych i wyboru strategii przeciwdziałania tym zagrożeniom. Wskazano na istnienie coraz większej liczby wzajemnych krytycznych zależności różnego rodzaju systemów infrastruktury oraz na skutki (zniszczenia) cybernetycznego i fizycznego ataku.

W raporcie *„National Strategy to Secure Cyberspace"* podkreślano: *„Do roku 2003 nasza gospodarka i bezpieczeństwo narodowe stały się w pełni zależne od technologii i infrastruktury teleinformatycznej. Sieć sieci wspiera wykonywanie operacji we wszystkich sektorach naszej gospodarki: energetyce (energia elektryczna, ropa, lotnictwo, marynarka handlowa), finansach i bankowości, informacji i telekomunikacji, służbie zdrowia, służbach ratunkowych, wodociągowych i kanalizacji, przemyśle chemicznym, przemyśle obronnym i spożywczym, poczcie i spedycji".*

Przedstawione sądy i opinie, w pełni uzasadnione realnymi przykładami incydentów różnej wagi i skali, potwierdzają potrzebę badań podjętych w projekcie badawczym. **Celem badań** było opracowanie metodologii analizy i oceny zagrożeń dla bezpieczeństwa informacyjnego państwa i modelowania procesów walki informacyjnej, która mogłaby stanowić podstawę projektowania ekspertowego systemu wspomagania decyzji – wyboru racjonalnych strategii przeciwdziałania zagrożeniom informacyjnym państwa.

Przyjęto następujące **ogólne założenia**:

(1) bezpieczeństwo informacyjne stanowi istotny czynnik bezpieczeństwa państwa (rysunek 1.1);

(2) istnieją – realnie i potencjalnie – różnorodne typy i rodzaje zagrożeń informacyjnych, w tym zagrożenia, których źródła i formy nie zostały w pełni zidentyfikowane (rysunek 1.2);

(3) obszarem wymagającym szczególnych środków zabezpieczenia jest tzw. krytyczna infrastruktura państwa, obejmująca następujące, wzajemne powiązania, systemy:

- **Energia elektryczna**: elektrownie, sieci przemysłowe i dystrybucyjne dostarczające elektryczność do użytkowników końcowych.
- **Produkcja, magazynowanie i dostarczanie gazu oraz ropy naftowej**: urządzenia do wydobywania i przechowywania gazu ziemnego i ropy naftowej, surowej i przetworzonej, oraz urządzenia rafineryjne i magazyny paliw.
- **Telekomunikacja**: sieci komputerowe i telekomunikacyjne, oprogramowanie, procesy i ludzie dbający o prawidłowe działanie wszystkiego – od publicznych sieci komputerowych po Internet.
- **Bankowość i finanse**: banki, towarzystwa kredytowe, fundusze inwestycyjne, giełdy, firmy handlowe, systemy rezerw finansowych, inwestycje służące oszczędzaniu, udzielaniu pożyczek, ubezpieczeń, a także dokonywaniu rządowych operacji finansowych i wspierających gospodarkę.
- **Systemy dostarczania wody**: zasoby wodne, rezerwy i zbiorniki wodne, akwedukty i inne systemy transportowania wody.
- **Transport**: sieci połączeń lotniczych z liniami lotniczymi, lotniskami i samolotami; drogi, autostrady, ciężarówki i samochody osobowe; flota handlowa; porty i drogi wodne; transport masowy; fracht i przewóz pasażerów przez kolej; wszystkie usługi doręczycielskie.
- **Służby do działań w sytuacjach wyjątkowych**: służby medyczne, policja, straż pożarna, wszystkie systemy ratownictwa.
- **Infrastruktura operacji rządowych**: wszelkie służby i działania władz centralnych, lokalnych, samorządowych konieczne do zapewnienia działania podstawowych służb publicznych.

(4) wszystkie systemy tworzące „krytyczną infrastrukturę państwa: pozostają w silnej zależności od bezpieczeństwa, niezawodności i sprawności systemów informacyjnych (teleinformatycznych) oraz jakości usług informacyjnych (w szczególności od Internetu); zależność ta będzie coraz większa (rysunek 1.3);

(5) wzrost „ilościowy i jakościowy" zagrożeń informacyjnych dla bezpieczeństwa systemów powoduje wzrost niepewności i ryzyka w procesach podejmowania decyzji strategicznych - ryzyko stało się kategorią podstawową (rysunek 1.4);

(6) istnieje potrzeba stworzenia systemu wczesnego ostrzegania przed zagrożeniami informacyjnymi i prognozowania zagrożeń;

(7) racjonalną metodą analizy prognostycznej zagrożeń informacyjnych dla bezpieczeństwa państwa jest technika scenariuszy, w ramach których mogą być prowadzone eksperymenty symulacyjne;

(8) środkiem racjonalizacji decyzji w zakresie bezpieczeństwa informacyjnego są ekspertowe systemy wspomagania decyzji (wyboru strategii przeciwdziałania zagrożeniom informacyjnym);

(9) w sferze bezpieczeństwa narodowego rozwój technologii informacyjnej przyniósł *"piąty wymiar"* walki zbrojnej – cybernetyczny obok *„tradycyjnych"*: lądowego, powietrznego, morskiego i kosmicznego (model Wardena rysunek 1.5.);

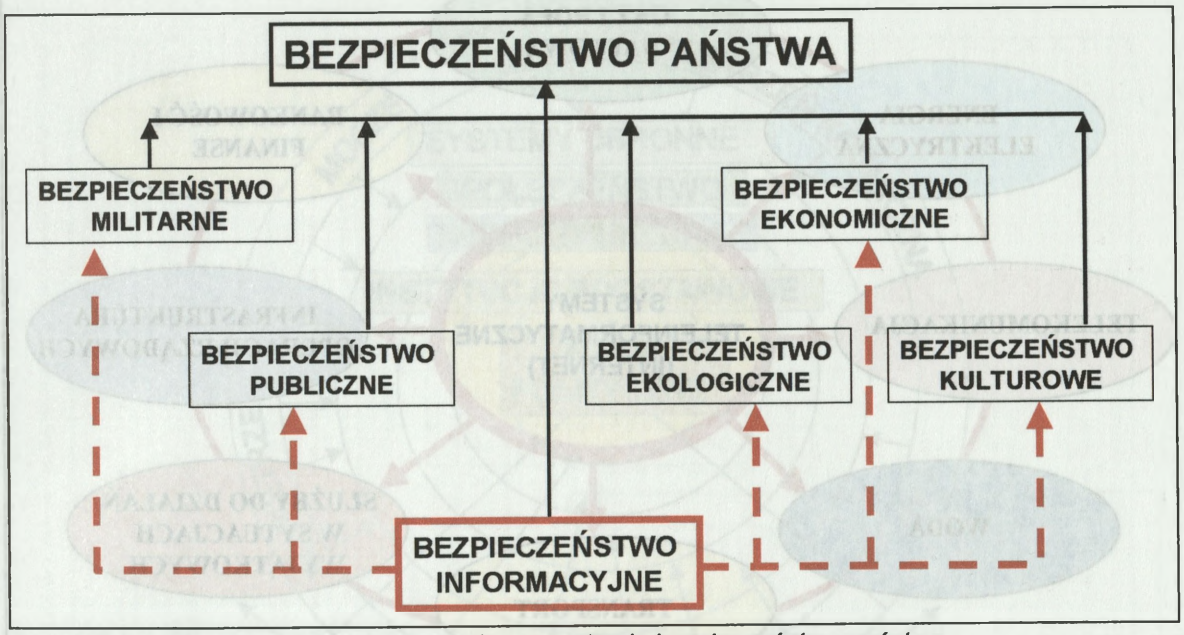
(10) walka informacyjna jako tradycyjnie immanentna składowa walki zbrojnej (rozpoznanie, wre itp.) uzupełniona niejako została o elementy *„infowar" („cyberwar", „netwar").*

Powyższe ogólne założenia złożyły się na ogólną konstatację, która legła u podstaw sformułowanego celu badań, a mianowicie:

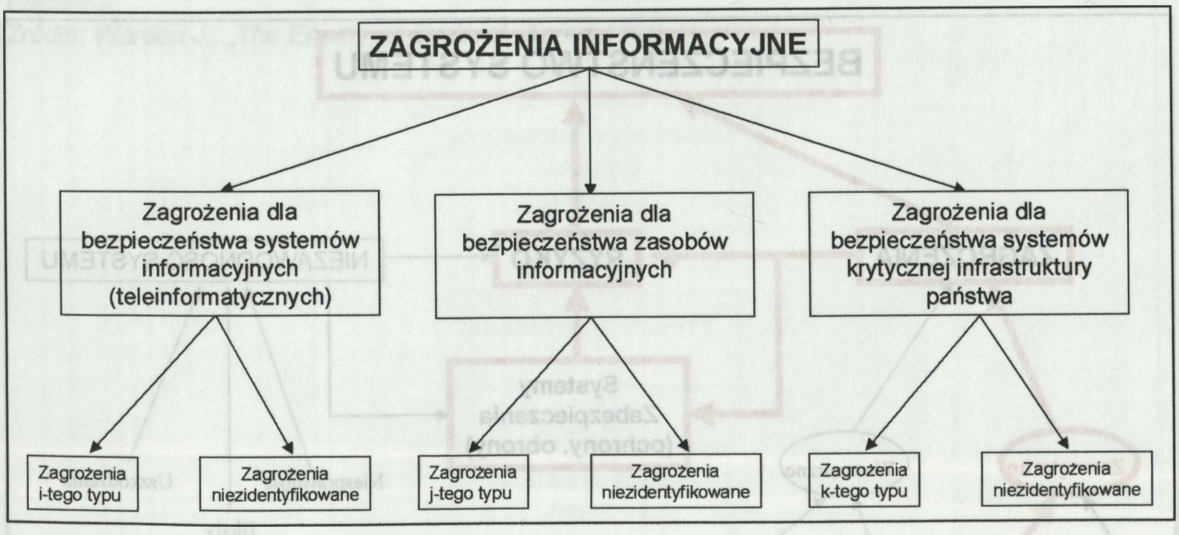
- brak jest systemowej koncepcji bezpieczeństwa informacyjnego pozwalającej na opracowanie modelu systemu bezpieczeństwa informacyjnego systemu (państwa, organizacji);
- brak jest jednolitych holistyczno-systemowych teoretycznych podstaw walki informacyjnej (cybernetycznej).

Badania systemowe nad bezpieczeństwem informacyjnym Państwa i modelami walki informacyjnej (cybernetycznej) stanowią istotny warunek projektowania:

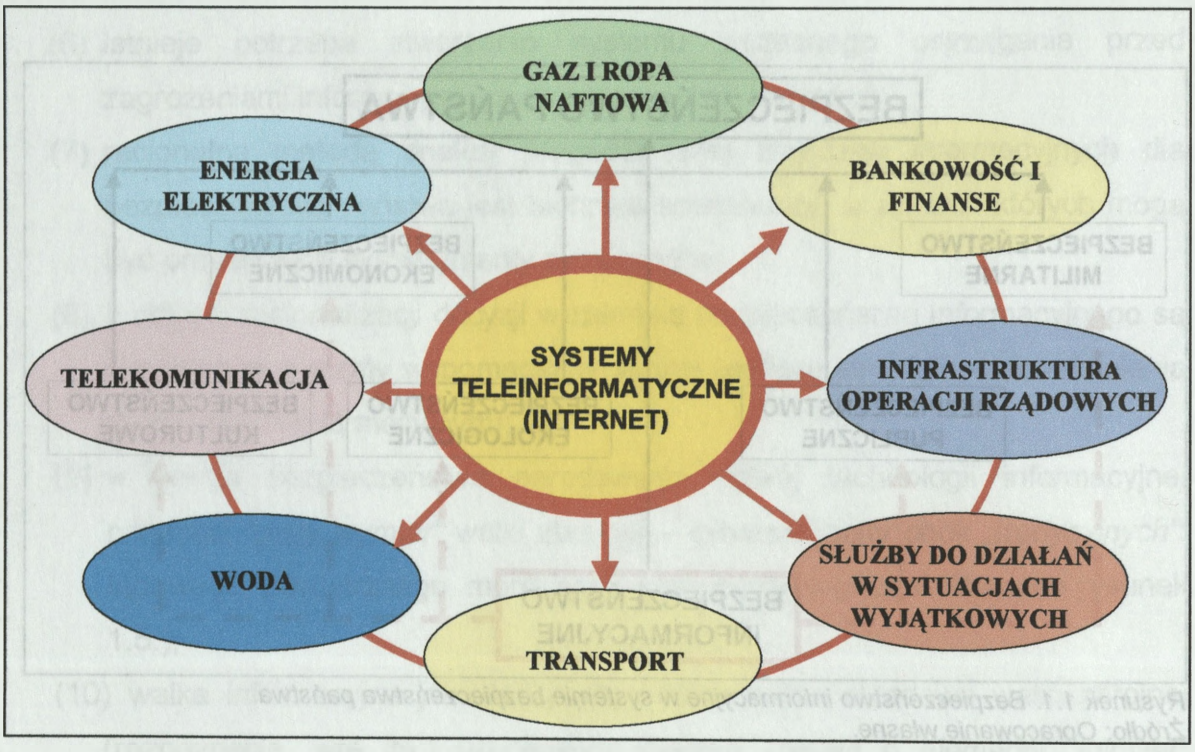
- polityki bezpieczeństwa informacyjnego (rysunek 1.6),
- strategii bezpieczeństwa informacyjnego,
- systemu zabezpieczenia przed zagrożeniami informacyjnymi,
- metod i środków wspomagania zarządzania bezpieczeństwem informacyjnym (w tym zarządzania ryzykiem).



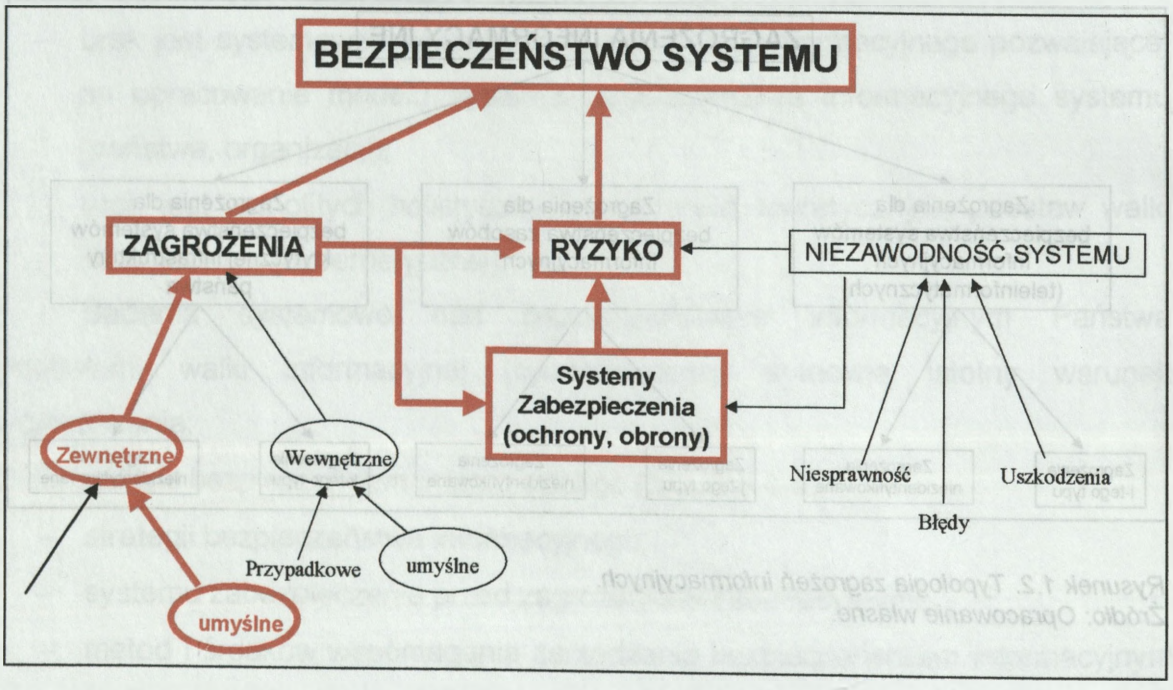
Rysunek 1.1. Bezpieczeństwo informacyjne w systemie bezpieczeństwa państwa.
Źródło: Opracowanie własne.



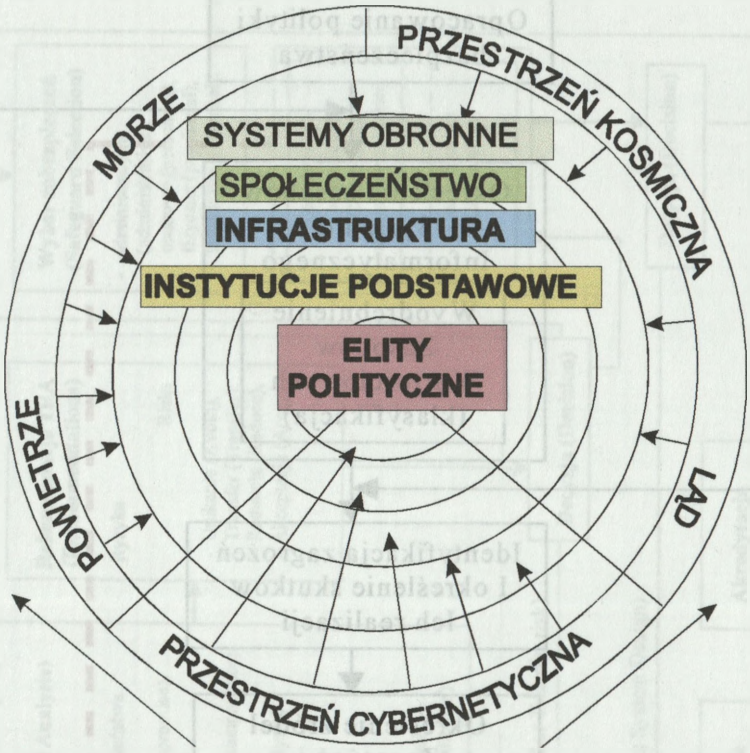
Rysunek 1.2. Typologia zagrożeń informacyjnych.
Źródło: Opracowanie własne.



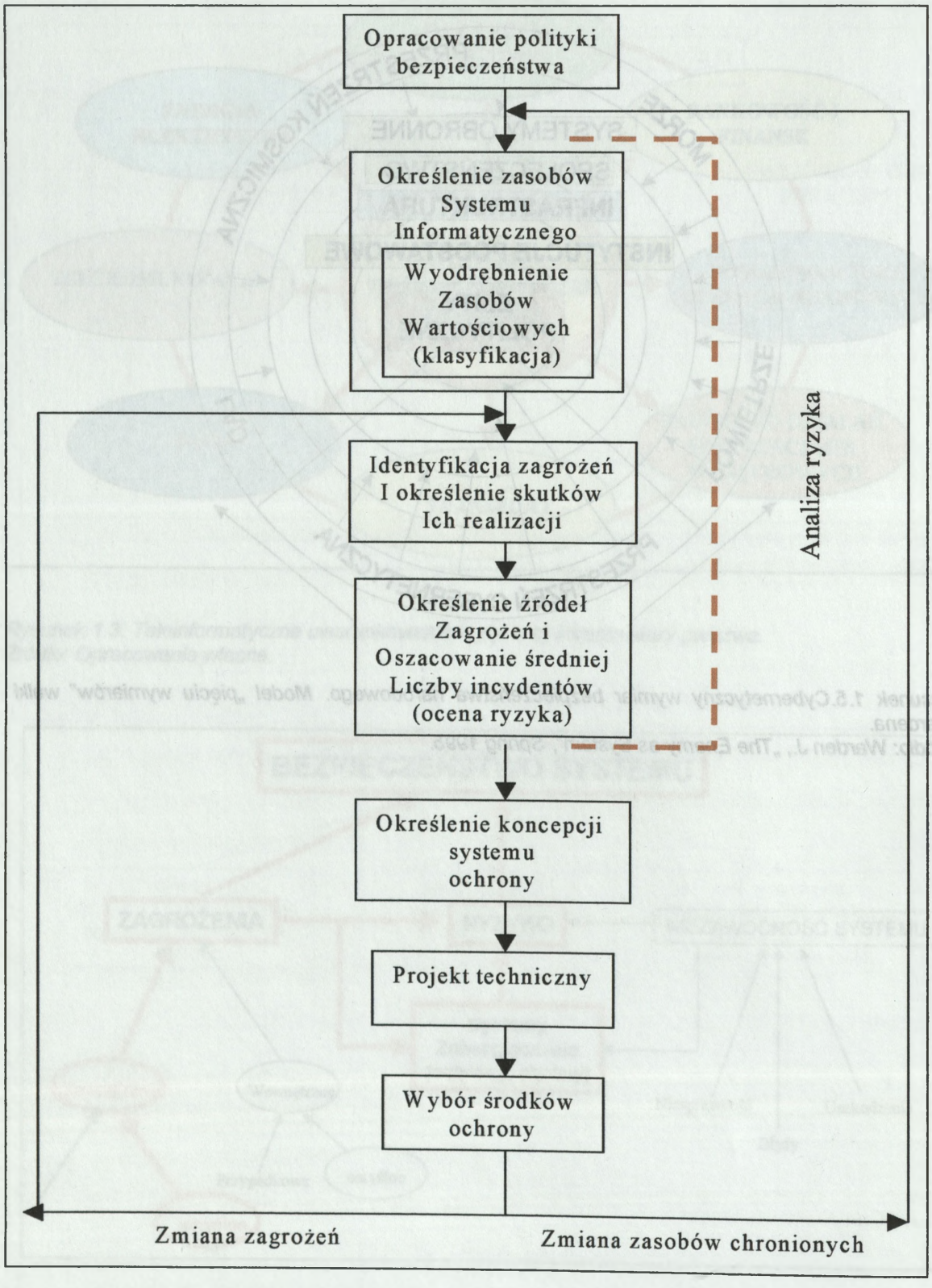
Rysunek 1.3. Teleinformatyczne uwarunkowania krytycznej infrastruktury państwa.
Źródło: Opracowanie własne.



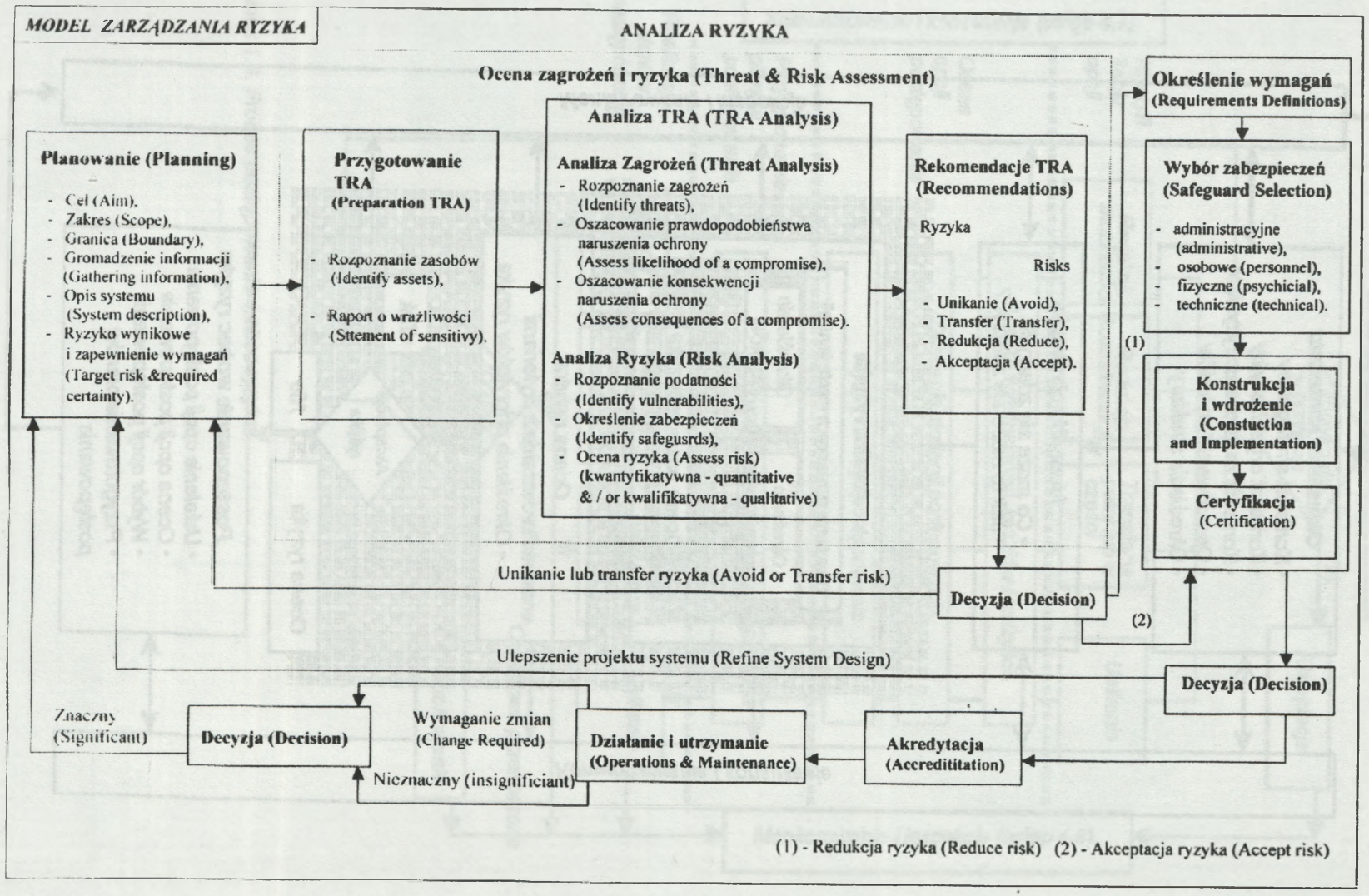
Rysunek 1.4. Koncepcja analizy systemowej bezpieczeństwa.
Źródło: Opracowanie własne.



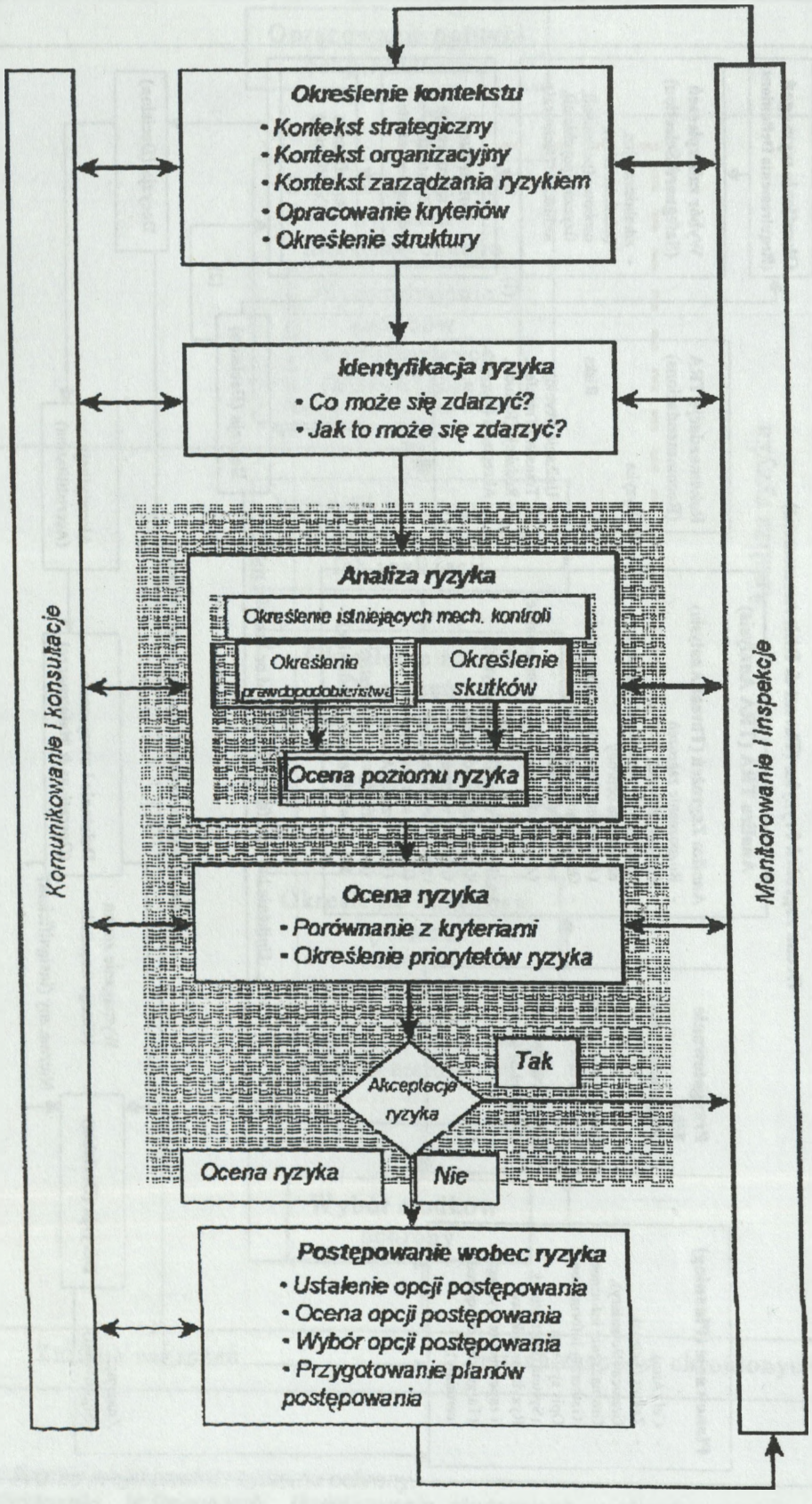
Rysunek 1.5.Cybernetyczny wymiar bezpieczeństwa narodowego. Model „pięciu wymiarów" walki Wardena.
Źródło: Warden J., „The Enemy as System", Spring 1995.



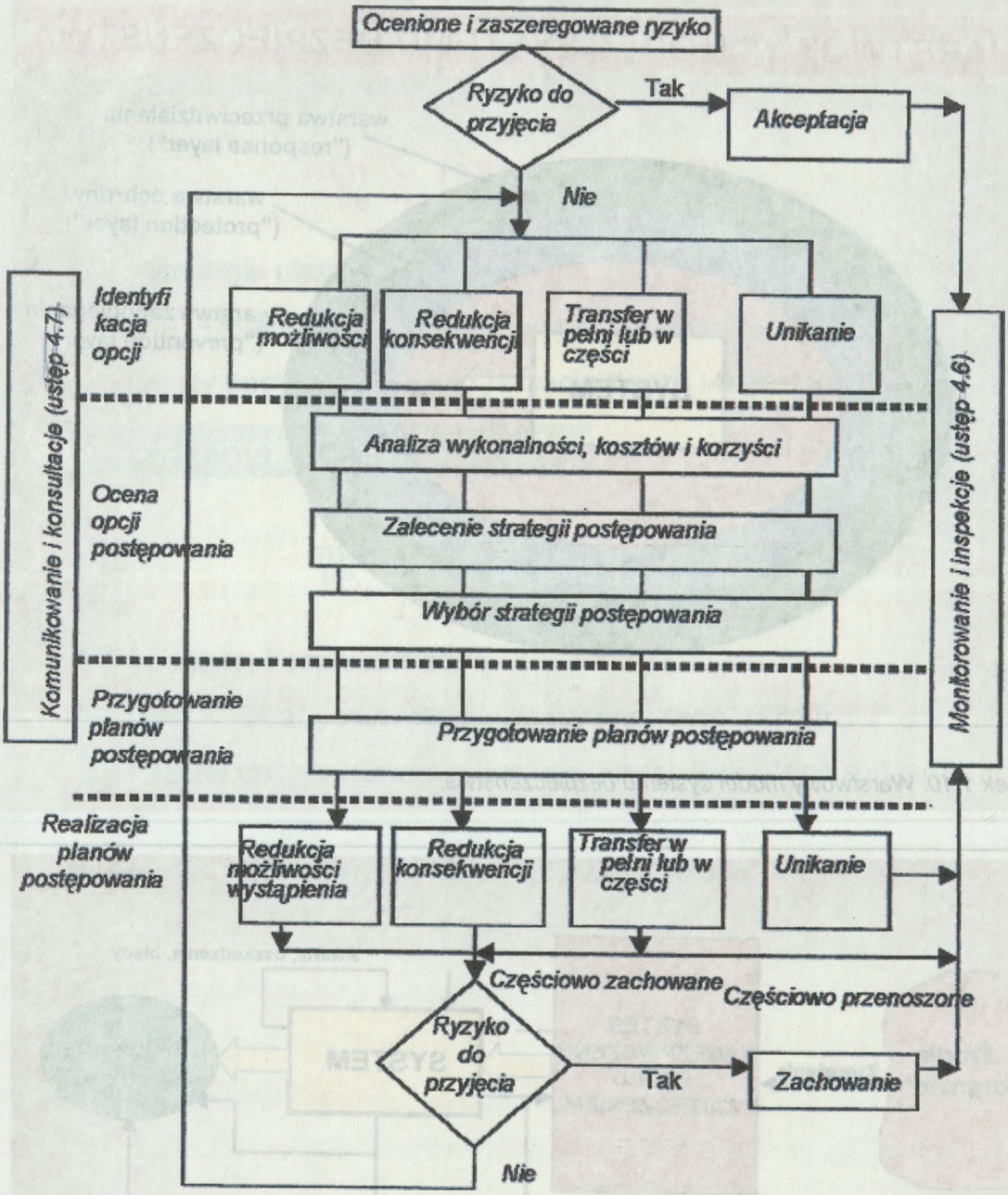
Rysunek 1.6. Proces projektowania systemu ochrony.
Źródło: J. Piotrowski, M.Szymaczek, Projektowanie skutecznych systemów ochrony informacji „Informatyka" 7.8/97, s.48.



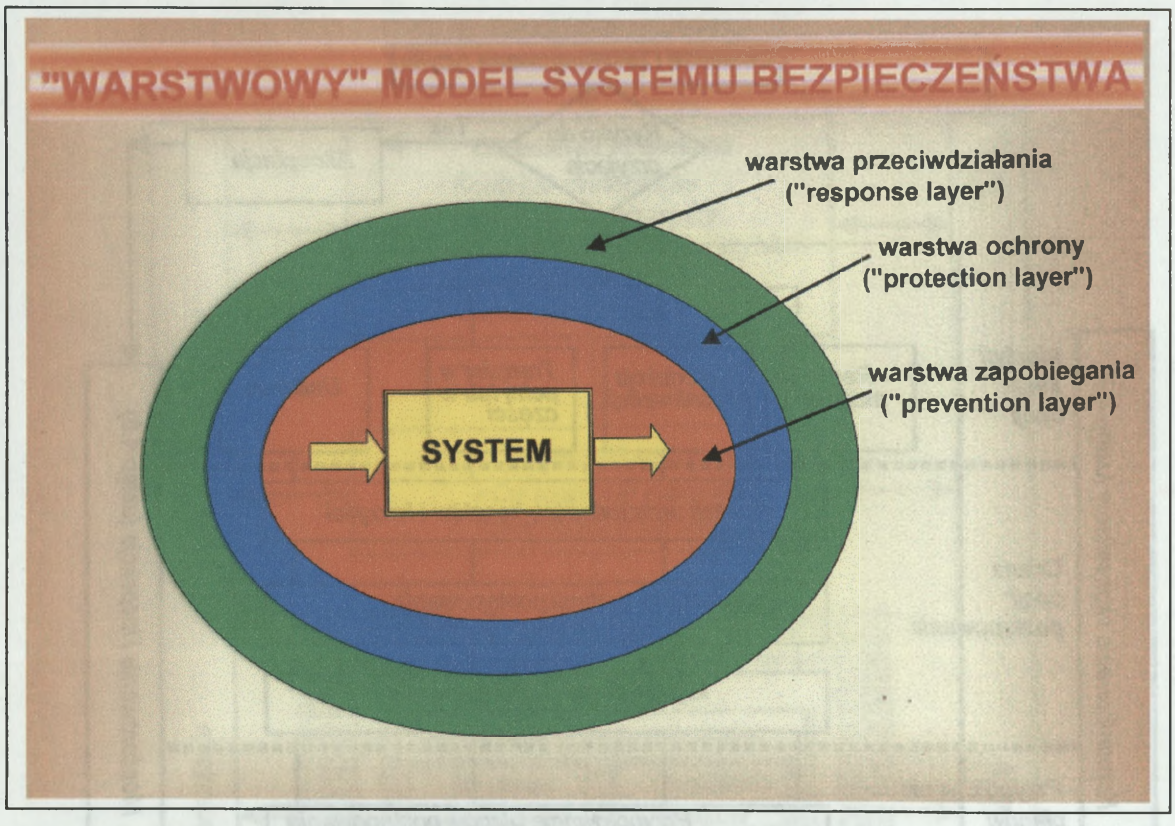
Rysunek 1.7. Analiza ryzyka.



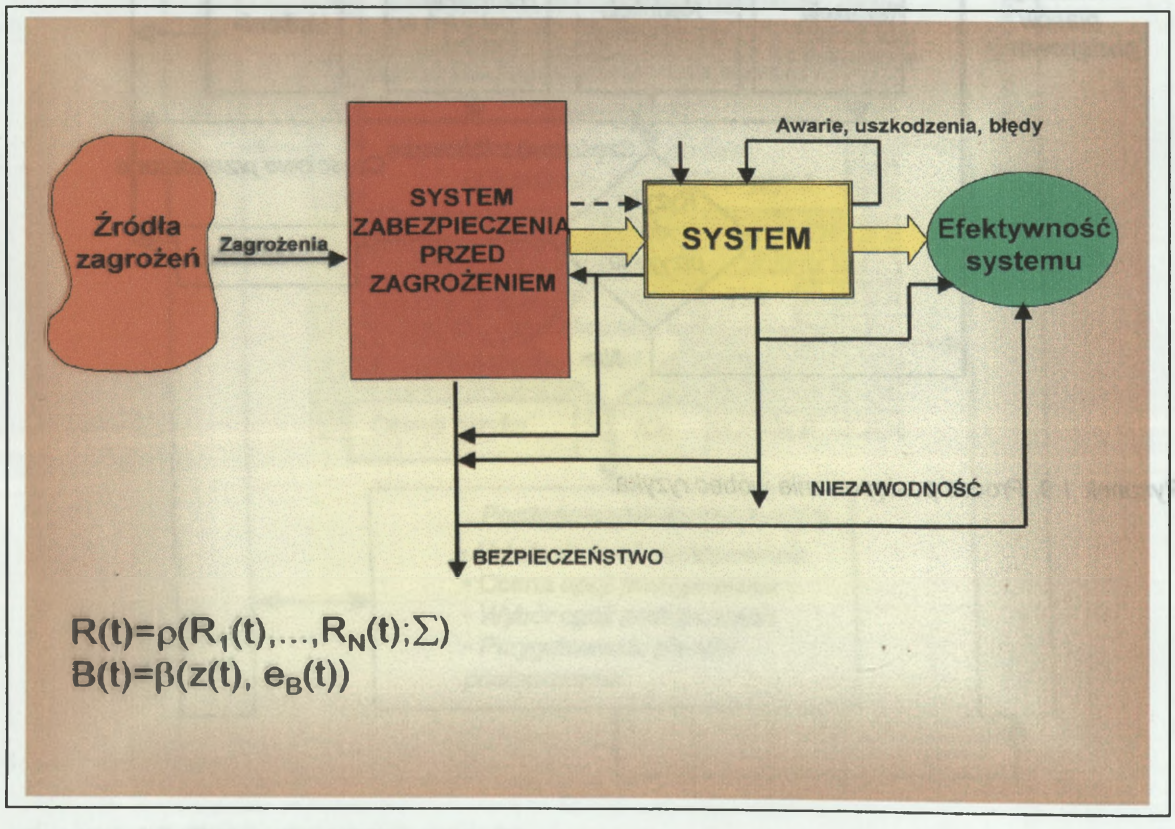
Rysunek 1.8. Proces zarządzania ryzykiem.



Rysunek 1.9. Proces postępowania wobec ryzyka.



Rysunek 1.10. Warstwowy model systemu bezpieczeństwa.



Rysunek 1.11. System zabezpieczenia przed zagrożeniem.

Zarządzanie niezawodnością

$$\min_{S_R} \sum_i \left(N_i^R(S_R) + S_i^R\right)$$

S_R - strategia niezawodności

$N_i^R(S_R)$ - nakłady na redukcję awarii i-tego rodzaju

S_i^R - straty spowodowane aktywizacją awarii i-tego rodzaju

Zarządzanie bezpieczeństwem

$$\min_{P^B} \sum_j \left(N_j^B(P^B) + S_j^B\right)$$

P^B - polityka bezpieczeństwa

$N_j^B(P^B)$ - nakłady na redukcję zagrożeń j-tego rodzaju

S_j^B - straty spowodowane aktywizacją zagrożeń j-tego rodzaju

Rysunek 1.12. Zarządzanie niezawodnością i bezpieczeństwem.

1.2. WYZWANIA I ZAGROŻENIA DLA GLOBALNEGO BEZPIECZEŃSTWA INFORMACYJNEGO W PIERWSZYCH DEKADACH XX WIEKU

1.2.1. Ogólne uwarunkowania globalnego bezpieczeństwa informacyjnego

Ataki terrorystyczne na *World Trade Center* w Nowym Jorku i Pentagon w Waszyngtonie z 11 września 2001 roku spowodowały gwałtowną zmianę sytuacji bezpieczeństwa w skali globalnej. Bezpośrednio po zamachach większość państw NATO, w tym Polska zostało zmuszonych do wprowadzenia w życie elementów narodowych systemów gotowości obronnej. Tragedia ta stała się też źródłem głębokiej refleksji społeczności międzynarodowej obejmującej zarówno przyczyny jak i konsekwencje tego wydarzenia, któremu mając na uwadze stosunki międzynarodowe, można nadać charakter niezaprzeczalnie przełomowy.

Zamach na symbole amerykańskiej potęgi w sposób jednoznaczny udowodnił, że "...dzisiejsze zagrożenia posiadają inna naturę i skalę niż dotychczas, a współczesna odpowiedź na te zagrożenia jest nieadekwatna. Broń projektowana w celu przeciwstawienia się zagrożeniom, w końcu ostatniego tysiąclecia, nie będzie w stanie sprostać im w pierwszych dekadach XXI wieku. Nowe często o asymetrycznym charakterze zagrożenia dla bezpieczeństwa globalnego wymagają nowego myślenia"[1].

Konieczność nowego podejścia jest nagląca, gdyż terroryzm jest tylko, jednym z wielu nietradycyjnych wyzwań dla bezpieczeństwa. Stanowią je także: konflikty etniczne i religijne, przemyt narkotyków, masowe migracje, regionalna niestabilność, pranie brudnych pieniędzy, działania różnych grup ekstremistycznych oraz kradzież informacji. Najczęściej bardzo trudno jest zidentyfikować przywódcę lub region, gdzie można by skoncentrować zainteresowanie w celu przeciwstawienia się im. Co więcej skala tych zagrożeń jest tak duża, że stanowi zagrożenie dla wielu krajów. Zagrożenia te nie znają bowiem granic państwowych i kontynentalnych. Istnieje też zasadnicza trudność we właściwej identyfikacji zjawisk (organizacji, przywódców) w celu podjęcia skutecznego przeciwdziałania im. Zagrożenia te mogą podważać

[1] *Por. R.Hall, C.Fox: Ponownie przemyśleć bezpieczeństwo, "Przegląd NATO", Zima 2001/2002, s.8.*

istotę i podwaliny funkcjonowania instytucji narodowych i międzynarodowych, a także doprowadzić do ruiny gospodarki wielu państw[2].

Jednocześnie także legalne organizacje działające w skali ponadpaństwowej zyskują na sile i wpływach dysponując technicznymi możliwościami dostosowania się do nowego środowiska bezpieczeństwa. Spekulanci giełdowi, handlowcy, korporacje międzynarodowe, firmy świadczące usługi internetowe posiadają obecnie możliwości znaczącego, globalnego wpływu na życie codzienne obywateli wielu państw. Globalizacja wspólnie z rewolucją w technologii informatycznej, dała tym instytucjom przewagę. Ich kontrola jest bardziej sprawowana za pośrednictwem rynków finansowych niż przez struktury globalne, a zakłócenia powstają według takiej samej zasady. Dlatego też nie powinno dziwić, że tradycyjne mechanizmy państwa oparte na idei granic, porządku, władzy, policji, struktur siłowych są zagrożone. Wydają się one także ze swojej natury niezdolne do przeciwstawienia się współczesnym wyzwaniom dla bezpieczeństwa. W miarę jak owa niezdolność staje się coraz bardziej widoczna, narasta rozczarowanie poprzednim systemem, i może powstać przekonanie, że wszystko w dziedzinie bezpieczeństwa zmierza ku gorszemu[3].

Można, zatem wnioskować, że w dającej się przewidzieć przyszłości jednym z ajistotniejszych problemów dla głównych aktorów współczesnej polityki światowej jest analiza trendów globalnych głównie politycznych i ekonomicznych. Kwestie globalne na początku obecnego stulecia maja także pierwszoplanowe znaczenie dla bezpieczeństwa światowego. Globalizacja oznacza, bowiem wzrost różnego rodzaju powiązań między podmiotami życia międzynarodowego oraz wzajemne, najczęściej asymetryczne oddziaływania we wszystkich sferach życia społeczeństwa, od umiędzynarodowienia rynków i kapitału po kulturę masową, migracje, finanse i apewnienie pokoju. Globalizacja w dziedzinie bezpieczeństwa wymusza konieczność większej coraz szybszej, wszechstronniejszej i bardziej skomplikowanej reakcji na zachodzące wydarzenia. Lapidarną ale bardzo wymowną formułę współzależności jakie tworzy globalizacja zdefiniował były zastępca sekretarza stanu USA S.Talbot: "co się dzieje tam, ma znaczenie tutaj" (*what happens there matters here*).

Spośród bogatego katalogu zagrożeń dla bezpieczeństwa Polski coraz bardziej realne stają się zagrożenia w sferze teleinformatycznej. Rośnie zagrożenie

---

[2] *Ibidem.*
[3] *R.Hall, C.Fox, Op.cit., s.8.*

operacjami mającymi na celu dezorganizację kluczowych systemów informacyjnych instytucji rządowych oraz niektórych sfer sektora prywatnego, oddziałujących na system bezpieczeństwa państwa, a także operacjami związanymi z penetracją baz danych i prowadzenia działań dezinformacyjnych[4].

Dynamiczny rozwój infrastruktury systemów komputerowych wpłynął w zdecydowany sposób na wzrost efektywności niemal każdej dziedziny ludzkiej działalności. Wraz z rozwojem informatyzacji pojawiły się nowe problemy związane z iewłaściwym zastosowaniem osiągnięć elektronicznego przetwarzania danych. Wzrost wykorzystania zaawansowanej technologii, a w szczególności systemów komputerowych i całej towarzyszącej przy tym infrastrukturze informatycznej spowodował pojawienie się nowego obszaru do nielegalnej działalności. Wraz ze wzrostem wykorzystania tej technologii pojawia się coraz częściej problem zapewnienia ich bezpieczeństwa.

Dostępność rozproszonych sieciowych ośrodków obliczeniowych nie ograniczonych tylko do jednego pomieszczenia, rozległość sieci, a także rozmycie pewnych działań związanych z komputerami i telekomunikacją powoduje, ze dokonywanie przestępstw w "*obszarze hi-tech*" nie jest już rzadkością, lecz staje się podstawą działalności coraz większej ilości grup przestępczych. Wzrastająca liczba tej grupy przestępstw jest wynikiem wielu przesłanek, do których zaliczyć można:

- kompatybilność coraz większej ilości zdalnych systemów;
- dostępność niezbyt drogiego sprzętu i oprogramowania;
- przyjmowane standardy dla sprzętu i oprogramowania.

Z dotychczasowych badań zagrożeń związanych z oddziaływaniem przestępstw na systemy komputerowe wynika, że najczęściej wykorzystują oni informacje uzyskane w wyniku prowadzonego rozpoznania dotyczącego podatności na uszkodzenia określonego rodzaju oprogramowania. Prowadzi to do sytuacji, w tórej zanim producent zdoła zaimplementować, a klient zainstalować odpowiednią łatę (*ang. patch*), przestępca z reguły zdoła do tego czasu uzyskać dostęp do informacji przechowywanych w danym systemie. Nie ulega wątpliwości, że o zroście ilości przestępstw decydują także takie elementy jak kompetencje *hackerów*, łatwość użytkowania systemów oraz unifikowalność narzędzi.

---

[4] *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej.*

W wielu przypadkach samo środowisko stworzone przez zaawansowaną technologię, ułatwia sposób dokonania przestępstwa. Zdarza się często, że informacje przechowywane w postaci papierowej są lepiej chronione od tych utrzymywanych w postaci elektronicznej. Pomimo, że w systemach są dane o przeprowadzonych transakcjach, numerach kart kredytowych, zawartych umowach, klientach, a także inne, które mogą być atrakcyjne, nie tylko dla przestępcy, co do konkurencji, to rzadko stosuje się silne mechanizmy zabezpieczeń pozwalające na utrzymanie poufności i integralności danych. Tam, gdzie się to stosuje, to znowu zapomina się o samej ochronie poszczególnych elementów zastosowanych zabezpieczeń, jak np. kluczy szyfrujących.

Ważnym zjawiskiem jest bezpieczeństwo informacyjne oraz legalność dokumentu elektronicznego i operacji elektronicznych. Autoryzacja przez podpis elektroniczny, personalizacja dostępu do sieci teleinformatycznej, systemy publicznych i prywatnych kluczy kryptograficznych, instytucja zaufanej trzeciej strony - to pilne zagadnienia związane z poufnością i wiarygodnością transmisji oraz zabezpieczeniem osobistych praw użytkowników. Nie ulega wątpliwości, ze brak ograniczeń terytorialnych jest jednym z podstawowych ułatwień dla wszelkiego rodzaju nadużyć dokonywanych przy wykorzystaniu sieci informacyjnych. Dlatego też istnieje duże zainteresowanie grup przestępczych wykorzystaniem infrastruktury sieciowej, jako nowego instrumentu nielegalnej działalności.

Z analiz przeprowadzonych przez specjalistów, jednoznacznie wynika, że grupy przestępcze prowadzą zakrojone na szeroką skalę rozpoznanie warunków ekonomicznych, prawnych i społecznych na obszarach, w których zamierzają długofalowo prowadzić nielegalną działalność. Dla dokonania obiektywnej oceny przestępcy opracowują swoiste wykazy problemów wymagających bliższego zbadania, co pozwala im na przeprowadzenie szybkiej oceny możliwości wykorzystania systemów informatycznych do prowadzenia działalności przestępczej na określonych obszarach. Najczęściej branymi pod uwagę elementami są:

- poziom wyszkolenia policji i służb finansowych państwa w zakresie zwalczania przestępczości komputerowej, finansowej itp.;
- stan przestrzegania dyscypliny w utrzymaniu tajemnicy np. bankowej;
- zakres współpracy i szybkość wymiany informacji o podejrzanych transakcjach pomiędzy np. instytucjami finansowymi a policją lub innymi organami odpowiedzialnymi za zwalczanie przestępczości finansowej;

- rzeczywista sprawność wewnętrznych mechanizmów kontroli instytucji finansowych przede wszystkim systemów ochrony oraz monitorowania wykonywanych transakcji.

Z dotychczasowej oceny działalności przestępczej wynika, że główna jej uwaga skoncentrowana jest na obszarach funkcjonowania państwa pod kątem prowadzenia nielegalnych operacji finansowych. Większość istotnych informacji stanowiących niekiedy tajemnice finansowe czy też handlowe jest przechowywana w postaci elektronicznej. Dlatego też grupy przestępcze w celu uzyskania istotnych dla nich informacji wynajmują wyspecjalizowanych w tej działalności włamywaczy (*hakerów*). Począwszy od uzyskania takich informacji najprostszymi rodzajami ataków od zewnątrz (poprzez sieć o ile docelowy system ma połączenie ze *"światem zewnętrznym"*), a skończywszy na zatrudnianiu włamywacza w firmie pozostającej w ainteresowaniu przestępców (tzw. atak od środka). Warto także zauważyć, że grupy przestępcze do swoich działań wykorzystują często "starych" pracowników firmy (zdarza się, że są to administratorzy systemów komputerowych), którzy kierując się chęcią np. łatwego zarobku przekazują w niepowołane ręce *"ważne"* dla państwa informacje. Na ogół działania ich maja charakter działań operacyjnych. Często pracownik firmy, który jest w środku systemu informatycznego pozostającego w zainteresowaniu, uzyskuje legalnie bądź też nie, kolejne poziomy zabezpieczeń (np. najpierw jedno hasło do systemu - zwykłego użytkownika, a potem nawet hasło superużytkownika). Na ogół zdarza się, że głównym zadaniem skorumpowanego użytkownika jest wprowadzenie do systemu specjalnie przygotowanego oprogramowania (*konia trojańskiego, bomby logicznej itp.)*, pozwalającego przestępcom osiągnąć zamierzony cel. Z reguły prowadzi to do *"wykradania"* informacji.

Nie można także pominąć działań prowadzonych przez grupy przestępcze, których głównym zadaniem jest uzyskanie jak największej ilości informacji o danym systemie informatycznym. Ma to na celu dokonanie ataku i w konsekwencji tego "wykradnięcia" danych lub unieruchomienia systemu.

Oprócz zorganizowanych grup przestępczych, interesujących się systemami komputerowymi mamy również do czynienia z pojedynczymi przestępcami tzw. "*crackerami*", którzy wykorzystują swoje umiejętności, np. do zabawy lub do potwierdzenia swojej wiedzy. Tego typu przestępcy tworzą najczęściej ściśle powiązane grupy na skalę międzynarodową. Relacje pomiędzy członkami takich grup

ograniczają się najczęściej do wymiany wszelkich informacji na temat nowych metod łamania zabezpieczeń, odkrytych słabych punktów ogólnie znanego i wykorzystywanego oprogramowania, a także wielu innych informacji ułatwiających penetrowanie systemów bez konieczności posiadania specjalnych uprawnień. Przełamywanie zabezpieczeń lub zdalna destrukcja dowolnego systemu staje się dla nich bagatelą.

1.2.2. Terroryzm informacyjny

Organizacje terrorystyczne coraz częściej dostrzegają infrastrukturę teleinformatyczną jako cenny do zaatakowania obiekt. Ze względu na dotychczasowe niskie możliwości działalności terrorystów w cyberprzestrzeni, główną uwagę skupiają oni na destrukcji fizycznej infrastruktury technicznej takich obiektów jak elementy stacji nadawczych i przekaźnikowych oraz kluczowe serwery internetowe. Niszczenia tych obiektów dokonują metodą ich wysadzania lub bezpośredniego pozbawiania cech ich używalności.

Fizyczne niszczenie wybranych elementów sieci komputerowych infrastruktury teleinformatycznej pozwolić może terrorystom na osiągnięcie efektów wyłącznie w skali lokalnej. Osiągnięcie przez terrorystów większego zakresu zniszczeń jest mało prawdopodobne ze względu na konieczność posiadania przez nich szczegółowych informacji dotyczących lokalizacji obiektów, dostępu do nich oraz sposobów ich chronienia. Nie bez znaczenia jest również fakt, iż w przypadku zniszczenia linii komunikacyjnych ruch w Internecie jest automatycznie przekierunkowany dzięki dużej liczbie systemów awaryjnych oraz heterogenicznej organizacji sieci internetowej.

Fizyczne niszczenie obiektów nazywane jest często terroryzmem technicznym. Pomimo lokalnych jego obiektów, główną jego zaletą jest fakt łatwości jego przeprowadzenia. Mogą tego dokonać terroryści nielegitymujący się nawet wykształceniem technicznym. Znaczenie lokalnego zasięgu akcji terrorystycznych rośnie wówczas, gdy stanowią one element wspierający główną operację terrorystyczną. Może nią być np. tymczasowe zdezorganizowanie systemów powiadamiania służb ratowniczych lub komunikacji między siłami ochrony atakowanego obiektu. Należy więc przypuszczać, że z tego powodu ilość ataków

terrorystycznych o charakterze technicznym będzie mieć tendencję rosnącą. Klasycznym przykładem ataku terrorystycznego o charakterze technicznym było zniszczenie przez terrorystów Al Qaidy systemów identyfikacji samolotu podczas zamachów w dniu 11 września 2001 roku.

1.2.3. Rodzaje atakowanych systemów informatycznych

Stosunkowo niewielka liczba ataków cybernetycznych w porównaniu do konwencjonalnych aktów terroru uwarunkowana jest wieloma czynnikami, do których można zaliczyć:

- stosunkowo niską wiedzę kierownictw organizacji terrorystycznych z zakresu działań w cyberprzestrzeni;
- stosunkowo niską medialność ataków cybernetycznych w porównaniu do konwencjonalnych aktów terroru;
- brak specjalistów z zakresu stosowania terroryzmu cybernetycznego.

W ostatnim okresie dostrzega się wyraźnie próby zainteresowania się organizacji terrorystycznych nowymi technologiami łącznie ze szkoleniem specjalistów w zakresie telekomunikacji i informatyki. Wynika z powyższego, iż cyberterroryzm będzie przybierał na znaczeniu stając się ważnym elementem podejmowanych współcześnie aktów terrorystycznych. W oparciu o analizę dotychczasowej strategii działań terrorystycznych należy przypuszczać, że prawdopodobnymi celami ataków terrorystycznych będą systemy informatyczne wykorzystywane w sferze wojskowej.

Nie ulega również wątpliwości, ze w przeciwieństwie do większości systemów informatycznych stosowanych w sferze militarnej, systemy cywilne nie są fizycznie odseparowane od innych sieci komercyjnych i publicznych co w znacznym stopniu ułatwia dostęp do nich.

Do najbardziej zagrożonych systemów informatycznych zaliczyć można:

- systemy wspomagające zarządzanie ruchem powietrznym oraz transportem zwłaszcza zaś kolejowym;
- systemy wykorzystywane w instytucjach państwowych pracujące na rzecz baz danych oraz powiadamiania służb ratowniczych i reagowania antykryzysowego;

- systemy pracujące w różnych sektorach jak w bankowości czy też stosowane przy produkcji i dystrybucji dóbr o znaczeniu strategicznym, jak ropa, energia elektryczna, gaz oraz woda pitna.

Biorąc pod uwagę zaprezentowane powyżej obszary zastosowań systemów informatycznych, łatwo jest dostrzec, że mogą być one obiektami szczególnego zainteresowania ze strony różnych grup terrorystycznych. Wywołanie zakłóceń w pracy tych systemów spowodować może duże straty ekonomiczne oraz negatywne zjawiska w sferze społecznej. Dlatego też pilnym zadaniem władz państwowych oraz kierownictw różnych instytucji prywatnych jest prowadzenie skutecznych działań na rzecz utrzymania wysokiego poziomu bezpieczeństwa zarówno w odniesieniu do sprzętu jak też i programów wykorzystywanych w systemach informatycznych.

1.2.4. Terroryzm informacyjny i jego wpływ na globalne środowisko bezpieczeństwa

Współcześni teoretycy i praktycy wojskowi mówiąc o sztuce wojennej *"czwartej generacji"* najczęściej mają na uwadze globalne, transnarodowe zagrożenia zwłaszcza zaś terroryzm. Spośród wielu zagrożeń o charakterze globalnym bardzo często wymienia się możliwość stosowania terroryzmu informacyjnego[5]. Terroryzm informacyjny lub *"piractwo informacyjne"* są odmianami wojny informacyjnej pozwalającej osiągnąć założone cele terroryzmu. Często są nimi przemoc względem obiektów cywilnych i wojskowych. Ryzyko ingerencji w systemy informatyczne będzie wzrastało wraz z rozwojem technologii informatycznych.

W przyszłości działania terrorystyczne będą prawdopodobnie miały na celu zapewnienie terrorystom dostępu do najnowszych technologii stanowiących swoistą "ochronę bogactwa" państw uprzemysłowionych. Dlatego też grupy terrorystyczne oprócz dotychczasowych zainteresowań bronią masowego rażenia, systemu komunikacji i innymi odmianami osiągnięć technologicznych będą uciekały się do terroryzmu informacyjnego. Ponieważ funkcjonowanie społeczeństw, zwłaszcza w państwach bogatych, staje się w coraz większym stopniu uzależnione od systemów informatycznych, stąd też terroryzm informacyjny przybiera formę szczególnego niebezpieczeństwa określonego nawet katastroficznym.

---

[5] *M.G.Devost, Politycal violence ia the Information Age.c.75*

Skutki konwencjonalnych działań terrorystycznych, jakkolwiek wielce dotkliwe i bolesne mają na ogół ograniczony zasięg. Natomiast w przypadku piractwa informatycznego (cyberterrorism) skala destrukcyjnych działań może mieć ogromny zasięg, co jest oczywiste, gdy uwzględni się postępujące uzależnienie społeczeństw od technologii informatycznych.

Równie groźną odmianą terroryzmu informacyjnego stanowić może ingerencja w sieci informatyczne z zamiarem zniszczenia lub uniemożliwienia ich funkcjonowania czy też sprawowania nad nimi kontroli (cyber-attack). Ten rodzaj terroryzmu może być realizowany generalnie przy zastosowaniu dwóch metod:

- fizycznego zniszczenia systemu informatycznego;
- objęcia całkowitej kontroli nad funkcjonowaniem systemu.

Przykładem drugiej metody może być przejęcie kontroli nad informatycznym systemem samolotowym przez terrorystów islamskich wykonujących uderzenie na Światowe Centrum Handlowe 11 września 2001 r.

Można zakładać, że cywilnymi obiektami zainteresowań tego rodzaju terroryzmu będą systemy informatyczne decydujące o bezpieczeństwie społeczeństwa, takie jak ochrony żywności, wody, transportu ruchu lotniczego itp. W odniesieniu do obiektów wojskowych mogą to być systemy dowodzenia i kontroli (C2) oraz logistyki.

Wielce prawdopodobnym obiektem zainteresowań terroryzmu informacyjnego może być sieć internetowa, która stopniowo przybiera charakter globalny. Pierwszymi oznakami tego typu działań są tzw. hakersi. Nie można także wykluczyć, że *"cyber-terrorism"* będzie swego rodzaju logicznym modelem przyszłego konfliktu, który prowadzony będzie w *"cyberprzestrzeni"*.

"Cyber-wojna" może się stać ekwiwalentem wojen prowadzonych do tej pory między państwami.

Wzrastające uzależnianie się sił zbrojnych, rządów i organizacji od systemów informatycznych stanowi dużą przestrzeń oddziaływań ze strony terrorystów. Niekoniecznie muszą to być działania dużych grup terrorystycznych. Tego typu zaplanowane operacje skierowane przeciwko społeczeństwom Zachodu wydają się wielce prawdopodobne. Przykładem tego typu operacji był atak terrorystyczny z września 2001 roku. Przeprowadzone w ostatnich latach w Stanach Zjednoczonych badania dotyczące możliwości włamania się do systemów informatycznych dużych

organizacji dowiodły, że w 80% było ono możliwe do przeprowadzenia[6]. Świadczy to o niemożliwości pełnej ochrony systemów przed działaniami terrorystycznymi typu *"cyber-terrorist attack"*.

W czasie konfliktu kosowskiego otwarte sieci dowodzenia stanowiły znakomitą pokusę dla hakerów. W tydzień po rozpoczęciu operacji NATO poniosło istotną porażkę prestiżową. Atakujący hakerzy z Serbii i Czarnogóry zablokowali oficjalny serwer WWW Sojuszu. Uczynili to wysyłając przez łącza poczty elektronicznej kilkadziesiąt tysięcy listów protestujących przeciwko operacji NATO w Jugosławii.

Kiedy informatycy Sojuszu odcięli możliwość wysyłania poczty, zaczęły się próby wejścia na stronę WWW z zamiarem jej zniekształcenia lub zniszczenia. Były one tak częste a hakerzy na tyle groźni, że po tygodniu działanie serwera trzeba było zawiesić na trzy dni. W tym czasie zmieniono strukturę sieci i oficjalną stronę internetową Sojuszu. Informatycy NATO założyli odpowiednie filtry wzmacniające moc serwerów.

Komputery NATO musiały odpierać ataki wirusów, które codziennie wysyłali hakerzy. Brytyjski analityk wojskowych technik i zastosowań cywilnych technik informatycznych w Alacan Perarson stwierdził, że wojna ta może dokonać "rewolucyjnych zmian w internecie" stwierdził również, że *"dotychczasowa otwarta formuła stron WWW nie da się prawdopodobnie utrzymać"*.

Może się także okazać, że do zadań wojsk walki radioelektronicznej należy również niszczenie stron i serwerów WWW należących do firm działających na terytorium przeciwnika. Obecnie jako przeciwdziałania zalecono *"odgraniczenie internetu od firmy"*, czyli wydzielenie fragmentu sieci pracującego stale on-line lub stosowanie przynajmniej trójstopniowych zabezpieczeń z *firewalkami* jako bramami systemu.

Powyższe każe zwracać uwagę na zmianę poglądów dotyczących wojny i sposobów planowania strategicznego. Nowe konflikty będą w coraz większym stopniu konfliktami informatycznymi.

Innym aspektem bezpieczeństwa informacyjnego pojawiającym się w ostatnim czasie jest terroryzm elektromagnetyczny. Obecnie w świecie jak i w Polsce zaczyna pojawiać się coraz więcej informacji z tego zakresu. Terroryzm elektromagnetyczny jest umyślnym, wytwarzaniem i wprowadzeniem

---

[6] *The New Threat the Millenium, (w:) Technology and terrorism., p.6*

elektromagnetycznej energii zakłócającej w pole emisji[7] pracującego sprzętu lub systemów elektronicznych w zamiarze uszkodzenia albo zniszczenia. Przy tym chodzi tu o akcje umotywowane terrorystycznie albo kryminalnie. Terroryzm elektromagnetyczny może być również rozpatrywany jako sposób (rodzaj) ofensywnej nowoczesnej walki informacyjnej. Bezprawne użycie energii elektromagnetycznej może być skierowane przeciw osobom, rządom, cywilnej gospodarce lub wybranym obiektom w połączeniu z politycznymi lub socjalnymi żądaniami. Tak postrzegany "terroryzm - elektromagnetyczny" charakteryzuje tylko jego ekstremalny kierunek, może on jednak również dotyczyć wandali, elementów kryminalnych lub kręgów aspołecznych.

Terroryzm elektromagnetyczny jako termin pojawił się w 1996 roku, wówczas to Generał Loborev wygłosił plenarny wykład podczas konferencji AMEREM w Albuquerque (USA). W wykładzie tym użył jako pierwszy terminu "terroryzm elektromagnetyczny" wskazując publicznie na problem, który do tej pory budził zaniepokojenie jedynie środowisk, zajmujących się problemami kompatybilności elektromagnetycznej. Komentarz generała na temat możliwości zastosowania energii elektromagnetycznej do pokonywania systemów alarmowych i systemów porozumiewania się przeciwnika, doprowadził do tego, że sprawa ta stała się przedmiotem ożywionej dyskusji zarówno podczas samej konferencji AMEREM, jak i po jej zakończeniu. Problem ten podnoszono w następnych latach w ramach spotkań różnych komisji i w czasie sympozjów EMC na temat kompatybilności elektromagnetycznej między innymi: w Tel Avivie rok 1998, Zurichu rok 1999 jak również we Wrocławiu w latach 1998 i 2000.

W chwili obecnej nie jest jasne jak łatwo lub jak skut można wykorzystać tego typu potencjalną broń, ale oczywiste jest, że środowiska zajmujące się problematyką kompatybilności elektromagnetycznej muszą być przygotowane (także w kraju) na poradzenie sobie z tym zagrożeniem, w momencie jego zaistnienia. Badania pokazują, że możliwe jest za pomocą generatorów mikrofalowych zakłócanie bądź ingerowanie w pracę większości dostępnych handlowo urządzeń stosowanych w technologii informacyjnej.

---

[7] *Każde elektroniczne urządzenie cyfrowe wytwarza, w zależności od częstotliwości pracy, szybkości impulsów sterujących, wielkości amplitudy tych impulsów, elektromagnetyczne pole emisji zakłócającej w ściśle określonym zakresie częstotliwości. Im większa jest szybkość impulsów sterujących i wyższa częstotliwość pracy, tym wyższa częstotliwość promieniowania zakłócającego.*

Przynieść to może następujące efekty:

- zniszczenie lub przepalenie urządzeń technicznych systemu informacyjnego;
- czasowe błędy lub zakłócenia urządzeń technicznych systemu informacyjnego;
- zredukowanie wydajności urządzeń technicznych systemu informacyjnego, np. ograniczenie możliwości systemów ochrony.

Należy stwierdzić, że w ostatnich pięciu latach technika mikrofalowa poczyniła ogromne postępy na polu miniaturyzacji tak, że obecnie silne impulsy można uzyskać przy wykorzystaniu stosunkowo niewielkich urządzeń. Stąd też potencjalnie dużym i coraz bardziej realnym zagrożeniem staje się wykonanie ataku terrorystycznego z wykorzystaniem promieniowania elektromagnetycznego. Możliwości te uzyskujemy wykorzystując urządzenia mikrofalowe o dużej sprawności (*High Power Microwave = HPM*) w celu niszczenia lub przynajmniej zakłócania.

Badania w zakresie technologii HPM prowadzone są przede wszystkim w Stanach Zjednoczonych głównie w obszarze militarnym na kierunku tworzenia nowych broni (oraz zabezpieczeń przed nią). Są to bronie dalekiego zasięgu do niszczenia elektroniki sterującej w rakietach. Przy okazji nie zapomniano o sektorze cywilnych technologii i odpowiedniej ochronie (zabezpieczeniu) przed atakiem mikrofalowym przeprowadzanym z małej odległości (mniej niż 1000m.). Atak taki może być przeprowadzany np. przez grupę terrorystów na budynek rządowy (pełen elektroniki) kompletnie do tego nie przygotowany.

Bibliografia:

1. Devost M.G.: Politycal violence ia the Information Age.
2. Hall R., Fox C.: Ponownie przemyśleć bezpieczeństwo, "Przegląd NATO", Zima 2001/2002.
3. Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej.
4. The New Threat the Millenium, (w:) Technology and terrorism.

1.3. DZIAŁANIA (OPERACJE) INFORMACYJNE: POJĘCIA, POGLĄDY, CECHY

1.3.1. Ocena piśmiennictwa

W stosunkowo niedługim czasie[1] pojawiło się wiele materiałów naukowych dotyczących wykorzystania sfery informacyjnej w działaniach różnych podmiotów. Dla zarysowania sytuacji badawczej warto syntetycznie omówić najważniejsze obszary i pozycje określonego piśmiennictwa.

Tuż po wojnie w Zatoce Perskiej w 1992 roku Alan Campen zebrał zestaw referatów wielu autorów, dodał kilka swoich i opublikował książkę[2]. Książka ta odnosiła się do niedawno zakończonej kampanii przeciwko Irakowi, jednakże jej uwaga koncentrowała się na informacyjnej stronie tej kampanii. Alan Campen, analizując zakończoną kampanię uznał, iż była ona *„pierwszą wojną informacyjną"* i tak też zatytułował całość opracowania. Opracowanie to stanowi cenny materiał w zakresie analizy informacyjnego aspektu konfliktu z Irakiem. Pojawia się tu wiele uogólnień i prawidłowości dotyczących wpływu informacji i informacyjnych systemów na przebieg współczesnej walki zbrojnej i wojny.

Opracowanie to nie zakończyło działalności badawczej Campena. Po wcześniejszym przygotowaniu pojedynczych artykułów w 1996 roku wspólnie z dwoma innymi głównymi autorami wydaje książkę[3] dotyczącą problematyki cyberwojny. Książka ta zawiera wiele stanowisk wobec omawianej problematyki, gdyż zamieszcza również referaty kilkunastu specjalistów w tym zakresie. Mimo popularnonaukowego charakteru całości wiele fragmentów stanowi dobrze udokumentowane i uargumentowane rozważania naukowe. Do wartościowych dokonań autorów zaliczyć należy autorskie propozycje definicji i charakterystyki walki informacyjnej w sferze cywilnej i militarnej oraz rozważania w zakresie moralnej, prawnej i organizacyjnej strony tej walki. Autorzy określają znaczenie rewolucji w sferze militarnej i rolę potencjału walki informacyjnej dla bezpieczeństwa narodowego. Uzasadniają konieczność posiadania narodowej strategii informacyjnej

---

[1] *Najistotniejszy dorobek naukowy w tym obszarze powstał w ostatnim dziesięcioleciu.*
[2] *A. Campen, The First Information War. The Story of Communications, Computers and Intelligence Systems in the Persian Gulf War, Fairfax 1992.*
[3] *A. Campen, D. H. Dearth, R. T. Goodden, Cyberwar: Security, Strategy, and Conflct in the Information Age, Fairfax 1996.*

dla przetrwania w XXI wieku. Proponowane szerokie rozumienie walki informacyjnej uwzględnia oddziaływanie mediów, jako komponentu tej walki. W treści zawarto także charakterystykę form oddziaływań medialnych i możliwości wpływania na świadomość odbiorców. Szczególnie interesująca jest propozycja wykorzystania telewizji do kształtowania woli innego narodu przez zmianę jego postrzegania rzeczywistości. Opracowanie zawiera także treści prognostyczne co do kształtu walki informacyjnej pod koniec bieżącego ćwierćwiecza.

Również stosunkowo wcześnie problematykę walki informacyjnej w obszernym studium zaprezentował Winn Schwartau[4]. W studium tym zamieścił, oprócz własnych poglądów, wypowiedzi 37 innych specjalistów w tym zakresie. W rezultacie praca ta, a szczególnie jej drugie wydanie, odnosi się do wielu aspektów wyłaniającej się nowej sfery walki. Sam Schwartau definiuje i charakteryzuje walkę informacyjną oraz dokonuje jej podstawowej dekompozycji[5].

Jego zasługą jest zwrócenie uwagi na szeroki kontekst nowego zjawiska i skalę zagrożenia zarówno dla bezpieczeństwa personalnego, jak też organizacji i państw. Ponadto obszernie charakteryzuje wiele rodzajów zagrożeń sfery informacyjnej oraz możliwych sposobów prowadzenia informacyjnych ataków oraz informacyjnej obrony. Część materiałów zawartych w opracowaniu ma charakter naukowy, większość z nich jest jednak popularnonaukowa.

Jednym z autorów, którzy należeli do grupy kształtującej pierwsze koncepcje walki w sferze informacyjnej, jest także Martin Libicki. Jest on autorem wielu książek, referatów, artykułów i wystąpień na ten temat. Do szczególnie interesujących zaliczyć należy opracowania[6]: *Czym jest walka informacyjna* i *Obrona cyberprzestrzeni.* Obie pozycje zostały wydane przez Uniwersytet Obrony Narodowej USA. Pierwsza zawiera, odmienne od często spotykanego, rozumienie walki informacyjnej. Autor twierdzi tu, że nie istnieje jakiś oddzielny sposób prowadzenia wojny, którym byłaby walka informacyjna. Tę zaś rozumie jako mozaikę różnych form walki w sferze informacyjnej. Zalicza do nich: walkę o przewagę w dowodzeniu, walkę w sferze rozpoznania, walkę elektroniczną, walkę psychologiczną, walkę hakerską, walkę ekonomiczną, walkę informacyjną i cyberwalkę (mającą się pojawić w przyszłości).

---

[4] *Już w 1994 r. opublikował Information Warfare: Cyberterrorism: Protecting Your Personal Security in the Electronic Age, New York. Drugie znacznie rozszerzone wydanie ukazało się w 1996r.1*

[5] *Propozycje tego autora omówiono w rozdziale 5.*

[6] *M. C. Libicki, What Is Information Warfare? Washington 1995 oraz M. C. Libicki, Defending Cyberspace and Other Metaphors, Washington 1997.*

Dokonuje także charakterystyki tych form oraz prowadzi analizę poszczególnych sposobów i technik tego obszaru, identyfikując istniejące od dawna i nowe. Ponadto, w przeciwieństwie do wielu specjalistów, nie zgadza się z tezą o wielkim zagrożeniu systemów informacyjnych działaniami walki informacyjnej. Czyni tak ze względu na przekonanie, iż systemy te są coraz bardziej rozproszone i łatwo mogą być redundantne co uodparnia je na zagrożenia.

Druga z publikacji *Obrona cyberprzestrzeni*, poświęcona jest wspomnianej wcześniej cyberwalce. Całe opracowanie koncentruje się na koncepcji obrony w sferze cyberwalki. Zauważa przy tym, że celem ataku może być raczej cywilna infrastruktura informacyjna niż siły zbrojne. Dostrzega także zagrożenie możliwością manipulowania społeczeństwem za pomocą technik medialnych, Internetu, multimediów. Zagrożenie to zawiera się w możliwości stosowania mieszanych technik tradycyjnej propagandy, manipulowania prawdą i nowych technik manipulacyjnych. W treści pracy znajdują się także ciekawe propozycje w zakresie odstraszania informacyjnych ataków. Interesująca jest też koncepcja organizacji obrony immunologicznej systemu informacyjnego opracowana na podstawie analizy systemu immunologicznego żywego organizmu.

Walka w sferze informacyjnej pozostawała od początków tworzenia się tej koncepcji w sferze zainteresowania amerykańskiego instytutu badań naukowych *RAND*. W rezultacie badań tego obszaru opublikowano kilka opracowań. Jednym z tych, które bezpośrednio odnoszą się do problematyki walki informacyjnej, jest publikacja[7] poświęcona przygotowaniu do konfliktu w informacyjnym wieku. Jest to zbiór 19 referatów będących wynikiem badań zamówionych przez Biuro Sekretarza Obrony USA oraz prowadzonych według planów instytutu. W toku badań stwierdzono, że rewolucja informacyjna transformuje naturę konfliktu w obszar rozległego spektrum rozciągającego się od otwartej walki przez terroryzm, przestępczość po radykalną aktywność socjalną. W konflikcie socjalnym Internet i inne media znacznie wzmacniają możliwości jednostek i małych grup w zakresie ich wpływania na działania państw. Przygotowania do konfliktu w takich warunkach wymagać będą zmiany form organizacji. Zmiana ta będzie jednakże trudna dla państw i tradycyjnych sił zbrojnych, które pozostają bastionem struktur hierarchicznych i będą się opierać radykalnym zmianom. Symbol tego świata - Mars,

---

[7] *J. Arguilla, D. Ronfeldt, In Athena's Camp: Preparing for Conflict in the Information Age, Santa Monica 1997.*

musi ustąpić Atenie, patronce informacyjnego wieku. Jest to warunkiem nie tylko przygotowania się do przyszłych konfliktów, lecz także skutecznego zapobiegania im. Według takiego głównego motywu określono charakterystykę nowych warunków, w jakich pojawią się konflikty, zidentyfikowano istotę zachodzącej rewolucji w sferze militarnej, dokonano identyfikacji cech walki toczącej się w informacyjnej cywilizacji oraz zaproponowano kilka podejść badawczych do walki informacyjnej. Jest wśród nich m.in. szeroka perspektywa (proponowana przez Martina Libickiego w omawianej wcześniej jego pracy) oraz podejście społeczne.

RAND prowadził także badania w omawianym obszarze na zlecenie Sił Powietrznych USA. Efektem tych badań jest publikacja[8] zatytułowana *Strategiczna ocena. Zmiana roli informacji w walce*. Jest to praca zbiorowa dwudziestu znanych badaczy. Niektórzy z nich byli współautorami wymienianych wcześniej publikacji. Prezentowana praca jest obszerną analizą nowej roli informacji w walce. Wiele miejsca poświęcono w niej badaniu wpływu informacyjnych technologii na społeczeństwa, gdyż wpływ ten wywoła największe implikacje dla narodowego bezpieczeństwa. Niektórzy autorzy[9] uważają, że zmiany te zmniejszą znaczenie państwa, zwiększając jednocześnie potencjał i znaczenie organizacji niepaństwowych. Zgodnie z zamówieniem badania koncentrują się na sytuacji Stanów Zjednoczonych, jednakże podłożem ich są zjawiska i ich prawidłowości.

Jednym z takich zjawisk jest zależność państwa od informacyjnej infrastruktury oraz wynikająca z tego wrażliwość. O ile wszyscy badacze akceptują istnienie takiej wrażliwości, to panuje odmienność poglądów na skalę tej zależności. Uzasadnione wydaje się przekonanie Davida Ochmanka, że dominacja informacyjna zapewni utrzymanie przewagi w sferze militarnej. Praca zawiera także interesujące propozycje utrzymywania zdolności projekcji siły i obezwładnienia broni masowego rażenia przeciwnika oraz osiągnięcia nowej jakości działań psychologicznych.

Autorzy dokonują analizy technik i taktyk, które mogą być zastosowane w ramach ataku na narodowe zasoby strategiczne, takie jak system finansowy, sieć telekomunikacyjna czy system transportu. Analizują także zależność działań sił powietrznych od informacji i systemów informacyjnych, wskazując na istniejące prawidłowości. Autorzy konstatują, że podobnie jak nie sposób całkowicie

---

[8] *Z. M. Khalilzad, J. P. White, Strategic Appraisal. The Changing Role of Information in Warfare, Santa Monica 1999.*

[9] *Należą do nich: J. Arquilla, D. Ronfeldt i M. Zanini.*

wyeliminować wrażliwość na atak jądrowy, tak i niemożliwe jest całkowite uodpornienie się na ataki informacyjne. Dlatego też najbardziej obiecująca jest strategia odstraszania tych ataków i zapobiegania uzyskiwaniu zdolności do ich prowadzenia przez przeciwników. Praca definiuje także walkę informacyjną oraz prezentuje jej dekompozycję z charakterystyką elementów. Badania te koncentrują się na strategicznym poziomie zastosowania. Zleceniodawcom, czyli siłom powietrznym, autorzy uświadamiają istnienie problemu decyzyjnego związanego z wybraniem obszaru swoich kompetencji w przyszłości. Siły powietrzne zawsze argumentowały konieczność istnienia samodzielnej organizacji specjalizującej się w eksploatacji jakiejś przestrzeni. Gdyby to było prawdziwe, oznaczać by mogło konieczność wyłonienia organizacji odpowiedzialnej za walkę w sferze informacyjnej.

Możliwe jest jednak przenoszenie akcentu z operacji powietrznych na informacyjne, z rozwijaniem zdolności działań zarówno w sferze powietrznej, jak i informacyjnej. Wymaga to jednak przynajmniej częściowego odchodzenia od kultury opartej na lataniu.

Kolejne badania zlecone RAND przez Biuro Sekretarza Obrony USA również dotyczyły problematyki walki informacyjnej, lecz na poziomie strategicznym. W rezultacie, w odstępie dwuletnim ukazały się dwa opracowania[10], w których zawarto wyniki badań. W pierwszym, zatytułowanym *Strategiczna walka informacyjna: nowe oblicze wojny*, badacze uznali obecną w wielu wypowiedziach tezę o zwiększającej się roli informacyjnej rewolucji dla narodowego bezpieczeństwa.

Zjawisko to wynika z rosnącego uzależnienia cywilnej i militarnej aktywności od komputerów i informacyjnej komunikacji. Autorzy przyznają, że wraz z wieloma korzyściami płynącymi z komputeryzacji i rozwoju telekomunikacji pojawiły się poważne zagrożenia. Strategicznie ważne elementy państwa znalazły się w zasięgu łatwego do przeprowadzenia informacyjnego ataku przez jakiegokolwiek przeciwnika.

Pojawiła się więc możliwość prowadzenia strategicznej walki informacyjnej. To z kolei stawia wyzwanie tradycyjnemu podejściu do obrony i obronności kraju. Bronią w tej nowej sytuacji może być program komputerowy, a nosicielem tej broni dowolny komputer, telefon komórkowy i Internet. Nowe wrażliwości i zagrożenia są ciągle słabo rozumiane i mało dostrzegane. Dla tego typu zagrożeń i napastników nie

---

[10] *R. C. Molander, A. S. Riddile, P. A. Wilson, Strategic Information Warfare. A New Face of War, Santa Monica 1996 oraz R. C. Molander, P. A. Wilson, D. A. Mussington, R. F. Mesic, Strategic Information Warfare Rising, Santa Monica 1998.*

istnieją granice i rubieże obrony. W tej sytuacji militarna obrona może być całkowicie nieskuteczna. Obrona ta musi być masowa, organizowana przez każdy komponent państwa, a nawet przez każdego obywatela. W sferze konstrukcji aparatu pojęciowego autorzy uznali, że ciągle jest za wcześnie na precyzyjne definiowanie walki informacyjnej. Określili więc przybliżony zakres dwóch zjawisk – walki informacyjnej i walki strategicznej, a następnie obszar swojego zainteresowania, jakim jest strategiczna walka informacyjna. Niezwykle ciekawy jest opis narzędzia badawczego, jakim jest specjalnie skonstruowane przez RAND ćwiczenie badawcze, które prowadzone jest z udziałem personelu odpowiedzialnego za kierowanie sprawami bezpieczeństwa narodowego oraz gospodarki, a także przedstawicieli biznesu. Autorzy prezentują także przebieg ćwiczenia.

W drugim opracowaniu – *Wyłanianie się strategicznej walki informacyjnej* – autorzy prezentują wyniki kontynuacji badań problematyki strategicznej walki informacyjnej. W rezultacie ustalają dwie kategorie zagrożeń dla bezpieczeństwa narodowego: zagrożenia dla narodowego bezpieczeństwa ekonomicznego oraz dla narodowej strategii militarnej. Identyfikują także dwie generacje koncepcji strategicznej walki informacyjnej: jedną składającą się z kompozycji różnych instrumentów walki strategicznej oraz drugą, samodzielną formę informacyjną składającą się z różnych właściwych jej komponentów. Praca zawiera także wiele sugestii o charakterze wdrożeniowym dla praktyki. Cenną wartością obu prac są zidentyfikowane prawidłowości dotyczące strategicznego poziomu walki informacyjnej.

Inną pracą w zakresie walki informacyjnej jest monografia Edwarda Waltza[11] *Walka informacyjna – zasady i działania*. Zawiera ona autorską koncepcję oraz charakterystykę walki informacyjnej. Jest rezultatem m.in. kilku seminariów prowadzonych w Stanach Zjednoczonych i Europie na ten temat. Waltz identyfikuje sferę walki informacyjnej, w której informacja jest zarówno obiektem ataku, jak i bronią oraz zagrożeniem dla cywilnych i militarnych systemów informacyjnych. Określa także rolę technologii w walce bazującej na informacji, koncepcję przewagi informacyjnej, środki rażenia, komponenty i zasady prowadzenia walki informacyjnej. Jego teoria jest syntezą koncepcji informacyjnej dominacji, informacyjnej obrony i informacyjnego ataku.

---

[11] *E. Waltz, Information Warfare Principles and Operations, Boston 1998.*

Także w 1998 roku wydana została obszerna monografia Dorothy Denning[12] zatytułowana *Walka informacyjna i bezpieczeństwo*. Autorka, profesor informatyki Uniwersytetu Georgetown, zawarła w swojej publikacji zarówno treści naukowe, jak i popularnonaukowe. Do treści naukowych zaliczyć należy koncepcję i zasady walki informacyjnej. Proponowany przez nią model walki informacyjnej składa się z czterech komponentów: informacyjnych zasobów, uczestników walki, działań ofensywnych oraz działań defensywnych. Walka informacyjna wiązana jest tu z czterema aspektami ludzkiej aktywności: zabawą, przestępczością, indywidualnymi wolnościami i prawami oraz bezpieczeństwem narodowym. Autorka dokonuje obszernej charakterystyki komponentów walki informacyjnej, ilustrując ją wieloma przykładami i zahaczając o poziom beletrystyki. Bada jednak walkę informacyjną zarówno w skali mikro, jak i makro. Dużo miejsca poświęca problematyce obrony narodowej oraz możliwości manipulowania społeczeństwami. Do niedostatków zaliczyć należy powierzchowne traktowanie niektórych zagadnień, co może wynikać z rozległości podjętej problematyki. Spowodowało to także zauważalną niespójność treści. Ponadto podejście autorki nie jest wolne od stronniczości w ocenach zachowań podmiotów areny międzynarodowej.

Kolejna podobna publikacja dotycząca problematyki walki informacyjnej ukazała się w 1999 roku. Jest to[13] *Sztuka walki informacyjnej: spojrzenie w głąb filozofii wojownika wiedzy* napisana przez dwóch autorów Richarda Forno i Ronalda Baklarza. Publikacja ta ma charakter popularnonaukowy. Jednakże znajdują się w niej oryginalne propozycje wywiedzione z analizy klasycznej chińskiej filozofii walki. Autorzy uznali, że jak Shakespeare jest przykładem dla dramatopisarzy, tak Sun Tzu dla twórców teorii militarnych. Dlatego też dużo uwagi poświęcili analizie poglądów tego klasyka. Z analizy tej wywiedli szereg wniosków dla poprawy bezpieczeństwa narodowego. Autorzy ci zwrócili również uwagę na zagrożenie możliwością stosunkowo łatwego manipulowania świadomością społeczeństw. Proponowane treści zabarwione są raczej społecznym niż technokratycznym podejściem do walki informacyjnej.

Polskie środowisko naukowe również wykazywało sporo zainteresowania najpierw problematyce znaczenia informacji w walce a następnie walki informacyjnej.

---

[12] *D. E. Denning, Information Warfare and Security, 1998.*
[13] *R. Forno, R. Baklarz, The Art Of Information Warfare: Insight into the Knowledge Warrior Philosophy, 1999.*

Przykładem mogą tu być m.in. prace Piotra Sienkiewicza. W jednej z nich: *Inżynierii systemów*[14] cały rozdział poświęca informacji i informowaniu dokonując nie tylko przeglądu definicji informacji lecz także określenia podstawowych zjawisk zachodzących w sferze informacyjnej, przede wszystkim zaś określenia informowania czyli procesu informacyjnego[15]. Prowadzi także analizę rozwoju systemów informacyjnych szczególnie w sferze społecznych procesów informacyjnych oraz systemową analizę tych procesów. Już wówczas wspomina o *„walce informacyjnej"*[16] mając jednak na myśli raczej nasilającą się wówczas walką propagandową miedzy przeciwstawnymi systemami ideologicznymi. Ponadto większość aktywności badawczej i publicystycznej tego autora poświęcona jest jakimś aspektom wykorzystania informacji w procesach zarówno współpracy, jak i walki[17].

Polski wkład w rozwój studiów nad rolą działań informacyjnych, w tym nad rolą czynnika informacji w zmaganiach zbrojnych wyraża się także w pracach Stanisława Kozieja. Już w 1978 roku zwracał on uwagę na rolę informacji jako jednego z podstawowych, elementarnych czynników walki zbrojnej – obok rażenia (ognia), ruchu (manewru) oraz uderzenia[18]. Następnie myśl tę rozwinął w kolejnych swoich publikacjach[19]. Koncepcje te znalazły swoje zastosowanie nie tylko w myśli naukowej ale i w praktyce szkoleniowej wojsk oraz dydaktyce na początku lat dziewięćdziesiątych[20]. Zostały one także wprowadzone do wydawanych wówczas regulaminów walki. W rezultacie zaczęto np. wyróżniać w systemach: obrony i natarcia podsystem informacyjny (oprócz tradycyjnych składników, jakimi były: ugrupowanie wojsk, infrastruktura pasa (rejon) działań i system ognia.

Prace te akcentowały rolę informacji w walce bądź jako ważnego elementu zabezpieczenia procesów walki bądź też, jako elementu systemu walki w postaci

---

[14] *P. Sienkiewicz, Inżynieria systemów, Warszawa 1983.*
[15] *Tamże, s. 73–74.*
[16] *Tamże, s. 111.*
[17] *Są to m.in.: P. Sienkiewicz, Wojna informatyczna, Computerworld, 1997, nr 31(1997); T. Goban-Klas, P. Sienkiewicz, Społeczeństwo informacyjne – szanse, zagrożenia, wyzwania, Kraków 1999, P. Sienkiewicz, Współczesne koncepcje walki informacyjnej, [w:] R. Szpyra, Informacyjny wymiar współczesnych działań powietrznych. Materiały z sympozjum naukowego, Warszawa 2002.*
[18] *Zob. S. Koziej, Ciągłość oddziaływania na przeciwnika podczas natarcia, Myśl Wojskowa 1978, nr 5.*
[19] *Por. S. Koziej, Współczesna myśl taktyczna, Myśl Wojskowa 1987, nr 10, czy S. Koziej, Teoria sztuki wojennej, Warszawa 1993.*
[20] *Por. podręczniki akademickie AON: Działania taktyczne wojsk lądowych, Warszawa 1992 oraz Działania operacyjne wojsk lądowych, Warszawa 1992.*

jego podsystemu. W rezultacie nowych przemyśleń i oddziaływania docierających rezultatów badań prowadzonych na Zachodzie pojawiły się pierwsze polskie koncepcje wykorzystania informacji jako narzędzia walki.

W 1999 roku ukazała się publikacja na temat walki informacyjnej, opracowana przez Leopolda Ciborowskiego[21]. Jest to cenny wkład polskiego środowiska naukowego do badań nad zjawiskiem walki informacyjnej. Autor w publikacji tej dokonał syntetycznego przeglądu problematyki w aspekcie historycznym oraz zaproponował swoją koncepcję walki informacyjnej. Koncepcja ta osadzona jest w matematyczno-cybernetyczno-prakseologicznym podejściu. Szczególnie cenne jest naukowe uzasadnienie wartości informacji w sferze militarnej. Autor dostrzega szeroki kontekst walki informacyjnej, m.in. obszernie cytując Sun Tzu; jednakże nie nawiązuje do ustaleń badaczy Zachodu. Koncepcja walki informacyjnej autora wywiedziona jest z dosłownego niemalże rozumienia konstatacji, że *„informacją jest wszystko to, co nie jest ani energią, ani masą, czyli nie jest zasilaniem"*[22], oraz że *„...informacja nie może istnieć bez umysłu ludzkiego"*[23]. Autor wyprowadza stąd m.in. wniosek, że *„informacji nie można też bezpośrednio zakłócać"*[24]. Tu rodzi się wątpliwość: jak należy rozumieć kategorię *„umysł ludzki"*? Jeżeli szeroko, jako rezultat procesu myślenia, to informacja może istnieć poza mózgiem – żywym organem. Wyobrażenia człowieka oraz jego wyobraźnia są przecież rejestrowalne na zewnątrz organizmu, w przeciwnym razie nie byłoby całego dorobku intelektualnego ludzkości. Wyobrażenia i wyobraźnia, o których pisze autor, to przecież sfera symboli, które mogą być przekazywane pomiędzy ludźmi. Poprzez celową preparację tych symboli można wywołać pożądane wrażenia. Powinna więc istnieć informacja poza umysłem, w przeciwnym wypadku nie można by mówić nawet o zakłócaniu informacji poza umysłem ludzkim, co jednak jest proponowane przez autora. Jeżeli kategorię *umysł* traktować wąsko, jako organ biologiczny, to znaczyłoby, że informacja istnieje tyko w obecności człowieka, co przeczyłoby możliwości prowadzenia walki informacyjnej przy nieobecności człowieka w czasie atakowania informacji. Ponadto, zdaniem autora, walka informacyjna *„nigdy nie może występować w oderwaniu"*[25], gdyż zawsze towarzyszy jakiejś walce, którą wspiera.

---

[21] *L. Ciborowski, Walka informacyjna, Toruń 1999.*
[22] *Tamże, s. 51.*
[23] *Tamże, s. 59.*
[24] *Tamże, s. 68.*
[25] *Tamże, s. 69.*

Jednocześnie przytacza słuszne tezy Sun Tzu, takie jak: *„...największym osiągnięciem jest pokonanie wroga bez walki"*, czy *„...najwyższą sztuką jest zwyciężyć wroga bez wydania bitwy. Zająć miasto wroga bez oblegania i zająć tereny jego państwa bez inwazji"*[26]. Przecież zwycięstwo bez wydania bitwy, czy bez inwazji, oznacza zwycięstwo przy umiejętnym wykorzystaniu informacji, jako broni.

Zwycięstwo może więc być osiągnięte w wyniku wygrania walki informacyjnej. Stąd kontrowersyjność tezy autora. Jest ona słuszna w wielu wypadkach, lecz nie we wszystkich. W warunkach rodzącej się cywilizacji informacyjnej przypadki samodzielnego występowania walki informacyjnej (a nie tylko towarzyszenia innym walkom) będą coraz powszechniejsze, a informacja stawać się będzie bronią podstawową. Przekonanie o tym wśród badaczy na całym świecie jest niemal powszechne.

Również w 1999 roku Gabriel Nowacki obronił pracę doktorską na temat *Walka informacyjna – próba kategoryzacji*[27], a w 2001 roku wydał studium teoretyczne *Współczesne poglądy na prowadzenie walki informacyjnej*[28]. W obu opracowaniach prezentuje zasadniczo tę samą co Leopold Ciborowski, koncepcję walki informacyjnej. Różnice dotyczą jedynie obszarów towarzyszących, takich jak poglądy innych państw na walkę informacyjną. Ponadto drugie opracowanie ma charakter syntezy w stosunku do pierwszego. Wartościowym dorobkiem autora jest tu przegląd poglądów na temat istoty informacji, aczkolwiek niektóre wnioski wydają się kontrowersyjne, jak chociażby ten, że *„informacja jest niezniszczalna i zawsze prawdziwa"*[29]. Podobnie jak poprzedni autor również twierdzi, że *„...informacja nie może istnieć bez umysłu ludzkiego"*[30]. Ponieważ ludzi można zniszczyć (teoretycznie istnieje możliwość zniszczenia całej ludzkości), to i informację można zniszczyć.

Można też inaczej niszczyć informację, jednak ten argument przeczy prawdziwości prezentowanej tezy. Ocena tego, czy informacja jest zawsze prawdziwa, również jest względna, zależy bowiem od pojmowania prawdy, a także od przyjętych założeń. Wydaje się słuszna teza autora o istnieniu trzech komponentów walki informacyjnej. Można mieć wątpliwości co do nazewnictwa tych

---

[26] *Tamże, s. 13.*
[27] *G. Nowacki, Walka informacyjna - próba kategoryzacji. Rozprawa doktorska, Warszawa 1999.*
[28] *G. Nowacki, Współczesne poglądy na prowadzenie walki informacyjnej. Studium teoretyczne, Warszawa 2001.*
[29] *Tenże, Walka ..., s. 36.*
[30] *Tamże, s. 27.*

komponentów, jednak polemika w tym zakresie jest prowadzona w toku dalszych rozważań[31]. Niezrozumiałe są wynikające z konstrukcji modelu struktury walki informacyjnej[32] - relacje, a dokładniej brak tych relacji między elementami zakłócania walczących stron. Znaczyłoby to, że komponent zakłócający jednej strony może jedynie oddziaływać na komponenty rozpoznania i obrony przeciwnika bez możliwości tego oddziaływania na komponent zakłócający przeciwnika. Nie wydaje się to słuszne również z powodów teoretycznych, gdyż w walce występuje wzajemne zakłócanie, nic więc nie stoi na przeszkodzie, by komponenty zakłócające zakłócały się wzajemnie. Również praktyka wskazuje na istnienie takich przedsięwzięć, jak kontrprzeciwdziałanie, kontrdezinformacja. Niezwykle wartościowe są badania nad definiowaniem przestrzeni walki informacyjnej. Wyniki tych badań mogą być przydatne również dla innych potrzeb. Autor, dokonując dekompozycji walki informacyjnej, stosując jednolite kryteria, wyodrębnił podziały, które częściowo należy zaakceptować, po części zaś zakwestionować. Słuszne wydaje się umieszczenie, w przeciwieństwie do stanowiska Leopolda Ciborowskiego, walki informacyjnej w równoważnej pozycji w stosunku do innych walk, a nie jako walki wspierającej inne walki. Wątpliwości zaś budzi zakwalifikowanie walki informacyjnej do walki niezbrojnej w sytuacji, gdy proponowane dalej sposoby i metody tej walki mieszczą się w arsenale walki zbrojnej. Przy okazji warto zaznaczyć, iż istnieją obecnie trudności ze znalezieniem precyzyjnego kryterium uznania jakiejś walki za zbrojną lub niezbrojną. Autor podjął też znaczny wysiłek w porządkowaniu sposobów prowadzenia walki informacyjnej. Zaproponowana metoda wydaje się racjonalna, w rezultacie czego zarysowany został interesujący obraz proponowanego przez autora modelu walki informacyjnej. Inne, bardziej szczegółowe polemiki z poglądami autora są treścią dalszych rozważań niniejszej pracy.

Powstanie omawianych dzieł w środowisku polskich naukowców wojskowych jest niezwykle cenne, gdyż wprowadza dostrzeganą powszechnie problematykę do sfery zainteresowań polskiego środowiska nauk wojskowych oraz inspiruje do dalszego twórczego rozwijania i pogłębiania badań walki w sferze informacyjnej.

Oprócz omówionych opracowań książkowych ukazało się także wiele innych publikacji. W rezultacie poszukiwań internetowych przy użyciu hasła *„information*

---

[31] *Patrz rozdział 5.*
[32] *Tenże, Walka ..., s. 42.*

warfare" w specjalistycznym sklepie internetowym *Barnes&Noble*[33] znaleziono około 70 publikacji książkowych. Podobne poszukiwania w sklepie *Amazon*[34] wyłoniły ponad 50 publikacji. Były wśród nich zarówno pozycje omówione, jak i takie, które dopiero się ukażą. Ponadto analiza informacji o nich sugeruje, że większość z nich ma charakter popularnonaukowy lub beletrystyczny. Wiele z nich odnosi się do wybranych aspektów walki informacyjnej. Niektóre mają w rzeczywistości niewielki związek z walką informacyjną[35].

Wiedzę o treści niektórych opracowań można czerpać w sposób pośredni, docierając do ich tłumaczeń i omówień. Przykładem może tu być omawiana na początku rozdziału praca chińskich badaczy wojskowych[36] postulująca walkę nieograniczoną. Propozycja ta wywodzi się z analizy rozwoju form walki oraz obecnych warunków cywilizacyjnych. Autorzy zauważają, że obserwuje się relatywną redukcję przemocy militarnej, której jednakże towarzyszy wzrost innych form przemocy. Zachodzi to m.in. w obszarze politycznym, ekonomicznym, technologicznym. Jednakże uznają oni, że niezależnie od formy, jaką przybiera przemoc, wojna jest wojną i mimo zmiany jej zewnętrznego wyglądu nadal prawdziwe pozostają prawidłowości nią rządzące. Autorzy są przekonani, że nową zasadą wojny nie jest użycie sił zbrojnych do wymuszenia na przeciwniku narzucanej mu woli, lecz raczej zastosowanie wszelkich dostępnych środków, łącznie z militarnymi, w odpowiedniej do potrzeb kombinacji komponentów i broni (zabójczych i niezabójczych) wymuszających akceptację czyichś interesów. Publikacja ta jest wielce inspirująca i twórcza, szczególnie w zakresie formułowania nowego paradygmatu wojny i walki.

Bogactwo publikacji książkowych, mimo swej rozległości, jest skromne w porównaniu z ilością artykułów, dotyczących omawianej problematyki, zamieszczonych w periodykach i Internecie. Rozmaite próby poszukiwań doprowadziły do ustalenia, że na pewno dostępnych jest ich ponad tysiąc. Artykuły te można podzielić na trzy grupy: prezentujące naukowo uzasadnione koncepcje, opisy faktograficzne i diagnozy oraz informacje o wydarzeniach bieżących. Niektóre z tych

---

[33] *Zob.* www.barnsandnoble.com
[34] *Zob.* www.amazon.com
[35] *Przykładem może być Biological Warfare and Chemical Gases.*
[36] *Qiao Liang and Wang Xiangsu, Unrestricted Warfare: Assumptions on War and Tactics in the Age of Globalization, Beijing 1999, tłumaczenie na język angielski dokonane przez: US CIA's Foreign Broadcast Information Service udostępnione w 2000 r. pod adresami:* http://www.terrorism.com/documents/unrestricted.pdf **lub** http://cryptome.org/cuw.zip

artykułów publikowane są w grupowych zestawieniach, jako materiały z przeprowadzonych konferencji. Zestawienia takie publikowane są także jako materiały zwarte w formie książkowej i jednocześnie w Internecie. Jednym z takich opracowań godnych omówienia są materiały z sympozjum[37] na temat działań informacyjnych, przeprowadzonego w 1999 roku w holenderskiej akademii wojskowej. Opublikowane tuż po sympozjum opracowanie[38] zawiera wprowadzenia i 18 referatów w większości autorów, którzy brali aktywny udział[39] w sympozjum.

Referaty dotyczyły poszczególnych sfer problematyki operacji informacyjnych i walki informacyjnej. Czterech autorów rozważało problematykę podstaw teoretycznych w poszukiwaniu koncepcji operacji informacyjnych i walki informacyjnej. Wśród tych autorów warto wymienić Geoge'a Steina, który także w innych swoich wypowiedziach[40] prezentuje wiele argumentów dla poparcia tezy o tym, że współcześnie informacja jest bronią i to niezwykle groźną. Jest on jednym ztych badaczy, którzy sięgają do chińskiego dorobku naukowego i intelektualnego. Kolejni czterej autorzy omawianego wydawnictwa koncentrują się na koncepcjach operacji informacyjnych prezentowanych z różnych perspektyw - teoretycznej i praktycznej. Pozostali prezentują albo poszczególne aspekty, albo istniejące poglądy na omawianą problematykę w różnych regionach świata.

Wśród artykułów szczególnie dużo jest tych, które prezentują opisy faktograficzne obserwowanych zdarzeń[41] oraz opisy stanu współczesnej sytuacji[42]. Różnorodność zawartych w nich podejść, szczegółowość analiz oraz tematyki

---

[37] *Było to międzynarodowe sympozjum zatytułowane „Informacja jako środek, obiekt ataku i broń. Operacje informacyjne, co to oznacza?", zorganizowane przez holenderską Królewską Akademię Militarną w grudniu 1999 r.*

[38] *J. M. J. Bosh, H. A. M. Luiijf, A. R. Mollema, NL Arms. Netherlands Annual Review of Military Studies 1999, Information Operations, Breda 1999.*

[39] *Wiedza ta wynika z bezpośredniego uczestnictwa w sympozjum autora niniejszych badań.*

[40] *G. Stein, Information War – Cyberwar – Netwar, [w:] Battlefield of the Future. 21st Century Warfare Issues. Air University Maxwel AFB 1995; oraz G. Stein, Information Warfare, [w:] A. D. Campen, D. H. Dearth, R. T. Goodden, Cyberwar: Security, Strategy, and Conflct in the Information Age, Fairfax 1996; oraz G. Stein, Information Warfare. Learning With Sun Tzu, [w:] J. M. J. Bosh, H. A. M. Luiijf, A. R. Mollema, NL Arms. Netherlands Annual Review of Military Studies 1999. Information Operations, Breda 1999.*

[41] *UK: cyber-attacks. www.infowar.com/mil_c4i/00/mil_c4i_120100a_j.shtml; Taiwan To Launch "Cyber Warfare" Unit. www.infowar.com/mil_c4i/00/mil_c4i_112400a_j.shtml; DOD Closes Off GPS Segment. www.infowar.com/mil_c4i/00/mil_c4i_033199a_j.shtml; Yugoslavia: Air War Leads Us Astray. www.infowar.com/mil_c4i/00/mil_c4i_041099b_j.shtml.*

[42] *B. Frezza, The Militarization of Cyberspace. http://techweb.cmp.com/nc/frezza/frezza.html; Joint Economic Committee Hearing. Radio Frequency Weapons and Proliferation: Potential Impact on the Economy. Wednesday, February 25, 1998. http://www.house.gov/jec/hearings/02-25-8h.htm; The Global Course of the Information Revolution: Technological Trends: Proceedings of an International Conference. http://www.rand.org/publications/CF/CF157/.*

umożliwiają uzyskiwanie wysokiej jakości diagnoz i są przesłanką do wykrywania istniejących prawidłowości. Treści artykułów naukowych, najogólniej ujmując, mieszczą się w granicach koncepcji prezentowanych przez badaczy w formie książkowej. Często są one elementami procesu badawczego, w wyniku którego powstają dzieła zwarte. Artykuły są oczywiście publikowane nie tylko w Internecie, ale też w różnych periodykach w formie pisemnej. Jednak obecnie jest niemalże powszechne jednoczesne publikowanie w formie papierowej i elektronicznej. Coraz częściej forma elektroniczna jest formą jedyną, dlatego wiele uwagi poświęcono Internetowi. Cenną wartością Internetu związaną z niniejszymi badaniami, jest także posiadanie niezwykle bogatych zestawień źródeł w postaci specjalistycznych witryn.

Niektóre z nich zawierają setki adresów źródeł informacji w zakresie operacji informacyjnych i walki informacyjnej. Adresy najciekawszych zestawione są w bibliografii. Treści zawarte w poszczególnych witrynach i pod kolejnymi adresami mają znacznie zróżnicowaną wartość. Spora część umieszczonego tam materiału jest niemalże bezwartościowa. Jednak znajdują się tam także wartościowe opracowania, m.in. te, które zostały omówione. Jedną z istotnych wartości źródeł internetowych jest zawarta tam wiedza na temat kierunków podejmowanych badań i ich rezultatów. Wskazuje ona dobrze zbadane obszary oraz obszary słabo penetrowane naukowo.

Odrębną grupę literatury stanowiły dokumenty doktryn. Nie mają one co prawda charakteru naukowego, jednakże prezentują stan istniejący w sferze praktyki. Z dokumentów tych wynika m.in. stan wdrażania koncepcji teoretycznych do praktyki. W tej grupie szczególnie cenne okazały się amerykańskie połączone doktryny operacji informacyjnych i walki informacyjnej[43] oraz odpowiadające im dokumenty rodzajów sił zbrojnych[44]. Również w dokumentach doktryny działań połączonych NATO pojawiła się już problematyka operacji informacyjnych i walki informacyjnej. Oczywiście, wartościowym materiałem okazały się także dokumenty wspomnianych doktryn dotyczące obszarów pokrewnych lub bardziej szczegółowych[45].

Literatura z pokrewnych dziedzin wiedzy, które znalazły zastosowanie w niniejszych badaniach, okazała się niezwykle pomocna. Cenne są publikacje

---

[43] *Pub 3-13 Joint Doctrine for Information Operations, Washington 1998.*

[44] *Zob. FM 100-6 Information Operations, Washington 1996; Information Operations. AFDD 2-5, Maxwell AFB 1998.*

[45] *Amerykańskie doktryny dostępne są m.in. pod adresem: http://www.dtic.mil/doctrine/ .*

dotyczące teorii informacji, problematyki bezpieczeństwa oraz stosunków międzynarodowych.

W zakresie teorii informacji z punktu widzenia potrzeb prezentowanych badań za najcenniejsze uznano prace: Mariana Mazura *Jakościowa teoria informacj*[46], zbiorowa *The Value and Impact of Information*[47], Leona Brillouina *Nauka a teoria informacj*[48]. Szczególnie wartościową publikacją, z powodu społecznego podejścia do informacji, okazała się praca Briana i Aliny Vickery'ch *Information Science in theory and practice*[49]. Istnieje oczywiście obszerniejsze piśmiennictwo w tym zakresie jednakże dużo materiałów poświęconych jest matematyczno-fizycznej koncepcji informacji, która mimo swojej wartości okazała się mniej przydatna w tych badaniach.

Kojarzący się z informacją jest także współczesny trend rozwoju cywilizacji, która została nawet nazwana *„społeczeństwem informacyjnym"*. Charakterystykę i analizę tego zjawiska najpełniej odzwierciedlały przede wszystkim prace Tomasza Gobana-Klasa[50], Piotra Sienkiewicza i Lecha Zachera. Ten ostatni jest redaktorem naukowym pracy zbiorowej[51] czternastu badaczy różnych aspektów społeczeństwa informacyjnego. Korzystano także z wielu publikacji dotyczących trendów rozwojowych współczesnej cywilizacji i ich charakterystyki.

Problematyka bezpieczeństwa i stosunków międzynarodowych obecna jest w rozległej grupie publikacji. Po wstępnym oglądzie najcenniejsze okazały się prace Raymonda Arona[52], Janusza Świniarskiego[53], Bolesława Balcerowicza[54], Edwarda Haliżaka[55], Ryszarda Zięby[56], Konstantego Wojtaszczyka[57]. Prace te stały się źródłem inspiracji w zakresie roli państwa w stosunkach z innymi podmiotami sceny

---

[46] *M. Mazur, Jakościowa teoria informacji, Warszawa 1970.*
[47] *M. Feeney, M. Grieves, The Value and Impact of Information, London 1994.*
[48] *L. Brillouin, Science and Information Theory. Wyd. pol. Nauka a teoria informacji, Warszawa 1969.*
[49] *B. i A. Vickery, Information Science in theory and practice, London, 1987.*
[50] *T. Goban-Klas, P. Sienkiewicz, Społeczeństwo informacyjne: Szanse, zagrożenia, wyzwania, Kraków 1999*
[51] *L. W. Zacher, Społeczeństwo informacyjne w perspektywie człowieka, techniki, gospodarki, Warszawa 1999.*
[52] *R. Aron, Pokój i wojna między narodami, Warszawa 1984.*
[53] *J. Świniarski, O naturze bezpieczeństwa. Prolegomena do zagadnień ogólnych, Warszawa-Pruszków, 1997.*
[54] *B. Balcerowicz, Sojusz a obrona narodowa, Warszawa 1999.*
[55] *D. B. Bobrow, E. Haliżak, R. Zięba, Bezpieczeństwo narodowe i międzynarodowe u schyłku XX wieku, Warszawa 1997.*
[56] *R. Zięba, Instytucjonalizacja bezpieczeństwa europejskiego, koncepcje – struktury – funkcjonowanie, Warszawa 1999.*
[57] *K. A. Wojtaszczyk, Kompendium wiedzy o państwie współczesnym, Warszawa 1998.*

międzynarodowej. Ponadto ugruntowały przekonanie autora o roli komponentu militarnego państwa we wspominanych stosunkach.

1.3.2. Geneza i rozwój poglądów na temat operacji informacyjnych

Główną wartością nowej cywilizacji XXI wieku jest informacja i systemy jej zdobywania, przetwarzania i dystrybucji. Każda sfera funkcjonowania współczesnego społeczeństwa staje się coraz bardziej zależna od informacji. Ponadto dokonuje się masowy proces automatyzacji i robotyzacji, który jest możliwy dzięki komputeryzacji systemów kierowania. Wszystkie te zjawiska pogłębiają się dzięki możliwości szybkiego przesyłania informacji pomiędzy praktycznie nieograniczoną rzeszą użytkowników. Dla potrzeb zbliżonego do czasu realnego zasilania informacyjnego coraz większych rzesz użytkowników ciągle rozbudowuje się sieci telekomunikacyjne i łączy je razem, co powoduje, że bardzo szybko rozrasta się globalna infrastruktura łączności. Infrastruktura ta staje się tak rozbudowana, że praktycznie niemożliwe jest wzbranianie dostępu do niej. To tworzy wrażliwość powstającej cywilizacji postindustrialnej. Jest ona niemalże całkowicie uzależniona od informacji i systemów informacyjnych. Jednocześnie łatwo z tej wrażliwości korzystać poprzez powszechny dostęp do globalnej sieci informacyjnej.

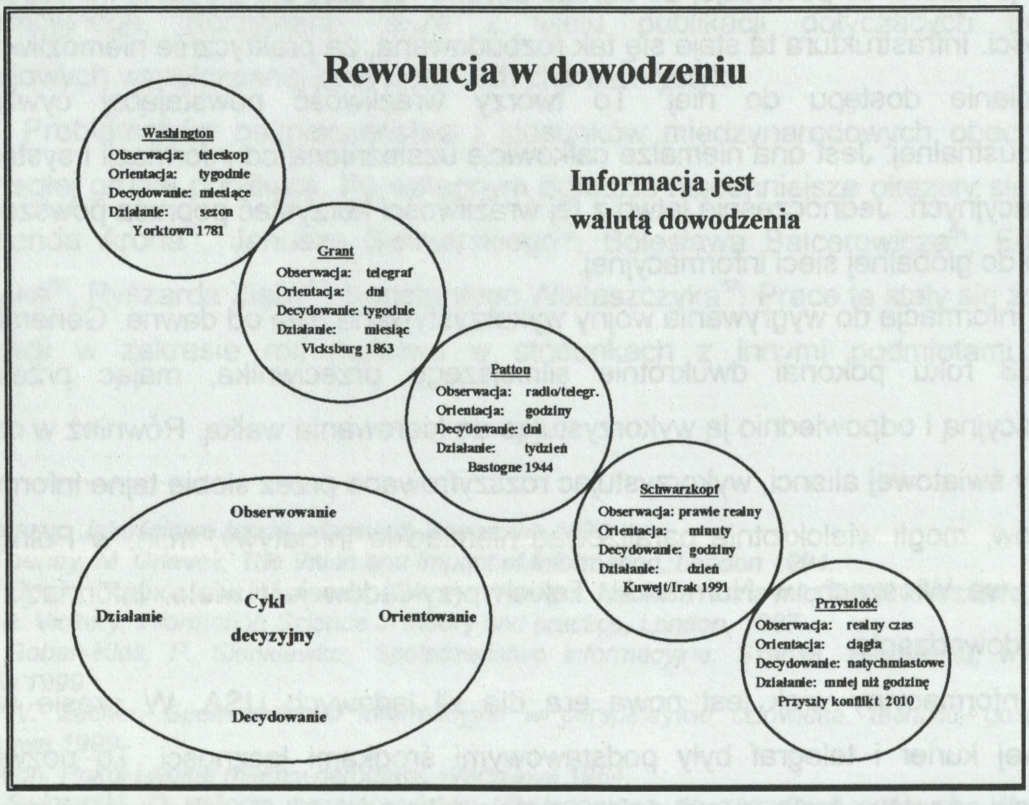
Informacja do wygrywania wojny wykorzystywana była od dawna. Generał Lee w 1863 roku pokonał dwukrotnie silniejszego przeciwnika, mając przewagę informacyjną i odpowiednio ją wykorzystując do kierowania walką. Również w czasie II wojny światowej alianci, wykorzystując rozszyfrowane przez siebie tajne informacje Niemców, mogli wielokrotnie paraliżować niemieckie inicjatywy, m.in. w Północnej Afryce, we Włoszech, w Normandii. Takich przykładów jest wiele. Informacja jest walutą dowodzenia.

Informacyjny wiek jest nową erą dla sił lądowych USA. W czasie wojny domowej kurier i telegraf były podstawowymi środkami łączności. To pozwalało dowódcy orientować się w sytuacji w czasie kilkunastu dni, podejmować decyzje w ciągu kilku tygodni i realizować je w ciągu miesiąca. W czasie II wojny światowej radio było podstawowym środkiem łączności, pozwalało na orientowanie się w sytuacji, w ciągu godzin, decydowanie w ciągu dni i wykonywanie decyzji w ciągu

tygodnia. Generał Schwarzkopf w czasie wojny z Irakiem obserwował sytuacje niemalże w czasie rzeczywistym, orientował się w czasie minut, decydował w czasie godzin i wcielał decyzje w czyn tego samego dnia[58].

W wyniku rozwoju elektroniki w toku automatyzacji procesów dowodzenia i kontroli uświadomiono sobie jeszcze bardziej konieczność dążenia do osiągania przewagi informacyjnej. Przewaga ta w połączeniu ze skracaniem cyklu decyzyjnego stała się podstawowym czynnikiem przewagi w dowodzeniu. W literaturze Zachodu często proces decyzyjny przedstawiany jest w postaci uproszczonego czterostopniowego modelu (rysunek 3.1).

W modelu tym zamknięty powtarzający się cykl składa się z obserwowania (zbierania informacji), orientowania (poznania sytuacji), decydowania, działania i ponownego obserwowania rezultatów działania oraz sytuacji, orientowania się w nowej sytuacji i podejmowania kolejnej decyzji i działania. Jakość działania zależy od jakości informacji, gdyż ta bezpośrednio wpływa na decyzje.



Rysunek 3.1. Rewolucja w dowodzeniu

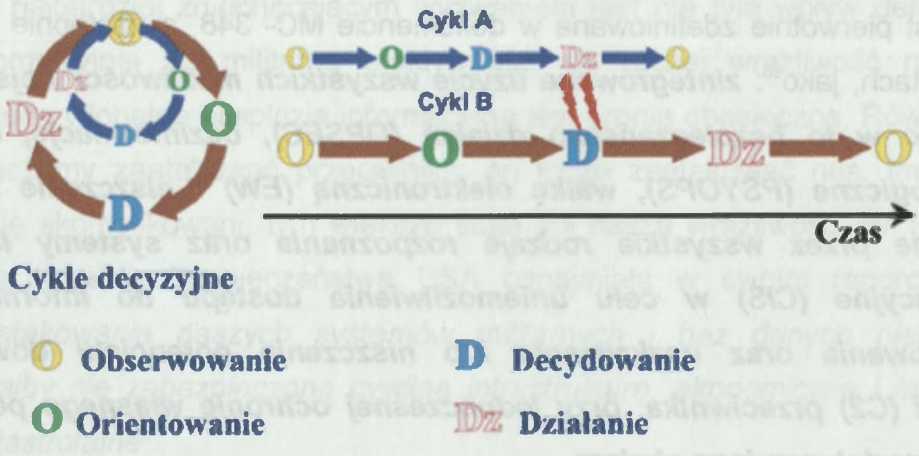
Źródło: Army Fokus 94. Force XXI America's Army In The 21st Century Department Of The Army, Washington DC 1994, s. 18.

---

[58] *R. Szpyra, Walka informacyjna w przyszłych działaniach sił powietrznych. Opracowanie pod kryptonimem CYBERAWIATOR, Warszawa 2000, s. 6, 49–50.*

W procesach walki dąży się do zwiększania racjonalności własnego działania oraz pogarszania racjonalności w działaniach przeciwnika. Wobec znaczenia informacji zmierza się do zapewnienia sobie jak najlepszej informacji oraz uniemożliwienia lub ograniczenia przeciwnikowi dostępu do informacji.

Kolejnym czynnikiem jest dynamika cyklu decyzyjnego wpływająca bezpośrednio na inicjatywę w działaniu. Gdy cykl decyzyjny jednej strony jest krótszy od cyklu drugiej, wówczas strona mająca krótszy cykl decyzyjny przejmuje inicjatywę w działaniu, a strona mająca ten cykl dłuższy musi dostosowywać swoje działanie do aktywności przeciwnika. Jeden z wariantów takiej sytuacji zobrazowany jest na rysunku 3.2.



Rysunek 3.2. Różne cykle decyzyjne

Widać na nim wyraźnie, że strona mająca krótszy cykl decyzyjny „A" już podejmuje działanie, podczas gdy strona „B" jest dopiero na etapie decydowania. W tej sytuacji będzie musiała reagować na działania przeciwnika. Wnika z tego, że oprócz walki o przewagę w jakości informacji toczy się również walka o wyprzedzenie przeciwnika w cyklu decyzyjnym. Innymi słowy, ten kto szybciej pozyska lepszą informację i szybciej zrealizuje swój cykl decyzyjny, uzyskuje co najmniej inicjatywę. Według teoretyków i praktyków Zachodu, jest to istota przewagi w dowodzeniu i kontroli. Walka o uzyskanie takiej przewagi polega przede wszystkim na zapewnianiu sobie lepszej informacji i szybszych procesów decyzyjnych oraz na niedopuszczaniu do osiągnięcia tego samego przez przeciwnika. **Walka tego typu nazywana jest *Command and Control Warfare* (C2W) a jej istotą jest walka o przewagę w dowodzeniu,** a koncepcja tej walki była próbą integracji różnych

działań w sferze informacyjnej w zorganizowaną całość. Walka ta przez niektóre źródła początkowo była utożsamiana z walką informacyjną. Obecnie w dalszym ciągu niektórzy traktują ją jako synonim walki informacyjnej.

Według treści amerykańskiej doktryny połączonej[59], walka o przewagę w dowodzeniu (Command And Control Warfare) to: Zintegrowane wykorzystanie bezpieczeństwa działań (OPSEC), mylenia, działań psychologicznych (PSYOP), walki elektronicznej (EW) i fizycznej destrukcji wspólnie wspieranych przez rozpoznanie w celu izolowania od informacji, wpływania, degradowania lub niszczenia systemów dowodzenia i kontroli przy zabezpieczaniu własnych tego typu systemów przed podobnymi akcjami.

W NATO walka o przewagę w dowodzeniu (*Command and Control Warfare* - C2W) jest pierwotnie zdefiniowana w dokumencie MC- 348, a następnie w innych dokumentach, jako[60]: ***zintegrowane użycie wszystkich możliwości wojskowych, włączając w to bezpieczeństwo działań (OPSEC), dezinformację, działania psychologiczne (PSYOPS), walkę elektroniczną (EW) i niszczenie fizyczne, wspierane przez wszystkie rodzaje rozpoznania oraz systemy łączności i informacyjne (CIS) w celu uniemożliwienia dostępu do informacji, jej modyfikowania oraz uszkadzania lub niszczenia potencjału dowodzenia i kontroli (C2) przeciwnika, przy jednoczesnej ochronie własnego potencjału przeciw podobnym jego akcjom***.

Podczas gdy walka o przewagę w dowodzeniu koncentruje się na dowodzeniu militarnym i kontroli w czasie użycia sił zbrojnych, to największe zainteresowanie wzbudziła ta część walki informacyjnej, która lokuje się poza obszarem tradycyjnego pola walki. Ten obszar zainteresowania jest uważany za najbardziej obiecujący. Rozwój technologiczny w elektronice, komunikacji, elektrooptyce i systemach komputerowych w połączeniu ze znanymi formami działań, takimi jak działania psychologiczne i mylenie oferują nowe formy osiągania celów narodowego bezpieczeństwa. Walka informacyjna może zniszczyć zdolność społeczeństwa do prowadzenia wojny bez wystrzelenia jednego pocisku poprzez destrukcję jego informacyjnej infrastruktury. W obszarze walki informacyjnej terytorium nie stanowi gwarancji jakiegokolwiek sanktuarium, granice są skrycie penetrowane w ciągu milisekund, a obiekty ataku są wszędzie. Przyszłe obiekty ataku należeć będą nie

---

[59] *JP 3-13 Joint Doctrine for Information Operations, Washington 1998, s. GL 4.*
[60] *Między innymi w: AJP-01(B), Glossary 3, a także w AAP-6.*

milisekund, a obiekty ataku są wszędzie. Przyszłe obiekty ataku należeć będą nie tylko do systemów militarnych, lecz także do infrastruktury cywilnej, takiej jak sieci bankowe, telekomunikacyjne, energetyczne, transportowe czy rurociągowe.

To cywilne zaangażowanie prowadzi do sedna obserwowanej ostatnio ewolucji walki informacyjnej. Wymyślona początkowo przez Departament Obrony USA koncepcja wewnętrznej odpowiedzi, wykorzystująca zarówno możliwości, jak i wrażliwości wynikające z informacyjnej eksplozji, okazała się rozleglejsza niż militarna sfera zainteresowania. Jeżeli realna użyteczność ofensywnej walki informacyjnej odnosi się również do pokoju, jak też do początkowych faz kryzysu, to dla uzyskania sukcesu niezbędne jest bezpośrednie zaangażowanie najwyższych władz państwowych oraz ścisła koordynacja i uczestnictwo wielu agend rządowych. Podobnie najbardziej zniechęcającym wyzwaniem jest nie tyle wpływ defensywnej walki informacyjnej na militarną efektywność, co raczej wrażliwość narodowej infrastruktury. Globalna eksplozja informacyjna jest bronią obosieczną. Równie łatwo jak my możemy zaatakować przeciwnika, on może zaatakować nas. Im bardziej stajemy się skomplikowani, tym większa staje się nasza wrażliwość. W 1994 roku Połączona Komisja Bezpieczeństwa USA oznajmiała w swoim raporcie: *jeżeli zamiast atakowania naszych systemów militarnych i baz danych nieprzyjaciel zaatakowałby nie zabezpieczoną cywilną infrastrukturę, ekonomiczne i inne skutki byłyby katastrofalne*[61].

Innym wymiarem walki informacyjnej jest wpływ mediów, takich jak CNN. Informacyjna rewolucja z bezpośrednimi transmisjami z pola walki, spowodowała zmiany tej walki. Wizualne przedstawienie konfliktu w niemal realnym czasie zintensyfikowało niechęć do śmierci i wojennej destrukcji na całym świecie, co nieprzyjaciel może eksploatować. Amerykański rząd jest przekonany o konieczności pełnego zaangażowania w wojnę mediów przez transmitowanie swoich własnych wiadomości, szczególnie w początkowej fazie kryzysu. Jest to kluczem do sukcesu informacyjnego odstraszania.

Potencjalne wrażliwości organizacji wykorzystujących sieci informatyczne związane z uzależnieniem od nich i małą troską o ich bezpieczeństwo zostały bardzo szybko dostrzeżone i wykorzystane. Jest już wiele informacji na ten temat. Warto przytoczyć charakterystyczne przykłady.

---

[61] *B. E. Fredericks, Information Warfare at the Crossroads, Joint Force Quarterly, Summer 1997, s. 98–99.*

„...W 1994 roku grupa rosyjskich hackerów ukradła kody i hasła klientów Citibanku, dzięki czemu zdołała przekazać dziesięć milionów dolarów na zamorskie konta. Sześciu Rosjan, jak podaje „NY Herald", zostało wszakże poddanych ekstradycji i przyznało się do przestępstwa. Według banku, udało się odzyskać pieniądze, z wyjątkiem 400 000 dolarów. [...]

Sumaryczne straty, jakie ponoszą amerykańskie korporacje rocznie, kiedy ów pojedynek czy raczej ową milczącą, bo cichą elektroniczną wojnę przegrywają, oceniają eksperci na kwotę trzystu miliardów dolarów, czyli straty są mniej więcej porównywalne z ekonomicznymi stratami ponoszonymi w wojnie najzupełniej *„normalnej"*. Głównymi celami ataków są chlubiące się światową supremacją przemysły, takie jak komputerowy, jak skoncentrowany na produkcji programów (*software*) i półprzewodników, jak molochy farmaceutyczne oraz wszystkie ośrodki, obsługujące zapotrzebowanie na broń[62].

„...Zaczęło się wszystko od zbuntowanego dwudziestolatka ze skłonnościami do science-fiction, komputerów i narkotyków, o pseudonimie Captain Hagbard. To on rozkręcił w 1985 roku hakerską akcję w Hanowerze, która dla niego samego zakończyła się samobójstwem, a dla kilku innych procesem sądowym."

"To niesamowite, że Hagbard potrafił włamać się do komputera w NORAD" – opowiadał później jeden z komputerowych maniaków z Hanoweru. Już w 1985 roku miał okazję oglądać niektóre z hakerskich sztuczek tego komputerowego pirata, który wyruszał w swoje wyprawy po informatyczne dane pod pseudonimem, zapożyczonym z powieści *science fiction.* Pod koniec 1985 roku Hagbard prezentował przy różnych okazjach sposób dotarcia do komputera amerykańskiego Dowództwa Obrony Powietrznej i Bombowców Strategicznych. Najczęściej droga prowadziła przez Fermi National Accelerator Laboratory (Fermilab), Laboratorium Badań Jądrowych w pobliżu Chicago, w którego sieci Hagbard czuł się jak w domu. Komputery serii VAX były jego komputerową ojczyzną. [...]

Dla Hagbarda dobrze się składało, że w Hanowerze znalazło się kilku hakerów, których zafascynowała możliwość włamania się do wojskowych komputerów połączonych siecią Milnet. Początkowo była to zabawa. Niewielka paczka hakerów z Hanoweru, do której należeli też profesjonalni programiści, interesowała się oprogramowaniem sieciowym i *"inteligentnymi"* programami. Bardzo

---

[62] *S. Lem, Bomba ..., s. 171 i 173.*

chcieli podejrzeć, co robią inni, żeby wiedzieć więcej niż konkurencja. Tak właśnie ujął to jeden z hakerów o pseudonimie Brainware. [...]

Hakerzy niemal osiągnęli swój cel. Znaleźli drogę do bazy danych Pentagonu oraz centrów badań jądrowych Los Alamos i Lawrence Livermore. Jednak szczególnie fascynował ich SAC. „Przez około 5 godzin byliśmy w SAC, w taktycznej grupie symulacyjnej Dowództwa Lotnictwa Strategicznego" – opowiadał jeden z hakerów biorących udział we włamaniu do wojskowej bazy danych na Sesji Hakerów w 1986 roku – *„Otworzyliśmy serwer".* Z odrobiną szczęścia i sprytu udało się przeniknąć do maszyny. Niezwykle pomocny okazał się napisany przez nich program, znany później pod nazwą *„kukułcze jajo".*

„Kukułcze jajo" umieszczano w obcym komputerze, a następnie uruchamiano jako podrzędny program. Zapewniał on hakerom, jako superuserom, pełną kontrolę nad komputerem. [...]

Już we wrześniu 1986 roku Stoll odkrył wojskową *„bazę wypadową"* hakerów: Redstone Anny Depot w Anniston w stanie Alabama. To stąd przeprowadzano większość udanych skoków komputerowych, a włamano się nie tylko do Dowództwa Lotnictwa Strategicznego. Ta wojskowa baza należy do tego samego dowództwa co White Sands Missile Range w Nowym Meksyku, gdzie testuje się rakiety, które następnie przesyła się do Anniston. Na należących do niej komputerach opracowywano przede wszystkim zamówienia i problemy w zaopatrzeniu. Przez całe miesiące przesiadywali tu hakerzy z Hanoweru, przeszukali całą bazę danych, wykradli plik z hasłami dostępu i przez cztery miesiące wykonywali stąd dalsze komputerowe skoki. Przenosili się dalej, na przykład do centrów badań jądrowych Los Alamos i Lawrence Liyermore oraz do baz danych Pentagonu OPTIMIS i RECON. Ktoś, kto powinien o tym wiedzieć, stwierdził, że sporo stąd wyczytano. [...]

Na ich liście znajdowały się nie tylko komputery wojska, ale również firm zbrojeniowych specjalizujących się w elektronice. W grudniu 1986 roku jeden z hakerów podłączył się na wiele godzin do TRW w Redondo Beach w Kalifornii. TRW jest zakładem produkującym na potrzeby Air Force i NSA, dostarcza komputery i satelity szpiegowskie KH-11. KH oznacza tutaj key hole, czyli dziurkę od klucza.

Haker poszukiwał danych o tym szpiegowskim satelicie, ale tego, co rzeczywiście mógł przeczytać, firma nie zdradziła"[63].

Opublikowana w 1992 roku przez Departament Obrony[64] Dyrektywa TS3600.1 zawierała zarys koncepcji walki informacyjnej. Była ona w istocie zbiorem wytycznych do dalszych badań i dyskusji. Jej szersze implikacje wyłoniły się z czasem w rezultacie studiów, gier wojennych i konferencji. Od początku szersze rozumienie walki informacyjnej ograniczane było przez sprawy bezpieczeństwa. Brak rozstrzygających detali definicji odnoszących się do sfery publicznej potęgowany był przez przedłużającą się nieobecność jawnej definicji walki informacyjnej.

W styczniu 1994 roku opublikowano pierwsze poważne rządowe wyjaśnienie sensu walki informacyjnej. Zawarte ono było w raporcie sekretarza obrony. Mimo iż raport ten nie zawierał definicji, to jednak stwierdzał, że ***walka informacyjna składa się z działań podejmowanych dla zachowania integralności własnych systemów informacyjnych i ich ochrony przed ich eksploatacją, degradacją lub destrukcją przy jednoczesnym eksploatowaniu, degradowaniu lub destrukcji systemów informacyjnych przeciwnika oraz w procesie użycia sił zbrojnych osiąganie przewagi informacyjnej***.

Ten opis wyraźnie podkreśla ofensywne i defensywne aspekty walki informacyjnej. Co więcej, raport stwierdzał, że jest to zintegrowana strategia, która uaktywnia bardziej zdecydowane działania, zwiększając prawdopodobieństwo ich sukcesu i minimalizując straty.

Zdolność do izolowania przeciwnika od środków prowadzenia wojny przez zniszczenie jego systemów informacyjnych tworzy głęboki efekt odstraszający. Walka informacyjna ma potencjał wypełnienia luki między sankcjami a bojowym użyciem sił zbrojnych. Jej odstraszająca wartość zwiększa się wraz z tym, jak potencjalny nieprzyjaciel orientuje się w jej efektywności i naszej woli użycia jej.

Zainteresowanie defensywną walką informacyjną systematycznie rosło w ciągu ostatnich lat. Jak stwierdziła Agencja Obrony Systemów Informacyjnych USA, w 1996 roku ponad 95 % globalnych potrzeb telekomunikacyjnych Departamentu Obrony zaspokajanych było przez cywilnych komercyjnych usługodawców telekomunikacyjnych, a establishment obronny jest integralną częścią

---

[63] *E. R. Koch, J. Sperber, Infomafia, szpiegostwo komputerowe handel informacją tajne służby, Gdynia 1999, s. 238–247.*
[64] *B. E. Fredericks, Information ..., s. 97–98.*

rosnącej globalnej infrastruktury informacyjnej, która wykracza poza przemysł, media i siły zbrojne. Defensywna walka informacyjna identyfikuje i zabezpiecza wrażliwe miejsca, które tworzą się w wyniku rosnącej zależności od światowej infrastruktury informacyjnej.

Utworzenie Prezydenckiej Komisji ds. Ochrony Krytycznej Infrastruktury w 1996 roku podkreśliło rosnącą świadomość potrzeby opracowania narodowej strategii ochrony funkcjonowania żywotnej dla kraju infrastruktury. Dotyczy to szczególnie systemów telekomunikacyjnych, finansowych, energetycznych, wodnych, rurociągowych i transportowych. Rosnąca zależność od wysoko rozwiniętych technologii jest nicią łączącą te systemy. Zagrożenie lokuje się w dwóch jego kategoriach: bardziej tradycyjne zagrożenia fizyczne i te powstające w wyniku zastosowania elektroniki, częstotliwości radiowych lub ataków typu komputerowego na informację lub komunikacyjne komponenty, które kontrolują krytyczną infrastrukturę. Celem działań prezydenckiej komisji jest proponowanie rozwiązań, które dotrzymywałyby kroku wyłaniającym się zagrożeniom w szybko zmieniającym się środowisku technologicznym. Integralną częścią pracy komisji jest ustanowienie kompletnego programu obejmującego sektor prywatny.

W dyskusji nad zagadnieniami walki informacyjnej uczestniczyli nie tylko wojskowi, ale także szerokie kręgi specjalistów cywilnych. Jednym z pierwszych takich badaczy, którzy zajęli się badaniem problematyki walki informacyjnej, był Winn Schwartau. Już w 1993 roku wydał w formie książkowej obszerny zbiór materiałów dotyczących szeroko rozumianej problematyki walki informacyjnej. W 1996 r. pojawiło się jej kolejne, jeszcze obszerniejsze wydanie[65]. Oto kilka istotnych spostrzeżeń tego autora.

„ ...Fundamenty współczesnego społeczeństwa oparte są na dostępności do informacji, która zabezpiecza prosperującej ekonomii wzrost lub spycha słabą w uzależnienie od silniejszej. W dzisiejszym elektronicznie wzajemnie połączonym świecie, informacja przemieszcza się z prędkością światła, jest nieuchwytna i niezmiernie wartościowa. Dzisiejsza informacja jest ekwiwalentem wczorajszych fabryk, lecz jest dużo bardziej wrażliwa.

Obecnie Stany Zjednoczone przodują w świecie w zakresie rozbudowy globalnie spiętego sieciami informacyjnymi społeczeństwa. Społeczeństwo to

---

[65] *W. Schwartau, Information Warfare. Cyberterrorism: Protecting Your Personal Security in the Electronic Age, New York 1996.*

wkracza w wiek informacji, gdzie informacyjne i ekonomiczne wartości stają się niemal synonimami. Ponad 125 milionów komputerów połączonych ze sobą przez kompleksowe lądowe i kosmiczne systemy łączności stanowi podstawę ponad gigantycznej ekonomii, która zależna jest od ciągłych i pewnych operacji. Walka informacyjna jest elektronicznym konfliktem, w którym informacja jest strategicznym dobrem wartym podboju lub destrukcji. Komputery i inne komunikacyjne i informacyjne systemy stają się atrakcyjnymi obiektami pierwszego uderzenia.

Współczesny złodziej może ukraść więcej z komputerem niż z karabinem. Jutrzejszy terrorysta może być w stanie dokonać więcej zniszczeń za pomocą klawiatury niż za pomocą bomby. [...]

Walka informacyjna jest integralnym komponentem nowego ekonomicznego i politycznego porządku światowego. Ekonomiczne bitwy są toczone i będą toczone, wpływając na każdego amerykańskiego obywatela i każdą firmę, jak również na bezpieczeństwo narodowe Stanów Zjednoczonych. Współczesny terroryzm to nie tylko ataki na linie lotnicze i systemy zaopatrzenia w wodę, ale także na systemy zasilania pieniężnego, to formy terroru uderzającego w miliony ludzi za pomocą pojedynczego uderzenia klawisza. [...]

Cyberprzestrzeń jest całkowicie nowym światem, który tylko luminarze, tacy jak Marshall McLuhan i Arthur C. Clarke, ujrzeli w oczach swojej wyobraźni, lecz nawet oni nie byli w stanie przewidzieć niepewności jaka zapanowała w ciągu ostatnich dwu dekad. Wyobraźmy sobie świat, gdzie informacja jest medium wymiany, a gotówka używana jest jedynie do zakupów podręcznych – świat, gdzie informacja, a nie język angielski, niemiecki, japoński czy rosyjski jest wspólnym językiem; świat, gdzie potęga wiedzy i informacji uzurpować sobie może siłę równą militarnej; świat całkowicie uzależniony od nowych narzędzi wysokiej techniki, która czyni informację dostępną permanentnie komukolwiek, gdziekolwiek w każdym czasie; świat gdzie ten, kto kontroluje informację, kontroluje ludzi; świat gdzie elektroniczna prywatność już nie istnieje.

Teraz wyobraźmy sobie konflikt między przeciwnikami, w którym informacja jest wygraną, wojennym łupem – konflikt ze zwycięzcą i pokonanym; konflikt, który określa komputery i systemy komunikacyjne (łączności) jako podstawowe cele zmuszone do samoobrony przeciwko zabójczym, niewidzialnym kulom i bombom. Wyobraźmy sobie rywalizujące ekonomie, które walczą o poszerzenie strefy globalnego wpływu na elektroniczne, finansowe infostrady, nie poświęcając żadnych

wydatków dla zapewnienia zwycięstwa. Następnie wyobraźmy sobie świat złożony z firm, które rywalizują i rozwiązują spory za pomocą regularnych wzajemnych najazdów – blitzkriegów na informacyjne infrastruktury; świat, gdzie elektroniczne i rywalizacyjne szpiegostwo jest oczekiwaną manierą prowadzenia biznesu.

Ponadto wyobraźmy sobie świat, w którym osobisty rewanż i odwet są w zasięgu uderzenia klawisza. Jakiego rodzaju jest to świat? To jest świat walki informacyjnej, a my jako jednostki i jako kraj nie jesteśmy przygotowani na przyszłość, którą sobie tworzymy. [...]

Walka informacyjna jako broń informacyjnego wieku zamieni bomby i naboje. Te bronie nie są już dłużej zastrzeżone dla rządu, CIA lub KGB. Komputerowe i informacyjne bronie są dostępne z katalogów i sklepów. Te arsenały mogą być budowane przez hobbystów w domu. Oczywiście, siły zbrojne rozwijają swoje arsenały broni, którymi prowadzi się walkę informacyjną.

Walka informacyjna dotyczy pieniędzy. Odnosi się do dystrybucji dóbr i polega na niedopuszczaniu ich do oponenta. Walka ta rodzi informacyjnych wojowników, którzy toczą walki na wskroś globalnej sieci w grze cyberryzyka.

Walka informacyjna dotyczy władzy. Ten, kto kontroluje informację, kontroluje pieniądze.

Walka informacyjna dotyczy także strachu. Ten, kto kontroluje informację, może zaszczepić strach tym, którzy chcą trzymać swoje sekrety w ukryciu. To jest strach, że np. bank Nowego Jorku upadnie, gdy tylko na jeden dzień powstanie w nim deficyt 23 miliardów dolarów i zostanie to ujawnione.
Walka informacyjna dotyczy także arogancji płynącej z przekonania, że popełnia się przestępstwo doskonałe.

Walka informacyjna dotyczy też polityki. Gdy niemiecki rząd sponsoruje agencję wywiadowczą włamującą się do amerykańskich komputerów, koncepcja sojusznika powinna być zdefiniowana od nowa. Także gdy Iran bierze na cel amerykańską ekonomię przez sponsorowane przez rząd fałszerstwa, powinno to być dla nas sygnałem, że konflikt nie jest tym czym był kiedyś.

Walka informacyjna dotyczy przeżycia. Francja i Izrael rozwinęły swoje ekonomie i oparły całe gałęzie przemysłu na kradzieży amerykańskich sekretów. Japonia i Korea z pomocą swoich rządów kradną amerykańską technologię, gdy tylko schodzi ona z desek kreślarskich.

Walka informacyjna dotyczy wyzwań. Z zaniedbanych dzielnic cyberprzestrzeni zjawią się hakerzy marginesu społecznego z niczym do stracenia. Część z nich zorganizuje się w działające w cyberprzestrzeni gangi, zorganizowaną przestępczość cyberprzestrzeni. Uznają oni i docenią korzyści ekonomiczne płynące z prowadzenia walki informacyjnej.

Walka informacyjna dotyczy także kontroli informacji. Jako społeczeństwo utrzymujemy coraz to mniej i mniej kontroli nad tym, jak cyberprzestrzeń się rozszerza i rozprzestrzenia się elektroniczna anarchia. Z uwagi na globalne warunki lat 80. i 90., walka informacyjna jest nieunikniona. Dzisiejsza planeta oferuje dojrzałe warunki dla walki informacyjnej, warunki, które nie były przewidywane nawet kilka lat temu.

Walka informacyjna kosztuje Stany Zjednoczone około 100–300 miliardów dolarów rocznie i finansowy wpływ na ekonomię tego kraju zwiększa się z każdym rokiem. Prawie 5% produktu krajowego USA wyślizguje się przez globalną sieć spoza kontroli narodowej, osłabiając tym samym wysiłki czynione w kierunku ograniczania deficytu budżetowego, negatywnie wpływając na potencjał eksportowy i nierównowagę eksportową. [...]

Jednak roczne straty w wysokości ponad 200 miliardów dolarów dotyczą głównie ludzi – około ośmiu milionów ludzi mogłoby mieć pracę, gdyby nie efekty walki informacyjnej. Ludzie ci są również ofiarami walki informacyjnej. Walka informacyjna korzysta z uzależnienia od współczesnych automatycznych skomputeryzowanych drobiazgów.

Zagrożenie przyszłym komputerowym Czernobylem nie jest gołosłowne. Jest tylko kwestią: kto i kiedy. Walka informacyjna jest dostępna dla każdego, kto ma plan i odpowiedni stosunek do tego przedsięwzięcia. Walka ta może być prowadzona na trzech wyraźnych poziomach intensywności, każdy ze swoimi celami, metodami i obiektami"[66].

Naturę walki informacyjnej dobrze ilustruje rysunek 3.3.

---

[66] *Tamże, s. 28–32.*



Rysunek 3.3. Natura walki informacyjnej
Źródło: Information Warfare Legal Regulatory, policy and Organizational Considerations for Assurance 2nd Edition, Washington 1996,s. 3.

Mimo wyraźnego związku wyłaniającej się walki informacyjnej z postępem cywilizacyjnym końca XX wieku, Leopold Ciborowski jest słusznie przekonany, że: „...Historia walki informacyjnej jest tak samo długa jak historia ludzkich dziejów. Nikt jej jednak nie spisał. Co więcej – nigdy nawet nie używano takiego pojęcia. Nie oznacza to jednak, że kojarzone z nią dziś funkcje zdobywania informacji, zakłócania informacyjnego i obrony informacyjnej zaistniały dopiero u schyłku XX wieku. Istniały zawsze. Teraz unaoczniają się tylko z niewspółmiernie większą wyrazistością.

Postępująca politechnizacja życia i szybki rozwój szeroko rozumianej komunikacji spowodowały, że samo słowo *informacja* stało się dziś pojęciem powszechnie używanym. Zawsze jednak walczące ze sobą strony rozpoznawały się wzajemnie. Zawsze starały się wzajemnie oszukiwać i wprowadzać w błąd. Zawsze też posiadały swoje sekrety, które z wielką skrupulatnością ukrywały przed wrogiem.

Odnosząc to do współczesności, wszystkie te czynności mieszczą się w obszarach funkcjonalnych zdobywania informacji, zakłócania informacyjnego i obrony informacyjnej, co w dwupodmiotowej kooperacji negatywnej wzajemnej tworzy przestrzeń walki informacyjnej [...]. Patrząc zatem na przeszłość pod takim kątem, widzimy, że historia walki informacyjnej zdaje się być tak samo długa jak

historia ludzkich dziejów. Najwięcej faktów na ten temat można znaleźć w historii wojen, bo i te w przeszłości stanowiły jedno z bardziej rozpowszechnionych zjawisk społecznych"[67].

Prawdopodobnie najobszerniejsza dyskusja[68] w sprawie walki informacyjnej toczyła się w związku z opublikowaniem w 1996 r. przez Kolegium Szefów Sztabów wydawnictwa *„Strategia dla pokoju: Decydujące ostrze wojny"*. Stwierdzono tam, że walka informacyjna odnosi się do całego spektrum działań militarnych i do wszystkich poziomów walki. Walka informacyjna, mimo że nie jest jedynym instrumentem narodowej potęgi, to jednak przyczynia się do odstraszania przez rozładowywanie kryzysów i opóźnianie lub eliminowanie użycia sił. Defensywna walka informacyjna integruje i zabezpiecza informację i jej systemy przez oddziaływanie ofensywną walką informacyjną na informację przeciwnika i jego informacyjne systemy.

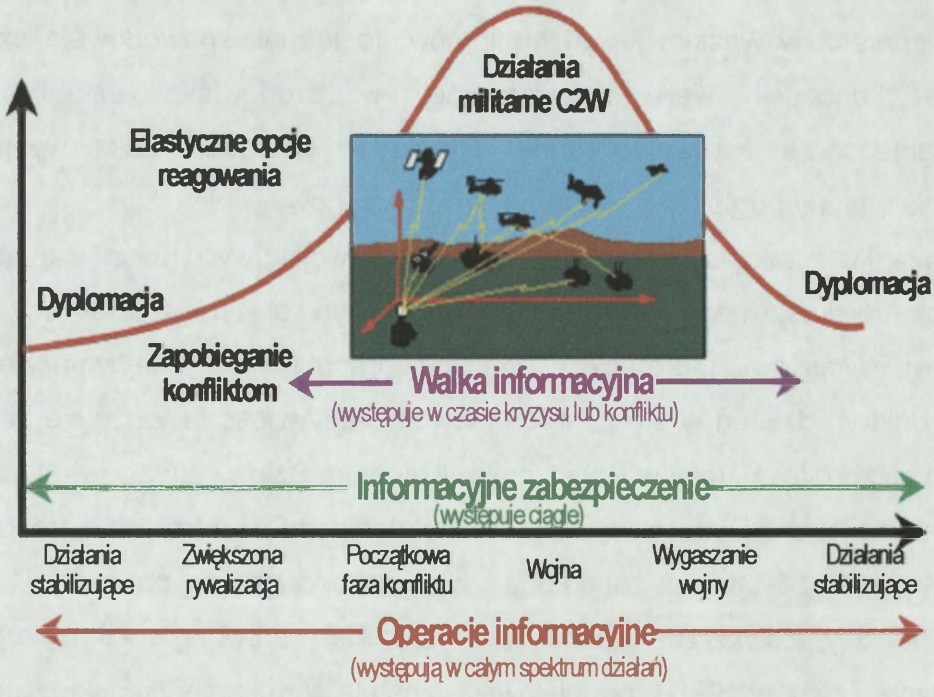
W rezultacie rozległej dyskusji uświadomiono sobie nieadekwatność nazwy „walka informacyjna" do zakresu desygnatów przypisywanych temu pojęciu. Szeroka gama przedsięwzięć sfery informacyjnej jest prowadzona już w czasie pokoju i trudno je kwalifikować jako walkę.

Również ze względów propagandowych prezentowanie np. działań prewencyjnych i zabezpieczających jako „walki" może rodzić pejoratywne oceny i nastawienie. Wiele przedsięwzięć może być także stosowanych w działaniach niemilitarnych i pozawojennych.

Dlatego też postanowiono poszukać bardziej adekwatnej nazwy dla całego spektrum działań w sferze informacyjnej. Uznano, że najodpowiedniejszym będzie przyjęcie ogólnej nazwy „operacje informacyjne" (*Information Operations*). Nazwa ta nie budzi negatywnych skojarzeń. Może obejmować przedsięwzięcia zarówno militarne, jak i niemilitarne, a także równie dobrze zawierać formy walki, jak i współpracy. W takim ujęciu „walka informacyjna" dalej istnieje, jest ona jednakże komponentem operacji informacyjnych i obejmuje szerszy od nich zakres (rysunek 3.4).

---

[67] *L. Ciborowski, Walka ..., s. 11. Znajduje się tam syntetyczna historia rozwoju walki informacyjnej.*
[68] *B. E. Fredericks, Information ..., s. 98.*



Rysunek 3.4. Sfera operacji informacyjnych
Źródło:B.E.Fredericks, Information Warfare at the Crossroads, Joint Force Quarterly 1997,Summer,s. 99.

W 1996 r. Biuro Asystenta Sekretarza Obrony USA[69] do spraw C3I wydało wytyczne w zakresie opracowania nowej dyrektywy w tej sprawie, zastępującej tę z 1992 roku (TS3600.1). Wytyczne te służyć miały trzem celom: zapewnieniu, mimo niejawności części zagadnień, szerokiego dostępu do unormowań, odpowiadającego powszechnemu zainteresowaniu; zapewnieniu jednolitego rozumienia wewnątrz Departamentu Obrony i koordynacji między różnymi agendami rządowymi oraz wskazaniu pełnego potencjału walki informacyjnej w całym spektrum działań militarnych ze skupieniem głównej uwagi na zachowaniu pokoju i zapobieganiu eskalacji konfliktu. Z tymi wskazaniami napisana została też nowa dyrektywa Departamentu Obrony. Mimo iż w dalszym ciągu zawiera ona elementy niejawne, to zasadnicza część jest jawna. W jawnej części znajdują się wszystkie kluczowe definicje. Jest prawdopodobne, że wraz z dalszym dojrzewaniem koncepcji kolejna jej wersja będzie całkowicie jawna.

W rezultacie już w grudniu 1996 roku opublikowano nową dyrektywę Departamentu Obrony S3600.1 *„Information Operations”,* co otworzyło nową fazę

---

[69] *Tamże, s. 97 i 100.*

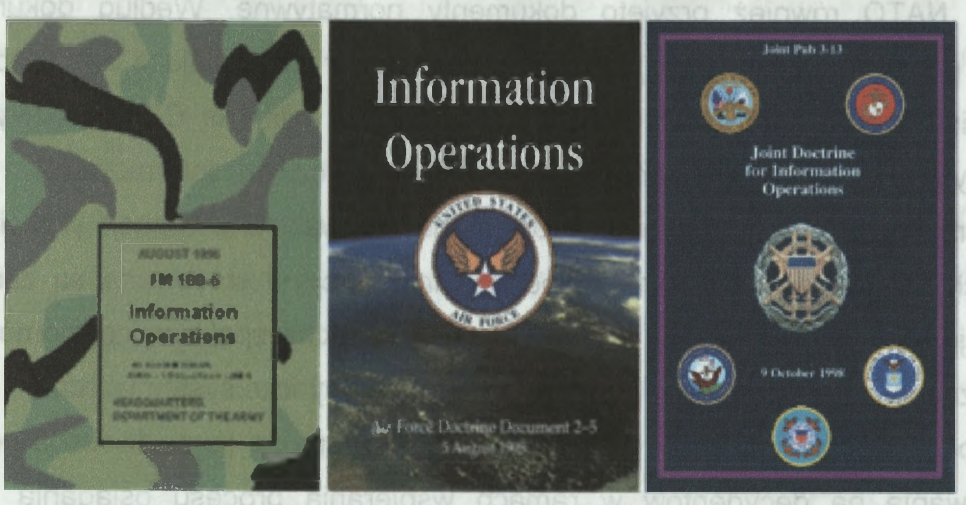
w rozwoju walki informacyjnej. Mimo iż dyrektywa ta była niejawna i rozpowszechniana w wąskim kręgu odbiorców, to jednak spowodowała szybsze dojrzewanie koncepcji walki informacyjnej w środowisku establishmentu odpowiedzialnego za sprawy obronne. Dyrektywa ta uwzględniła wynikające z dojrzewania zmiany poglądów i wprowadziła USA w nowy wiek.

W związku z taką sytuacją w środowiskach wojskowych toczy się obecnie coraz szersza dyskusja nad problemami zagrożeń wynikających z działań w sferze informacyjnej. Wojskowi teoretycy i praktycy pracują nad kolejnymi wersjami koncepcji i doktryn działań w sferze informacyjnej. Aktywność ta toczy się zarówno w rodzajach sił zbrojnych, jak i w Połączonym Kolegium Szefów Sztabów. W 1996 r. wydano doktrynę operacji informacyjnych Amerykańskich Sił Lądowych w postaci FM 100-6. Doktryna ta została już zmieniona i wydana pod kolejną postacią. Również Amerykańskie Siły Powietrzne opublikowały w 1998 r. swoją doktrynę operacji informacyjnych. Także w 1998 r. opublikowana została przez amerykańskie Kolegium Szefów Sztabów Połączona Doktryna Operacji Informacyjnych (rysunek 3.5).

Opublikowanie przez Stany Zjednoczone połączonej militarnej doktryny operacji informacyjnych wielu ekspertów[70] uznało za ważny moment historyczny oznaczający początek wyścigu zbrojeń w sferze działań informacyjnych. Zgodnie z nowym dokumentem (Joint Doctrine for Information Operations JP 3-13) pierwszy raz oficjalnie uznano, iż ofensywne ataki na sieci komputerowe stają się nieodłączną częścią arsenału walki USA, a co jeszcze ciekawsze, arsenał ten może być używany także w czasie pokoju. W rezultacie każdy kraj musi zatroszczyć się o uzyskanie zdolności do prowadzenia ofensywnych i defensywnych operacji informacyjnych. Jeśli tego zaniecha, pozostanie bezbronny. Oficjalne wprowadzenie operacji informacyjnych do doktryny militarnej dokonało się między innymi wobec wyraźnych deklaracji wielu krajów (jak np. Chiny), gotowości wykorzystania tej sfery w walce. Jednocześnie wprowadzenie tej sfery do doktryny militarnej oznacza, że rozwinięte zostały możliwości gwarantujące pewność osiągania pożądanych efektów.

---

[70] *G. I. Seffers, Joint Chiefs Inaugurate Information Combat Era, Defense News 1998, November, s. 9–15,.*



Rysunek 3.5. Doktryny operacji informacyjnych amerykańskich sił lądowych i powietrznych oraz doktryna połączona

Stany Zjednoczone jeszcze przed opublikowaniem doktryny operacji informacyjnych prowadziły wiele badań i rozwijały swoje możliwości w zakresie operacji informacyjnych. Przykładowo, przygotowywano się do sparaliżowania systemu energetycznego przeciwnika lub jego węzłów telekomunikacyjnych przed wykonaniem ataku ogniowego lub brano pod uwagę informacyjne uderzenie jako alternatywę ataku ogniowego.

Po wielu rozważaniach uświadomiono sobie, że operacje informacyjne niosą za sobą korzyści i możliwości niemożliwe do osiągnięcia przy użyciu broni konwencjonalnej arsenałów epoki pozimnowojennej.

Podstawową kwestią godną szczególnej uwagi jest to, że operacje informacyjne są „bronią masowego rażenia". Właściwe zidentyfikowanie infrastruktury, połączone z wartościową informacją rozpoznawczą, wsparte dobrymi programami symulacyjnymi i wspomagającymi proces decyzyjny - może skutkować zniszczeniem narodu.

W formułowaniu doktryn przodują Amerykanie. Mimo koordynacji dokumenty poszczególnych rodzajów sił zbrojnych i połączonych nie są jednakowe. Istnieją pewne różnice w podejściu i mimo opublikowania nieraz kolejnych już wersji doktryn operacji informacyjnych dyskusja nabiera rozmachu.

W NATO również przyjęto dokumenty normatywne. Według dokumentu doktryny połączonej[71] AJP-01(B), wydanego w 2000 r., wyłaniająca się koncepcja operacji informacyjnych (INFO OPS) wiąże strategię militarną C2W z polityczną, dyplomatyczną i cywilno-militarną współpracą, publicznym informowaniem oraz innymi formami aktywności Sojuszu, które mogą wpływać na percepcję przeciwnika lub innych zaangażowanych stron. Operacje informacyjne stosowane są zarówno jako akcje defensywne, jak i ofensywne w szerokim spektrum poziomów od strategicznego przez operacyjny i taktyczny aż po pojedyncze systemy broni.

Operacje informacyjne w tej doktrynie definiowane są jako „działania podjęte dla wpływania na decydentów w ramach wspierania procesu osiągania celów politycznych i militarnych mające charakter wpływania na informację, procesy informacyjne, systemy dowodzenia i kontroli oraz systemy komunikacyjno-informacyjne (CIS) przy eksploatowaniu i ochronie własnej informacji i systemów informacyjnych."

W prezentacji poglądów akcent położono na poglądy doktrynalne, bo są one wypadkową ogromnej ilości badań wielu zespołów ekspertów oraz pojedynczych badaczy. W wyniku tego odzwierciedlają zarówno szeroki horyzont potencjalnych możliwości, jak i realia rzeczywistości. Są w znacznym stopniu zweryfikowanymi w praktyce teoriami. W sferze teorii istnieje wielkie bogactwo poglądów na temat walki informacyjnej ale też i coraz więcej w zakresie operacji informacyjnych. Niektóre zostały już zacytowane, warto przytoczyć jeszcze kilka z nich.

Według Roda Starka[72], „...Nie istnieje powszechnie uzgodniona definicja walki informacyjnej. Jest jednak wspólna treść większości spotykanych definicji. Treść ta sprowadza się do tego, że walka informacyjna jest konfliktem, w którym informacja jest jednocześnie zasobem, obiektem ataku i bronią. Walka informacyjna obejmuje także fizyczną destrukcję infrastruktury, która wykorzystywana jest przez przeciwnika do działań operacyjnych. [...]

Walka informacyjna jest ważnym elementem strategii Stanów Zjednoczonych bo może działać jako **mnożnik siły**, umożliwiając planistom planującym walkę oraz decydentom politycznym podejmować racjonalne decyzje przed rozmieszczeniem wojsk. Umożliwia także zwiększenie narodowych zasobów.

---

[71] *Allied Joint Doctrine AJP-01. NATO. Wydanie 1999, s. 14-1.*
[72] *R. Stark, Future Warfare: Information Superiority through Info War, http://www.smsu.edu*

Głównym aspektem walki informacyjnej jest wysiłek zmierzający do zdobycia i utrzymania kontroli środowiska informacyjnego, który prowadzi do dominacji informacyjnej.

Dla potrzeb walki XXI wieku walka informacyjna obejmuje:

- walkę o przewagę w dowodzeniu (Command and control warfare C2W);
- walkę bazującą na wiedzy rozpoznawczej *(Intelligence-based warfare IBW)*;
- walkę elektroniczną *(Electronic Warfare EW)*: uniemożliwianie przeciwnikowi dostępu do dokładnej informacji;
- działania psychologiczne *(Psychological informations PSYOPS)*: używanie informacji do wpływu na jego rozumowanie;
- wojnę hakerską *(Hackerwar)*: ataki softwareowe na systemy informacyjne;
- informacyjną walkę ekonomiczną *(Information economic warfare IEW)*: wojna za pomocą kontroli informacji handlowej;
- cyberwojnę *(Cyberwar)*: walka w wirtualnej rzeczywistości;
- dezinformację militarną *(Miliatry Deception)*: wprowadzanie w błąd co do możliwości i zamiarów;
- fizyczne niszczenie *(Physical Destruction)*: użycie spektum broni od konwencjonalnej do impulsu elektromagnetycznego;
- przedsięwzięcia bezpieczeństwa *(Security Measures)*"[73].

Według Piotra Sienkiewicza: „W ostatnich latach wyróżniono informacyjne operacje (działania) ofensywne i defensywne.

Do operacji ofensywnych zalicza się takie działania, jak:

- osłona operacji (*operations security*);
- operacje psychologiczne (*psychological operations*);
- pozoracja (military deception);
- destrukcja (physical attack);
- walka elektroniczna (*electronic warfare*);
- atak informatyczny (computer network attack);
- działania typu „civil affairs" i „public affairs".

Natomiast w ramach operacji defensywnych:

---

[73] *Tamże.*

- bezpieczeństwo informacyjne (*information assurance);*
- osłona (operation security);
- działania kontrpropagandowe (*counterpropaganda);*
- działania kontrwywiadowcze (*counterintelligence);*
- walka elektroniczna (*electronic warfare);*
- informacyjne działania specjalne (special information operations)"[74].

Według Ryszarda Szpyry[75] operacje informacyjne państwa to zorganizowana aktywność państwa prowadząca do osiągnięcia określonych celów politycznych, skierowana na zewnętrzne i wewnętrzne systemy informacyjnego komunikowania lub przepływającą przez nie informację.

Odpowiednio do tego właściwe sferze militarnej państwa militarne operacje informacyjne to zorganizowana aktywność militarna państwa prowadząca do osiągnięcia określonych celów politycznych, skierowana na zewnętrzne i wewnętrzne systemy informacyjnego komunikowania lub przepływającą przez nie informację.

Operacje informacyjne składają się z trzech głównych komponentów, którymi są: współpraca informacyjna (kooperacja pozytywna); walka informacyjna (kooperacja negatywna) i informacyjne zabezpieczenie. Dwie pierwsze formy aktywności odnoszą się do stosunków między państwami, a więc do relacji zewnętrznych. Tymczasem istnieje jeszcze inny ważny obszar potrzeb. Jest nim zasilanie informacyjne własnych procesów wewnętrznych. Zaspokajanie tych potrzeb jest domeną trzeciej formy: informacyjnego zabezpieczenia.

Walka informacyjna jest formą kooperacji negatywnej operacji informacyjnych. Ponieważ istotą walki jest przemoc[76], a przedmiotem tej walki są systemy informacyjnego komunikowania przeciwnika oraz przepływająca przez nie informacja, to można przyjąć, że **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**

---

[74] P. *Sienkiewicz, Współczesne koncepcje ...*
[75] *R. Szpyra, Operacje informacyjne państwa w działaniach sił powietrznych. Rozprawa habilitacyjna, Warszawa 2002.*
[76] *Tamże rozdział 1.3.*

informacyjnego komunikowania i przesyłanej przez nie informacji przed podobnym działaniem przeciwnika.

Częścią walki informacyjnej państwa jest militarna walka informacyjna. Główną cechą wyróżnialności tego podzbioru jest podmiot prowadzący działania, jakim jest komponent militarny państwa. W związku z tym **militarna walka informacyjna to zorganizowana w formę przemocy militarna aktywność zewnętrzna państwa prowadząca do osiągnięcia określonych celów politycznych, skierowana na niszczenie lub modyfikowanie systemów informacyjnego komunikowania przeciwnika lub przepływającej przez nie informacji oraz aktywność zapewniająca ochronę własnych systemów informacyjnego komunikowania i przesyłanej przez nie informacji przed podobnym działaniem przeciwnika.**

Zarówno więc praktyka, jak i badania teoretyczne wykazały, że każda sfera aktywności państwa, nie tylko militarna, znajduje się w ogniu intensywnego oddziaływania informacyjnego mającego często charakter kooperacji negatywnej, czyli walki informacyjnej. Tak więc w atmosferze teoretycznych poszukiwań i wobec wysokiej dynamiki negatywnych zjawisk zachodzących w informacyjnej sferze praktyki pojawiły się zarysy różnych koncepcji walki informacyjnej oraz operacji informacyjnych. Przegląd wybranych definicji walki informacyjnej i operacji informacyjnych zawiera tabela 3.1 i 3.2.

Tabela 3.1

Definicje walki informacyjnej – przegląd

Walka informacyjna	
Joint Chiefs of Staff, Washington 1998.	Walka informacyjna to działania informacyjne prowadzone w czasie kryzysu lub konfliktu dla osiągnięcia pożądanych celów w relacjach z przeciwnikiem lub wsparcia działań prowadzących do tych celów.
AFDD Joint Doctrine for Information Operations. Joint Pub 3-13, 2-5 Information Operations. USAF	Walka informacyjna to działania informacyjne prowadzone dla obrony własnej informacji i systemów informacyjnych lub prowadzone dla atakowania i wywarcia wpływu na informację lub systemy informacyjne przeciwnika. Ta walka jest prowadzona głównie w czasie kryzysu lub konfliktu. Jednak defensywny komponent tej walki, podobnie jak obrona powietrzna, jest prowadzony w całym spektrum działań militarnych, od pokoju do wojny.
DOD & Joint Staff – CJCSI 3210.01, [w:] *FM 100-6*	Walka informacyjna to działania podejmowane dla osiągnięcia przewagi informacyjnej przez wpływanie na informację przeciwnika,

Information Operations, Headquarters, Department of the Army, 1996, s.2-2.	jego zależne od informacji procesy, informacyjne systemy i sieci komputerowe przy jednoczesnej obronie własnej informacji, zależnych od informacji procesów, informacyjnych systemów i sieci komputerowych.
S. Widnall, R. Fogleman, *Cornerstones of Information Warfare*, Headquarters, Department of the Air Force, Washington 1995.	Walka informacyjna to jakiekolwiek działania mające na celu wzbranianie przeciwnikowi dostępu do informacji i jej funkcji lub ich eksploatację, degradację bądź niszczenie; ochrona siebie przeciwko takim działaniom oraz eksploatowanie własnych militarnych funkcji informacyjnych.
W. Schwartau, *Information Warfare. Cyberterrorism: Protecting Your Personal Security in the Electronic Age*, Thunder's Mouth Press. 1996, s. 28 – 32	Walka informacyjna jest elektronicznym konfliktem, w którym informacja jest strategicznym dobrem wartym podboju lub destrukcji.
E. Paige, [za:] G. Ivefors, *Information Warfare. Defeat the enemy before battle – a warfare revolution in the 21st century?* http://www.ida.liu.se/~guniv/Infowar/ 26.01.2001.	Walka informacyjna to działania podejmowane dla osiągnięcia przewagi informacyjnej, prowadzone w ramach wspierania narodowej strategii militarnej. Działania te mają na celu wpływanie na informację i systemy informacyjne przeciwnika przy wpływaniu i obronie własnej informacji i jej systemów.
J. Arquilla, D.Ronfeldt, *Cyberwar is Coming*, [w:] *Comparative Strategy 12-1993*, s. 41-65 [za:] G. Stein, *Information Warfare*, [w:] A. D. Campen, D. H. Deart, R. T. Goodden, *Cyberwar: Security, Strategy, and Conflct in the Information Age*, AFCEA International Press, Fairfax 1996, s. 175.	Walka informacyjna w najogólniejszym sensie jest użyciem informacji dla osiągnięcia naszych narodowych celów. Podobnie jak dyplomacja, ekonomiczna rywalizacja czy użycie sił zbrojnych, informacja sama w sobie jest kluczowym czynnikiem narodowej potęgi. Ponadto, co jeszcze ważniejsze, informacja staje się głównym narodowym zasobem, który wspiera dyplomację, ekonomiczną rywalizację oraz przemoc militarną. Walka informacyjna w tym sensie może być postrzegana jako konflikt między państwami lub narodami prowadzony częściowo przez globalnie połączoną infrastrukturę informacyjną i komunikacyjną.
R. Szafranski, *Cyberwar: A Theory of Information Warfare: Preparing For 2020*, [w:] A.D. Campen, D. H. Deart, R T. Goodden, *Cyberwar: Security, Strategy, and Conflct in the Information Age*, AFCEA	Walka informacyjna jest formą konfliktu, w którym bezpośrednie atakowanie systemów informacyjnych jest środkiem atakowania wiedzy i przekonań przeciwnika. Walka informacyjna może być prowadzona jako komponent kompleksowej wrogiej działalności – w postaci wojny sieciowej (*netwar*) lub cyberwojny (*cyberwar*) – lub może przybierać formę walki samodzielnej.

International Press, Fairfax 1996, s. 233.	
R. J. Knecht, *Thoughts About Information Warfare*, tamże, s. 165.	Walka informacyjna jest przygotowaniem do użycia lub użyciem fizycznej lub cyfrowej broni dla dezorganizacji lub niszczenia informacji lub systemów informacyjnych w celu degradowania lub przerywania wykonywania funkcji, które zależą od informacji lub informacyjnych systemów.
R. Stark, *Future Warfae: Information Superiority through Info War*, Southwest Missouri State University, http://www.smsu.edu	Walka informacyjna jest konfliktem, w którym informacja jest jednocześnie zasobem, obiektem ataku i bronią. Walka informacyjna obejmuje także fizyczną destrukcję infrastruktury, która wykorzystywana jest przez przeciwnika do działań operacyjnych.
L. Ciborowski, *Walka informacyjna*, Toruń 1999.	Walka informacyjna to działania kooperacji negatywnej wzajemnej, w których cel destrukcyjnego oddziaływania skoncentrowany jest na systemach informacyjno-sterujących przeciwnych sobie stron. Przedmiotem walki informacyjnej jest system informacyjno sterujący.
G. Nowacki, *Walka informacyjna - próba kategoryzacji. Rozprawa doktorska*, AON, Warszawa 1999, s. 112-113.	Walka informacyjna – kooperacja negatywna wzajemna, w której cel destrukcyjnego oddziaływania skoncentrowany jest na systemach informacyjno-sterujących przeciwnych sobie stron. „Przedmiotem walki informacyjnej" – są systemy informacyjno-sterujące i ich otoczenie.
M. Libicki, *What is Information Warfare?* NDU, Washington 1995, s. x.	Walka informacyjna jako samodzielna technika prowadzenia wojny nie istnieje. W zamian istnieje kilka oddzielnych form walki informacyjnej, z których każda pretenduje do bycia ogólniejszą koncepcją. Obecnie wyróżnić można siedem form walki informacyjnej – konfliktu, który zawiera ochronę, manipulację, degradację lub uniemożliwianie dostępu do informacji. Formami tymi są: walka o przewagę w dowodzeniu, walka bazująca na wiedzy, walka elektroniczna, walka psychologiczna, walka hackerska, ekonomiczna walka informacyjna i cyberwalka.
P. Sienkiewicz, *Współczesne koncepcje walki informacyjnej*, [w:] R.Szpyra, *Informacyny wymiar współczes n-ych działań powietrznych. Materiały z sympozjum naukowego*, Warszawa 2002.	Walką informacyjną (*information warfare, infowar*) nazywamy całokształt działań ofensywnych i defensywnych koniecznych do uzyskania przewagi informacyjnej nad przeciwnikiem i osiągnięcia zamierzonych celów militarnych (politycznych). Istotą tak rozumianej walki informacyjnej jest: (1) zniszczenie (lub degradacja wartości) zasobów informacyjnych przeciwnika oraz stosowanych przez niego systemów informacyjnych; (2) zapewnienie bezpieczeństwa własnych zasobów informacyjnych i wykorzystywanych systemów informacyjnych.

R. Szpyra, *Operacje informacyjne państwa w działaniach sił powietrznych. Rozprawa habilitacyjna*, Warszawa 2002.	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. Militarna walka informacyjna to zorganizowana w formę przemocy militarna aktywność zewnętrzna państwa prowadząca do osiągnięcia określonych celów politycznych, skierowana na niszczenie lub modyfikowanie systemów informacyjnego komunikowania przeciwnika lub przepływającej przez nie informacji oraz aktywność zapewniająca ochronę własnych systemów informacyjnego komunikowania i przesyłanej przez nie informacji przed podobnym działaniem przeciwnika.

Tabela 3.2

Definicje operacji informacyjnych - przegląd

Operacje informacyjne	
Joint Doctrine for Information Operations. Joint Pub 3-13, Joint Chiefs of Staff, Washington 1998	Operacje informacyjne to akcje podjęte dla wpływania na informację i systemy informacyjne przeciwnika przy jednoczesnej ochronie własnej informacji i systemów informacyjnych.
FM 100-6 Information Operations, Headquarters, Department of the Army, 1996, s.2-3.	Operacje informacyjne to ciągłe działania militarne w militarnym środowisku informacyjnym, które uaktywniają, wzmacniają i chronią zdolności własnych sił do gromadzenia, przetwarzania i działania na informacji dla osiągnięcia (korzyści) przewagi w pełnym spektrum działań militarnych. Operacje informacyjne zawierają interakcje z globalnym środowiskiem informacyjnym i eksploatację informacji przeciwnika lub uniemożliwianie mu dostępu do informacji i zdolności do podejmowania decyzji.
AFDD 2-5 Information Operations, USAF.	Operacje informacyjne obejmują przedsięwzięcia podejmowane dla zdobycia, wykorzystania, obrony lub ataku na informację lub systemy informacyjne i łączą zarówno aspekt informacji w walce, jak i walkę informacyjną. Operacje te prowadzone są przez wszystkie fazy kampanii i w całym zakresie działań militarnych.
MC 422 – NATO Information Operations Policy.	Operacje informacyjne są zdefiniowane jako „przedsięwzięcia podjęte w celu wywarcia wpływu na decydentów w ramach wsparcia

	politycznych i militarnych celów poprzez oddziaływanie na informację innych, ich procesy informacyjne oraz systemy dowodzenia, kontroli, łączności i informacyjne, przy wykorzystaniu i ochronie własnej informacji i systemów informacyjnych".
Allied Joint Doctrine AJP-01, NATO, Wydanie 1999.	Operacje informacyjne to działania podjęte dla wpływania na decydentów w ramach wspierania procesu osiągania celów politycznych i militarnych, mające charakter wpływania na informację, procesy informacyjne, systemy dowodzenia i kontroli oraz systemy komunikacyjno-informacyjne (CIS) przy eksploatowaniu i ochronie własnej informacji i systemów informacyjnych.
R. Szpyra, *Operacje informacyjne państwa w działaniach sił powietrznych. Rozprawa habilitacyjna*, Warszawa 2002.	Operacje informacyjne państwa rozumiane będą jako zorganizowana aktywność państwa prowadząca do osiągnięcia określonych celów politycznych, skierowana na zewnętrzne i wewnętrzne systemy informacyjnego komunikowania lub przepływającą przez nie informację. Militarne operacje informacyjne to zorganizowana aktywność militarna państwa prowadząca do osiągnięcia określonych celów politycznych, skierowana na zewnętrzne i wewnętrzne systemy informacyjnego komunikowania lub przepływającą przez nie informację.

Piotr Sienkiewicz jest zaś przekonany, że „Nowoczesne koncepcje walki zbrojnej bazują na tworzeniu wieloczynnikowej przewagi militarnej (*multifactor mulitary superiority*) w oparciu o kontrolowaną, rozstrzygającą przewagę informacyjną (*information superiority)* i technologiczną (technological *superiority*). Aczkolwiek potencjał informacyjny stanowił zawsze istotny czynnik potencjału bojowego, to w rozważaniach dotyczących sposobów tworzenia przewagi na polu walki był on raczej pomijany. W szczególności w matematycznych modelach walki (typu modele Lanchestera) uwaga koncentrowała się na *stosunku sił* uwzględniającym przede wszystkim *potencjały rażenia* stron walczących.

Potencjał informacyjny jako czynnik potencjału militarnego tworzą zasoby informacyjne systemu obronnego państwa oraz systemy informacyjne kształtujące infrastrukturę informacyjną państwa. Oznacza to, że potencjał informacyjny to wszelkie zasoby informacyjne (dane, informacje, wiedza), które tworzą infosferę określonego systemu działania (organizacji, instytucji). Ale także systemy

informacyjne (informatyczne, telekomunikacyjne) niezbędne do efektywnego prowadzenia określonych, zamierzonych działań. [...]

Konsekwencją analizy systemowej procesów informacyjnych na współczesnym polu walki jest wprowadzenie **stosunku wiedzy** (*relative knowledge)* stron walczących, jako czynnika decydującego o rezultatach walki"[77].

W stosunkowo wczesnej fazie badań nad walką informacyjną uświadomiono sobie jej rozległy i wszechogarniający charakter. Dostrzeżono, iż dotyczy ona sfery pozamilitarnej w jeszcze szerszym zakresie niż militarnej. Również w układzie podmiotowym wyodrębnić można wiele obszarów. Winn Schwartau[78] wyróżnił np. indywidualną, zespołową (korporacyjną) i globalną walkę informacyjną.

Wnioski

Istnieje powszechna zgodność wśród badaczy, iż rola sfery informacyjnej w jakichkolwiek działaniach w warunkach wyłaniającej się cywilizacji informacyjnej staje się pierwszoplanowa.

Rola ta dla komponentu militarnego państwa jest jeżeli nie większa, to przynajmniej taka sama, jak dla komponentów niemilitarnych.

Zarówno refleksja teoretyczna, jak i praktyka dostrzegają dwa obszary zastosowania informacji w walce: tradycyjny - jako zasilanie informacyjne i nowy - jako wyłaniający się rodzaj broni.

Problematyka walki oraz innych działań w sferze informacyjnej staje się przedmiotem powszechnego zainteresowania badaczy.

Mimo mnogości prób definiowania nie ustalił się powszechnie akceptowany aparat pojęciowy. Poszczególne koncepcje adekwatne są dla określonych *„szkół myślenia".*

Bibliografia:

1. AJP-01(B), Glossary 3, a także w AAP - 6.
2. Allied Joint Doctrine AJP-01. NATO. Wydanie 1999.
3. Amerykańskie doktryny militarne.: http://www.dtic.mil/doctrine/.

---

[77] *Tamże.*
[78] *W. Schwartau, dz. cyt., s. 33–35.*

4. Arguilla J., Ronfeldt D.: In Athena's Camp: Preparing for Conflict in the Information Age, Santa Monica 1997.
5. Aron R.: Pokój i wojna między narodami, Warszawa 1984.
6. Balcerowicz B.: *Sojusz a obrona narodowa*, Warszawa 1999.
7. Biological Warfare and Chemical Gases.
8. Bobrow D. B., Haliżak E., Zięba R.: Bezpieczeństwo narodowe i międzynarodowe u schyłku XX wieku, Warszawa 1997.
9. Bosh J. M. J., Luiijf H. A. M., Mollema A. R.: NL Arms. Netherlands Annual Review of Military Studies 1999, Information Operations, Breda 1999.
10. Brillouin L.: Science and Information Theory. Wyd. pol. Nauka a teoria informacji, Warszawa 1969.
11. Campen A., Dearth D. H., Goodden R. T.: Cyberwar: Security, Strategy, and Conflct in the Information Age, Fairfax 1996.
12. Ciborowski L.: Walka informacyjna, Toruń 1999.
13. Denning D. E.: Information Warfare and Security 1998.
14. DOD Closes Off GPS Segment. www.infowar.com/mil_c4i/00/mil_c4i_112400a_j.shtml;
15. Feeney M., Grieves M.: *The Value and Impact of Information*, London 1994.
16. FM 100-6 Information Operations, Washington 1996; Information Operations. AFDD 2-5, Maxwell AFB 1998.
17. R. Forno, R. Baklarz, The Art Of Information Warfare: Insight into the Knowledge Warrior Philosophy 1999.
18. Fredericks B. E.: *Information Warfare at the Crossroads*, Joint Force Quarterly, Summer 1997.
19. Frezza B.: The Militarization of Cyberspace.
20. Goban-Klas T., Sienkiewicz P.: Społeczeństwo informacyjne – szanse, zagrożenia, wyzwania, Kraków1999.
21. Information Warfare: Cyberterrorism: Protecting Your Personal Security in the Electronic Age, New York 1994. Drugie wydanie rozszerzone 1996.
22. JP 3-13 Joint Doctrine for Information Operations, Washington 1998.
23. Joint Economic Committee Hearing. http://techweb.cmp.com/nc/frezza/frezza.html;
24. Khalilzad Z. M., White J. P.: Strategic Appraisal. The Changing Role of Information in Warfare, Santa Monica 1999.

25. Koch E. R., Sperber J.: Infomafia, szpiegostwo komputerowe handel informacją tajne służby, Gdynia 1999.
26. Koziej S.: Ciągłość oddziaływania na przeciwnika podczas natarcia, Myśl Wojskowa 1978, nr 5.
27. Koziej S.: Współczesna myśl taktyczna, Myśl Wojskowa 1987, nr 10, Teoria sztuki wojennej, Warszawa 1993.
28. Libicki M. C.: What Is Information Warfare? Washington 1995, Defending Cyberspace and Other Metaphors, Washington 1997.
29. Mazur M.: Jakościowa teoria informacji, Warszawa 1970.
30. Molander R. C.: Riddile A. S., Wilson P. A.: Strategic Information Warfare. A New Face of War, Santa Monica 1996.
31. Molander R. C., Wilson P. A., Mussington D. A., Mesic R. F.: Strategic Information Warfare Rising, Santa Monica 1998.
32. Nowacki G.: Walka informacyjna - próba kategoryzacji. Rozprawa doktorska, Warszawa 1999. Współczesne poglądy na prowadzenie walki informacyjnej. Studium teoretyczne, Warszawa 2001.
33. Podręczniki akademickie AON: Działania taktyczne wojsk lądowych, Warszawa 1992, Działania operacyjne wojsk lądowych, Warszawa 1992.
34. Pub 3-13 Joint Doctrine for Information Operations, Washington 1998.
35. Radio Frequency Weapons and Proliferation: Potential Impact on the Economy. Wednesday, February 25, 1998.
36. Schwartau W.: Information Warfare. Cyberterrorism: Protecting Your Personal Security in the Electronic Age, New York 1996.
37. Seffers G. I.: Joint Chiefs Inaugurate Information Combat Era, Defense News 1998, November.
38. Sienkiewicz P.: Inżynieria systemów, Warszawa1983.
39. Sienkiewicz P.: Wojna informatyczna, Computerworld 1997, nr 31(1997);
40. Sienkiewicz P.: Współczesne koncepcje walki informacyjnej, [w:] R. Szpyra, Informacyjny wymiar współczesnych działań powietrznych. Materiały z sympozjum naukowego, Warszawa 2002.
41. Stark R.: Future Warfare: Information Superiority through Info War,
42. Stein G.: Information War – Cyberwar – Netwar, [w:] Battlefield of the Future. 21st Century Warfare Issues. Air University Maxwel AFB 1995; oraz Information Warfare, [w:] Campen A. D., Dearth D. H., Goodden R. T.: Cyberwar: Security,

Strategy, and Conflct in the Information Age, Fairfax 1996; i Information Warfare. Learning With Sun Tzu, [w:] Bosh J. M. J., Luiijf H. A. M., Mollema A. R.: NL Arms. Netherlands Annual Review of Military Studies 1999. Information Operations, Breda 1999.

43. Świniarski J.: O naturze bezpieczeństwa. Prolegomena do zagadnień ogólnych, Warszawa-Pruszków, 1997.
44. Szpyra R: Walka informacyjna w przyszłych działaniach sił powietrznych. Opracowanie pod kryptonimem CYBERAWIATOR, Warszawa 2000.
45. Szpyra R.: Operacje informacyjne państwa w działaniach sił powietrznych. Rozprawa habilitacyjna, Warszawa 2002.
46. The Global Course of the Information Revolution: Technological Trends: Proceedings of an International Conference. http://www.house.gov/iec/hearings/02-25-8h.htm;
47. UK: cyber-attacks. Taiwan To Launch "Cyber Warfare" Unit.
48. Qiao Liang and Wang Xiangsu, Unrestricted Warfare: Assumptions on War and Tactics in the Age of Globalization, Beijing 1999, tłumaczenie na język angielski dokonane przez: US CIA's Foreign Broadcast Information Service udostępnione w 2000 r. pod adresami: http://www.terrorism.com/documents/unrestricted.pdf lub http://cryptome.org/cuw.zip
49. Vickery B. i A.: Information Science in theory and practice, London, 1987.
50. Waltz E.: Information Warfare Principles and Operations, Boston, 1998.
51. Wojtaszczyk K. A.: Kompendium wiedzy o państwie współczesnym, W-wa 1998.
52. Zacher L. W.: Społeczeństwo informacyjne w perspektywie człowieka, techniki, gospodarki, Warszawa 1999.
53. Zięba R.: Instytucjonalizacja bezpieczeństwa europejskiego, koncepcje – struktury – funkcjonowanie, Warszawa 1999.

1.4. SPECYFIKACJA TYPÓW I OBIEKTÓW ZAGROŻEŃ INFORMACYJNYCH

„Życie i działanie we współczesnym świecie wymaga korzystania z wielu informacji"[1]. Stwierdzenie to wydaje się bardzo dobrze oddawać istotę znaczenia informacji w naszym życiu. Trudno obecnie nie doceniać ogromu wagi gromadzenia, posiadania, przetwarzania i wykorzystywania wszelkich informacji, zarówno o otaczającym nas świecie jak i o nas samych. Żyjemy w epoce społeczeństwa informacyjnego i to determinuje konieczność dobrego wykorzystania zdobywanych informacji. Informacje stały się najlepszym, najbardziej poszukiwanym i najcenniejszym towarem. Nic, co dotyczy człowieka i jego życia nie może odbywać się bez udziału informacji. Jest ona potrzebna wszędzie - tam gdzie chodzi o ratowanie życia ludzkiego, zgłębianie tajników wiedzy, odkrywanie wynalazków, zdobywanie pieniędzy czy chociażby komunikowanie się. Informacja jest więc ogromnym kapitałem – zasobem, którego obecnie nie można pominąć.

Trudno więc wyobrazić sobie dzisiejszą organizację bez informacji i to bez informacji, które są w organizacji bezpieczne. Skoro informacja jest tak dużym kapitałem nie sposób pominąć aspektu jej bezpieczeństwa.

W XXI wieku informacje praktycznie nie są już gromadzone, przechowywane, przetwarzane jako dokumenty papierowe, chronione w sejfach, segregowane w plastikowych teczkach, przewożone w pancernych samochodach pod eskortą kilku strażników i rozsyłane do wszystkich pracowników przez kurierów czy pocztą. Nastał wiek komunikacji elektronicznej, kartki zostały zastąpione przez pliki, foldery zamieniły teczki, a pancerne samochody i poczta zostały wyparte przez sieci komputerowe. Nie tylko funkcjonalność starych nośników i kanałów komunikacji została zastąpiona. Przede wszystkim wydatnie wzrosła jakość i szybkość tych działań.

Dla sprawnej, efektywnej i nowoczesnej organizacji proces zarządzania nie może odbywać się bez udziału technik informatycznych, a w szczególności sieci komputerowych. Sieci komputerowe w organizacjach to przede wszystkim współdzielenie informacji posiadanych przez firmę oraz szybka komunikacja pomiędzy pracownikami lub pracownikami a światem. To dwa główne czynniki

[1] *P. Sienkiewicz, T. Goban-Klas: Społeczeństwo informacyjne: szanse zagrożenia, wyzwania, Wydawnictwo Fundacji Postępu Telekomunikacji, Kraków 1999*

konieczne do dobrego zarządzania. Pozostaje jeszcze tylko jedna, kluczowa kwestia – zapewnienie bezpieczeństwa informacji gromadzonych, przechowywanych i przetwarzanych w sieciach komputerowych a wykorzystywanych w procesie zarządzania. Nie ma wątpliwości, że informacje w sieciach komputerowych nie są bezpieczne, istnieje szereg zagrożeń, które wpływają na bezpieczeństwo informacji. Problematyka ta obecnie staje się coraz bardziej popularna, ukazują się liczne publikacje, przeprowadzane są konferencje, odkrywane są coraz to lepsze metody i środki zabezpieczeń, powstają też niestety ciągle nowe i to co raz bardziej wyrafinowane zagrożenia. Dynamiczny rozwój tej tematyki jest tak ogromny, że trudno jest za nim nadążyć.

Dużą wagę w roli informacji dla zarządzających odgrywa łatwość jej powielania i przenoszenia. Wydaje się oczywistym, że dużo łatwiej jest skopiować informacje np. na dyskietce czy przesłać ją za pomocą poczty elektronicznej w przeciwieństwie do przeniesienia infrastruktury takiej jak maszyny czy budynki.

Obecnie stosunkowo nietrudno jest pozyskiwać wszelkie pożądane informacje. Taka sytuacja może jednak prowadzić do niebezpiecznego zjawiska, jakim jest zbędny nadmiar informacji. Często zdarza się, że redundancja informacji może powodować przytłaczanie pracowników, co może prowadzić do innych od zamierzonych efektów. Aby temu zapobiec we współczesnych przedsiębiorstwach tworzy się systemy informacyjne, których celem jest takie wykorzystywanie informacji, które będzie jak najbardziej pożądane z punktu widzenia potencjalnych odbiorców tej informacji.

Techniki informatyczne umożliwiają redukcję zużycia materiałów i energii, przyśpieszają i czynią efektywniejszymi metody projektowania i eksploatacji. Nowoczesne metody transmisyjne i systemy sieciowe umożliwiają nie tylko szybką wymianę informacji, ale także efektywne jej poszukiwanie i dystrybucję[2]. Szybka globalna, multimedialna wymiana informacji pozwala w znaczący sposób ograniczyć wszelkie koszty związane z działalnością organizacji. Nowoczesne systemy teleinformatyczne, a w szczególności wszelkiego rodzaju sieci umożliwiły i wydatnie poszerzyły zakres możliwości komunikowania się ludzi w skali globalnej, przy jednoczesnym wzroście szybkości tego komunikowania się. Pozwoliły także na znaczące zwiększanie się ilości gromadzonej i przetwarzanej informacji, co ma

[2] *K. Wydro: Problemy ochrony informacji, Transformacje – Pismo interdyscyplinarne, Maj 2001*

niewątpliwy wpływ na rozwój wszelkich sfer życia, w szczególności zaś na funkcjonowanie organizacji.

Systemy informatyczne integrują kluczowe procesy zachodzące w firmie. Za ich pomocą można śledzić dane finansowe, informacje związane z zarządzaniem kadrą pracowników, zestawienia danych związanych z procesami produkcyjnymi i wiele innych.

Systemy informacyjne oparte są przede wszystkim na sieciach komputerowych. Technologie pracy sieciowej umożliwiają użytkownikom wspólne korzystanie z informacji i innych zasobów przedsiębiorstwa. Dzięki temu uzyskiwanie informacji staje się łatwiejsze i bardziej efektywne. Wielki wpływ na to ma również niewątpliwie współczesny Internet i jego zasoby. Technologia internetowa oferuje organizacjom przeróżne informacje o otoczeniu gospodarczym, które niezbędne są do prawidłowego funkcjonowania.

Łatwość komunikacji i realizacji różnych usług drogą teleinformatyczną niesie jednak ze sobą oprócz walorów – również zagrożenia i stwarza możliwości jej nadużywania.

Mając na uwadze te zagrożenia oraz znaczenie informacji we współczesnym świecie jawi się olbrzymi problem jakim jest bezpieczeństwo i ochrona tych informacji. Dotyczy on szczególnie sieci komputerowych, w których te dane są przechowywane. Niestety jakiekolwiek gromadzenie danych jest zawsze narażone na nieuprawnione wykorzystanie.

Nieuprawnione użycie może wiązać się z różnymi działaniami, od ograniczenia prywatności po przestępstwa.

Istnieje więc pilna potrzeba na opracowywanie środków ochrony stosowanych w dzisiejszych narzędziach i sposobach gromadzenia, przetwarzania i przechowywania informacji.

1.4.1. Internet – atrakcja informatyczna czy zagrożenie

Przedsiębiorstwo lub też prywatny użytkownik powinien zdawać sobie sprawę z niewyobrażalnej liczby zagrożeń, na jakie zostaje narażony. Wraz ze wzrostem ilości komputerów podłączonych do globalnej sieci nasila się fala przestępstw elektronicznych. Pośród użytkowników Internetu znajdują się osoby wykorzystujące możliwości sieci komputerowej do działań przestępczych. Internet pomimo swojej

bezsprzecznej „atrakcyjności informacyjnej" oraz bycia ważną częścią życia wielu osób i instytucji posiada pewne luki. Do jego słabych stron z pewnością należą:

- brak centralnej kontroli;
- wady protokołu TCP/IP i protokołów pokrewnych;
- brak jednolitej polityki bezpieczeństwa;
- anonimowość użytkowników.

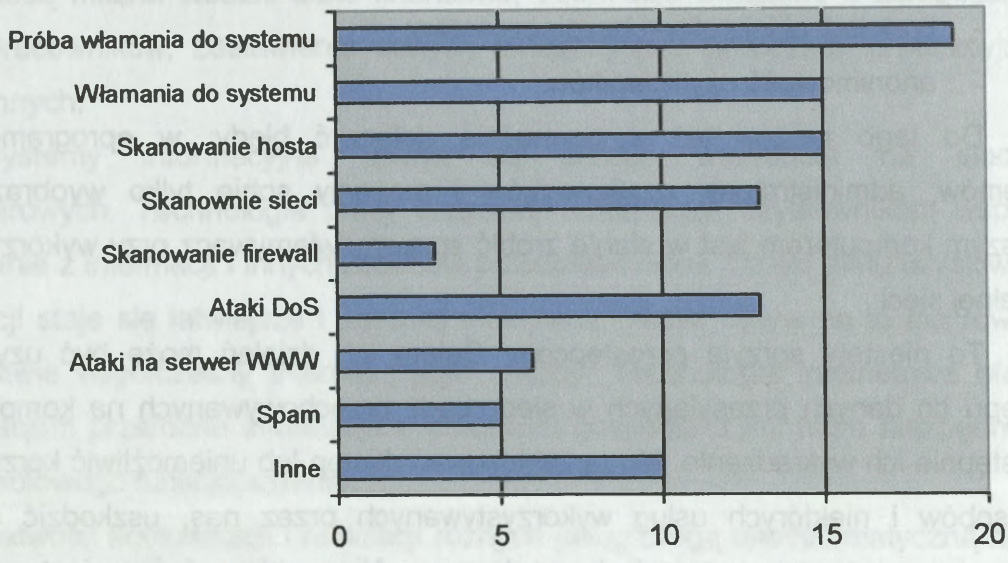
Do tego można też z pewnością dołączyć błędy: w oprogramowaniu systemów, administratora, użytkowników i możemy sobie tylko wyobrazić, co z naszym komputerem jest w stanie zrobić sprawny włamywacz przy wykorzystaniu globalnej sieci.

To niestety sprzyja przestępcom. Celem ich działań może być uzyskanie dostępu do danych przesyłanych w sieci, bądź przechowywanych na komputerze, a następnie ich wykradzenie. Mogą zablokować dostęp lub uniemożliwić korzystanie z zasobów i niektórych usług wykorzystywanych przez nas, uszkodzić system operacyjny, programy, sprzęt komputerowy. Niezwykle groźne jest również fałszerstwo, zniekształcania, modyfikowanie i kasowanie danych. Naraża to organizacje oraz przedsiębiorstwa na ogromne koszty finansowe. Wyobraźmy sobie, że np. ktoś włamuje się do systemu komputerowego naszej firmy i wykrada ważne, poufne informacje (o strategii, o nowych technologiach, dane klientów, itp.), niszczy nasz system informatyczny oraz jego zasoby. Prowadzi to do wielkich, niejednokrotnie nieodwracalnych strat. Szkody mogą wywołać ogólny kryzys jak również upadłość firmy. Dla głębszego zrozumienia istoty problemu warto jest zwrócić uwagę na zaistniałe zagrożenia. Według CERT[3] Polska w roku 2000 doszło do 126 przypadków naruszenia bezpieczeństwa teleinformatycznego (wykres 4.1.). Zaatakowano łącznie 292 komputery.

[3] *Computer Emergency Response Team – jest to zespół stworzony do reagowania na zdarzenia naruszenia bezpieczeństwa w sieci Internet. Bada i przygotowuje również statystyki dotyczące polskich zasobów sieciowych.*

Wykres 4.1.

Typy odnotowanych ataków w roku 2000 (%)

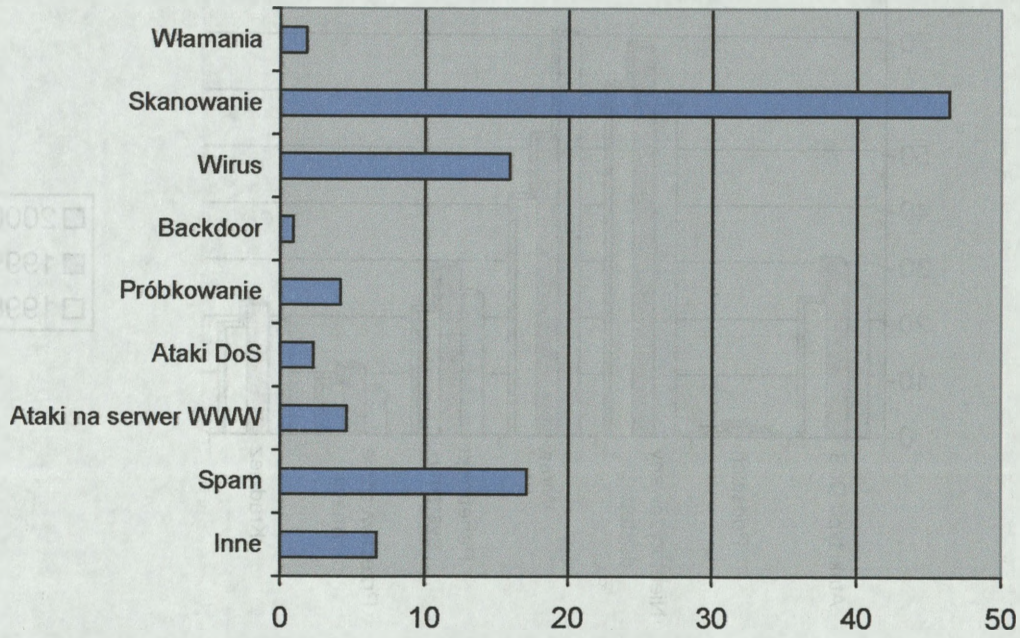


Źródło: Raport 2000 CERT POLSKA Przypadki naruszające bezpieczeństwo teleinformatyczne

Aż 70% przypadków było związane z włamaniami do systemu. Rok 2001 był znacznie gorszy (wykres 4.2.) – odnotowano 741 przypadków naruszenia bezpieczeństwa (większość z tych ataków była przeprowadzona na więcej niż jeden komputer). Dane te jednak nie są w pełni kompletne. Niestety występuje duża niechęć do zgłaszania tego typu incydentów, więc ich liczba w polskich zasobach Internetu jest znacznie większa od ujawnionej.

Wykres 4.2.

Typy odnotowanych ataków w roku 2001 (%)



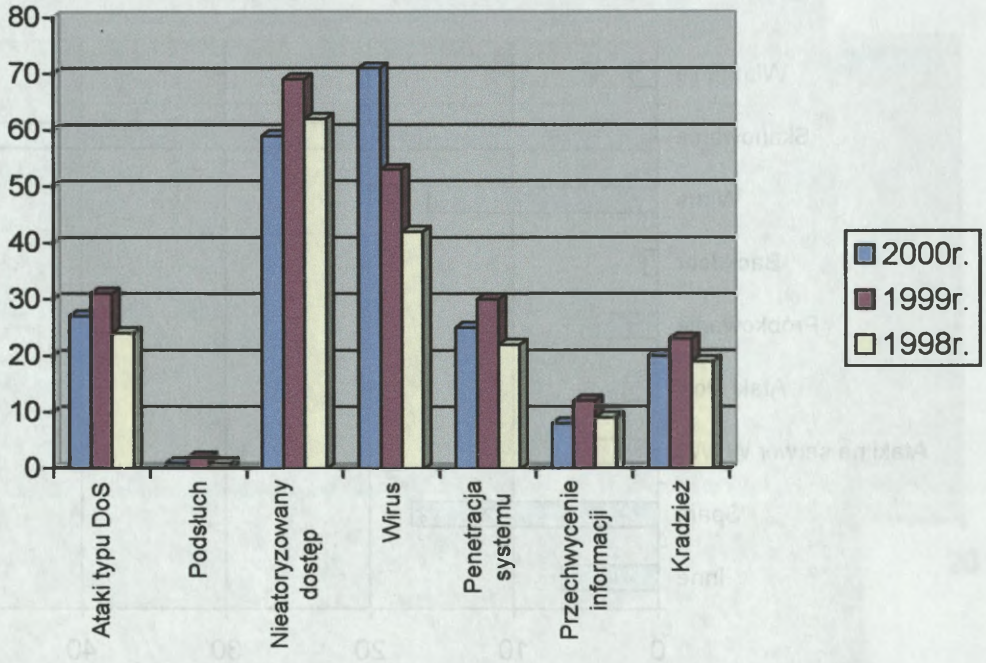
Źródło: Raport 2001 CERT POLSKA Przypadki naruszające bezpieczeństwo teleinformatyczne

Ciekawe statystyki przedstawia także wspólny raport FBI i CSI[4] o nazwie Computer Crime and Security Survey. Zawiera on dane dotyczące typów ataków dokonanych w USA (wykres 4.3.) oraz ich źródła (wykres 4.4.) na przekroju lat 1997-2000. W roku 2001 ujawniono 528 zgłoszonych (w rzeczywistości było znacznie więcej) przypadków naruszenia bezpieczeństwa. Zaledwie 186 zgłoszeń zawierało informacje na temat szacowanych strat finansowych poniesionych w wyniku ataków. Była to kwota około 370 mln USD.

[4] *Computer Security Institute – jest to amerykański Instytut Bezpieczeństwa Komputerowego zajmujący się opracowywaniem i realizowaniem programu bezpieczeństwa, który ma na celu ochronę organizacji przed atakami teleinformatycznymi i ich skutkami.*

Wykres 4.3.

Typy ataków w latach 1997-2000



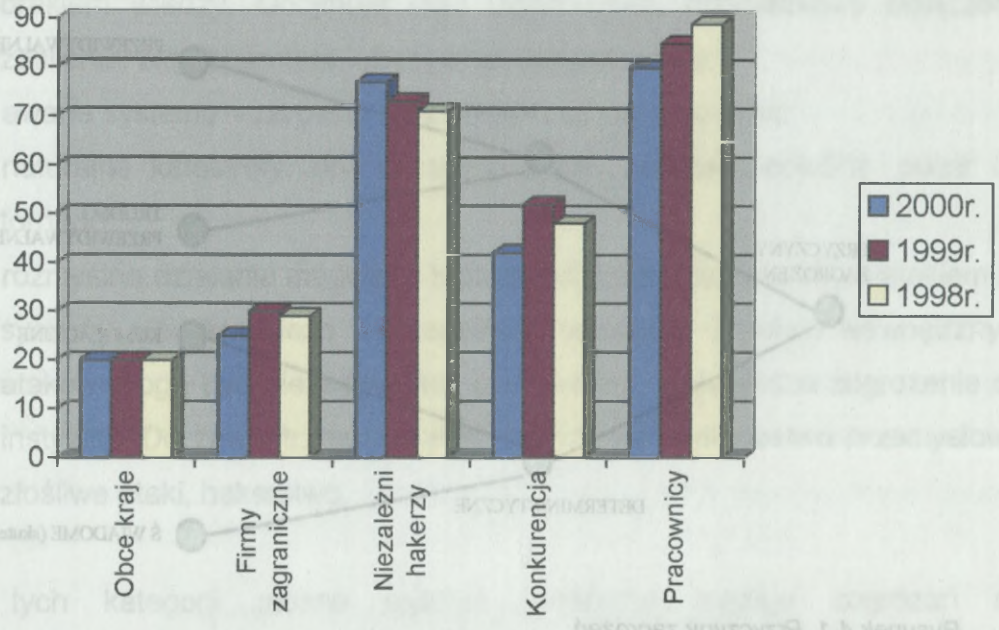
Źródło: www.pckurier.pl/itforum/secure/secure2000/15.ppt

Większość z poniesionych strat spowodowana była w wyniku kradzieży informacji (ponad 40 %), oszustw finansowych (25%) oraz działalności wirusów komputerowych (12%).

W 2001 roku w Stanach Zjednoczonych najczęstszym typem potwierdzonych ataków były wirusy komputerowe i nieautoryzowany dostęp do zasobów. Choć odnotowano również takie przestępstwa jak sabotaż i oszustwa finansowe. Patrząc wstecz, aż do ostatnich lat panowało przekonanie, że 80% zagrożeń bezpieczeństwa teleinformatycznego pochodzi z wewnątrz przedsiębiorstwa, zaś pozostałe 20% z zewnątrz. Jednak sytuacja diametralnie się odwróciła. Obecnie uznaje się, że ponad 70 procent to zagrożenia wynikające z dostępu do Internetu, a najgroźniejszym ich źródłem są hakerzy komputerowi. Coraz częściej również dochodzi do ataków ze strony nieuczciwej konkurencji oraz szpiegostwa na rzecz innych państw. Oczywiście znacząca większość takich przypadków nie zostaje nawet podana opinii publicznej.

Wykres 4.4.

Źródła ataków w latach 1997-2000



Źródło: www.pckurier.pl/itforum/secure/secure2000/15.ppt

1.4.2. Klasyfikacja zagrożeń

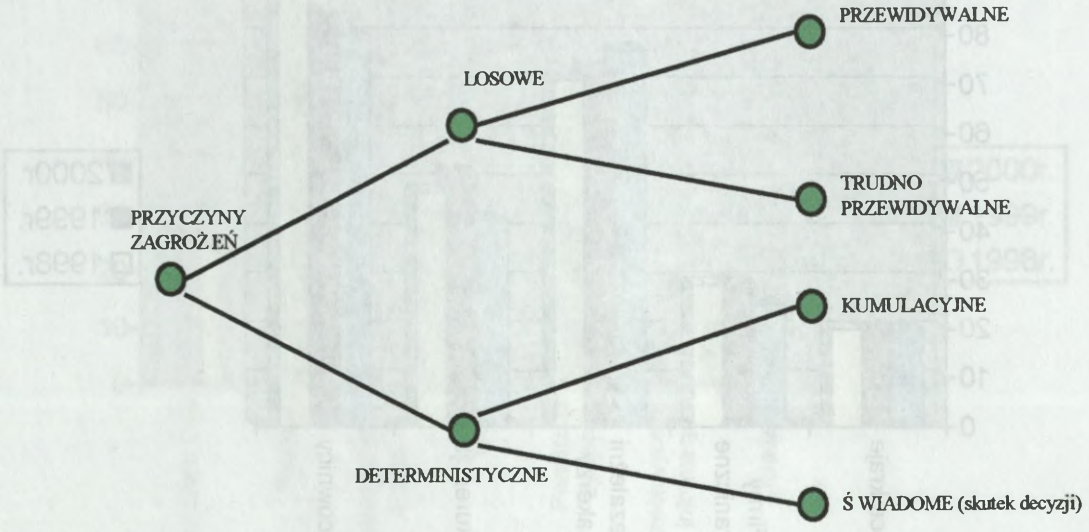
Identyfikacja zagrożeń informacyjnych wymaga oprócz wyodrębnienia konkretnych niebezpieczeństw, również analizy przyczyn i źródeł ich powstawania.

Najprostszą klasyfikacją zagrożeń ze względu na źródła niebezpieczeństw jest podział na:

- zagrożenia wewnętrzne – inicjowane wewnątrz organizacji;
- zagrożenia zewnętrzne – powstające poza organizacją.

Podział ten jest jednak stosunkowo ogólny i może on być jedynie traktowany jako pomocniczy dla rozważań bardziej szczegółowych. Podział ten może być przydatny w szczególności przy konstruowaniu organizacyjnej polityki bezpieczeństwa, gdzie rozróżnienie miejsca powstawania zagrożenia ma przełożenie na wybierane metody zabezpieczeń.

Kolejnym krokiem w identyfikacji zagrożeń dla informacji może być spojrzenie na możliwe przyczyny ich powstawania. Jednym z wykładników dla takiej analizy może być podział przedstawiony na rysunku 4.1.



Rysunek 4.1. Przyczyny zagrożeń
Źródło: P. Sienkiewicz, P. Górny: Analiza systemowa sytuacji kryzysowych, Zeszyty Naukowe AON Nr 4, Warszawa 2001

Rysunek ten przedstawia podział zagrożeń ze względu na rozpoznanie przyczyn powstawania wszelkich niebezpieczeństw grożących informacjom w organizacji. Dla przykładu jako losowe, przewidywalne zagrożenie można uznać skasowanie pliku przez nieostrożnego pracownika. Za trudno przewidywalne zagrożenie można uznać np. utratę danych na skutek wybuch jądrowego – trudno przypuszczać, że każda organizacja bierze go pod uwagę i chroni przed nim swoje dane. Jako zagrożenie kumulacyjne można uznać przykładowo nieodpowiednią procedurę niszczenia przechowywanych dokumentów – kolejne zaszyfrowane wydruki wyrzucane na śmietnik mogą posłużyć do przeprowadzenia na ich podstawie kryptoanalizy i złamania szyfru stosowanego do zabezpieczania poufnych dokumentów w sieci. Wybór niewystarczająco skutecznego algorytmu szyfrowania, a co za tym idzie zagrożenie dla tajności danych może być skutkiem błędnej decyzji organizacyjnej.

Taka analiza, w połączeniu z identyfikacją źródeł powstawania możliwych zagrożeń pozwala na wyodrębnienie kategorii podstawowych zagrożeń dla bezpieczeństwa informacji. Należą do nich[5]:

- błędy ludzkie – wypadki spowodowane niedbalstwem, nieuwagą lub brakiem wiedzy. Obejmują błąd użytkownika, przypadkowe odłączenie zasilania, błąd operatora lub niewłaściwe procedury;
- awarie systemu – zarówno sprzętu, jak i oprogramowania;
- naturalne katastrofy, np. trzęsienie ziemi, huragan, powódź, pożar lub tornado;
- rozmyślne działania mogą być ludzkim lub zautomatyzowanym atakiem na systemy albo kradzieżą wyposażenia i zasobów. Źródłem wewnętrznych ataków mogą być niezadowoleni pracownicy - największe zagrożenie dla instytucji. Do zewnętrznych ataków zalicza się szpiegostwo przemysłowe, złośliwe ataki, hakerstwo.

Z tych kategorii można wyłonić konkretne rodzaje zagrożeń dla bezpieczeństwa informacji w sieciach komputerowych. Należą do nich:

- utrata (zniszczenie, skasowanie) danych (informacji);
- utrata poufności danych;
- utrata integralności danych;
- utrata dostępu do systemu przechowującego lub przetwarzającego informacje;
- utrata dostępu do usług oferowanych przez system;
- włamanie do systemu – działanie nieuprawnionych osób w systemie;
- utrata autentyczności informacji;
- zniszczenie lub modyfikacja oprogramowania i sprzętu;
- opóźnienia w transmisji krytycznych czasowo danych;
- zaprzeczenia nadania określonych wiadomości.

Zagrożenia dla informacji w systemach informacyjnych organizacji przybierają w ostatnich latach coraz bardziej wymierne znaczenie. Przekładają się one na

[5] *D. L. Pipkin,* Bezpieczeństwo informacji, *WNT, Warszawa, 2002, s.26.*

bardzo duże środki finansowe. Pochłaniają zarówno straty związane z wystąpieniem określonych niebezpieczeństw jak i zastosowanie nowoczesnych środków ochrony.

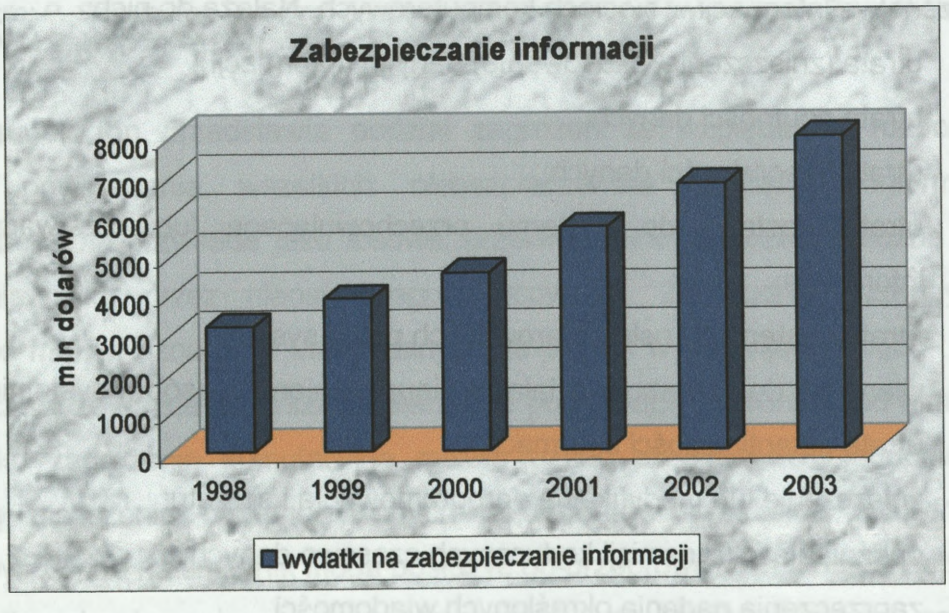
Największe straty w ostatnich latach spowodowane były działaniem przestępczym Kevina Mitnicka. Spowodował on straty dla firmy NEC rzędu 2 mln dolarów oraz pozbawił Nokię przychodu o wartości 135 mln dolarów z powodu opóźnień w dostawach. Całość strat jakie spowodował Mitnick szacuje się na ponad 290 mln dolarów.

Działanie wirusa Melisa – makrowirusa szablonów w programie Word – spowodowało straty około 80 mln dolarów. Ataki Denial of service na całym świecie spowodowały straty rzędu dziesiątek milionów dolarów[6].

Biorąc pod uwagę te ogromne sumy strat, które są konsekwencjami wystąpienia określonych zagrożeń nie dziwi fakt, że dzisiejsze organizacje przeznaczają olbrzymie pieniądze na zabezpieczanie swoich systemów i sieci komputerowych (wykres 4.5).

Wykres 4.5

Wydatki na zabezpieczanie informacji



Źródło: A. Meller, Gry wojenne, CHIP Marzec 2002

Jak widać na tym rysunku wydatki na bezpieczeństwo danych stale wzrastają i szacuje się, że w 2003 roku sięgną ponad 8 miliardów dolarów. Liczby te

[6] *A. Grabowski: Technologia WebQoS, Bezpieczne systemy teleinformatyczne, Warszawa 2000*

potwierdzają tezę, że wartość informacji w obecnych czasach jest przeogromna i nie pozostawiają wątpliwości, że informacje te trzeba chronić.

1.4.3. Zagrożenia informacyjne związane z przestępczością komputerową

Przestępczość komputerowa to zjawisko kryminologiczne obejmujące wszelkie zachowania przestępcze związane z funkcjonowaniem elektronicznego przetwarzania informacji, godzące bezpośrednio w przetwarzaną informację, jej nośniki i obieg w systemie komputerowym, a także w sam sprzęt komputerowy oraz prawa do programu komputerowego[7].

Mogą to być zarówno czyny popełniane przeciwko systemowi komputerowemu (komputer jako cel), jak i popełniane przy jego użyciu (komputer jako narzędzie).

Przestępstwa komputerowe skierowane przeciwko informacjom przechowywanym, przetwarzanym bądź przesyłanym w sieciach komputerowych mogą być realizowane następującymi drogami[8]:

- poprzez fizyczny dostęp do systemu komputerowego;
- poprzez sieć komputerową lub sieć komutacji pakietów – dostęp do zasobów może uzyskać każdy posiadający dostęp do sieci i odpowiednie uprawnienia;
- poprzez połączenie z wykorzystaniem modemu;
- poprzez podłączenie się do linii dzierżawionej;
- poprzez wejście na odpowiednie pasmo częstotliwości w sieciach radiowych;
- poprzez wykorzystanie promieniowania ujawniającego.

Zagrożenia dla informacji powodowane zjawiskiem przestępczości komputerowej można podzielić na dwa rodzaje[9]:

- zagrożenia, które nie powodują informacyjnego bądź materialnego zysku dla osób czyniących szkodę;

[7] *K. Liderman:* Bezpieczeństwo informacji w systemach informatycznych, *WSISIZ, Warszawa 2001*
[8] *Tamże*

- zagrożenia, które przynoszą wymierny zysk osobom czyniącym szkodę.

Pierwsza grupa zagrożeń to te zagrożenia, które charakteryzuje występowanie szkody bez bezpośredniego materialnego lub informacyjnego zysku. Zagrożenia te wiążą się niekiedy z sabotażem, czy umyślnym niewypełnianiem lub umyślnym wypełnianiem w sposób wadliwy nałożonych obowiązków po to, by wywołać dezorganizację, straty lub szkody. Formą dezintegracji lub destrukcji informatycznej mogą być programy złośliwe - wirusy komputerowe, bomby logiczne i konie trojańskie.

Drugą grupę zagrożeń związanych z przestępczością komputerową stanowi infiltracja, czyli działania osób nieupoważnionych mające na celu przenikanie do różnych elementów systemu informatycznego lub sieci telekomunikacyjnej w celu zdobycia informacji za pomocą rozmaitych sposobów i środków. Od sabotażu infiltrację różni dążenie do osiągnięcia przez sprawcę konkretnego zysku z tytułu dostępu do określonych informacji. Wyróżnia się przy tym infiltrację czynną i bierną.

Programy złośliwe

Programy złośliwe to programy jak sama nazwa wskazuje uciążliwe i nieprzyjemne. Potrafią naprawdę uprzykrzyć życie wielu osobom. Ich działania wielokrotnie narażały firmy, instytucje, organizacje oraz pojedyncze osoby na znaczne straty i koszty. Zaklasyfikować do nich możemy: wirusy komputerowe, konie trojańskie, robaki, bakterie, a także bomby logiczne. Pomimo, że znalazły się w jednej grupie istnieją między nimi znaczące różnice.

Wirusy komputerowe

Wirusy komputerowe to programy, które przyłączają się do innych programów (nosicieli) i są wraz nimi przenoszone pomiędzy komputerami. Stanowią szczególne zagrożenie w obliczu Internetu, ponieważ są niezwykle niebezpieczne w chwili, gdy znajdują się w środowisku sieciowym. Posiadają możliwość samoreplikacji tzn. potrafią się rozmnażać i rozprzestrzeniać poprzez tworzenie kopii samego siebie. Na początku dochodzi do infekcji – oryginalny kod wirusa zostaje dopisany do zawartości innych plików w systemie. Potem następuje replikacja, gdzie

[9] *P. Sienkiewicz, T. Goban-Klas:* Społeczeństwo informacyjne: szanse zagrożenia, wyzwania, *Wydawnictwo Fundacji Postępu Telekomunikacji, Kraków 1999*

zainfekowany plik zostaje nosicielem i sam może infekować inny plik. Później rozprzestrzenia się po całym dysku twardym i infekuje cały system.

Wirusy dołączają się do programów (pliku) na trzy sposoby:

1. Na końcu – najpierw dochodzi do zakończenia działania programu do którego przyłączony jest wirus, a następnie do replikacji i infekcji innych plików.



Źródło: http://www.oeiizk.edu.pl/informa/jazdzewska/wirusy.html

2. Na początku – wirus najpierw się replikuje, a dopiero potem program jest wykonywany.



Źródło: http://www.oeiizk.edu.pl/informa/jazdzewska/wirusy.html

3. Na początku i na końcu – w tym przypadku wykonywane są czynności z poprzednich dwóch punktów.



Źródło: http://www.oeiizk.edu.pl/informa/jazdzewska/wirusy.html

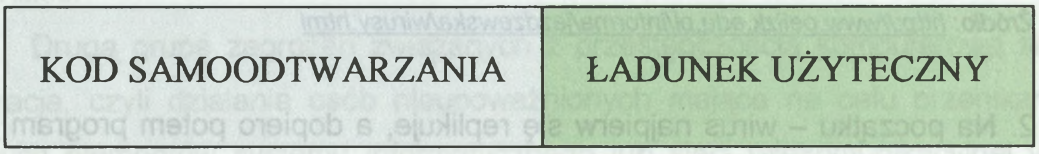
Wirusy komputerowe jako programy charakteryzują się czterema ważnymi cechami:

1) Samoodtwarzaniem – tworzy swoją własną kopię.
2) Ścieżką wykonawczą – musi być wykonywany, ale może to również nastąpić bez udziału użytkownika.
3) Efekty uboczne – wirusy zawierają kod wytwarzający efekty uboczne.

4) Maskowanie – wirus jest najbardziej efektywny, gdy jest nie wykryty. Wirusy są pisane w taki sposób, aby fakt ich wykonywania był niejawny i następował bez świadomości użytkownika.

W strukturze wirusa (rysunek 4.2.) można wyróżnić dwa elementy:

- kod samoodtwarzania – umożliwiający samoreplikacje,
- ładunek użyteczny – powodujący zjawiska uboczne prowadzące do uszkodzenia systemu.



Rysunek 4.2. Struktura budowy wirusa
Źródło: J. Hruska, Wirusy komputerowe i ochrona antywirusowa, s. 38.

Za pierwszą formę wirusa historycy uznają modyfikację systemu operacyjnego komputera Apple powstałą w 1981 roku. Program ten działał w dyskowym systemie operacyjnym i powielał się tylko przy kopiowaniu pirackich wersji gier, uniemożliwiając granie. Pojęcie „wirusa komputerowego" powstało trochę później, bo w roku 1983. Za jego twórcę uważa się dr Freda Cohena. Celem pierwszych autorów wirusów było odwiedzenie użytkowników komputerów od praktyk powszechnego kopiowania oprogramowania. To właśnie było przyczyną szybkiego i gwałtownego rozprzestrzenienia się wirusów, a z nimi coraz większego zagrożenia.

Wirusy głównie atakowały pliki wykonywalne. Gdy taki plik (z doczepionym wirusem) został uruchomiony zaczynał infekować pozostałe pliki prowadząc do sparaliżowania i infekcji całego systemu. W ostatnich latach powstały tysiące wirusów komputerowych. Zmieniła się ich budowa, funkcje oraz rodzaj atakowanych przez nie plików. Obecnie najczęstszymi obiektami infekcji są:

- pliki: .EXE, .COM, . XL?, .DOC, .OVL, .BIN, .SYS, .HTA, .OCX, .SHS, .VBS;
- boot-sector dysku twardego lub dyskietki;
- pliki systemu operacyjnego: command.com, msdos.sys, io.sys;
- tablica partycji dysku twardego FAT;
- biblioteki DLL;
- tablice partycji dysku;

- bazy danych programu ACCESS;
- załączniki do e-maili.

Destrukcyjne działania wirusów mogą polegać na:

- formatowaniu dysków i dyskietek;
- zamazywaniu części lub całości informacji w pliku;
- zapisywaniu w obszarach systemowych nieprawdziwych informacji (np. ukrywanie napędu, zmiana jego gęstości; zwiększenie, zmniejszenie lub ukrycie partycji);
- podawanie fałszywych komunikatów, których celem jest wprowadzenie w błąd lub zakłopotanie użytkownika;
- niszczenie struktury plików, obszarów systemowych i sprzętu.

W przypadku wirusów komputerowych bardzo często proces ich replikacji oraz jego oznaki są niezauważalne, aż do momentu infekcji systemu. Niestety, wtedy jest już za późno. Należy zwracać uwagę na typowe objawy zainfekowania systemu:

- nagły brak miejsca na dysku;
- nagły brak miejsca w pamięci RAM;
- wolne działanie komputera;
- zawieszanie się programów, które wcześniej pracowały poprawnie;
- występowanie dziwnych komunikatów (dotyczących przeróżnych błędów);
- sygnały dźwiękowe – trzaski, melodie, nietypowe dźwięki;
- manipulacje klawiaturą i tekstem – przełączanie klawiszy, umieszczanie nowych znaków w buforze klawiatury;
- spontaniczne przeładowanie systemu;
- niespodziewane pojawianie się różnych obrazów na ekranie;
- gubienie plików lub zmiana ich atrybutów[10].

Wirusy komputerowe zostały sklasyfikowane według wielu kategorii w zależności od stosowanych kryteriów podziału. Podstawowy podział obejmuje:

- *wirusy MBR* (głównego modułu rozruchowego) – atakują przy każdym użyciu dyskietki, ładują się do pamięci, a ich celem jest początkowy sektor

[10] *M. Molski, S. Opala,* Elementarz Bezpieczeństwa Systemów Informatycznych.

dysku. Wirus modyfikuje informację zawarte w głównym module rozruchowym. Jest na przykład w stanie uniemożliwić dostęp do dysku lub przejąć kontrolę nad programami przeznaczonymi do jego unicestwienia;

- *wirusy atakujące pliki* – zarażają określony rodzaj plików, najczęściej pliki wykonywalne (com, exe);
- *wirusy boot sektora* – są podobne w działaniu do wirusów MBR, z tym, że ich celem jest infekcja dyskietki.

Biorąc pod uwagę sposób działania i metody ich tworzenia są to:

- *wirusy utajnione* (ukryte) – Za wszelką cenę ukrywają swoją obecność w systemie. Podczas zagrożenia (to znaczy możliwości ich wykrycia przez program antywirusowy) potrafią w mgnieniu oka naprawić uszkodzone dane i zatuszować swoją obecność. Dzieje się to dzięki temu, że w chwili ataku wirus zachowuje informacje, a dopiero potem je modyfikuje. W każdej chwili jest w stanie je przywołać i udawać, że wszystko jest w porządku. Pośród wirusów utajnionych występuje również ich specjalna odmiana – wirusy binarne (zawierają tylko połowę *„ładunku"* służącego do ataku, po napotkaniu drugiej uaktywniają się);
- *wirusy polimorficzne* – są wyposażone w możliwości modyfikowania własnego kodu i szyfrowania. Wielokrotnie się mutują stając się niezwykle trudnymi do wykrycia. Zmieniają swój rozmiar i strukturę;
- *makrowirusy* – atakują aplikacje biurowe (np. MS Office) umożliwiające tworzenie makr. Wirus uaktywnia się podczas otwarcia zainfekowanego dokumentu, a następnie atakuje inne zbiory. Konsekwencją może być utrata lub zniszczenie treści zaatakowanego dokumentu;
- *wirusy złożone* – posiadają cechy i właściwości kilku wirusów (np. atakującego pliki oraz sektor ładujący). Korzystają z różnych technik, aby opanować system.

Ze względu na cel ataku wyróżnia się także wirusy:

- *dyskowe;*
- *programowe;*
- *aplikacyjne;*
- *rozprzestrzeniające się drogą sieciową.*

Wirusy przez wiele lat ewoluowały, zostały w przeróżne sposoby przekształcane. Obecnie tworzy się ich nowe odmiany, czasem nawet odbiegające od ich ścisłej definicji. Nowe czasy i nowe metody, a w szczególności zasięg globalny, otwierający odległe horyzonty potęgują zagrożenie.

Internet dał wirusom ogromne pole manewru. Wykorzystując to medium rozprzestrzeniają się w zastraszającym tempie i są w stanie zainfekować znacznie więcej komputerów niż w minionych latach. Popularne wirusy pamiętające *„czasy DOS-u"* przenosiły się za sprawą dyskietek. Obecnie są zmorą wielu administratorów sieci jak również zwyczajnych użytkowników. Zaledwie w ciągu paru tygodni mogą doprowadzić do ogólnoświatowej epidemii. Internet to ogromny skarbiec pełny łakomych kąsków w postaci słabo chronionych komputerów. Dlaczego tak się dzieje? Wirus po dostaniu się do sieci wysyła swoje kopie przy pomocy poczty elektronicznej dołączając się do załączników. Używa wymyślnych, bądź zabawnych listów zachęcających do ich odebrania i otwarcia. Dzieje się też to za sprawą samych użytkowników sieci. Wymieniają się bardzo często nieświadomie zainfekowanym oprogramowaniem, przekazują sobie dane lub po prostu ściągają je z nieznanych stron WWW i serwerów FTP. Należy przyznać, iż osoby piszące komputerowe wirusy mają naprawdę wielką wyobraźnie. Kim oni właściwie są i dlaczego to robią? Tu właściwie występuje duża dowolność, lecz przeważającą grupą są ludzie młodzi, zdolni, posiadający szersze pojęcie o informatyce. Robią to z pasji, chęci wykazania się, udowodnienia sobie czegoś, poczucia się silnym, z powodu poglądów, bądź po prostu z czystej złośliwości lub chęci zemsty. Powodów może być nieskończenie wiele tak samo jak i wirusów.

Według danych firmy McAfee w sieci krąży obecnie ponad 50 tysięcy aktywnych wirusów komputerowych. Jednym z bardziej złośliwych wirusów ostatnich lat był Win95.CIH znany także jako Chernobyl. Został ujawniony w 1998 roku na Tajwanie. Po paru miesiącach swojego działania spowodował on globalną epidemię w USA, a po roku uszkodził około miliona komputerów na świecie. Niszczył BIOS, dyski twarde oraz zapisane na nich dane.

Konie trojańskie

Kolejnym z programów złośliwych są konie trojańskie (ang. trojan horses) popularnie zwane także trojanami.

Koń trojański jest programem, który robi więcej, niż oczekuje od niego użytkownik i te jego dodatkowe właściwości są z punktu widzenia użytkownika niepożądane[11].

Koń trojański to program, który może zrobić coś pożytecznego, ale zawsze coś interesującego, np. wykraść hasła lub skopiować pliki bez naszej wiedzy[12].

To programy z pozoru użyteczne, lecz w istocie spełniające destrukcyjne funkcje. W wielu przypadkach służą włamywaczom do poznania i zdobycia poufnych informacji znajdujących się w naszym komputerze. Niezwykle trudno jest je wykryć, ponieważ „schowane" są w aplikacjach, których nikt nie podejrzewa o złe intencje. Pracują cicho w tle i nie zdradzają swojej obecności.

Podstawowe niebezpieczeństwa, jakie niesie koń trojański to:

- może atakować dużą liczbę komputerów;
- jest trudny do zlokalizowania i wykrycia;
- zbiera informacje o systemach umożliwiając jego twórcom włamanie (np. hasła autoryzacji);
- wykrada tajne dane przechowywane w komputerach;
- może ukrywać ważne informacje o systemie;
- w niektórych przypadkach niszczy dane oraz systemy.

Powinniśmy uważać na programy, które ściągamy z Internetu, ponieważ trudno jest stwierdzić czy są bezpieczne. Można je „zaszyć" w dowolnym programie, na każdej platformie systemowej. W przedsiębiorstwach pracownicy bardzo często pobierają aplikacje im potrzebne z Internetu. Gdy taki trojan zostanie zapisany na dysku firmowego komputera może spowodować: zakażenie sieci lokalnej, zagrożenie poufności danych, destrukcję oprogramowania, bądź inne niebezpieczeństwa.

Nawet oficjalne programy markowych firm mogą zawierać konie trojańskie. Zdarzyło się tak w 1999 roku w przypadku programu aktualizującego popularnego Internet Explorera. Był rozprowadzany za pośrednictwem poczty elektronicznej. Po uruchomieniu aktualizacji trojan zagnieżdżał się w systemie.

Można powiedzieć, że istnieją właściwie dwa podstawowe typy koni trojańskich:

---

[11] *Dr Alan Solomon, „Wszystko o wirusach", http://stud.wsi.edu.pl/~dratewka/index.htm*

[12] *"Internet Agresja I Ochrona", wyd. Robomatic, str.199-200. RFC 1244 Site Security Handbook*

- trojany, których szkodliwy kod został dołączony do autoryzowanych programów;
- specjalnie napisane od początku programy, w których programiści zaimplementowali dodatkowe destrukcyjne funkcje. Np. INTRUDER 1.02 dla Linuxa imitujący działanie skanera systemowego służącego do wykrywania luk oraz błędów konfiguracyjnych systemu. Symulował prawidłową pracę i po wykryciu rzekomych błędów wymuszał powtórne logowanie się do systemu. Następnie zapisywał hasło udostępniając je twórcy tego konia trojańskiego.

Ze względu na sposób działania wśród koni trojańskich można z kolei wyróżnić trzy kategorie:

- umożliwiające włamywaczom zdalny dostępu do komputera na, którym się znajdują. Działają na zasadzie klient-serwer. Napastnik może zdalnie wydawać polecenia, które trojan wykona na naszej stacji roboczej;
- niszczące dane na zaatakowanym komputerze;
- wykradające informacje.

Przykłady kilku najpopularniejszych koni trojańskich[13]:

1. BACK ORFICE to potężne narzędzie do administracji komputerem ofiary. Pakiet instalacyjny składa się z plików: bo.txt, plugin.txt, boserve.exe, bogui.exe, boclient.exe, boconfig.exe, melt.exe, freeze.exe. Uruchomienie pliku boserve.exe instaluje go w katalogu systemowym. Potem następują procesy związane z konfiguracją. Ostatecznie przydziela sobie port o numerze 31337 i oczekuje na komendy napastnika (twórcy tego programu). W zależności od otrzymanej komendy może m.in.: kopiować i usuwać pliki i katalogi, przeszukiwać zasoby, wyświetlać informacje o sieci, podawać hasła dostępu do serwera, wykonywać różne czynności związane z kluczami rejestrów, pingować serwer, przekierunkować zasoby połączenia oraz kilka innych czynności.

2. DEEP THROAT REMOTE 1.0. Zawiera dwa pliki: systempatch.exe i RemonteControl.exe. Gdy ofiara zainstaluje je na swoim komputerze napastnik uzyskuje zdalny dostęp poprzez klienta programu.

---

[13] *Dane pochodzą z serwisu „Sciąga.pl", http://www.sciaga.pl*

3. MASTER'S PARADISE – dołączony do popularnej gry „Pie Bill Gates" rozpowszechnionej w Internecie. Koń trojański wkrada się do systemu po uruchomieniu gry na komputerze.

4. NETBUS – z pozoru jest programem shareware, a w dodatku wymaga rejestracji. Uzyskanie na niego licencji wymaga uiszczenia odpowiedniej opłaty. To prawdziwa ironia losu płacimy za to, aby napastnik korzystał z zasobów naszego systemu.

5. T5Port 1.0 – jeden z prostszych koni trojańskich. Nie posiada żadnego programu instalacyjnego. W swoich działaniach wykorzystuje TELNET.

Robaki

Robak (ang. worm) to program podobny do wirusa komputerowego, ale nie mieszczący się w jego klasycznej definicji. Główną różnicą jest to, że robak istnieje samodzielnie i nie potrzebuje programu-nosiciela. Robaki przemieszczają się w sieciach komputerowych i wykorzystują połączenia pomiędzy komputerami jako nośnik transmisji. Posiadają zdolność samoreplikacji. Ich podstawowym celem jest ciągłe powielanie samych siebie i rozprzestrzenianie się po sieciach komputerowych. Wielu hakerom lub innym intruzom służą jako podstawowe narzędzie włamań do serwerów. Ich stworzenie wymaga jednak od autora szerokiej znajomości środowiska sieciowego.

Robak po zagnieżdżeniu się w nowym systemie może się zachowywać jak wirus, bakteria albo koń trojański[14]. Dzieje się tak, ponieważ co prawda „robaki nie zmieniają innych programów, ale mogą przenosić kod, który to robi (na przykład prawdziwy wirus)"[15].

Oto przykłady robaków (z ostatnich miesięcy)[16]:

1. DUKSTEN B. – robak działający w oparciu o pocztę elektroniczną. Rozsyła swoje kopie do wszystkich adresatów znajdujących się w książce adresowej zaatakowanego systemu. Pojawia się na komputerze ofiary jako załącznik (PROTECT.ZIP) do listu, którego nadawcą jest „Alerta RaPida".

---

[14] *http://wiem.onet.pl/wiem*
[15] *S. Garfinkel, G. Spafford, „Bezpieczeństwo w Unixie i Internecie".*
[16] *Dane pochodzą z MKS Sp. z.o.o.*

2. MERKUR – to robak internetowy, który przenosi się przy pomocy programów do wymiany plików oraz poczty elektronicznej. Działa na dwa sposoby. W przypadku e-maila jest to plik TASKMAN.EXE dołączony do listu o temacie: „Update your Anti-virus Software". Wysyła wtedy swoje kopie adresatom znalezionym w książce adresowej systemu Windows. Natomiast w przypadku programów do wymiany i ściągania aplikacji tworzy swoje kopie na dysku ofiary zagnieżdżając się m.in. w plikach systemowych (np. autoexec.exe, screensaver.exe) oraz niektórych plikach programów Kazaa, Bearshare, Edonkey. Tworzy również plik o nazwie PrOn.bat, którego uruchomienie powoduje usunięcie plików zawierających rozszerzenia jpg, mpg, bmp, avi z katalogów programów wymienionych powyżej. Robak Merkur wysyła też własne kopie do wszystkich uczestników kanałów IRC, na który wejdzie zarażony użytkownik.

Bakterie

Bakteria (ang. bacteria) nazywana również królikiem to program dążący do pochłonięcia zasobów systemu. Bakterie nie uszkadzają i nie niszczą plików i programów. Ich działanie ogranicza się do nieustannego kopiowania się i uruchamiania swoich replik. Każda bakteria dzieli się na dwie kolejne, które następnie są uruchamiane. One z kolei mnożą się dalej tworząc nowe. Proces ten może powtarzać się w nieskończoność, aż do zajęcia całego wolnego obszaru dysku zainfekowanego komputera. Działanie tego typu przysparza ofiarom ataku wielu problemów. Szkodniki te pożerają ogromne zasoby przestrzeni dyskowej, pamięci oraz obciążają pracę procesora. Skutkiem jest także w wielu przypadkach zawieszanie się, przeładowywanie oraz awaria systemu.

Bomby logiczne

Bomba logiczna to program, którego destrukcyjne działanie aktywuje się w określonych okolicznościach. Wymaga spełnienia odpowiednich warunków, jakie zostały wpisane w kod źródłowy tej złośliwej aplikacji. Może to być np. obecność lub brak określonych plików w systemie, logowanie się wybranego użytkownika albo kryteria czasowe (mówimy wtedy o bombie czasowej[17]). Czasami jest to wystarczająca liczba uruchomień komputera, wystąpienie jakiegoś hasła, nazwy,

[17] *Bomba czasowa – to program złośliwy, którego ukryte funkcje zaczynają działać po określonym czasie.*

bądź daty. Sposób działania bomby logicznej łatwo jest wytłumaczyć na przykładzie prostego algorytmu. Bomba czeka na spełnienie warunków, które potrzebne jej są do uwolnienia ładunku użytecznego i eksplodowania. Jeśli natomiast warunki te nie zostaną spełnione nic się nie stanie. Skutki wybuchu są kłopotliwe i mogą prowadzić do dużych strat. Podobnie jak w przypadkach wcześniej opisywanych wirusów lub robaków bomba logiczna wykonuje działania destrukcyjne. Jest w dodatku bardzo trudna do wykrycia i nie potrzebuje programu nosiciela. Co więcej jej kod może zostać dopisany do komputerowego wirusa. Jest to niebywale groźne, ponieważ opóźnienie przed atakiem, jakie umożliwia pozwala wirusowi na rozwinięcie swoich skrzydeł i zainfekowanie większej ilości aplikacji. Bomba logiczna jest zdolna do wywołania ogromnych szkód, a jakie one będą, to zależy od inwencji twórczej jej autora.

Programy skanujące

Programy skanujące służą do wykrywania słabych stron zabezpieczeń systemów komputerowych. Wykorzystywane są zarówno przez intruzów, którzy chcą się włamać jak i przez osoby, które chcą się przed nimi zabezpieczyć. To właśnie sprawia, że programy te wzbudzają wiele kontrowersji.

Intencje pierwszych autorów programów skanujących były jak najbardziej poprawne. Zdawali sobie sprawę, że komputery przyłączone do sieci coraz bardziej są narażone na ataki. W założeniu miały być narzędziami pomagającymi administratorom w wykrywaniu luk w systemie tak, aby oni mogli je załatać.

Występują dwie kategorie skanerów:

- *skanery systemowe* – testują lokalne hosty, koncentrują się na problemach wywołanych przez niewielkie błędy i przeoczenia (np. zła konfiguracja systemu, słabe hasła, nieodpowiedni dostęp do plików i katalogów). Przykładem skanera systemowego jest COPS (Computer Oracle and Password System);
- *skanery sieciowe* – badają hosty wykorzystując do tego łącza sieciowe. Wykrywają luki przeszukując porty i usługi. Ich działanie nastawione jest na znajdowanie w szczególności słabych punktów w związku z atakiem zdalnym. Do tego typu skanerów należą m.in: ISS (Internet Security Scanner) oraz SATAN (Security Administrator's Tool for Analyzing Networks).

Programy skanujące są najczęściej wykorzystywane w pierwszej fazie ataku, podczas gdy napastnik wybiera i bada cel. Skanowanie dostarcza intruzowi wiele istotnych informacji. Przy jego pomocy może dowiedzieć się o: oferowanych przez serwer usługach, wymogach logowania, występujących procedurach autoryzacji, strukturze sieci oraz wykorzystywanym oprogramowaniu i systemie operacyjnym. Hakerzy, krakerzy oraz inne osoby zainteresowane wniknięciem do naszego komputera używają wielu technik skanowania:

- Ping scanning – polega na przeszukiwaniu sygnałami ping adresów IP I bloków sieci. Umożliwia sprawdzenie komputerów. To znaczy, które z nich są podłączone do sieci i pod którymi numerami IP się znajdują;
- TCP connect() scanning – nawiązuje połączenia z wybranymi portami i skanuje je. Jeśli dojdzie do połączenia to, dany port jest otwarty. W przeciwnym przypadku oznacza, że port jest nie osiągalny;
- TCP SYN scanning, – tzw. skanowanie półotwarte, w którym nie dochodzi do pełnego połączenia TCP. Na początku, aby zainicjować połączenie wysyłany zostaje pakiet SYN[18] i oczekuje się na wiadomość od skanowanego hosta. Jeśli otrzymamy w odpowiedzi pakiet SYN/ACK[19] to port jest otwarty. Teraz kolejnym krokiem w procesie jest wysłanie do hosta pakietu RST[20] w celu przerwania pełnego połączenia. Natomiast, jeśli zamiast pakietu SYN/ACK otrzymamy pakiet RST to port jest niedostępny;
- TCP FIN scanning (stealth scanning) – polega na tym, że do wybranego serwera przesyłany zostaje pakiet FIN. W odpowiedzi odsyła on pakiet RST dla wszystkich zamkniętych portów. Metoda działa jedynie w systemach UNIX-owych;
- FTP bounce attack – jest bardziej skomplikowany niż poprzednie sposoby. Wykorzystuje się tu pewne cechy protokołu FTP. Przy pomocy polecenia PORT informującego o porcie i IP osoby łączącej się z serwerem protokół FTP kontroluje połączenie. Wystarczy, więc tylko wysłać do hosta informacje, że numerem portu i IP jest obiekt, który chcemy przeskanować. Serwer ten wysyła dane na wskazany przez nas port i oczekuje na

---

[18] *SYN – to jeden z bitów kontrolnych nagłówka TCP. Wydaje polecenie dla strony odbierającej pakiet dokonania synchronizacji numerów sekwencji.*

[19] *ACK – bit kontrolny nagłówka TCP. Sygnalizuje modułowi strony odbierającej, że pole potwierdzenia zawiera właściwy numer potwierdzenia.*

[20] *RST – bit kontrolny nagłówka TCP. Potwierdza reset połączenia.*

odpowiedź. Jeśli komunikatem zwrotnym będzie wiadomość o błędzie to port jest zamknięty;

- UDP scanning – w technice tej wysyłamy pakiet UDP[21] do każdego portu skanowanej maszyny. Jeśli któryś z nich odpowie komunikatem *„ICMP port unreachable"* to wiemy, że jest zamknięty. Jeśli nie otrzymamy tego komunikatu to port może być otwarty lub zabezpieczony firewallem;
- ACK scanning – służy głównie do sprawdzania rodzaju zapór ogniowych. Może pomóc przy określaniu czy dany firewall to rozbudowana, trudna do przejścia zapora, czy też prosty filtr pakietów;
- Window scanning – w zastosowaniu i działaniu metoda ta jest podobna do ACK scanning. Różnica polega na tym, że oprócz sprawdzenia zapory ogniowej dodatkowo może określić czy badany port jest otwarty;
- Reverse ident – najpierw dochodzi do nawiązania pełnego połączenia, a następnie przy użyciu protokołu ident do ustalenia właściciela procesu na danym porcie;
- Fragmentacja – metoda polega na fragmentacji pakietów. Nagłówek TCP jest fragmentowany na kilka mniejszych części tak, aby był trudniejszy do odrzucenia przez filtry pakietów;
- ip.id scanning – metoda umożliwia sfałszowanie adresu źródłowego pakietu dzięki wykorzystaniu pośredniego komputera w procesie skanowania. Wszystkie wysyłane przez nas pakiety najpierw przechodzą przez „pośrednika", co znacznie zmniejsza ryzyko wykrycia.

Programy analizy ruchu

Nazywane są analizatorami protokołów, programami analizującymi ruch w sieci, węszycielami oraz snifferami (z języka angielskiego). Informatycy twierdzą, że stwarzają największe zagrożenie dla poufności danych w sieciach komputerowych. To programy używane do przechwytywania pakietów. Pierwotnie stosowano je do wyszukiwania problemów, jakie mogą wystąpić podczas przesyłania danych w sieci. Potrafią analizować różne protokoły: TCP/IP, IPX, Ethernet, DECNet. Są niezwykle groźne. Przy ich pomocy można przechwytywać poufne informacje,

[21] *UDP (User Datagram Protocol) – protokół, który służy do przesyłania danych pomiędzy aplikacjami.*

hasła, a w konsekwencji uzyskać dostęp do zabezpieczonych zasobów i sieci. Typowi węszyciele potrafią m.in.:

- znajdywać hasła i loginy;
- śledzić ruch w sieci;
- odkrywać oraz analizować problemy wynikające podczas przesyłania danych;
- wykrywać niepożądanych osobników;
- monitorować wydajność sieci.

W celu wyjaśnienia zasady działania snifferów chciałbym się oprzeć o sieć LAN (Local Area Network). Komputery w sieci lokalnej współdzielą jeden kabel, którym podróżują różne informacje. Informacje te docierają do wszystkich komputerów w sieci, choć dostęp do nich ma jedynie adresat. Pozostałe stacje robocze filtrują i ignorują niedotyczące ich dane, nie podejmując żadnego działania. Za większość tych funkcji odpowiedzialne są karty sieciowe, w które muszą być wyposażone wszystkie komputery w sieci. Wystarczy jednak odpowiednio skonfigurować i przestawić kartę, aby móc przechwycić każdy pakiet danych.

Dużym walorem węszycieli jest to, że właściwie można je zainstalować w każdym miejscu. Mogą być umiejscowione na poszczególnych komputerach (gdzie dochodzi do logowania, bądź, z których inicjowane są połączenia), pomiędzy różnymi sieciami LAN, między Internetem, a siecią lokalną. Nie oznacza to jednak, że w każdym z tych miejsc będą działały jednakowo efektywnie. Włamywacza najbardziej interesują punkty strategiczne. Są to przede wszystkim miejsca, w których dokonuje się autoryzacji. Nie jest również możliwe podsłuchiwanie całego Internetu przy pomocy jednego węszyciela. Nie pozwalają na to ograniczenia techniczne. Internet jest zbyt rozległy i nie ma nawet jednego centralnego punktu, z którego można by było monitorować wszystkie przesyłane w nim dane. Dlatego zazwyczaj sniffer przygląda się tylko niewielkiej wybranej jego części. Ale nawet to sprawia właścicielowi węszyciela wielkie utrudnienia. W ciągu niewielkiego czasu dane przechwytywane przez sniffer mogą zapełnić ogromne ilości miejsca na komputerze, na który są składowane. Dlatego najczęściej są skonfigurowane w taki sposób, aby zapisywały tylko początkowe bajty pakietów (w nich znajdują się informacje o hasłach i nazwach użytkowników).

Programy analizy ruchu występują w dwóch wersjach: komercyjnej i freeware. Wersje komercyjne są bardzo drogie i ukazują się w postaci sprzętowo-programowej. W szczególności przeznaczone są dla administratorów sieci. Przykładami mogą być: ATM Sniffer Network Analyser, PacketView, LANWatch. Grupa druga, freeware jest ogólno dostępna i nie wymaga ponoszenia kosztów zakupu. Najbardziej znane sniffery w tej wersji to: Gobbler, Esniff, BUTTsniffer.

Infiltracja

Infiltracja to działania osób nieupoważnionych mające na celu przenikanie do różnych elementów systemu informatycznego lub sieci telekomunikacyjnej w celu zdobycia określonych informacji.

Infiltracja bierna to śledzenie informacji w określonym miejscu jej obiegu, przy czym do najczęściej stosowanych metod należą[22]:

- przechwytywanie elektromagnetyczne, polegające bądź na uzyskaniu dostępu do połączeń między komputerem a terminalami, lub do kierunkowej emisji promieniowania i na analizie sygnału odbitego od promieniującego urządzenia;
- dołączenie się do linii transmisji danych w sieciach telekomunikacyjnych lub przechwytywanie sygnałów drogą radiową;
- badanie i kopiowanie zbiorów niezabezpieczonych (piractwo komputerowe);
- analiza makulatury lub pozostałości po nośnikach informacji, będąca rezultatem bądź niefrasobliwości w gospodarce makulaturą, bądź zlekceważenia obowiązku demagnetyzacji nośników informacji;
- stosowanie ukrytych nadajników.

Infiltracja czynna polega głównie na świadomym uzyskiwaniu dostępu do systemu w celu ingerencji w najbardziej wrażliwe oraz najważniejsze elementy systemu. Przybiera ona najczęściej następujące formy:

- łamanie zabezpieczeń w celu dostępu do dowolnego miejsca w systemie informatycznym przy ominięciu zabezpieczeń stosowanych przez legalnego użytkownika systemu (np. dotarcie do rejestru zabezpieczeń,

[22] *P. Sienkiewicz, T. Goban-Klas: Społeczeństwo informacyjne..., op. cit.*

programowa analiza oprogramowania oraz zbiorów danych, stosowanie specjalnych programów narzędziowych itp.);
- ingerencja w struktury systemów operacyjnych;
- podszywanie się pod uprawnionego użytkownika systemów komputerowych;
- stosowanie programów i procedur dodatkowych (umieszczanych w fazie pisania oprogramowania lub podczas eksploatacji oprogramowania).

Gdy obiektem działania sprawcy jest komputer i jego zasoby a w szczególności zasoby w sieci komputerowej, mówi się o bezpośredniej przestępczości komputerowej. Dokonanie tego typu przestępstwa może obejmować [23]:

- kradzież informacji, która może być punktem wyjścia innych czynów przestępczych lub przybiera formę szpiegostwa;
- nieuzasadniony zakup;
- zakup z osiągnięciem nieuzasadnionych korzyści;
- kradzież oprogramowania;
- kradzież myśli technicznej;
- kradzież sprzętu;
- kradzież czasu pracy komputera;
- przemyt;
- sabotaż i dywersję sprzętowo-programową, mające tło gospodarcze, ekologiczne lub osobiste.

Hakerzy

Hacking to przede wszystkim postępowanie polegające na włamywaniu się i penetrowaniu systemów komputerowych. Wiąże się z tym łamanie zabezpieczeń oraz naruszanie bezpieczeństwa informacyjnego. Trudno byłoby się z tym nie zgodzić. Istnieje natomiast wiele sprzeczności w związku ze znaczeniem terminu haker. W opinii publicznej hakerzy są postrzegani jako sieciowi włamywacze, niebezpieczni przestępcy, niejednokrotnie niszczący i wykradający dane. Uważa się ich za sprawców większości szkód wywoływanych w Internecie. Dzieje się tak głównie za sprawą mediów oraz niedoinformowania społeczeństwa. Zarzuty padające pod adresem hakerów komputerowych są często przesadzone.

---

[23] *P. Sienkiewicz, T. Goban-Klas: Społeczeństwo informacyjne...*

W języku angielskim haker dosłownie oznacza stolarza lub cieślę, posługującego się w swojej pracy siekierą. Haker jest pasjonatem, człowiekiem bardzo inteligentnym, posiadającym spory zasób wiedzy informatycznej. W swoich działaniach kieruje się pewną etyką. Włamuje się do komputerów, ale nie kasuje i nie zmienia danych.

Najbardziej sprawiedliwą wydaje się definicja Guya L. Steela:

Haker (rzeczownik) 1. Osoba, której sprawia przyjemność poznawanie szczegółowej wiedzy na temat systemów komputerowych i rozszerzanie tej umiejętności – w przeciwieństwie do większości użytkowników komputerów, którzy wolą uczyć się niezbędnego minimum.

2. Osoba, która entuzjastycznie zajmuje się programowaniem i nie lubi teorii dotyczącej tej dziedziny[24].

A jak jest naprawdę? Trudno to sprecyzować. Opierając się na informacjach, jakie można znaleźć w Internecie, książkach poświęconych tej tematyce oraz innych źródłach hakerzy to osoby przekraczające pewne określone granice, zwiększające swoje możliwości. Są bardzo często genialnymi programistami. Dla niektórych z nich to całe życie, to swoista pasja. Posiadają ponadprzeciętną znajomość systemów komputerowych, języków programowania (C, Perl, Lisp). Nieustannie dążą do podnoszenia swoich kwalifikacji. Ich głównym celem jest pogłębianie swojej wiedzy o sieciach komputerowych, o oprogramowaniu, a co za tym idzie dalsze rozwijanie swoich umiejętności.

Hakerzy wyszukują luki w zabezpieczonych systemach. Wkradają się do nich I przejmują nad nimi kontrolę. Uwielbiają podejmować wyzwania intelektualne w postaci forsowania kolejnych zabezpieczeń. Chcą poznawać techniczne aspekty systemów. Największą satysfakcję sprawia im sam proces włamywania się.

Istnieje podział hakerów, w którym możemy wyróżnić następujące grupy:

1. Nowicjusz (The Novis) – to osoba początkująca i mało doświadczona. Jej działanie jest bardzo trudno przewidzieć.
2. Badacz (The Student) – nie niszczy systemów ani danych w nich zawartych. Dąży do pogłębiania swojej wiedzy. Ma małe doświadczenie.

[24] *Guy L. Steele, The Hacker's Dictionary*

3. Turysta (The Tourist) – wkradanie się do komputerów traktuje jak intelektualne zagadki, które chce za wszelką cenę rozwiązać. Raz po razie wybiera sobie nowe nieosiągnięte jeszcze cele.
4. Wandal (The Crasher) – dąży do spowodowania jak największych szkód. Posiada ogromną wiedzę i jest trudny do schwytania.
5. Złodziej (The Thief) – wykrada poufne dane z komputerów celem osiągnięcia korzyści finansowych. Może pracować dla konkurencji. Handluje zdobytymi informacjami.

Hakerzy tworzą odrębną społeczność. Kierują się własnymi prawami, mają swoje zasady. W ich świecie najcenniejszą walutą jest informacja. Uważają, że kluczem do wszystkiego jest wiedza. Dlatego też nieustannie ją pogłębiają. Mają obowiązek dzielenia się nią. Poza tym każdy szanujący się haker musi przestrzegać kodeksu (to znaczy zbioru pewnych zachowań i zasad postępowania). Jego główne założenia to:

- zakaz uszkadzania systemów i zmieniania plików systemowych z wyjątkiem konieczności przeciwdziałania wykryciu obecności i aby zyskać bezpieczny dostęp w przyszłości;
- zakaz mówienia o swojej działalności z wyjątkiem osób zaufanych;
- należy zawsze uważać i być ostrożnym, aż do przesady;
- nie używać konkretów, prawdziwego nazwiska, numeru telefonu podczas korzystania z sieci komputerowej;
- jeśli to możliwe należy zostawiać system w stanie w jakim się go zastało;
- nie włamywać się do komputerów rządowych;
- swoje wszelkie materiały należy trzymać bezpieczne i zakodowane;
- prawdziwy haker zawsze hakuje i robi to tylko w celu poszerzenia swojej wiedzy;
- nie wolno używać wirusów komputerowych w żadnych innych celach jak poznanie ich działania;
- nie wolno modyfikować danych poza paroma wyjątkami;
- haker dzieli się swoją wiedzą i pomaga innym, usuwa wykryte błędy i usprawnia istniejącą infrastrukturę,
- haker chce by ludzie poznawali słabe strony zabezpieczeń i mogli je usprawniać;

- haker nie łamie zasad etyki;
- haker korzysta z oprogramowania komercyjnego i nie używa wersji pirackich;
- przestrzega zasad poufności prywatnych informacji;
- przestrzega zasad społeczności hakerskiej.

Zawsze jak w każdej z grup lub społeczności występują ludzie, którzy nie przestrzegają pewnych zasad, bądź też nie chcą się im podporządkować. Na ogół znajdują się jednostki, które łamią istniejące prawa, ale nie możemy na ich podstawie oceniać ogółu.

W czasie lat działalności wytworzyła się wśród hakerów pewnego rodzaju elita. Skupia ona najznakomitszych hakerów wszechczasów. Bycie jej członkiem to swoisty zaszczyt i wielkie uznanie pośród innych. Do elity tej z pewnością należą: Richard Stallman, Dennis Ritchie, Ken Thompson, Brian Kernighan, Paul Baran, Eugene Spafford, Dan Farmer, a także Bill Gates i Paul Allen. Należy dodać, iż mieli oni ogromny, także pozytywny wpływ na rozwój informatyki i sieci komputerowych. Pomagali w projektowaniu nowych systemów i technologii. Odkrywali nowe techniki i sposoby programowania, tworzyli programy mające ogólnoświatowe zastosowanie.

Ci, którzy przysparzali największe problemy to:

Kevin Mitnick (Kondor) – to prawdziwy geniusz komputerowy. Naraził wiele korporacji na liczne koszty finansowe. Jego osiągnięcia to m.in. wtargnięcie do Narodowego Centrum Bezpieczeństwa Komputerowego, przedsiębiorstwa Santa Cruz Operation, komputera Tsutomu Shimomury (guru zabezpieczeń i ochrony teleinformatycznej) oraz ogromna liczba oszustw finansowych i komputerowych. Kevin Mitnick był jak dotąd najbardziej poszukiwanym hakerem na świecie.

Kevin Poulsen (Dark Dante) – określany również mianem „24 godzinnego hakera". W dzień zajmował się testowaniem zabezpieczeń Pentagonu, natomiast w nocy działał na własny koszt. Na jego koncie znalazły się takie wybryki jak: liczne włamania do systemów telefonicznych, serwerów sił lotniczych, oszustwa finansowe, pocztowe i komputerowe. Słynna sprawa z manipulacją podczas konkursu stacji radiowej, gdy wygrał samochód Porsche. Kevin Poulsen został nawet oskarżony o szpiegostwo.

Ehud Tenenbaum (Analyzer) – uzyskał dostęp do ponad tysiąca serwerów, w tym znaczna większość to systemy wojskowe, a także organizacje terrorystyczne.

Zawsze wybierał sobie trudne i dobrze chronione cele. Działania Tenenbauma opierały się o jego ideologie. Walczył z pedofilami, rasistami i osobami propagującymi pornografię.

Najbardziej spektakularne włamania hakerskie ubiegłych lat:

- 1990 rok – grupa „Legion of Doom" wykradła techniczną specyfikację sieci 911 firmy BellSouth (mogli doprowadzić do zablokowania numerów 911 w całych Stanach Zjednoczonych). W ręce hakerów wpadły również hasła, adresy dostępu oraz numery kont do sieci komputerowej tej firmy;
- 1991 rok – niejaki Justin Petersen dokonał włamania do jednej z wiodących firm specjalizujących się w wojskowych systemach informatycznych. Także w tym samym roku grupa hakerów z Holandii spenetrowała komputery Departamentu Obrony. Zawierały one dokładne dane o operacji w „Zatoce Perskiej" (m.in. rozmieszczenie jednostek, dane osobowe);
- 1992 rok – grupa „Masters of Deception" dokonała włamań do komputerów TWR, Narodowej Agencji Bezpieczeństwa, Bank of America oraz AT&T;
- 1993 rok - Kevin Poulsen dopuścił się oszustwa w telefonicznym konkursie sieci radiowej. Wraz z dwójką znajomych przejął kontrolę nad telefonami stacji. W ten sposób sprawił, że on wygra główną nagrodę w postaci samochodu Porsche i kilkudziesięciu tysięcy dolarów;
- 1994 rok - dwójka hakerów, włamała się do komputerów NASA, Bazy Sił Powietrznych, Koreańskiego Instytutu Badań Atomowych i wielu innych systemów. W tym roku dał również o sobie znać Kevin Mitnik atakując sieć komputerów Supercomputer Center;
- 1995 rok – Rosjanin Wladimir Levin nielegalnie przetransferował cztery miliony dolarów z nowojorskiego Citibanku na swoje konta ulokowane na całym świecie. Pod koniec roku do Sieci został wpuszczony program Satan demaskujący luki zabezpieczeń w systemie Unix. Jego współautorem był Dan Farmer;
- 1996 rok – pewien haker dokonał ataku na skrzynki e-mailowe około czterdziestu wysoko postawionych osób (głównie polityków i biznesmenów). Polegało to na subskrypcji ich adresów e-mail na listach dyskusyjnych w Internecie w wyniku czego poszkodowani otrzymywali setki tysięcy wiadomości;

- 1998 rok – Kilku nastolatków zaatakowało system Departamentu Obrony w Pentagonie, a ich łupem padły dane dotyczących płac i akt osobowych. Znacznie groźniejszy był wybryk innego nastolatka, który zablokował komputery jednego z lotnisk w Massachussets. W kwietniu natomiast kolejna grupa hakerska włamała się do sieci NASA;
- 1999 rok – ten rok obfitował w trzy znaczące wydarzenia. Kradzież 300 000 numerów kart kredytowych firmy eUniverse, atak na strony WWW Białego Domu, amerykańskiego senatu i wojska oraz rozszyfrowanie zabezpieczeń DVD;
- 2000 rok – przeciążono i zablokowano serwery internetowe CNN, Buy, Amazon, Yahoo. Rok ten zasłynął także włamaniami do laboratoriów badawczych pracujących nad bronią nuklearną.

Hakerzy wykorzystują przeróżne sposoby umożliwiające im dostanie się do upatrzonego komputera. Do najczęściej stosowanych przez nich metod należą:

- Exploit;
- ataki DoS (Denial of Service);
- ataki DdoS (Distributed Denail of Service);
- ataki Buffer Overflow;
- Spoofing;
- Sniffing;
- Social Engineering;
- Łamanie haseł;
- PoD (Ping of Death);
- Network Snooping;
- Konie trojańskie.

Przykładowy haker może wykraść z komputera poufne informacje i udostępnić je innym (np. lista klientów, zamówień oraz ofert). Jest w stanie monitorować nasze poczynania lub sparaliżować cały system informatyczny naszej firmy. W samej Polsce występuje po kilka włamań do sieci przedsiębiorstw w ciągu jednego tylko miesiąca. Większość z nich nie jest jednak podawana do opinii publicznej. Firmy nie chcą, aby ktokolwiek dowiedział się o włamaniu.

Krakerzy

Krakerzy to osoby łamiące zabezpieczenia. Bardzo często nazywani są gorszymi braćmi hakerów. Są nielubiani przez użytkowników komputerów.

W języku angielskim słowo crack oznacza łamać, trzaskać, pękać natomiast cracker to dziadek do orzechów. W języku polskim słowo kraker można rozumieć dwuznacznie.

Pierwsze znaczenie określa osobę, którą cechują destrukcyjne zamiary. Programistę-włamywacza uszkadzającego komputery swoich ofiar. Robi to z chęci osiągnięcia korzyści materialnych, satysfakcji lub wyrządzenia szkód. W tym przypadku definicja brzmi następująco:

Kraker włamuje się lub w inny sposób narusza bezpieczeństwo komputera zdalnego. Po uzyskaniu nieautoryzowanego dostępu niszczy kluczowe dane, zamyka dostęp prawowitym użytkownikom i ogólnie przyczynia się do powstawania problemów. Krakera jest łatwo poznać: kierują nim złe pobudki[25].

Kraker by osiągnąć swój cel posługuje się również niektórymi technikami hakerskimi. Jest prawdziwym utrapieniem dla administratorów sieci. Jego wybryki niejednokrotnie narażają firmy na wielkie koszty. W odróżnieniu od hakera kraker nie tylko włamuje się do systemów, ale czyni w nich prawdziwe spustoszenie.

Drugie znaczenie obrazuje krakera jako człowieka, który usuwa zabezpieczenia programów. Wykonuje działania likwidujące ograniczenia funkcjonalne i czasowe zabezpieczonego programu komputerowego. Osiąga to dzięki modyfikacji kodu źródłowego albo poprzez nieuprawnioną rejestrację danego produktu. Tym samym zyskuje możliwość nielegalnego korzystania z programu. Podczas swojej „pracy" najczęściej napotyka na takie zabezpieczenia jak:

- klucz rejestracyjny (serial numer);
- sprawdzanie obecności płyty CD (CD check);
- program rejestracyjny (upgrade patch);
- plik kluczowy (key file);
- klucz sprzętowy;
- ograniczenia programów trial[26].

---

[25] *Internet Agresja i Ochrona*

[26] *trial – to najczęściej program w wersji demonstracyjnej, czas jego użytkowania jest ograniczony (np. kilkanaście dni lub uruchomień).*

Kraker podejmuje się łamania wszystkich zabezpieczonych aplikacji komputerowych. Bardzo często pisze również niewielkie programiki, tzw. cracki. Przekształcają one automatycznie wybrany program tak, aby można było z niego dowolnie korzystać. Cracki najczęściej spotykane są w Internecie, gdzie są dostępne dla szerokiej gamy użytkowników. Przyczynia się to do powstawania coraz większej ilości pirackich kopii komercyjnych produktów.

Promieniowanie ujawniające

Promieniowanie ujawniające jest zagrożeniem, które ze względu na swój charakter bardzo często jest niedoceniane i lekceważone. Nierzadko zdarza się, że użytkownicy nie zdają sobie z niego sprawy. Promieniowanie ujawniające może przybierać formę[27]:

- promieniowania akustycznego – np. praca drukarek;
- promieniowania elektromagnetycznego – w miejscach gdzie odbywa się przepływ prądu elektrycznego.

Rozprzestrzenianie się informacji w formie promieniowania może zatem odbywać się jako[28]:

- fale elektromagnetyczne, które podobnie jak fale radiowe mogą się rozprzestrzeniać w wolnej przestrzeni;
- promieniowanie rozprzestrzeniające się wzdłuż metalicznych przewodników (kable, urządzenia klimatyzacyjne, itp.);
- sprzężenia (pojemnościowe, indukcyjne) kabla przenoszącego informację z kablem ułożonym do niego równolegle;
- promieniowanie akustyczne, które może być wychwycone za pomocą odpowiednich mikrofonów;
- sprzężenie akustyczne z innymi urządzeniami;
- oddziaływanie zewnętrzne na urządzenia przetwarzające i przenoszące informacje.

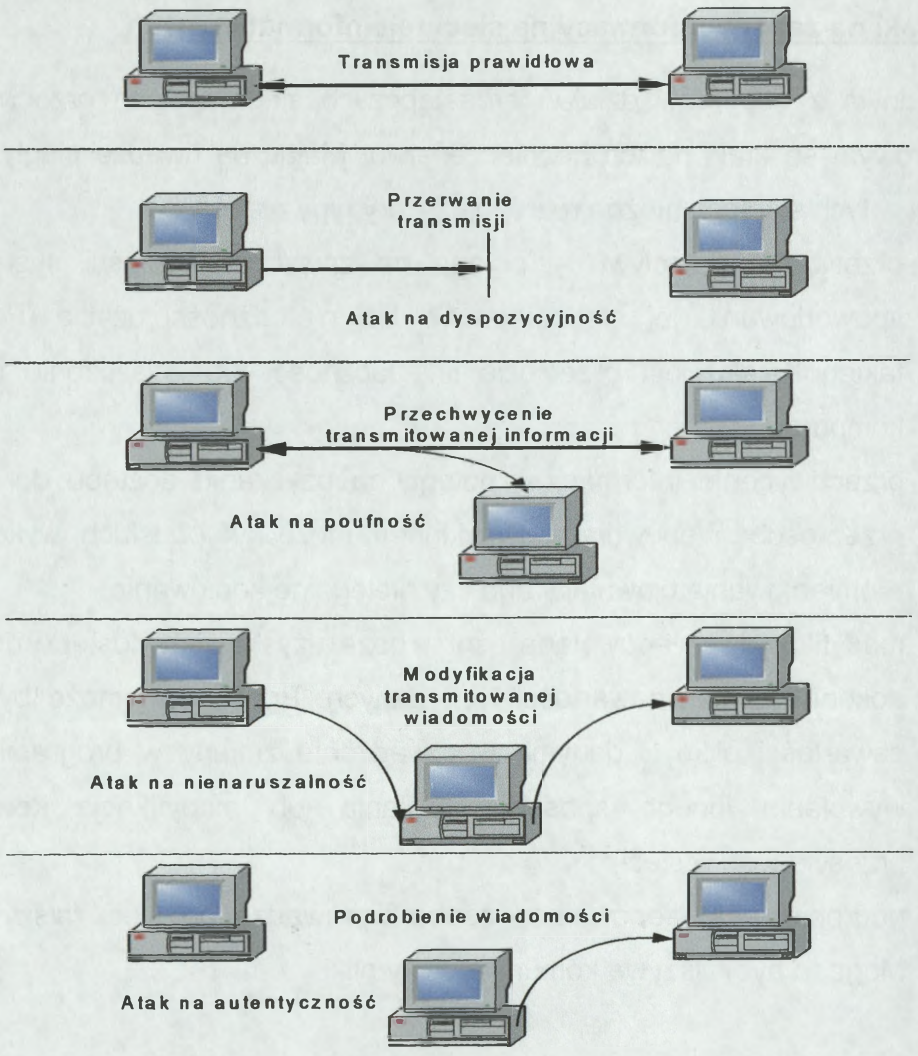
---

[27] *K. Liderman:* Bezpieczeństwo informacji w systemach informatycznych, *WSISIZ, Warszawa 2001*
[28] *Tamże*

Ataki na zasoby informacyjne sieci teleinformatycznych

Jednym z aspektów działań przestępczych skierowanych przeciw sieciom komputerowym są ataki na ich bezpieczeństwo. Mając na uwadze ciągły przepływ informacji w tych sieciach można rozróżnić cztery typy ataków:

- przerwanie przepływu – polega na zniszczeniu części systemu albo spowodowaniu jej niedostępności lub niemożności użycia. Przykładem takiego ataku jest przecięcie linii łączności lub zniszczenie fragmentu komputera;
- przechwycenie informacji – polega na uzyskaniu dostępu do informacji przez osobę niepowołaną. Przykładem może być podsłuch, wykorzystanie promieniowania ujawniającego czy nielegalne kopiowanie;
- modyfikacja – niepowołana osoba poza uzyskaniem dostępu do danych, dokonuje zmian zawartości tych danych. Przykładem może być zmiana zawartości pliku z danymi, wprowadzenie zmiany w programie w celu wywołania innego sposobu działania lub modyfikacja komunikatów przesyłanych w sieci;
- podrobienie – niepowołana osoba wprowadza do sieci fałszywe dane. Mogą to być fałszywe komunikaty czy pliki.



Rysunek 4.3. Ataki na bezpieczeństwo informacji przesyłanej w sieciach komputerowych

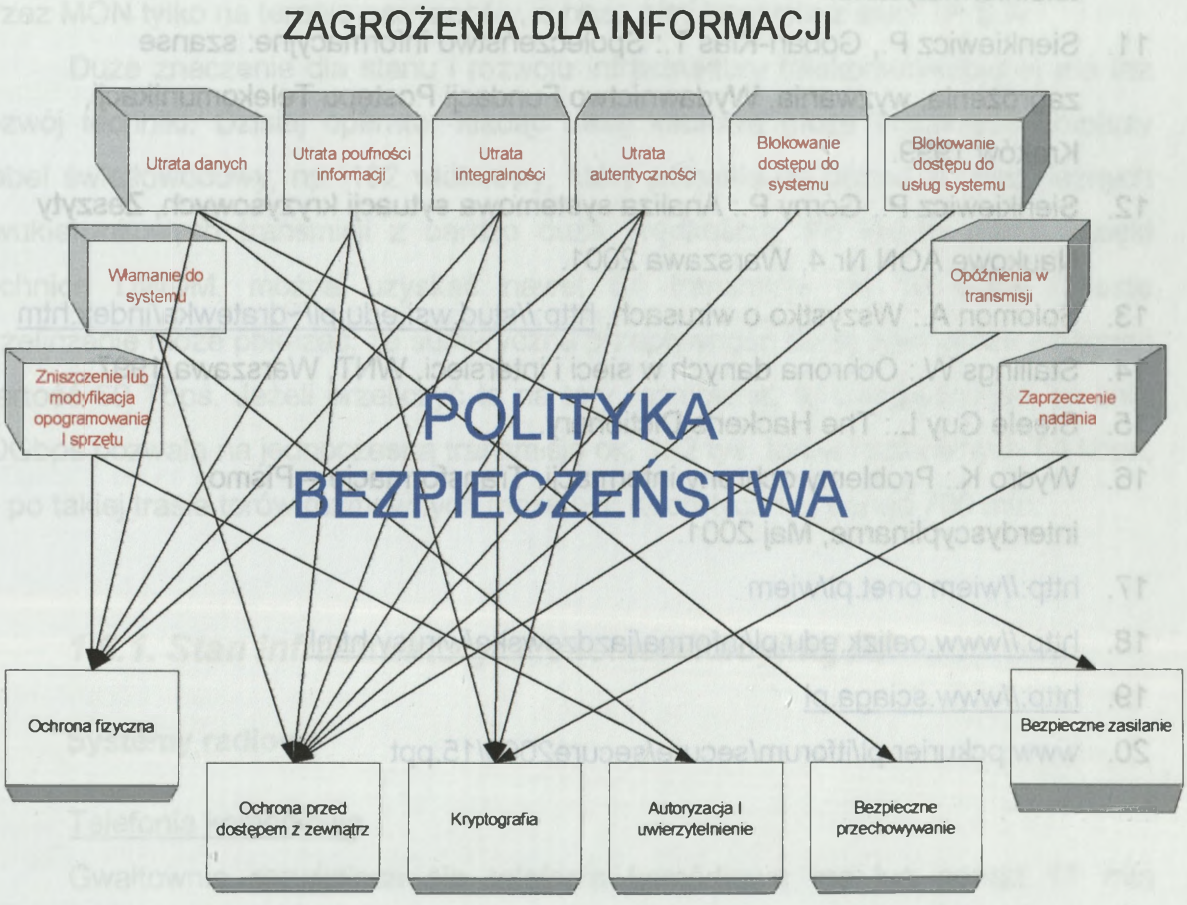
Źródło: opracowanie na podstawie W. Stallings Ochrona danych w sieci i intersieci, WNT, Warszawa 1997

1.4.4. Ochrona informacji

Systemy i sieci teleinformatyczne, a szczególnie sieci komputerowe i informacje w nich przechowywane i przetwarzane muszą być odpowiednio chronione. To niezbędne w dzisiejszych organizacjach, które posiadają szereg istotnych, nierzadko gromadzonych latami informacji. Czym byłby proces zarządzania bez informacji – ślepym losem, ruletką? Chyba nikt w dzisiejszych czasach nie wyobraża sobie takiej sytuacji. Bezpieczna informacja jest krytyczna dla efektywnego, nowoczesnego zarządzania.

Niestety informacje w sieciach komputerowych narażone są na wiele niebezpieczeństw. Zagrożenia dla nich płyną zarówno z otoczenia jak i z samej organizacji. Bardzo często zagrożenia te są niedostrzegane, nierzadko przyczyną takiego faktu jest lekceważenie potencjalnych zagrożeń przez osoby odpowiedzialne za bezpieczeństwo informacji w organizacji. Dlatego też wypracowanie solidnych metod ochrony jest zadaniem bardzo trudnym, aczkolwiek możliwym do zrealizowania. Rzetelna analiza zagrożeń, czytelna, zrozumiała i przestrzegana przez wszystkich pracowników organizacji polityka bezpieczeństwa i wypracowane w niej metody, środki i narzędzia ochrony danych mogą zapewnić bardzo wysoki stopień bezpieczeństwa informacji w organizacji.

Właściwie zidentyfikowane zagrożenia informacyjne pozwalają wyodrębnić metody ochrony informacji, które z kolei pozwalają zapobiegać i przeciwdziałać tym zagrożeniom. Na rysunku 4.4. przedstawione zostały proponowane metody ochrony informacji w odniesieniu do zidentyfikowanych zagrożeń.



Rysunek 4.4. Metody ochrony informacji

Bibliografia:

1. Garfinkel S., Spafford G.: Bezpieczeństwo w Unixie i Internecie.
2. Grabowski A.: Technologia WebQoS. Bezpieczne systemy teleinformatyczne, Warszawa 2000.
3. Hruska J.: Wirusy komputerowe i ochrona antywirusowa.
4. Internet Agresja I Ochrona, wyd. Robomatic, RFC 1244 Site Security Handbook
5. Liderman K.: Bezpieczeństwo informacji w systemach informatycznych, WSISIZ, Warszawa 2001.
6. Meller A.: Gry wojenne, CHIP, Marzec 2002.
7. Molski M., Opala S.: Elementarz Bezpieczeństwa Systemów Informatycznych.
8. Pipkin L.: Bezpieczeństwo informacji, WNT, Warszawa 2002.
9. Raport 2000 CERT POLSKA Przypadki naruszające bezpieczeństwo teleinformatyczne.
10. Raport 2001 CERT POLSKA Przypadki naruszające bezpieczeństwo teleinformatyczne.
11. Sienkiewicz P., Goban-Klas T.: Społeczeństwo informacyjne: szanse zagrożenia, wyzwania, Wydawnictwo Fundacji Postępu Telekomunikacji, Kraków 1999.
12. Sienkiewicz P., Górny P.: Analiza systemowa sytuacji kryzysowych, Zeszyty Naukowe AON Nr 4, Warszawa 2001.
13. Solomon A.: Wszystko o wirusach, http://stud.wsi.edu.pl/~dratewka/index.htm
14. Stallings W.: Ochrona danych w sieci i intersieci, WNT, Warszawa 1997.
15. Steele Guy L.: The Hacker's Dictionary.
16. Wydro K.: Problemy ochrony informacji, Transformacje – Pismo interdyscyplinarne, Maj 2001.
17. http://wiem.onet.pl/wiem
18. http://www.oeiizk.edu.pl/informa/jazdzewska/wirusy.html
19. http://www.sciaga.pl
20. www.pckurier.pl/itforum/secure/secure2000/15.ppt

1.5. ZAGROŻENIA DLA BEZPIECZEŃSTWA INFRASTRUKTURY TELEINFORMATYCZNEJ PAŃSTWA

Dokonujące się przemiany zarówno w zakresie uregulowań prawnych jak i technologicznych stanowią podstawę gwałtownego rozwoju infrastruktury telekomunikacyjnej naszego Państwa.

Wśród uregulowań prawnych można wyróżnić powolne odchodzenie od monopolu jednego dostawcy usług telekomunikacyjnych, którym do roku 1992 było przedsiębiorstwo „Poczta Polska, Telegraf i Telefon". Po roku 1992 operatorem sieci telekomunikacyjnych wymienionego przedsiębiorstwa została Telekomunikacja Polska S.A. TP S.A. straciła kolejno monopol na łącza lokalne, następnie na międzymiastowea po 1 stycznia 2003 - także na łącza zagraniczne. Dopuszczenie innych podmiotów gospodarczych do usług telekomunikacyjnych zaowocowało szeregiem inwestycji, które zwiększyły zasoby infrastruktury telekomunikacyjnej RP i jej możliwości. Warto zaznaczyć, że sieć telekomunikacyjna MON jest zarządzana przez MON tylko na terenie garnizonów, a poza nimi korzysta z sieci TP S.A.

Duże znaczenie dla stanu i rozwoju infrastruktury telekomunikacyjnej ma też rozwój techniki. Dzisiaj operator kładąc trasę kablową może instalować zbiorczy kabel światłowodowy, np. 192 włóknowy, który pozwala na ponad 90 niezależnych dwukierunkowych transmisji z bardzo dużą prędkością. Po każdej parze, dzięki technice DWDM, można uzyskać nawet 64 transmisje po 10 Gbps. Proste przeliczenie może pokazać, że sumaryczna przepływność takiej trasy może osiągnąć wartość 60 Tbps. Jeżeli przeliczyć to na tory rozmowne, to uwzględniając, że linia 10Gbps pozwala na jednoczesną transmisję ok. 122 tys. torów rozmownych 64 kbps, to po takiej trasie torów rozmownych może być (teoretycznie) ponad 700 mln.

1.5.1. Stan infrastruktury telekomunikacyjnej RP

Systemy radiowe

Telefonia komórkowa

Gwałtownie rozwijająca się telefonia komórkowa ma już ponad 11 mln abonentów. Systemy telefonii komórkowej rozwijane są w Polsce przez trzech operatorów: Centertel (Idea), Polkomtel (Plus GSM) i Polska Telefonia Cyfrowa (Era

GSM). Wykorzystywane są głównie dwa systemy GSM 900 (poza dużymi miastami) i GSM 1800 (w dużych miastach). Analogowy system NMT jest już w zaniku. Technicznie na obszarze, na którym ma być zasięg danej sieci montuje się gęstą sieć stacji bazowych (co kilka kilometrów dla GSM 1800 i co kilkanaście do 30 km dla GSM 900). Powoduje to, problemy z dostępem do sieci w rejonach słabo zaludnionych (np. poligony, duże zespoły leśne). Systemy komórkowe (tak jak wszystkie systemy radiowe) są słabo odporne na zakłócenia celowe.

Systemy przywoławcze (pagingowe)

Są to systemy łączności jednokierunkowej, które umożliwiają abonentowi wyposażonemu w odbiornik otrzymywanie komunikatów. Wyróżnia się tu systemy informujące:

- sygnałem tonowym (bez dodatkowych informacji);
- sygnałem numerycznym (tylko cyfry na wyświetlaczu);
- sygnałem alfanumerycznym (cyfry i tekst).

Systemy przywoławcze mogą być rozwijane jako systemy lokalne (dla sieci zakładowych) lub systemy dużych mocy. Obecnie są w zaniku z uwagi na rozwój telefonii komórkowej.

Systemy trankingowe

Systemy trankingowe obecne są na naszym rynku pod nazwami RADIO-NET (w Trójmieście) oraz TETRA. Działanie systemu opiera się na automatycznym przydzielaniu i podziale puli kanałów radiowych pomiędzy znacznie wyższą od tej puli liczbę użytkowników. Kanały informacyjne przydzielane są użytkownikowi na żądanie i zwalniane natychmiast po zakończeniu rozmowy. Systemy takie rozwijane są przez ich operatorów tylko na bardzo ograniczonym terenie.

Systemy WLL

Bezprzewodowa pętla abonencka WLL (Wireless Local Loop) łączy abonentów z publiczną siecią telefoniczną poprzez sygnał radiowy - eter radiowy w tej technologii zastępuje połączenie drutem miedzianym do centrali telefonicznej. Pod koniec 2000 roku w USA było niespełna 200 tys. użytkowników WLL. Gartner Group przewiduje jednak, że w roku 2004 liczba ta sięgnie 1,5 mln. W Stanach Zjednoczonych technologia WLL rozwija się głównie dzięki możliwości wykorzystywania nielicencjonowanej częstotliwości 2,4 GHz. Miesięczny koszt

abonamentu WLL wynosi około 100 USD za łącze 1 Mb/s. Instalacja jest jednak dość droga - około 1500 USD wraz z anteną.

W Polsce technologię WLL wykorzystuje sieć Air2Net, należąca do firmy Tele2. Pracuje ona w licencjonowanym paśmie częstotliwości 3,5 GHz, umożliwiając użytkownikowi stałe połączenia z Internetem z prędkością transmisji danych od 64 kb/s do 2 Mb/s. System Air2Net udostępnia funkcje zarządzania pasmem transmisji danych. Parametrami określającymi jakość usługi są: maksymalna prędkość transmisji danych (MIR) oraz gwarantowana prędkość transmisji danych (CIR). Pętla WLL w sieci Air2Net używa protokołu FH-CDMA (FH Code Division Multiple Access - wielodostęp z podziałem kodu z modulacją FH).

Digital Enhanced Cordless Telecommunication jest standardem opracowanym dla telefonii bezprzewodowej przez ETSI w 1988 roku. Do innych jego zastosowań należą m.in. dostęp radiowy do sieci teleinformatycznych, bezprzewodowa pętla abonencka, dostęp i współpraca z GSM oraz sieci bezprzewodowe (wireless LAN).

Początkowo DECT wykorzystywał pasmo od 1880 do 1900 MHz, podzielone na 10 kanałów o szerokości 1,728 MHz. Później zakres częstotliwości został rozszerzony do 1938 MHz, co zwiększyło liczbę kanałów do 32. W ramach każdego kanału stosuje się ramki składające się z 24 szczelin czasowych. Przy najszybszej ośmiowartościowej modulacji pozwala to na osiągnięcie prędkości transmisji 2 Mb/s (w jedną stronę), dzięki czemu DECT nadaje się nawet do korzystania z usług multimedialnych. W standardzie DECT stosuje się komórki o niewielkim rozmiarze - zwykle nie przekracza on 3 km, choć w niektórych zastosowaniach może wynosić nawet kilkanaście kilometrów.

Uzyskiwane przepływności to 1Mbps symetrycznie lub 2Mbps na 100Kbps asymetrycznie, przy rozmiarze komórki do 500m.

Sieci LMDS

LMDS (Local Multipoint Distribution Services, czyli wielopunktowe lokalne usługi dystrybucyjne) to system transmisji radiowej wykorzystujący pasmo wysokich częstotliwości. Sieć LMDS składa się ze stacji bazowej i komunikujących się z nią niewielkich stacji odbiorczych (terminali). Małe rozmiary urządzeń nadawczych i odbiorczych sprzyjają łatwej instalacji na dachach lub elewacjach budynków. Do rozprowadzenia sygnału do komputerów użytkowników można wykorzystać istniejące okablowanie strukturalne.

LMDS, zwany też B-WLL, jest rozwiązaniem dostępowym działającym w paśmie 28 GHz, co zapewnia uzyskanie dość dużych szybkości transmisji. Ponieważ pasmo to charakteryzuje się silnym tłumieniem, promień komórki (obszaru działania stacji nadawczej) wynosi ok. 2,5 - 3 km. Aby skompensować tłumienie, stacje końcowe wyposażone są w silne kierunkowe anteny. LMDS to system stacjonarny, w którym nie można przemieszczać stacji końcowych - jest to podstawowa różnica w stosunku do GSM. W porównaniu z sieciami kablowymi, budowa bezprzewodowej sieci radiowej pozwala na szybsze tempo realizacji projektu i mniejsze koszty początkowe inwestycji. Jednak ze względu na nieduży zasięg stacji końcowych zastosowanie LMDS jest ograniczone do terenów miejskich.

Firma Formus oferuje dostęp przez LMDS na obszarze Warszawy, Poznania, Trójmiasta, Szczecina, Wrocławia, Krakowa i Katowic. Formus przeżywa ostatnio poważne problemy związane z finansowaniem bieżącej działalności i inwestycji i wstrzymała inwestycje Firma prowadzi zaawansowane negocjacje z dwoma inwestorami, pierwsze oficjalne informacje na ten temat poznamy zapewne jeszcze we wrześniu.

Natomiast sieć Futuro obejmuje swoim zasięgiem: Trójmiasto, Szczecin, Bydgoszcz, Warszawę, Łódź, Wrocław, Lublin, Katowice, Kraków, Bielsko-Białą i od lipca - Poznań. Za pośrednictwem infostrady Futuro udostępniane jest pasmo w zakresie od 256 kb/s do 2 Mb/s.

W pierwszym etapie budowy sieci Datastar uruchomione zostały węzły sieci ATM zlokalizowane w czterech regionach: w Warszawie, Trójmieście, Poznaniu i w Okręgu Katowickim. W kolejnych latach Datastar planuje rozbudować sieć do ponad 70 węzłów sieci ATM, rozmieszczonych na terenie całego kraju. Podobnie, jak w przypadku dostępu przez DSL czy łączy stałych klasy T1-T3 (E1-E3), o jakości połączenia ze światem decydują nie tyle „ostatnia mila" i przepustowość, którą gwarantuje dostawca na tym odcinku, co jakość połączenia ze światem. Węzły sieci miejskich Datastar połączone są radioliniami o dostatecznie dużej jak na rozmiar sieci przepustowości 155 Mb/s.

Systemy satelitarne

Pomysł wykorzystania łącz satelitarnych do transmisji danych wiąże się z uruchomieniem przekazów DVB (Digital Video Broadcasting) z satelity, doskonale nadających się do szybkiej transmisji danych zawierających przede wszystkim grafikę i dźwięk.

Największym dostawcą satelitarnych łączy internetowych jest Hughes Network Systems - 200 tys. klientów korzysta z jego usługi DirecPC. Według szacunków Gartner Group, w 2004 roku 2,4 mln Amerykanów będzie korzystało z dostępu do Internetu poprzez łącze satelitarne. W USA koszt takiego łącza wynosi 60-70 USD miesięcznie, a szacunkowy koszt instalacji wynosi około 300 USD. Dobre łącze satelitarne jest więc droższe od dostępu przez DSL, a jakość połączenia uzależniona jest od warunków atmosferycznych. Dostęp satelitarny wiąże się także z opóźnieniem (0,7 sekundy), spowodowanym przesyłaniem sygnału na orbitę okołoziemską i z powrotem - z orbity do anteny. Łącza satelitarne nie nadają się więc do transmisji głosu w sieci (VoIP) ani do gier interaktywnych. Mimo tych wad, na łącze satelitarne decydują się firmy ulokowane z dala od obszarów zurbanizowanych.

Niestety, korzystanie z łącza satelitarnego w większości przypadków wymaga drugiego połączenia z Internetem, na przykład poprzez tradycyjny modem telefoniczny. Tym drugim łączem wysyłane są dane do centrum operacyjnego sieci satelitarnej, a stamtąd informacja kierowana jest do właściwego serwera WWW. Odpowiedź, która może być np. transmisją multimedialną lub przesyłanym plikiem, trafia za pośrednictwem operatora do satelity, a następnie do komputera odbiorcy.

Niedawno pojawiły się na rynku łącza satelitarne dwukierunkowe. W Stanach Zjednoczonych oferuje je m.in. firma StarBand (wspólne przedsięwzięcie EchoStar Communications, Dish Networks, Microsoft i RadioShack) w cenie zbliżonej do łącza jednokierunkowego - ok. 70 USD. Do wysyłania sygnałów służy antena o czaszy 24-36 cali, pozwalająca na transmisję do 150 kb/s. Natomiast średnia prędkość obierania sygnałów wyniosła w okresie testowym 575 kb/s (maksimum 900 kb/s, minimum 300 kb/s). Uzyskiwana prędkość transmisji zależy od liczby użytkowników korzystających równocześnie z dostępu przez satelitę.

Dostęp satelitarny daje się z powodzeniem stosować w małych i średnich firmach. Po zmianach w ustawieniach sieci LAN, łatwo można skonfigurować grupowy dostęp do Internetu oraz skrzynek pocztowych. Każdy węzeł sieci wymaga stałego (nieroutowalnego) adresu IP i każdy klient pocztowy oraz przeglądarka muszą używać tego samego adresu proxy, udostępnionego przez StarBand. Wprawdzie każde połączenie przez satelitę jest szyfrowane w osobnym kanale VPN, nie ma jednak możliwości stworzenia kanałów wirtualnych w obrębie przedsiębiorstwa.

Nad uruchomieniem łącza dwukierunkowego pracują także: Hughes (największy operator w USA) wspólnie z EarthLink - funkcjonuje już system DIRECWAY DW4000, oraz firma Wildblue.

Do grupy krajowych dostawców Internetu oferujących przesyłanie danych za pośrednictwem łączy satelitarnych należą m.in. Telekomunikacja Polska, zależna od Elektrimu spółka Polish Phonesat oraz KKI (Krakowski Komercyjny Internet). Łącza satelitarnej transmisji danych są również oferowane przez Telbank, jako zapasowe kanały do przesyłania informacji.

Centrum Usług Satelitarnych TP SAT w Psarach k. Kielc świadczy usługi transmisji danych przy użyciu systemów VSAT KYSTAR ADVANTAGE oraz VSAT CLEARLINK 400. Abonenci sieci VSAT mają możliwość połączenia z abonentami sieci transmisji danych Polpak i Polpak-T.

KKI oferuje dostęp do Internetu poprzez satelitę Astra. Usługa jest możliwa dzięki Europe OnLine Networks. Na potrzeby "podniebnego Internetu" zarezerwowane są trzy transpondery satelity ASTRA 19.2 E, każdy o przepustowości 34 Mb/s. System umożliwia uzyskanie 2 Mb/s maksymalnej przepustowości dla jednego abonenta. Do korzystania z niego potrzebna jest czasza z konwerterem, modem telefoniczny lub inne połączenie z Internetem, karta DYB do komputera (koszt ok. 1200 zł) oraz abonament za 15 euro miesięcznie (ok. 60 zł).

Bezprzewodowe sieci mieiskie 802.16

Początki standardu 802.16 sięgają roku 1998, w którym powołano grupę IEEE zajmującą się sieciami WMAN (Wireless MAN). Chodziło o opracowanie uniwersalnego odpowiednika systemów LMDS i LMCS, które są rozwiązaniami własnymi producentów sprzętu sieciowego. W zamyśle 802.16 miał być odpowiednikiem standardu 802.11 opisującego bezprzewodowe sieci LAN. Dokument "Standard Air Interface for Fixed Broadband Wireless Access Systems" specyfikuje warstwę fizyczną i warstwę MAC sieci WMAN pracujących w paśmie 10 - 66 GHz, zwykle w topologii punkt-wiele punktów. Jednym z ważnych wymagań była możliwość przesyłania różnego rodzaju ruchu: danych, głosu i wideo.

Architektura systemu 802.16 wygląda identycznie jak LMDS. Do publicznej sieci stacjonarnej dołączone są stacje bazowe (BS - Base Station), a do nich podłączają się bezprzewodowo stacje użytkowników (SS - Subscriber Station). Jest

to jednak sieć stacjonarna: zarówno stacje BS, jak i SS mają stałą lokalizację, a przejście terminala (hand-over) z jednej komórki do drugiej nie jest możliwe.

Różnice między oferowanymi dotychczas rozwiązaniami LMDS a standardem 802.16 leżą w interfejsie radiowym. W zależności od odległości między stacją bazową a stacją użytkownika, stosowany jest jeden z trzech sposobów modulacji: QPSK dla najdalszych stacji, 64 QAM dla najbliższych i 16 QAM dla tych, które znajdują się pośrodku. Ponadto połączenia mogą różnić się także szerokością kanałów (20, 22 i 28 MHz). Zaletą 802.16 jest możliwość zestawienia kanału o wyższej przepustowości w obie strony. W systemach LMDS jest to zwykle możliwe tylko w kierunku stacji użytkownika. Transmisja w trybie duplex może być realizowana zarówno poprzez nadawanie w różnych szczelinach czasowych (TDD - Time Division Duplex), jak i na różnych częstotliwościach (FDD - Frequency Division Duplex). W przypadku FDD możliwe jest sterowanie pakietami w sposób pozwalający osiągnąć optymalną wydajność przy współpracy z różnymi typami terminala. Dane są wysyłane w paczkach, a nad przydziałem zasobów czuwa stacja bazowa. Pasmo można przydzielić na stałe danej stacji użytkownika albo oddzielnie dla każdego połączenia.

Zdefiniowana w standardzie warstwa MAC dzieli się na trzy podwarstwy: wspólną MAC Common Part Sublayer, zależną od usługi Service Specific Convergence Sublayer i zapewniającą bezpieczeństwo Private Sublayer. Przypomina to sieci ATM, gdzie usługi mogą korzystać z różnych warstw AAL, w których kodowanie i podział danych na ramki są zależne od wymagań usługi. Standard 802.16 jest niezależny od protokołu i może przenosić zarówno ruch IPv4 czy IPv6, jak i ATM lub Ethernet. W kolejnych latach należy oczekiwać rezultatów prac grup przygotowujących standardy obejmujące inne zakresy częstotliwości: 2-11 GHz 802.16a) i 5-6 GHz (802.16b). Systemy te pozwalają na uzyskanie przepustowości od 32 do 135 Mbps.

Bezprzewodowe sieci lokalne

Popularne dziś sieci WLAN (wireless LAN) pracują na elementach opartych na standardzie IEEE 802.11b, wykorzystują one niewymagające koncesji pasmo częstotliwości 2,4 GHz i umożliwiają transmisję danych z prędkością 1, 2.5, 5 lub 11 Mb/s. Używanie pasma 2,4 GHz powoduje konflikty z innymi urządzeniami - korzystają z niego m.in. standardy Bluetooth i Home RF (standard sieci radiowej do zastosowań domowych i małych firm - w wersji 2.0 ma przepustowość 10 Mb/s),

a także niektóre urządzenia domowe. Nowy standard 802.11a "ucieka" więc w trzy pasma o wyższej częstotliwości (5 - 6 GHz), dzięki temu może transmitować więcej danych (do 54 Mb/s), jednak na krótsze odległości - maksymalną przepustowość osiąga się nie dalej niż 20 m od punktu dostępu (w 802.11b - do 50 m). W obu standardach prędkość transmisji spada wraz z odległością. Dzięki przełączaniu częstotliwości podczas transmisji (metodą FHSS lub DHSS) urządzenia radiowe potrafią w miarę bezkolizyjnie zagospodarować dostępne pasmo, powinny też w założeniu być bardziej odporne na podsłuch.

Standard 802.11a nie jest jeszcze dopuszczony do stosowania w Europie, trwają jednak negocjacje między amerykańską IEEE a europejskim ETSI (European Telecommunications Standard Institute) i jest nadzieja, że zostaną one uwieńczone sukcesem zanim urządzenia pojawią się na rynku. Kłopoty z 802.11a polegają na tym, że w Europie górne z trzech pasm 802.11a jest używane przez satelity komunikacyjne, natomiast pozostałe dwa objęte są konkurencyjnym europejskim standardem HiperLAN/2, praktycznie nieznanym w USA.

Sieci światłowodowe

Światłowody są medium szybkich technologii transportu danych takich jak: SDH, ATM, GigabitEthernet i innych. Światłowody cechuje między innymi: ogromna przepustowość, odporność na zakłócenia elektromagnetyczne oraz brak emisji ujawniającej. Aby wykorzystać zalety światłowodów należy wyposażyć węzły sieci w odpowiednie elementy aktywne. Stosowane są w Polsce trzy techniki układania światłowodów:

- wewnątrz przewodu odgromnikowego linii wysokiego napięcia – Telenergo;
- pod torami kolejowymi w specjalnej instalacji pierwotnej – Telekomunikacja Kolejowa;
- w instalacji pierwotnej w terenie zurbanizowanym lub po prostu zakopane w szczerym polu – TP SA i reszta inwestorów.

Elementami sieci światłowodowej układanej przez TP SA są węzły sieci - zwykle - Centrale Telefoniczne oddalone pomiędzy sobą od kilku do kilkudziesięciu kilometrów. Połączenia pomiędzy nimi wykonywane są poprzez ułożenie specjalnego kabla wielowłóknowego (24-192 włókna). W terenie niezabudowanym kolejne

odcinki[1] kabla układa się w ziemi na głębokości około 1,5 m i łączy specjalnymi mufami. Naturalnie wykonanie takiej trasy wymaga odpowiednich uzgodnień z właścicielami terenu przez który biegnie trasa. Stosowane obecnie techniki transmisji pozwalają bez większych problemów transmitować dane na odległość 70-100 km bez żadnych stacji wzmacniakowych. W terenie zurbanizowanym, kable układa się w kanalizacji kablowej.

Kanalizacja kablowa składa się z rur instalacji pierwotnej o średnicy 15cm wykonanymi z betonu, kamionki, żeliwa lub obecnie z rur PCV. Odcinki takiej kanalizacji są łączone betonowymi lub murowanymi studzienkami telekomunikacyjnymi.

Budowa własnej kanalizacji kablowej jest dosyć droga i wymaga szeregu uzgodnień z właścicielem terenu i architektem (prawo budowlane). Mniejsi operatorzy telekomunikacyjni wykorzystują kanalizację dużych operatorów (np. TP S.A.). Uszkodzenie jednej studzienki może oznaczać przerwę w pracy wielu sieci światłowodowych.

Operatorzy sieci światłowodowych w Polsce

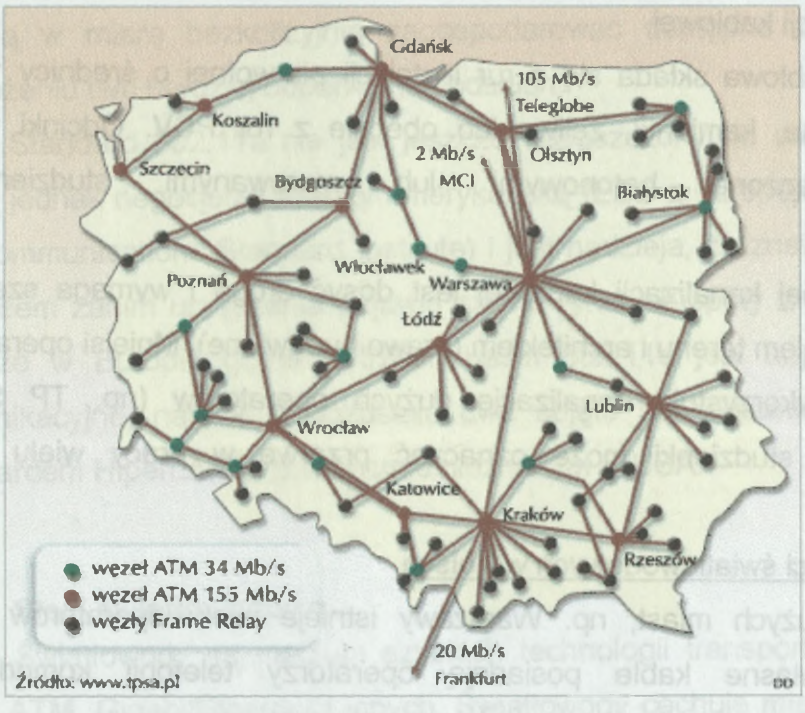
Na terenie dużych miast, np. Warszawy istnieje wielu operatorów sieci światłowodowych, własne kable posiadają operatorzy telefonii komórkowej i stacjonarnej, sieci telewizji kablowej i banki. W miastach, w których istnieją garnizony swoje sieci ma również wojskowy Centralny Węzeł Łączności. Niewielu operatorów może pochwalić się sieciami łączącymi ważniejsze aglomeracje w Polsce.

Sieć TP S.A.

TP S.A. stale rozbudowuje swoje sieci światłowodowe. Aktualnie posiada łącza pozwalające osiągnąć maksymalną szybkość transmisji 400 Gb/s. Wykorzystano w niej technologię DWDM firmy Lucent Technologies, zwiększającą przepustowość istniejącej infrastruktury dzięki przesyłaniu jednym przewodem od 40 do 80 fal świetlnych. Zastosowany system WaveStar OLS 400G pozwoli w przyszłości podwoić przepustowość łączy do 800 Gb/s. TP S.A. łącza swoje wykorzystuje przede wszystkim dla transmisji głosu, traktując transmisję danych nieco po macoszemu.

[1] *Kabel dystrybuowany jest w odcinkach od kilkuset metrów do 4 km, najczęściej na bębnie.*

Dla transmisji internetowych partnerem zagranicznym TP S.A. do roku 2001 była firma Teleglobe. Od sierpnia 2001 roku umowa między TP S.A. a Telią zapewnia polskiemu operatorowi połączenia o sumarycznej przepustowości ponad 600 Mb/s. Plan sieci Polpak przedstawia rysunek 5.1.



Rysunek 5.1. Stan sieci Polpak przed rozbudową do STM – 16

Pierwsze dwa łącza (typu STM-1) po 155 Mb/s zaczęły działać w połowie 2001, co oznaczało dwukrotne zwiększenie przepustowości połączeń wychodzących z Polski w porównaniu ze stanem z początku roku. Umowa będzie obowiązywać przez rok z możliwością jej przedłużenia na kolejne lata i rozbudowy łączy ze światem do 2,5 Gb/s.

Trzeba zaznaczyć, że TP S.A. dzierżawi miejsce w swojej kanalizacji kablowej innym firmom telekomunikacyjnym.

Kable Tel-Energo

Na ogólnopolską sieć światłowodową Tel-Energo składają się: sieć szkieletowa, sieci regionalne (wykonane w technologiach OPGW - Optical Ground Wire i ADSS - All-Dielectric Self Supporting) oraz sieci dostępowe, budowane na indywidualne zamówienia klientów. Tel-Energo planuje zwiększyć przepustowość sieci szkieletowej za pomocą technologii DWDM (Dense Wavelength Division

Multiplexing). Rozważa również stworzenie odrębnego pierścienia optycznego SDH obsługującego tylko połączenia międzynarodowe. Sieć Tel-Energo jest wyposażona w urządzenia STM-1, STM-4 oraz STM-16 i oferuje przepustowości 155 Mb/s, 622 Mb/s oraz 2,5 Gb/s. Tel-Energo zarządza siecią ponad 11000 km (rysunek 5.2).



Rysunek 5.2. Sieć Tel-Energo wraz z łączami międzynarodowymi
Źródło: materiały reklamowe firmy

Do najważniejszych klientów sieć Tel-Energo zalicza: NOM, Telefonia Lokalna, POL-34, PTC, Polkomtel, TELBANK, Netia, Pro Futuro, Energis, PKO BP, Kredyt Bank PBI, BIG Bank GDAŃSKI, BRE Bank, NASK, AGORA, H. Bauer, i inni

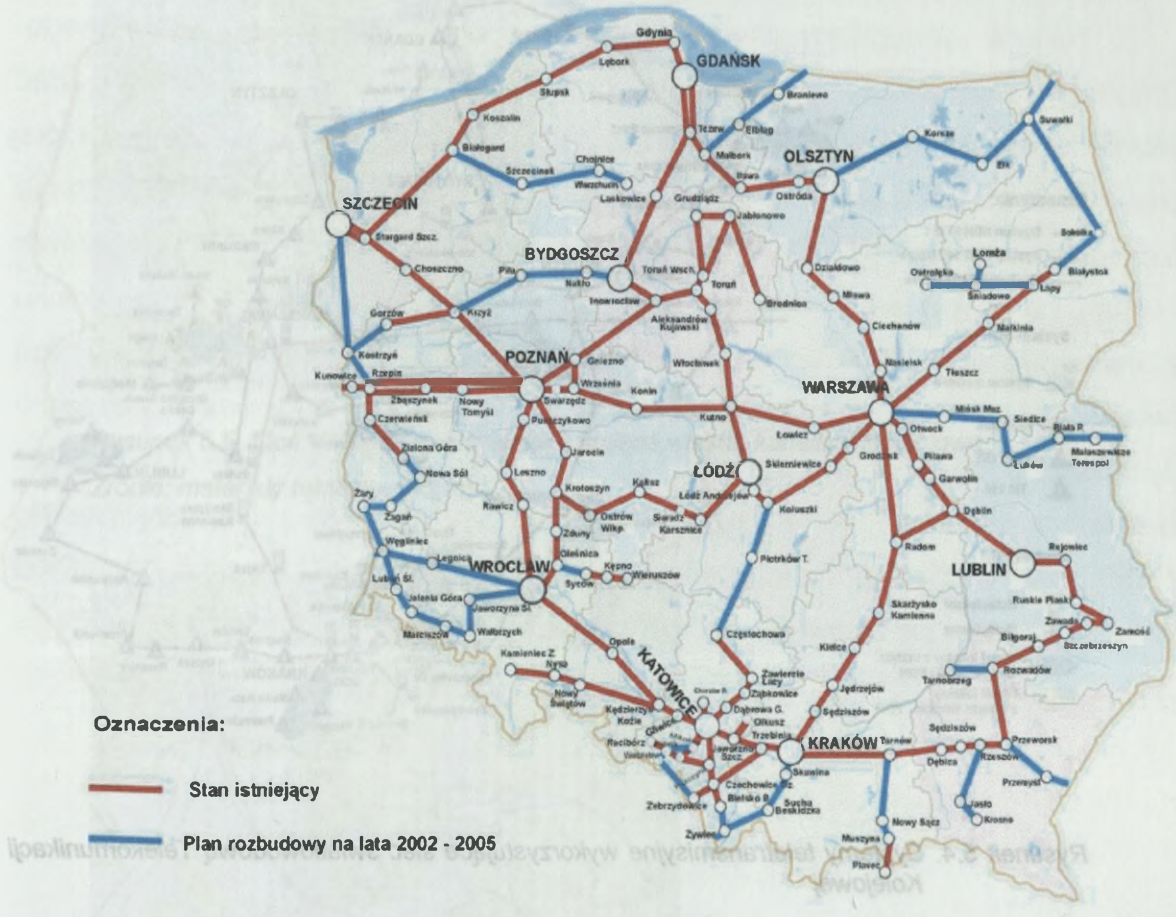
Umowę z Tel-Energo podpisała polsko-amerykańska spółka Pattern Communications, która od lipca 2001r. prowadzi w zakładach energetycznych próby technologii PLC, umożliwiającej dostęp do Internetu przez gniazdka elektryczne. Firma zawarła już wcześniej takie umowy z 5 zakładami energetycznymi, m.in. z największym w Polsce Górnośląskim Zakładem Elektroenergetycznym SA Pattern Communications wykorzystuje technologię izraelskiej firmy Main.net i chce zaoferować usługi energetycznego Internetu najpierw dla ok. 5 tys. odbiorców. W trzech zakładach energetycznych testy PLC prowadzi również konkurent Patterna, firma Ascom Poland. Dzięki PLC możliwy jest także zdalny pomiar zużycia prądu,

w Polsce pierwszy test tej technologii prowadzony jest w Zakładzie Energetycznym w Krakowie.

Sieć Telekomunikacji Kolejowej

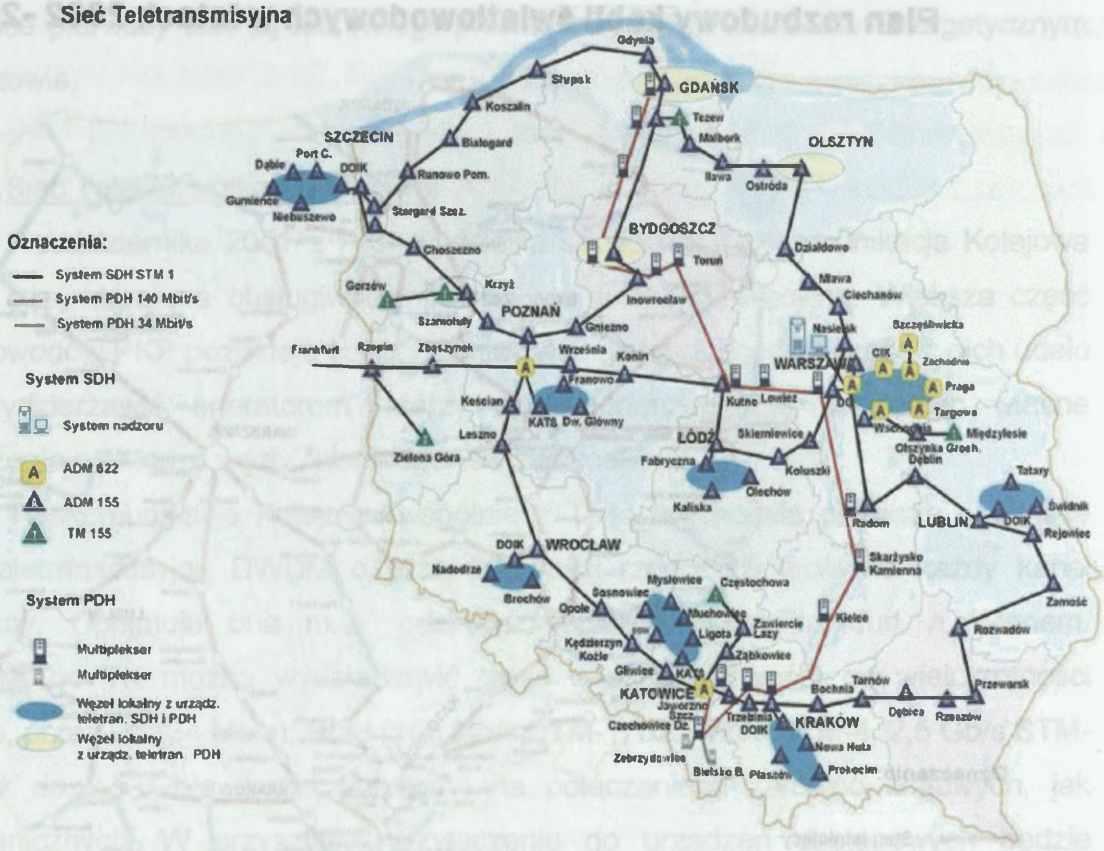
1 października 2001 z PKP wydzieliła się spółka Telekomunikacja Kolejowa Sp. z o.o., która ma obsługiwać infrastrukturę telekomunikacyjną. Większa część światłowodów PKP pozostaje cały czas niewykorzystana, chociaż część z nich udało się wydzierżawić operatorom, którzy zagospodarowują je, włączając własne urządzenia pomiędzy węzły *"ciemnego"* światłowodu.

Telekomunikacja Kolejowa wspólnie z Telią uruchomiła pierwszą w Polsce sieć teletransmisyjną DWDM o przepustowości rzędu 2,5 Gb/s na każdy kanał optyczny. Obejmuje ona m.in. odcinek Warszawa-Berlin-Frankfurt n. Menem. Obecnie od TK można wydzierżawić łącza o przepustowości od wielokrotności 2 Mb/s, przez E3 (34 Mb/s), SDH (155 Mb/s STM-1, 622 Mb/s STM-4, 2,5 Gb/s STM-16) aż do 2,5 Gb/s (kanał optyczny) na połączeniach zarówno krajowych, jak i zagranicznych. W przyszłości przyłączenie do urządzeń dostępowych będzie możliwe nie tylko w Warszawie, ale również w Łodzi, Poznaniu i innych miastach. Spółka planuje też udostępnić klientom kanały optyczne o maksymalnej przepustowości 32 x 10 Gb/s.



Rysunek 5.3. Sieć światłowodowa Telekomunikacji Kolejowej, dawniej KOPLAK
Źródło: materiały reklamowe firmy

Sieć Telekomunikacji Kolejowej (dawniej KOLPAK) - rysunki 5.3 i 5.4 - posiada dobre możliwości techniczne. Dzięki zastosowaniu specjalnego wagonu pozwalającego układać światłowody wzdłuż torów kolejowych. Na odcinkach pozbawionych rozjazdów i innych utrudnień terenowych w ten sposób można było układać nawet po kilkadziesiąt kilometrów kabla światłowodowego dziennie. Potencjał w postaci rozległej sieci torów kolejowych przechodzącej przez centra praktycznie wszystkich większych miast w Polsce (dworce to doskonała lokalizacja dla węzłów sieci) nie jest jednak w pełni wykorzystany. Problemy finansowe PKP przełożyły się na brak środków inwestycyjnych. Choć budowanie sieci światłowodowej wzdłuż torów jest tańsze od wielu innych metod, to w znacznej mierze zostało sparaliżowane przez niemoc deficytowej firmy państwowej.



Rysunek 5.4. Systemy teletransmisyjne wykorzystujące sieć światłowodową Telekomunikacji Kolejowej

Sieć światłowodowa Telia

Jeden z największych operatorów telekomunikacyjnych na świecie skandynawski operator telekomunikacyjny Telia AB jest właścicielem sieci światłowodowej Viking Network obejmującej łącza o dużej przepustowości w Europie i USA. Do końca 2001 r. sieć osiągnęła długość 40 000 km (18 000 w USA) i połączyła 50 światowych metropolii. W lipcu 2002 r. Telia uruchomiła łącze 155 Mb/s z Warszawy do Hamburga i do sieci Viking. W październiku firma utworzyła w Warszawie biuro zajmujące się rozbudową sieci Viking Network w Europie Środkowej i Wschodniej, i rozpoczęła budowę sieci typu city-carrier, która połączy kraje nadbałtyckie. Projekt ten będzie realizowany w trzech fazach. Pierwsza to połączenie Szwecja-Finlandia-Rosja, druga - Estonia-Litwa-Łotwa i ostatnia - Litwa-Rosja (Królewiec) - wybrzeże polskie planowano zakończyć w 2003 r. Część sieci Viking położona jest we własnych instalacjach (rysunek 5.5), część w instalacjach dzierżawionych od innych operatorów (rysunek 5.6).



Rysunek 5.5. Sieć Viking Network wykorzystująca własną kanalizację kablową
Źródło: materiały reklamowe firmy



Rysunek 5.6. Sieć Viking Network wraz z dzierżawionymi przez nią włóknami
Źródło: materiały reklamowe firmy

NETIA

Sieć szkieletowa Netii to 3100 km światłowodów łączących 12 głównych miast Polski. Składa się z 8 rurociągów po 48 włókien światłowodowych. Przepustowość w pierwszym etapie została ustawiona na STM-16, czyli 2,5 Gb/s.

TELBANK

Telbank, obsługujący głównie klientów należących do sektora finansowego, korzysta w dużej mierze z łączy TP SA oraz Tel-Energo. Posiada jednak już dość dobrze rozwiniętą własną sieć szkieletową o przepustowości STM-16 (2,5 G/s), którą cały czas rozbudowuje. Pod koniec maja 2001 Telbank uruchomił połączenie światłowodowe pomiędzy Warszawą a Bydgoszczą (przez Płock, Włocławek i Toruń), a w połowie listopada 2001 zakończone zostały prace na odcinku Warszawa-Kraków. Do końca roku 2002 położono kolejnych 2,5 tys. km światłowodów, m.in. na odcinkach Katowice-Wrocław oraz Wrocław – Poznań - Bydgoszcz (rysunek 5.7). Telbank jest także właścicielem największej w Polsce sieci satelitarnej, służącej głównie jako łącze zapasowe. Sieć Telbank wyodrębniła się z NBP. Powinna obsługiwać cały sektor bankowy, jednak część z banków (np. PKO BP) zdecydowała się zainwestować we własne sieci.



Rysunek 5.7. Stan sieci Telbank na koniec 2002

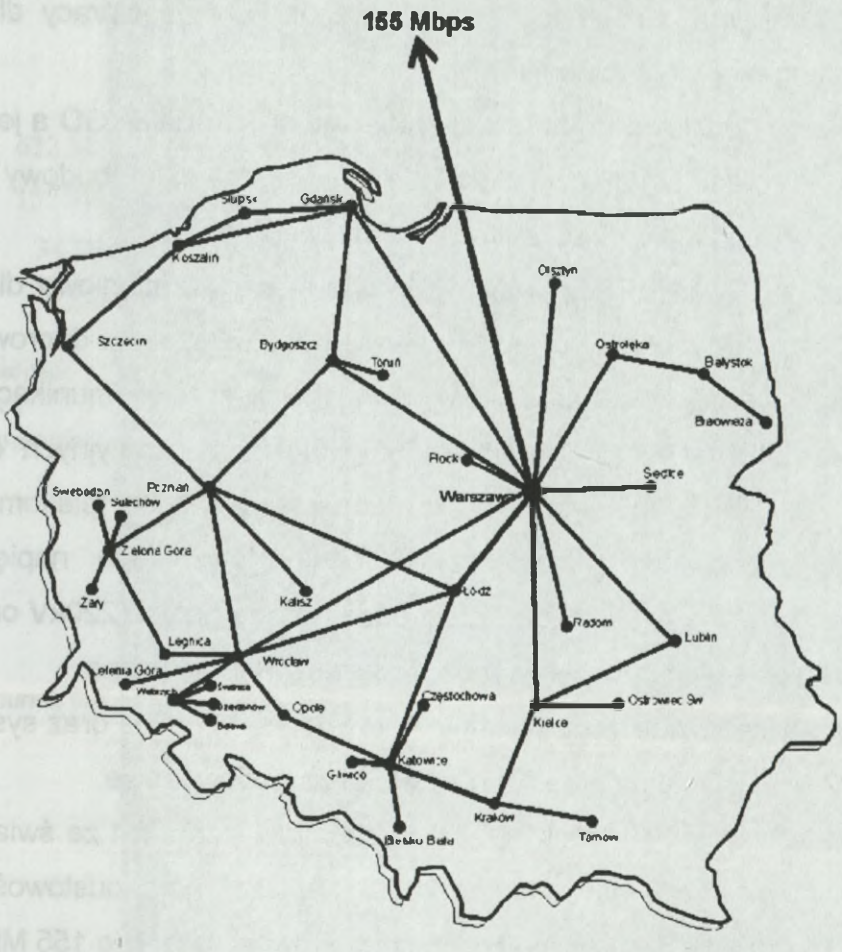
Źródło: materiały reklamowe firmy

Energis

Europejska sieć tego giganta rynku telekomunikacji ma już ponad 30 tys. km. Za 46,5 mln USD Energis uzyskał prawo do dzierżawy 5300 km sieci należącej do PKP. Do tej pory zagospodarowano już około 3 tys. km światłowodu, oddając do użytku północny pierścień wykonany w technologii SDH/DWDM.

NASK

NASK jest jedną z dwóch (obok POL-34/622) siecią polskiej nauki. Sieć NASK łączy 38 miejskich sieci komputerowych. Do NASK należy też warszawska sieć WARMAN. Sieć NASK przede wszystkim dzierżawi włókna światłowodowe, ale ma też kilkaset kilometrów własnych tras.



Rysunek 5.8. Stan sieci NASK przed modernizacją łącz międzynarodowych
Źródło: materiały reklamowe firmy

Sieć POL34/622

W środowisku Warszawy znacznie mniej znana jest druga duża sieć nauki i edukacji: sieć POL34/622. Sieć ta wywodzi się z projektu Komitetu Badań Naukowych „Pionier". Przez początkowy okres związana tylko z siecią miejską Poznania (POZMAN). Sieć POZMAN jest dzisiaj głównym węzłem tej sieci.

Sieć POL 34 zaprezentowano po raz pierwszy na międzynarodowych targach Informatyki i Telekomunikacji INFOSYSTEM 97 w Poznaniu podczas stowarzyszonej konferencji „POLMAN 97" polegający na zbudowaniu heterogenicznej rozległej sieci ATM 34 Mb/s w środowisku telekomunikacyjnym SDH 622 Mb/s operatora TEL-ENERGO.

Przedstawiona możliwość powiązania nowoczesnej infrastruktury informatycznej nauki z infrastrukturą telekomunikacyjną energetyki uświadomiła równocześnie partnerom z obu tych sfer znaczenie ich współpracy dla rozwoju zastosowań informatyki i telekomunikacji.

Stanowiło to podstawę do porozumienia między TEL-ENERGO a jednostkami wiodącymi operatorami MAN-ów akademickich w zakresie budowy krajowej, naukowej sieci ATM 34 Mb/s. Sieć ta otrzymała nazwę POL-34.

Wspólnie z TEL-ENERGO podjęto również prace wdrożeniowe dla krajowej sieci ATM 155 Mb/s o typologii trójkąta: Gdańsk - Łódź - Poznań z doprowadzeniem do Katowic. Budowę naukowej sieci ATM oparto na sieci telekomunikacyjnej TEL-ENERGO. TEL-ENERGO jest operatorem usług telekomunikacyjnych dla branży energetycznej, ale działa również na rynku komercyjnym. Sieć telekomunikacyjna TEL-ENERGO wykorzystuje podwieszone do linii wysokiego napięcia kable światłowodowe, zarówno w tak zwanej sieci bazowej energetyki (220kV oraz 400kV) jak i sieciach regionalnych budowanych przez zakłady energetyczne.

Struktura tej sieci obejmuje systemy PDH 8 Mb/s i 34 Mb/s oraz systemy SDH 155 Mb/s i 622 Mb/s . Dostępne są również włókna światłowodowe.

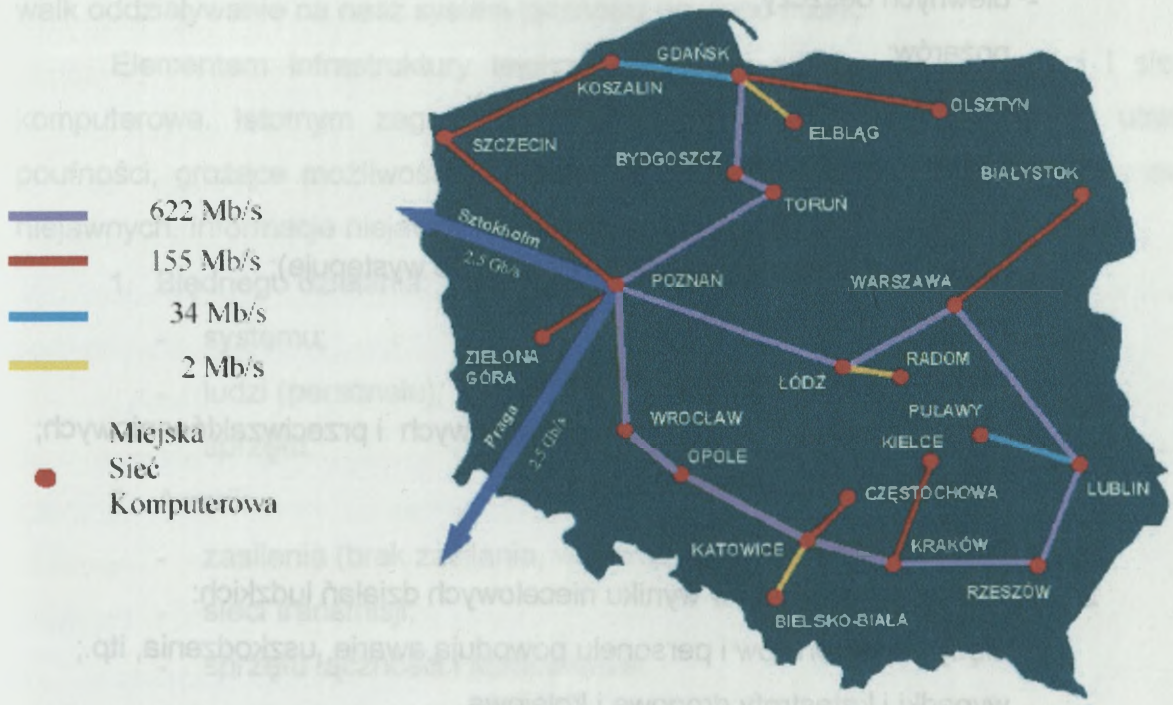
W połowie marca 1999 sieć POL34 uruchomiła łącze ATM ze światem relacji Poznań - Frankfurt nad Menem. 1 marca 2000 zwiększono przepustowość łącza do 45 Mbps. Od 1 listopada 2000 zwiększono przepustowość łącza do 155 Mbps:

- 77 Mbps do USA;
- 78 Mbps - do TEN155.

Od połowy kwietnia 2000 funkcjonuje także łącze testowe na 1 Gbps Ehthernet pomiędzy Poznaniem i Wrocławiem, które w październiku zostało przedłużone do Opola.

Od grudnia 2002 Sieć POL34/622 uruchomiła nowe łącza Internetowe za granicę, są to dwa łącza po 2,5 Gbps do sieci GEANT, następcy europejskiej sieci naukowej TEN-155.

Sieć GEANT pracuje od 1 grudnia 2001 łącząc ponad 3000 ośrodków naukowych i edukacyjnych w ponad 30 krajach. Dziewięć połączeń tej sieci pracuje z prędkością 10 Gbps, a jedenaście z prędkością 2,5 Gbps. Sieć nauki polskiej POL34/622 posiada około 700 km własnych tras światłowodowych. Aktualna architektura sieci widoczna jest na rysunku 5.9.



Rysunek 5.9. Sieć nauki polskiej POL34/622 w grudniu 2002

1.5.2. Zagrożenia infrastruktury telekomunikacyjnej w czasie pokoju, kryzysu i wojny

Przygotowanie obronne sieci telekomunikacyjnej polega na zwiększeniu jej żywotności na uszkodzenia wywołane różnymi czynnikami. Żywotność tę zwiększa się zwielokrotniając drogi i węzły, zwiększenie żywotności polega też na sprawnym przywracaniu uszkodzonych elementów do pracy.

Każdy z elementów infrastruktury może być niszczony poprzez oddziaływania zewnętrzne:

1. W wyniku oddziaływań środowiskowych:
   - powodzi;
   - zatopień;
   - ulewnych deszczy;
   - pożarów;
   - trzęsień ziemi (w Polsce nie występuje);
   - tąpnieć;
   - szkód górniczych;
   - erupcji wulkanów i gejzerów (w Polsce nie występuje);
   - wyładowań atmosferycznych;
   - uszkodzeń linii wysokiego napięcia;
   - uszkodzeń urządzeń przeciwprzepięciowych i przeciwzakłóceniowych;
   - erozji brzegu morskiego i rzecznego;
   - działania fauny i flory[2].
2. Oddziaływań losowych w wyniku niecelowych działań ludzkich:
   - błędy użytkowników i personelu powodują awarie, uszkodzenia, itp.;
   - wypadki i katastrofy drogowe i kolejowe.
3. Oddziaływań celowych:
   - oddziaływania radioelektronicznego (głównie rozpoznania radioelektronicznego);
   - dywersji;
   - wypadki wandalizmu;
   - ataki terrotystyczne;
   - kradzieży elementów systemu[3];

---

[2] *Trasy kablowe powinny być dobrze zabezpieczone przez oddziaływaniem zwierząt np. gryzoni. Stara kanalizacja kablowa wykonana z nieelastycznych materiałów bywa uszkadzana przez korzenie drzew.*

- próby przerwania funkcjonowania sieci;
- próby nieautoryzowanego przekonfigurowania elementów sieci;
- atak na system zabezpieczenia poufności informacji;
- ingerencje w system w celu korzystania z niego bez ponoszenia opłat

Wszystkie wymienione powyżej zagrożenia istnieją również w czasie kryzysu i wojny, mogą się nawet nasilić, ponadto mogą wystąpić:

1. Oddziaływania niszczące:
   - bronią konwencjonalną, głównie precyzyjną;
   - bronią masowego rażenia – bronią jądrową[4].
2. Oddziaływanie radioelektroniczne – walka radioelektroniczna.

W trakcie zmian stanów gotowości obronnej państwa należy spodziewać się narastania dezintegrujących system łączności oddziaływań zewnętrznych. W trakcie walk oddziaływanie na nasz system łączności powinno maleć.

Elementem infrastruktury telekomunikacyjnej są systemy łączności i sieci komputerowe. Istotnym zagrożeniem dla tych systemów jest zagrożenie utraty poufności, grożące możliwością pozyskania przez nieuprawnione osoby informacji niejawnych. Informacje niejawne mogą zostać ujawnione wskutek:

1. Błędnego działania:
   - systemu;
   - ludzi (personelu);
   - sprzętu.
2. Awarii:
   - zasilania (brak zasilania, wahania napięcia, przepięcia, przebicia);
   - sieci transmisji;
   - sprzętu łączności i komputerów.
3. Infiltracji dokonywanej poprzez:
   - podsłuch bierny;
   - podsłuch aktywny;
   - obejście zabezpieczeń fizycznych systemów teleinformatycznych.

---

[3] *Kradzieże instalacji, zwłaszcza miedzianych przez „zbieraczy złomu" są bardzo częstym zjawiskiem w dzisiejszej Polsce.*

[4] *Zniszczenia fizyczne, napromieniowanie systemu uniemożliwiające pracę obsłudze oraz impuls elektromagnetyczny uszkadzający niezabezpieczone urządzenia elektroniczne.*

Bibliografia:

1. Materiały reklamowe Telekomunikacji.
2. Materiały reklamowe Telekomunikacji Kolejowej.
3. Materiały reklamowe fitmy Tel-Energo.
4. Materiały reklamowe sieci NASK.
5. Materiały reklamowe firmy Viking-Network.
6. Standard Air Interface for Fixed Broadband Wireless Access Systems.
7. www.tpsa.pl

1.6. IDENTYFIKACJA ZJAWISKA INFOTERRORYZMU

„Terroryści w przyszłości mogą dokonać więcej zniszczeń przy pomocy klawiatury niż z użyciem bomb"

Manuel W. Wik

W historii ludzkości olbrzymią rolę w osiąganiu celów politycznych odgrywały zawsze działania mające na celu narzucenie siłą swoich poglądów. W stosunkach między państwami prowadziło to na ogół do wojny, natomiast w relacjach wewnętrznych przejawiało się najróżniejszymi formami terroryzmu. Zjawisko to wymyka się jednoznacznej definicji. W 1986r. wiceprezydent USA George Bush stwiedził, że *„...terroryzm to bezprawne użycie przemocy przeciwko osobom lub własności z przyczyn politycznych lub społecznych..."*[1], natomiast wśród polskich definicji można znaleźć takie jak: *„... stosowanie gwałtu przez jednostki i grupy osób w celu wywarcia wpływu na rząd i opinię publiczną, jak i na grupy osób i poszczególne osoby ..."*[2] czy *„... forma przemocy polegająca na przemyślanej akcji wymuszenia bądź zastraszenia rządów lub określonych grup społecznych w celach politycznych, ekonomicznych lub innych"*[3].

***„Terroryzm**, metoda działania polegająca na przemocy wobec pojedynczych osób aparatu władzy (terroryzm indywidualny) lub wobec przypadkowych członków społeczeństwa, przez zamachy na urzędy, lokale publiczne, koszary (terroryzm zbiorowy). Terroryzm był stosowany od wieków jako metoda walki politycznej (asasyni w XI w.). Na szerszą skalę działalność terrorystyczna rozwinęła się w XIX w., w związku z ukształtowaniem się doktryny i ruchu anarchizmu. Powstały wyspecjalizowane bojówki, związane z partiami politycznymi. Akty terroryzmu usprawiedliwiano niekiedy koniecznością walki narodowowyzwoleńczej"*[4].

Współcześnie często mówi się też o terroryzmie państwowym, czyli pozaprawnym używaniu przemocy przez różne agendy reprezentujące rządzący

---

[1] *Public Report of the Vice President's Task Force on Combating Terrorism, Goverment Printing Office, Washington, February 1986*
[2] *A. Pawłowski – Terroryzm w Europie XIX – XX wieku, Zielona Góra, 1980*
[3] *B. Balcerowicz – Słownik terminów z zakresu bezpieczeństwa narodowego, AON, Warszawa 1996*
[4] *Wielka Internetowa Encyklopedia Multimedialna*

układ polityczny, który obawiając się utraty władzy zastrasza grupy społeczne bądź liderów przeciwnych ugrupowań.

Stosowanie terroru, poza terrorem państwowym, jest i było charakterystyczne dla ugrupowań skrajnych, ekstremistycznych, które nie mogąc osiągnąć swoich celów w drodze demokratycznej musiały uciekać się do przemocy. Zamachy, porwania, sabotaż czy zastraszanie z użyciem broni lub materiałów wybuchowych to metody, które swoje apogeum osiągnęły w latach siedemdziesiątych ubiegłego wieku. Rozwój technologii miał zawsze duży wpływ na sposób realizacji tego typu działań. Chociaż podkładanie bomb czy zabójstwa będą zawsze charakterystyczne dla terrorystów to jednak również i oni znajdują zastosowanie nowych technologii dla swoich celów. Tak charakterystyczne na początku lat siedemdziesiątych porwania dla okupu ludzi znaczących na arenie politycznej (Aldo Moro) czy gospodarczej właściwie w państwach najbardziej rozwiniętych skończyły się wraz z rozbiciem grup takich jak Rote Armee Fraktion w Niemczech czy Czerwone Brygady we Włoszech. Bardzo charakterystyczne dla tego okresu porwania samolotów również przestały być najważniejszym sposobem realizacji celów od czasu wprowadzenia szczególnych środków bezpieczeństwa na lotniskach i w samolotach.

Świat zawsze pełen był konfliktów: społecznych, politycznych, narodowościowych czy religijnych, które stanowiły znakomitą pożywkę dla rozwoju ruchów separatystycznych a w konsekwencji terrorystycznych. Pogłębiające się różnice między Północą i Południem, nierównomierny rozwój gospodarczy, będące często pozostałością systemu kolonialnego to jeszcze jeden aspekt wpływający na głębokość istniejących konfliktów. Wygasaniu ognisk zapalnych w jednym regionie towarzyszy na ogół powstawanie nowych w innym miejscu. Wydaje się, że ostatnim „tradycyjnym" miejscem stanowiącym jednocześnie źródło powstawania zagrożeń na całym świecie jest Bliski Wschód. Odwieczny konflikt palestyńsko izraelski ma bardzo duży wpływ na stymulację działań terrorystycznych na całym świecie. Fakt, że żyjemy w dobie gwałtownego rozwoju środków komunikowania społecznego powoduje, że wszystkie wydarzenia tam zachodzące odbijają się szerokim echem na całym świecie. Niekończąca się spirala przemocy, w której nie widać już ani początku ani końca, gdzie atak powoduje odwet a ten z kolei kolejny atak, ma znakomite przełożenie na stosunki międzypaństwowe. Mimo różnic w podejściu do samego zjawiska widać zdecydowane różnice w postawie państw w stosunku do terroryzmu. Grupa państw najbardziej rozwiniętych widzi w nim zagrożenie dla stabilnego

rozwoju i poprawy i tak wysokiego standardu życia. Państwa, które mają świeżo w pamięci swoje problemy z uzyskaniem suwerenności, często rządzone przez dyktatorów, którzy sami doszli do władzy niekoniecznie drogą demokratycznych wyborów często patrzą z *„sympatią"* na działania przypominające światu o nierównomiernym rozłożeniu biedy i bogactwa. Są w końcu państwa, dla których istnienie zjawiska terroryzmu jest celem samym w sobie. Toczą one bezustanną walkę o osiągnięcie celu jakim jest szerzenie określonych idei. Po wydarzeniach z 11 września 2001 roku wyraźnie zmalało werbalne poparcie dla grup identyfikowanych jako niosące ze sobą zagrożenie terroryzmem ale nie należy tego utożsamiać z faktycznym zniesieniem pomocy dla nich.

Przywołane tu tragiczne wydarzenia z Nowego Jorku i Waszyngtonu wskazują, że wchodzimy w nową fazę, w której terroryści posiedli tak dużą wiedzę, że ich działania stają się trudne do przewidzenia i przeciwdziałania. Już na przełomie lat siedemdziesiątych i osiemdziesiątych, w czasie ogromnego rozwoju technologii nuklearnych zarówno w sferze militarnej jak i niemilitarnej, zaobserwowano zainteresowanie grup terrorystycznych wykorzystywaniem takich instalacji jak np. elektrowni atomowych czy laboratoriów prowadzących badania nad wykorzystaniem energii jądrowej, do celów prowadzonych przez nich działań. Katastrofa w Czarnobylu uświadomiła społeczności międzynarodowej skutki jakie może przynieść ze sobą działalność terrorystyczna wymierzona w tego typu urządzenia. Z kolei zamach wtokijskim metro uświadomił, że również inne składniki broni masowego rażenia przestały być domeną państw i mogą być użyte przez organizacje nie dysponujące wystarczającymi środkami na prowadzenie badań nad nimi. Wiedza o istnieniu tych środków, ich działaniu i możliwościach wykorzystania przestała być tajemnicą, stała się dobrem ogólnie dostępnym, a stało się tak głównie za sprawą rozwoju technik komunikowania.

Gwałtowny rozwój technologii teleinformatycznych pod koniec XX w. stał się przyczyną znacznego zmniejszenia odległości między ludźmi. Dążenie do stworzenia społeczeństwa, dla którego możliwość zdobywania i korzystania z informacji jest nieograniczona spowodowało powstanie nowej jakości życia ale jednocześnie stworzyło nowe pole dla działalności terrorystycznej. Informacje dotychczas zdobywane w mozolny sposób stają się dostępne w krótkim czasie zarówno dla tych, którzy traktują je jako źródło wiedzy jak i dla tych, którzy będą starali się wykorzystać tę wiedzę przeciwko innym. Pozwala to na lepsze przygotowanie i realizację

„tradycyjnych" działań terrorystycznych a równocześnie staje się kolejnym polem walki, na którym organizacje krajowe i międzynarodowe muszą przeciwstawić się pomysłowości tych, dla których walka, bez względu na podtekst ideologiczny jest celem samym w sobie.

Istniejące unormowania prawne nie nadążają za rozwojem technologii i jej wpływem na powstawanie nowych zagrożeń dlatego często istnieje duża trudność w zaklasyfikowaniu prowadzonych działań. O ile takie akty prawne jak: „Konwencja o zwalczaniu bezprawnych czynów przeciwko bezpieczeństwu lotnictwa cywilnego" z 1971r., *„Konwencja w sprawie zapobiegania i karania przestępstw przeciwko osobom korzystającym z ochrony międzynarodowej"* z 1973r. jak i *„Konwencja europejska o zwalczaniu terroryzmu"* z 1976r. wskazują wprost na dziedziny aktywności terrorystycznej i sposoby przeciwdziałania im, to powstanie nowej jakości w dziedzinie kontaktów międzyludzkich i wykreowanie nowego pola konfrontacji wymyka się na razie spod międzynarodowej jurysdykcji. Globalizacja wszelkiej działalności służącej rozwojowi społecznemu powoduje, że stworzony został system, który stał się jednocześnie dogodnym obiektem ataku terrorystycznego. Obiekt, którego unicestwienie może mieć daleko idące konsekwencje dla działalności struktur państwa i gospodarki.

1.6.1. Cyberprzestrzeń - nowe pole konfrontacji

Rola informacji w prowadzeniu działań zmierzających do uzyskania określonych korzyści była zawsze bardzo duża. Sposoby jej zdobywania, przekazywania, przechowywania czy przetwarzania były zawsze jedną z najbardziej chronionych tajemnic dowódców, szefów firm czy innych organizacji konkurujących na różnego rodzaju „rynkach". Umiejętność wykorzystania tych informacji jest ważnym źródłem uzyskania przewagi konkurencyjnej tak więc można uznać, że jest to istotny środek walki, który w przeciwieństwie do tradycyjnych *„twardych"*, nazwać można *„miękkim"* ze względu na to, że efekt oddziaływania nie da się określić wprost liczbą zabitych czy wyeliminowanych przeciwników, ale jakością podejmowanych decyzji. Wśród potencjalnych pól konfrontacji wyróżnić można cztery różne obszary, które mogą stać się *„polem bitwy"*. Najlepiej scharakteryzowanym i rozpoznanym jest trójwymiarowa otaczająca nas przestrzeń dająca możliwość prowadzenia walki na lądzie, wodzie, w powietrzu i przestrzeni kosmicznej; drugi obszar, który określić

należałoby logicznym obejmuje ludzki umysł i wolę, umiejętność i narzędzia gromadzenia i przetwarzania informacji; trzecie, fizyczne (fizykalne) pole walki to obszar wpływania na charakterystyki fizyczne a więc umiejętność wpływania i wykorzystania takich zjawisk fizycznych jak elektromagnetyzm, akustyka, warunki mechaniczne czy chemiczne; ostatnim ale z punktu widzenia każdego pojedynczego żywego stworzenia najważniejszym obszarem działań jest jego biologiczne trwanie[5].

Fakt, że informacja i wiedza mogą być wykorzystane zarówno do dobrych jak i złych celów powoduje, że ich znaczenie dla bezpieczeństwa narodowego jest oczywiste. Pojęcie wojny informacyjnej związane jest z pojmowaniem informacji jako *„miękkiego narzędzia zabijania"* i określa działania zmierzające do osiągnięcia przewagi wynikającej z asymetrii informacyjnej skutkującej uzyskaniem przewagi w sferach strategicznej, operacyjnej i taktycznej. Osiągnięcie tej przewagi możliwe jest zarówno poprzez działanie ofensywne jak i defensywne. Celami oddziaływań w walce informacyjnej mogą być:

- źródła informacji;
- ścieżki transmisyjne;
- systemy przetwarzania informacji;
- odbiorniki informacji.

Każda z tych grup składa się ze sprzętowych elementów informatycznych (teleinformatycznych) jak również z oprogramowania i to wyznacza możliwości zaatakowania systemu informacyjnego. Atrakcyjność ataku wynika z takich jego cech jak:

- łatwość;
- skrytość;
- anonimowość;
- taniość.

Mimo ciągłego doskonalenia sposobów ochrony informacji, nadal stosunkowo łatwo sforsować zabezpieczenia. Napastnicy wykorzystują fakt, że sieć stwarza duże możliwości do zachowania anonimowości a zidentyfikowanie prawdziwego źródła zagrożenia jest bardzo trudne zwłaszcza, że i sposoby jego przeprowadzenia mogą być bardzo różne.

---

[5] *Manuel W. Wik: „Information power and information warfare – tradition or revolution?", InfoWarCon Proceedings, Brussels, May 8-9, 1997*

Stosunkowo najłatwiejsi do zidentyfikowania są sprawcy ataków fizycznych takich jak:

- ataki na elementy infrastruktury teleinformatycznej takie jak komputery, środki łączności, oprogramowanie, dane, przewody itp.;
- ataki na infrastrukturę pomocniczą jak budynki, zasilanie energetyczne czy inne środki pozwalające na sprawne funkcjonowanie urządzeń teleinformatycznych (klimatyzacja);
- ataki na personel zatrudniony bezpośrednio przy obsłudze systemów lub wspomagający systemy.

Te ataki aczkolwiek skierowane przeciwko systemom informacyjnym noszą w sobie znamiona tradycyjnych działań terrorystycznych czy sabotażowych. Znacznie groźniejsze i trudniejsze do zidentyfikowania są ataki, które nazwać można logicznymi i realizowane bez użycia siły fizycznej a przy pomocy specjalnego oprogramowania, takie jak:

- ataki na elementy infrastruktury teleinformatycznej;
- ataki na komputerowo sterowane urządzenia zapewniające sprawne działanie systemów informatycznych;
- ataki na dane w celu ich zniszczenia lub zmienienia.

Wszystkie te ataki mogą być realizowane autonomicznie bądź razem w postaci łączonego fizycznego i logicznego ataku, w którym jedne działania mogą być podejmowane w celu ukrycia innych i odwrócenia uwagi od rzeczywistego zagrożenia.

Opisane powyżej działania są intuicyjnie przewidywalne, natomiast zupełnie nową formą oddziaływania na człowieka - operatora komputera są zjawiska opisane i przedstawione przez rosyjskich naukowców[6].

Operatorzy komputerów mogą stać się celem ataku, który jest niezwykle trudny do zidentyfikowania. Człowiek jest otwartym systemem komunikującym się z otoczeniem przez przepływy materialne, energetyczne i informacyjne. Ochrona operatorów komputerów musi dotyczyć fizycznych i psychicznych efektów oddziaływań natury informacyjnej i/lub energetycznej. Ludzkie możliwości są determinowane przez poziom potencjału fizycznego, mentalnego, intelektualnego i duchowego. Mózg, centralny system nerwowy, system odpornościowy a także

---

[6] *Victor I. Solntsev – Information war and some aspects of a computer operator's defense, InfoWarCon5*

oddechowy, krwionośny i inne systemy i organy pełniące ważne role życiowe mogą stać się celem ataku. Szczególnym celem ataku może być psychika. Świadomość i podświadomość nie są właściwie chronione przed przemyślanym atakiem. W sierpniu 1994r. miał miejsce niezwykle znamienny przypadek. Operator komputera po niespełna dwudziestu minutach pracy stracił świadomość a jego przyjaciel, również pracujący przy komputerze, odczuwał dziwne zjawiska takie jak ból głowy ihałas w uszach oraz identyfikację swojej osoby z zawartością ekranu komputera. Wyłączenie komputera spowodowało ustąpienie tych zjawisk. Pierwszy z opisanych operatorów zmarł nie odzyskawszy świadomości. Stwierdzono jeszcze około pięćdziesięciu podobnych, śmiertelnych przypadków na całym świecie. Okazało się, że był to efekt działania wirusa komputerowego o nazwie „666", który produkował na ekranie obraz o specjalnie dobranych kolorach i częstotliwości zmian co powodowało, że osoba poddana działaniu tak zmodyfikowanego ekranu popadała w pewien rodzaj hipnotycznego transu połączonego z arytmią serca i gwałtownymi skokami ciśnienia krwi. To z kolei powodowało zmiany w mózgu prowadzące do śmierci.

Inną formą ataku na operatora mogą być ataki energetyczne. Istnieją rozpoznane i nierozpoznane efekty oddziaływania promieniowania jonizującego czy wysokich częstotliwości. Możemy sobie wyobrazić, że komputer jest potencjalnym źródłem zagrożenia atakiem energetycznym ze względu na to, że ze swej natury ma on wbudowane elementy, emitujące strumienie energetyczne, które po uzyskaniu odpowiedniego polecenia mogą przemienić się w strumienie groźne dla zdrowia iżycia operatora komputera.

Wszystkie wymienione powyżej możliwości wykorzystania zdobyczy teleinformatyki do działań destrukcyjnych wskazują jak wielkie pole konfrontacji utworzyło się w momencie otwarcia *„cyberprzestrzeni"* dla szerokiej rzeszy użytkowników. Pojęcie *„cyberprzestrzeni"* dopiero niedawno weszło do powszechnego użytku i oznacza wirtualną przestrzeń, w której wszystkie obiekty połączone są za pomocą infostrady stworzonej przez globalne sieci telekomunikacyjne i teleinformatyczne[7]. W niedalekiej przeszłości państwa koncentrowały się na obronie szczególnie ważnych miejsc, które miało żywotne znaczenie dla istnienia państwa. W momencie kiedy szczególne zagrożenie może

[7] *te dwa pojęcia w chwili obecnej można stosować zamiennie, gdyż trudno znaleźć jakieś punkty, w sposób jednoznaczny, rozróżniające obydwie sieci*

nadejść z przestrzeni wirtualnej, oprócz ochrony miejsc, w których znajduje się sprzęt pozwalający na korzystanie z dobrodziejstw globalizacji informacji bardzo ważne staje się również chronienie środków przechowujących wiedzę. Istnieje wiele sposobów, aby ta wiedza była nieuchwytna dla ludzi chcących uniemożliwić korzystanie z niej. Można to osiągnąć poprzez umieszczenie jej w wielu miejscach równocześnie bądź ciągłym przesyłaniu jej w różne dobrze dobrane lokalizacje.

Opisane wyżej zagrożenia dla systemów informacyjnych nie zawsze są wynikiem działań terrorystycznych. Zgodnie z cytowaną na wstępie definicją trzeba rozróżnić przestępczość pospolitą, której celem jest nielegalne zdobycie określonych korzyści od terroryzmu, którego celem jest wymuszenie na obiektach użycia terroru (najczęściej konstytucyjnych organach władzy państwowej lub organizacjach międzynarodowych) określonych działań (np. zwolnienie więźniów politycznych) lub zwrócenie uwagi na głoszone przez te ugrupowania hasła i idee (np. niektóre działania *„ekologów"* czy antyglobalistów). Oczywiście rozpoznanie intencji przestępcy nie jest proste i każde działanie przestępcze może mieć podtekst terrorystyczny ale sam fakt realizacji nielegalnego przedsięwzięcia nie może decydować o zaklasyfikowaniu go do działań terrorystycznych. Istotne jest kto i z jakich pobudek dokonuje tego czynu przestępczego oraz to czy te działania wymierzone są w elementy Infrastruktury Krytycznej rozumianej jako ten zasób, materialny i niematerialny, będący zarówno w posiadaniu instytucji państwowych jak i prywatnych, który decyduje o możliwości realizacji przez państwo podstawowych zadań; takich jak: zaopatrzenie w środki niezbędne do życia (energia, żywność itp.), prowadzenie działalności przez instytucje zarządzające państwem (Rada Ministrów, banki), zapewnienie właściwego poziomu bezpieczeństwa wewnętrznego i zewnętrznego, transport. Dlatego w rozpoznaniu i przeciwdziałaniu terroryzmowi najistotniejsza jest identyfikacja terrorystów i umiejętność przewidzenia rodzaju stosowanych przez nich środków.

Zarówno w Polsce jak i innych krajach, powołane zostały organizacje, których zadaniem jest przeciwdziałanie przestępczości komputerowej. Fakt, że instytucje te sytuuje się zarówno w organach policyjnych jak i kontrwywiadowczych świadczy o niejednoznaczności zagrożeń jaką niosą ze sobą działania przestępcze realizowane przy wykorzystaniu możliwości teleinformatyki. W Polsce, w sferze cywilnej podstawowymi komórkami zwalczającymi tą nielegalną aktywność są: Biuro Bezpieczeństwa Łączności i Informatyki Agencji Bezpieczeństwa Wewnętrznego

i Zespół do Zwalczania Przestępczości Komputerowej w Wydziale ds. Przestępczości Gospodarczej Komendy Głównej Policji. Poniższa tabela określa zakres odpowiedzialności instytucji wymiarów sprawiedliwości i ścigania w Stanach Zjednoczonych w zależności od aktu przestępczego (tabela 6.1.).

Tabela 6.1.

AKT PRZESTĘPCZY	JURYSDYKCJA
Intruz i system znajdują się w tym samym stanie	Stanowa
Intruz znajduje się w jednym stanie a system w innym	Federalna
Intruz penetruje system używany w handlu lub łączności międzystanowej	Federalna
Intruz penetruje system Federalny z intencją kryminalną	FBI; United States Secret Service
Intruz penetruje Federalny system z intencją szpiegowania	FBI; National Security
Zagraniczny obywatel penetruje w USA system, który wyświetlił ostrzeżenie o niedozwolonym działaniu; brak umów z tym państwem regulujących podstawy prawne ścigania	Zatrzymanie i osądzenie możliwe tylko w zakresie istniejących porozumień
Zagraniczny obywatel penetruje w USA system, który wyświetlił ostrzeżenie o niedozwolonym działaniu; istnieją umowy z tym państwem regulujące podstawy prawne ścigania	W zależności od porozumień ściganie w USA lub w tym państwie

Ze względu na to, że większość aktów o charakterze infoterrorystycznym będzie miało charakter zewnętrzny w stosunku do systemów istnieje konieczność podjęcia działań zmierzających do umiędzynarodowienia ich ścigania.

1.6.2. Charakterystyka działań przestępczych w cyberprzestrzeni

Międzynarodowa Organizacja Policji Kryminalnych określiła, że przestępczość z wykorzystaniem komputerów obejmuje takie zjawiska jak[8]:

- oszustwa – prowadzące do nieuprawnionego zdobycia środków finansowych;
- fałszerstwa – zarówno dokumentów tradycyjnych jak i elektronicznych;
- nieuprawnione wejścia do systemu komputerowego – hacking;

---

[8] *J. Hajdukiewicz – e-przestępczość, zagrożenia dla gospodarki, materiały z II Sympozjum „Bezpieczeństwo systemów informacyjnych", Warszawa 2001*

- niszczenie danych lub programów komputerowych – przy po oprogramowania destrukcyjnego;
- sabotaż komputerowy – czyli umyślne zniszczenie części lub c systemu informacyjnego (sprzętu i / lub oprogramowania);
- podsłuch komputerowy – polegający na przechwytywaniu info przemieszczającej się w sieci;
- piractwo komputerowe – polegające na nielegalnym kopio rozpowszechnianiu lub publikowaniu programów komputer chronionych prawem autorskim;
- bezprawne kopiowanie topografii półprzewodników – w celu prz rozwiązań technologicznych;
- rozpowszechnianie materiałów pornograficznych;
- rozpowszechnianie materiałów rasistowskich;
- używanie sieci komputerowych do celów komunikacyjnych zorganizowane grupy przestępcze.

Jak widać nie wszystkie z tych działań mogą mieć charakter terrorys w związku z czym nie ma potrzeby w każdym z nich widzieć zagrożeni bezpieczeństwa państwa. Wśród specjalistów zajmujących się bezpieczeńs informacyjnym stosuje się następującą klasyfikację osób próbujących swoi w przełamywaniu systemów zabezpieczeń:

- nowicjusze – zainteresowani grami lub zawartością plików znajdujący u innych użytkowników sieci, charakteryzuje ich brak sprecyzowani penetracji i trudny do określenia efekt ich działań;
- „badacze" – dla własnej satysfakcji przełamujący bariery bez wyrząd szkody w systemach, do których udało im się dotrzeć;
- turyści – wędrujący po sieci w celu zaspokojenia swojej ciekawości;
- wandale – ich celem jest złamanie systemu zabezpieczeń i znisz zawartości zdobytego komputera;
- złodzieje – wykradający tajemnice najczęściej w związku z toczo rynku walką konkurencyjną.

Inna klasyfikacja dzieli osoby dokonujące ataki na:

- zdobywców – sprawdzających swoje umiejętności w przełam zabezpieczeń;

- szpiegów – wykradających informacje;
- infoterrorystów – niszczących, lub destabilizujących systemy informacyjne w celu osiągnięcia swoich celów poprzez zastraszenie lub szantaż.

Najczęściej wykorzystywanym sposobem agresji są różne formy ataków uniemożliwiających świadczenie przez system usług, do których został powołany – Denial of Service (DoS). Wśród tego typu działań najpopularniejsze są:

- ataki typu „nuke" – polegające na przesyłaniu na adres „ofiary" pakietu z danymi wraz z ustawionym wskaźnikiem (OOB – Out of Band) powodującym na ekranie zaatakowanego komputera pojawienie się niebieskiego ekranu i komunikatu o błędzie systemu. Celem tego typu ataków są komputery z systemem Windows, który w ogólnej opinii jest wyjątkowo źle zabezpieczony przed nieuprawnionym dostępem i posiada błędy ułatwiające działania przestępcze. Microsoft, poczuwając się do winy, przygotował szereg poprawek mających za zadanie usunięcie tych błędów, ale również przestępcy modyfikują ataki;
- zapychanie portów – najczęściej stosowane jako retorsja za ataki typu „nuke" polegające na przesłaniu, przy wykorzystaniu programu typu portfucker, na określony port komputera lawiny prób połączenia uniemożliwiając w ten sposób korzystanie z tego portu;
- ping of death – polegający na wysyłaniu do atakowanego komputera sygnałów (ping) sprawdzających czy jest on obecny w sieci. Komputer musi odpowiedzieć na przysłany sygnał w związku z czym nie jest w stanie realizować innych zadań;
- smurfing – to nowa forma ataku wykorzystująca zasadę, że komputer musi odpowiedzieć na przesłany do niego sygnał ping. W tej metodzie atakowanym jest nie bezpośredni użytkownik lecz router kierujący transmisjami do i z podłączonych do niego komputerów. Wykorzystując błędną konfigurację routera napastnik podszywa się pod jego adres i odpowiedź na sygnał ping kierowana jest do routera, a następnie do innych komputerów zarządzanych przez niego. Odpowiedzi kolejnych komputerów powodują całkowite uniemożliwienie pracy w sieci podłączonej do tego routera, który działa jak wzmacniacz zwielokrotniający liczbę przychodzących sygnałów ping;

- ataki typu „land" – gdzie atakujący podszywając się pod adres IP innego użytkownika wysyła pakiet danych, w którym adresy nadawcy i odbiorcy są takie same. Zaatakowany serwer próbuje odpowiedzieć na informację wpadając w pętlę i blokując sobie możliwości innych działań.
- ataki typu SYNflood – wykorzystują fakt, że w czasie nawiązywania łączności w protokole TCP strona inicjująca ustawia wskaźnik (flagę) SYN żądania rozpoczęcia synchronizacji transmisji, potwierdzający odebranie tej flagi wysyła potwierdzający sygnał ACK. Wysyłanie sygnałów SYN bez przesłania właściwych danych powoduje, że atakowany komputer może tylko realizować wysyłanie sygnałów ACK i nie realizuje innych zadań;
- atak poprzez rozsynchronizowanie połączenia – wykorzystujący tę właściwość protokołu połączeniowego Transmission Control Protocol, że pakiety przesyłane podczas połączenia mają określone numery i jeśli ta numeracja zostanie zakłócona przez intruza to pakiety będą odrzucane a oczekiwane nie będą nadchodziły;
- Distributed Denial of Service – to najnowsza wersja ataków typu DoS, realizowana z wielu opanowanych wcześniej komputerów. Haker opanowuje najpierw wiele małych komputerów umieszczając na nich swoje narzędzia ataku i w określonym czasie dokonuje zmasowanego ataku na wybrany cel;
- ataki wynikające z błędów konfiguracji usługi File Transfer Protocol – kiedy to dostęp do usługi nie wymaga podania nazwy użytkownika i hasła co powoduje, że nieupoważniony użytkownik (poprzez zalogowanie się jako anonymous z podanym adresem e-mail) może uzyskać dostęp do zasobów informacyjnych, do których nie powinien mieć dostępu;
- ataki typu „FTP bounce" – pozwalające na pokonywanie zabezpieczeń w postaci zapór sieciowych i wykorzystujące fakt, że większość serwerów nie ma ograniczeń co do możliwości przesyłania plików za pośrednictwem innego hosta co powoduje, że istnieje możliwość przesyłania na dowolny port danych ze sfałszowanym adresem źródłowym i uzyskanie w ten sposób dostępu do chronionych usług.

Duże możliwości zaatakowania systemów informacyjnych stwarza też poczta elektroniczna. Jedna z form ataku pocztowego polega na takim przesyłaniu informacji, aby uniemożliwić korzystanie z tego typu usługi poprzez:

- spam – czyli zaśmiecanie skrzynki pocztowej niechcianą korespondencją obciążając serwery, łącza i skrzynki co generuje koszty ich obsługi;
- spam – relay – polegający na rozsyłaniu spamu na serwery pocztowe a następnie przekierowywania go bez wiedzy administratora systemu na inne serwery. Ten rodzaj działalności jest możliwy w przypadku błędnej konfiguracji serwerów;
- anonimowe maile – wykorzystujące oprogramowanie służące do ukrycia nadawcy w celu przesłania informacji najczęściej o charakterze niecenzuralnym lub nawet karalnym;
- mailbombing – będący najbardziej złośliwą formą zakłócania komunikacji przy pomocy poczty elektronicznej. Zaatakowany odbiorca poczty w krótkim czasie ma zapchaną skrzynkę i samodzielne próby jej odblokowania nie przynoszą efektu. W takiej sytuacji tylko interwencja administratora systemu może przynieść skutek.

Drugą formą wykorzystania poczty elektronicznej w celu zaatakowania systemów informacyjnych jest przesyłanie za jej pomocą oprogramowania złośliwego takiego jak:

- „tylne wejścia" – specjalne oprogramowanie, które niewidoczne dla użytkownika lub widoczne lecz bez oznak jego charakteru (program użytkowy, który ma w sobie funkcje umożliwiające bezśladowe penetrowanie sieci) umożliwiają przez długi czas kontrolowanie systemu przez osobę nieupoważnioną. Kod tego oprogramowania jest *„wzbogacony"* o sekwencję pozwalającą na wejście do systemu nieupoważnionemu użytkownikowi;
- bomby logiczne – będące takim kodem w legalnie istniejącym oprogramowaniu, który kontroluje wystąpienie w systemie określonego zbioru warunków i wykonuje wtedy pewną szczególną funkcję nie będącą funkcją systemu;
- wirusy – są to części innych programów, które po zainstalowaniu się w komputerze powodują niszczenie znajdujących się tam plików

a dołączając się do poczty wychodzącej mają zdolność do przenoszenia się na inne komputery;

- robaki – samodzielne programy przenoszące się z urządzenia na urządzenie przez połączenia sieciowe, nie zmieniające innych programów chociaż mogące być nosicielem wirusa. Ich głównym zadaniem jest spowalnianie ruchu w sieci przez jej absorbowanie;
- konie trojańskie – przypominające program, który użytkownik chce uruchomić a realizujące zupełnie inne zadania udostępnienia zasobów nielegalnemu użytkownikowi. Często rozprowadzane w sieci jako programy shareware;
- bakterie (króliki) – programy samopowielające się przez co zajmują całą moc obliczeniową komputera.

Wszystkie wymienione powyżej zagrożenia, wynikające ze stosowania oprogramowania mogą być przenoszone zarówno przez pocztę elektroniczną jak i ściąganie z sieci niesprawdzonego oprogramowania, ale również poprzez instalowanie oprogramowania pochodzącego z niepewnych źródeł.

Aby uzyskać informacje potrzebne do zaatakowania sieci przestępca musi znaleźć jej czułe miejsca, niedostatecznie zabezpieczone przed penetracją. Używane są do tego techniki skanowania portów i/lub sniffery czyli programy *„węszyciele"*. Pierwsza z tych metod wykorzystuje fakt, że każda z aplikacji komunikujących się z Internetem ma przypisany adres zwany portem, którego otwarcie oznacza, że można skorzystać z jej usług. Jeżeli istnieją luki w oprogramowaniu, jak to ma miejsce np. w oprogramowaniu Microsoft Windows (łącznie z wersją XP), to będzie to zaproszenie do działalności szkodliwej. Znalezienie takiej luki w komputerze, będącym celem ataku powoduje, że agresor będzie miał ułatwione zadanie w opanowaniu zasobów informacyjnych, do których ma dostęp operator opanowanego komputera. Programy *„węszyciele"* realizują zadania podobne do skanerów portów, z tym że działają one w sieciach wewnętrznych. Są to programy, które monitorują ruch w tych sieciach umożliwiając rozwiązanie wielu problemów, jeśli wykorzystywane są przez administratorów sieci ale jeżeli zostały one tam umieszczone przez nieuprawnionego użytkownika to mogą posłużyć do ujawnienia haseł lub innych istotnych informacji o sieci i jej użytkownikach.

Najbardziej oczywistą formą zagrożenia informacjom jest atak fizyczny prowadzony przy użyciu różnego typu środków tradycyjnych, poczynając od np. wykradzenia komputera czy nośników informacji (dysku twardego, dyskietek, płyt CD) aż po materiały wybuchowe, bądź elektromagnetyczny realizowany przy pomocy specjalnie skonstruowanych urządzeń, które emitując odpowiednio silną i skoncentrowaną dawkę promieniowania elektromagnetycznego są w stanie zakłócić pracę urządzeń albo zniszczyć informację zapisaną na nośnikach nie pozostawiając żadnych widocznych śladów ataku.

1.6.3. Przeciwdziałanie zagrożeniom infoterrorystycznym

Przedstawione w powyższych rozdziałach zagrożenia dla użytkowników sieci stają się szczególnie groźne jeśli dotyczą systemów istotnych dla funkcjonowania państwa takich jak:

- telekomunikacja;
- sektor finansowy;
- systemy wodociągowe i kanalizacyjne;
- energia;
- transport;
- służba zdrowia;
- rząd centralny.

Państwo ma obowiązek przedsięwziąć wszelkie możliwe środki aby uniemożliwić działania przestępcze i terrorystyczne. Istnieją już unormowania prawne w polskich przepisach umożliwiające ściganie sprawców przestępstw komputerowych. Jako przykład rozwiązań w polskim prawie niech posłuży prawnicza interpretacja możliwości ścigania ataków typu DoS[9].

„Niezależnie od zastosowanej techniki ataku podstawowym jego celem jest „unieruchomienie" komputera, uniemożliwienie pracy oraz komunikacji z innymi maszynami. Działania tego typu stanowią zatem naruszenie jednego z podstawowych praw człowieka - wolności komunikowania się.

---

[9] *http://www.prawnik.net.pl/pw/faqDOS.htm*

Jak stanowi art. 49 Konstytucji RP „Zapewnia się wolność i tajemnice komunikowania się. Ich ograniczenie może nastąpić jedynie w przypadkach określonych w ustawie i w sposób w niej określony."

Powyższy przepis Konstytucji znajduje realizację zarówno w przepisach prawa karnego jak i cywilnego. W przypadku ataków typu DoS znajdzie zastosowanie art. 268 kodeksu karnego stanowiący, że:

„§ 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. Jeżeli czyn określony w § 1 dotyczy zapisu na komputerowym nośniku informacji, sprawca podlega karze pozbawienia wolności do lat 3.

§ 3. Kto, dopuszczając się czynu określonego w § 1 lub 2, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 4. Ściganie przestępstwa określonego w § 1-3 następuje na wniosek pokrzywdzonego."

Niewątpliwie skuteczny atak typu DoS będzie można zakwalifikować jako działanie udaremniające lub znacznie utrudniające zapoznanie się z informacją przez uprawnionego.

Jak wskazuje się w literaturze nie dochodzi do popełnienia przestępstwa gdy uprawniony posiada kopię danych i gdy ich odtworzenie nie stworzy przy tym szczególnych trudności.

Zauważmy, że w przypadku informacji zamieszczonych na serwerze www (podobnie serwerze poczty) osobą uprawnioną do zapoznania się z informacją będzie każdy użytkownik (internauta), a nie tylko osoba, która zamieściła informację, lub która administruje serwerem. A zatem możliwość zapoznania się z danymi przez administratora systemu oraz ograniczony krąg osób uprawnionych (np. po odłączeniu serwera od Internetu dane mogą przeglądać jedynie użytkownicy sieci LAN) nie wyłączy odpowiedzialności karnej sprawcy ataku. Pozostanie bowiem cała rzesza użytkowników (uprawnionych), którzy w wyniku ataku nie będą mogli zapoznać się z informacją zgromadzoną na serwerze.

Na gruncie omawianego przepisu podlega ochronie jedynie *„istotna"* informacja. Przestępstwem będzie zatem atak udaremniający lub utrudniający zapoznanie się z *„istotną"* informacją.

Jak wskazuje się w literaturze chodzi w tym przypadku o ISTOTNĄ informację w znaczeniu obiektywnym. Przy ocenie *„istotności informacji"* należy brać również pod uwagę interes dysponenta informacji oraz w pewnych przypadkach interes podmiotu którego dotyczy informacja. Słusznym wydaje się postulat oceny *„istotności"* informacji odnosząc jej wartość do pewnego standardu obowiązującego w dziedzinie, której dana informacja dotyczy. Moim zdaniem oceniając *„istotność"* informacji należy kierować się również nakładem pracy i środków koniecznych do *„uzyskania"* danej informacji.

Ustawodawca wprowadził surowszą odpowiedzialność za udaremnienie lub utrudnienie zapoznania się z informacją zgromadzoną na *"komputerowym nośniku informacji"*. A zatem zgodnie *z art. 268 § 2 k.k. w przypadku ataków typu DoS sprawca będzie podlegał karze pozbawienia wolności do lat 3.*

Odpowiedzialność sprawcy będzie jeszcze surowsza jeżeli w wyniku ataku wyrządzona zostanie *„znaczna szkoda majątkowa"*. Zgodnie *z art. 268 § 3 k. k. sprawca wyrządzający znaczną szkodę majątkowa podlega karze pozbawienia wolności od 3 miesięcy do lat 5.*

Zgodnie *z art. 115 § 7 k. k. w zw. z § 5 znaczną szkodę majątkową stanowi szkoda przekraczająca dwustukrotną wartość najniższego miesięcznego wynagrodzenia.*

Przestępstwo *z art. 268 § 2 k. k. jest przestępstwem umyślnym. Nie będzie zatem podlegał karze użytkownik który np. w wyniku awarii programu lub sprzętu przypadkowo dokonał ataku DoS na inny host."*

Fakt, że istnieją przepisy prawne pozwalające na ściganie działań przestępczych realizowanych w sieci oraz normy i przepisy[10], których stosowanie powinno zapewnić bezpieczeństwo informacyjne państwa nie może być powodem do zaniechań w dziedzinie ciągłego monitorowania zagrożeń ze strony terrorystów, którzy mogą wykorzystać cyberprzestrzeń do ataku na struktury państw demokratycznych bądź instytucji ponadnarodowych. Bardzo ważną rolę mają tu do spełnienia instytucje monitorujące wszelkie podejrzane zjawiska (incydenty) w sieci. Powołane w USA Infrastructure Protection Task Force (IPTF) mają za zadanie chronić narodową infrastrukturę krytyczną przed zagrożeniami fizycznymi i cyberzagrożeniami realizując zadania takie jak:

---

[10] *wykaz istotnych dokumentów normatywnych i dyrektywnych zamieszczony został w załączniku*

- identyfikacja incydentów i koordynacja działań w celu:
  - wykrywania;
  - zapobiegania;
  - powstrzymywania;
  - ograniczania skali zagrożenia i strat;
  - odzyskiwania utraconych informacji;
- ewidencjonowanie i rozpowszechnianie informacji o zagrożeniach;
- prowadzenie szkoleń i edukacji;
- prowadzenie analiz po akcjach antyterrorystycznych;
- koordynowanie działań ułatwiających śledzenie działań przestępczych.

Również w Polsce istnieje coraz większa świadomość konieczności obrony przed zagrożeniami cyberterrorystycznymi. Istniejące przepisy normujące standardy ochrony informacji są zgodne ze standardami światowymi, a zwłaszcza przepisami obowiązującymi w NATO a powołane organy mają zadanie swoimi działaniami pogłębić poczucie bezpieczeństwa informacyjnymi. Do tych instytucji należą:

1. Komitet Ochrony Informacji Niejawnych, który składa się z przedstawicieli resortów i instytucji najbardziej zaangażowanych w zagwarantowanie bezpieczeństwa i jest odpowiedzialny za:
   - ustalanie projektów generalnych założeń ochrony informacji niejawnych;
   - opiniowanie kierunków i planów postępowania w sytuacjach szczególnego zagrożenia o zasięgu ogólnokrajowym;
   - analiza i ocena oddziaływania na stan ochrony informacji niejawnych sytuacji szczególnego zagrożenia – formułowanie opinii;
   - opracowywanie projektów dokumentów rządowych koordynujących spójność polskiego prawa ochrony informacji niejawnych z umowami międzynarodowymi;
   - opiniowanie projektów aktów normatywnych, projektów programów, sprawozdań analiz.
2. Agencja Bezpieczeństwa Wewnętrznego (Biuro Bezpieczeństwa Łączności i Informatyki), która w instytucjach niepodlegających Ministerstwu Obrony Narodowej realizuje zadania takie jak:
   - kontrola ochrony informacji niejawnych;

- realizacja zadań w zakresie bezpieczeństwa systemów i sieci teleinformatycznych;
- prowadzenie postępowania sprawdzającego;
- ochrony informacji niejawnych w wymianie międzynarodowej;
- szkolenia i doradztwo w zakresie ochrony informacji niejawnych.

3. Wojskowe Służby Informacyjne (Centrum Analiz Kryptograficznych i Bezpieczeństwa Teleinformacyjnego) – realizuje zadania jak w punkcie 2 dla jednostek organizacyjnych Ministerstwa Obrony Narodowej.
4. Urząd Generalnego Inspektora Ochrony Danych Osobowych.
5. Policja.
6. TP S.A. (Zespół Abuse – Zespół ds Bezpieczeństwa Sieciowego w Centrum Systemów Teleinformatycznych).
7. Computer Emergency Response Team (CERT Polska) realizujący następujące zadania:

- rejestrowanie i obsługa zdarzeń naruszających bezpieczeństwo sieci;
- alarmowanie użytkowników o wystąpieniu zagrożenia;
- współpraca z innymi Incident Response Teams;
- prowadzenie działań zmierzających do wzrostu świadomości bezpieczeństwa informacyjnego;
- prowadzenie badań i przygotowywanie raportów dotyczących bezpieczeństwa informacyjnego polskich zasobów Internetu;
- testowanie produktów i rozwiązań bezpieczeństwa informacyjnego;
- tworzenie wzorców obsługi i rejestracji incydentów.

Wszystkie te instytucje mają zadania wynikające z ich usytuowania w krajowym i światowym systemie bezpieczeństwa informacyjnego ale łatwość realizacji działań przestępczych w tym terrorystycznych w cyberprzestrzeni prowadzi również do działań kuriozalnych jak np. zamieszczona poniżej propozycja działań hakerskich skierowanych przeciwko państwom podejrzanym o wspieranie terroryzmu[11].

„Propozycja skierowania wszelkich działań hakerskich na organizacje i państwa wspierające terroryzm.

---

[11] *http://www.3d.shnet.pl/abi/index.php*

1. *Wytypować potencjalne cele, to jest: strony zawierające treści popierające działania terrorystyczne, strony państw popierających terroryzm jak Irak, Libia, Syria itp. Potencjalne IP mogłyby być gromadzone na ogólnodostępnej stronie (każdy mógłby dodać podejrzany adres, który byłby weryfikowany i klasyfikowany przez wybraną grupę osób koordynujących działania).*
2. *Opracowanie metod jakimi można by dokonać ataków.*
3. *Znalezienie osób, które zajęłyby się upowszechnianiem akcji w Internecie: sformułowanie maili po polsku i angielsku i rozsyłanie ich, tworzenie stron informacyjnych, itp.*
4. *Po znalezieniu wystarczającej liczby osób (mniej lub bardziej znających się na rzeczy) i wyposażeniu jej w odpowiednie oprogramowanie w miarę potrzeb rozpoczęcie "bombardowania" obcych serwerów.*

Celem akcji byłoby całkowite sparaliżowanie a docelowo wyeliminowanie potencjalnych celów (serwerów). Z powodu skomplikowania operacji niezbędna byłaby międzynarodowa współpraca."

Fakt istnienia zagrożeń terrorystycznych z wykorzystaniem Internetu nie podlega dyskusji i wydaje się, że są one coraz większe ze względu na to, że zachłyśnięcie się możliwościami tego medium spowodowało osłabienie czujności odpowiednich służb i nie w pełni uświadomiono sobie jaki może być wpływ łatwego komunikowania się na sprawność grup przestępczych. Wydarzenia z 11 września 2001 roku wskazały, że terroryści potrafią posługiwać się informacją do swoich celów a dotychczasowe doświadczenia z atakami na elementy ważnych systemów informacyjnych świadczą o tym, że należy się bardzo poważnie liczyć z możliwością ataku na dużo większą skalę.

Załącznik

Ustawy

1. o ochronie informacji niejawnych z 22.01.1999r. – zasady ochrony informacji stanowiącej tajemnicę państwową lub służbową
2. o ochronie danych osobowych z 29.08.1997r. – zasady postępowania z danymi osobowymi
3. o ochronie osób i mienia
4. o ochronie praw autorskich
5. o łączności
6. prawo bankowe
7. kodeks handlowy i cywilny
8. umowa o bezpieczeństwie między rządem RP i NATO
9. o zwalczaniu nieuczciwej konkurencji

Rozporządzenia

1. Ministra SWiA z 3.06.98 w sprawie określenia warunków technicznych i organizacyjnych jakim powinny odpowiadać SI, w których przetwarzane są dane osobowe;
2. Ministra SWiA z 9.02.99 w sprawie stanowisk i rodzajów prac zleconych w organach administracji rządowej, których wykonywanie może łączyć się z dostępem do informacji niejawnych stanowiących tajemnicę państwową;
3. Ministra SWiA z 9.02.99 w sprawie organizacji kancelarii tajnych;
4. Ministra SWiA z 9.02.99 w sprawie wzorów kwestionariusza bezpieczeństwa przemysłowego;
5. Prezesa RM z 25.02.99 w sprawie szczegółowego trybu funkcjonowania Komitetu Ochrony Informacji Niejawnych;
6. Prezesa RM z 25.02.99 w sprawie szczegółowego zakresu, warunków i trybu współdziałania organów, służb i innych państwowych jednostek organizacyjnych ze służbami ochrony państwa w toku postępowań sprawdzających
7. Prezesa RM z 25.02.99 w sprawie szczegółowego trybu prowadzenia przez SOP (Służby Ochrony Państwa) kontroli w zakresie Ochrony Informacji Niejawnych stanowiących tajemnicę państwową;

8. Prezesa RM z 25.02.99 w sprawie sposobu i trybu udostępniania danych z ewidencji;
9. Prezesa RM z 25.02.99 w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych;
10. Ministrów SWiA oraz ON z 26.02.99 w sprawie sposobu oznaczania materiałów, w tym klauzulami tajności oraz sposobu umieszczania klauzul na tych materiałach;
11. Ministrów SWiA oraz ON z 26.02.99 w sprawie trybu i sposobu przyjmowania, przewożenia, wydawania i ochrony materiałów.

Wykaz norm ustanowionych w NKP nr 182 ds. Zabezpieczenia Systemów i Ochrony Danych

Lp.	Numer i tytuł normy	Nr uchwały PKN	Data ustanow.
1.	**PN-I-02000:1998** Technika Informatyczna - Zabezpieczenia w systemach informatycznych - Terminologia	2/98	1998.01.07
2.	**PN-I-13335-1:1999** Technika informatyczna - Wytyczne do zarządzania bezpieczeństwem systemów informatycznych - Pojęcia i modele bezpieczeństwa systemów informatycznych	3/99	1999.01.28
3.	**PN-ISO 8372:1996** Przetwarzanie informacji - Tryby pracy algorytmu szyfrowania bloków 64-bitowych	50/96	1996.12.30
4.	**PN-ISO 9160:1997** Przetwarzanie informacji - Szyfrowanie danych - Wymagania dotyczące współpracy w warstwie fizycznej	11/97	1997.03.20
5.	**PN-ISO/IEC 9796:1997** Technika informatyczna -. Techniki zabezpieczeń - Schemat podpisu cyfrowego z odtwarzaniem wiadomości	45/97	1997.12.19
6.	**PN-ISO/IEC 9797:1996** Technika informatyczna - Techniki zabezpieczeń - Mechanizm integralności danych wykorzystujący kryptograficzną funkcję kontroli z algorytmem szyfrowania blokowego	4/96	1996.02.16
7.	**PN-ISO/IEC 9798-1:1996** Technika informatyczna - Techniki zabezpieczeń. Mechanizmy uwierzytelniania podmiotów - Model ogólny	27/96	1996.07.17
8.	**PN-ISO/IEC 9798-2:1996** Technika informatyczna - Techniki zabezpieczeń. Uwierzytelnianie podmiotów -. Mechanizmy wykorzystujące symetryczne algorytmy szyfrowania	50/96	1996.12.30
9.	**PN-ISO/IEC 9798-3:1996** Technika informatyczna - Techniki	4/96	1996.02.16

Lp.	Numer i tytuł normy	Nr uchwały PKN	Data ustanow.
	zabezpieczeń. Mechanizmy uwierzytelniania podmiotów - Uwierzytelnianie podmiotów z wykorzystaniem algorytmu klucza publicznego		
10.	**PN-ISO/IEC 9798-4:1997** Technika informatyczna - Techniki zabezpieczeń. Uwierzytelnianie podmiotów - Mechanizmy wykorzystujące kryptograficzną funkcję kontrolną	10/97	1996.03.12
11.	**PN-ISO/IEC 10116:1996** Technika informatyczna - Tryby pracy algorytmu szyfrowania bloków n-bitowych	50/96	1996.12.30
12.	**PN-ISO/IEC 10118-1:1996** Technika informatyczna - Techniki zabezpieczeń. Funkcje skrótu - Postanowienia ogólne	3/96	1996.02.05
13.	**PN-ISO/IEC 10118-2:1996** Technika informatyczna - Techniki zabezpieczeń. Funkcje skrótu - Funkcje skrótu wykorzystujące n-bitowy algorytm szyfrowania blokowego	4/96	1996.02.16
14.	**PN-ISO/IEC 10118-3:1999** Technika informatyczna - Techniki zabezpieczeń. Funkcje skrótu - Dedykowane funkcje skrótu	47/99	1999.12.09
15.	**PN-ISO/IEC 11770-1:1998** Technika informatyczna -. Techniki zabezpieczeń. Zarządzanie kluczami - Struktura	52/98	1998.12.10
16.	**PN-ISO/IEC 11770-2:1998** Technika informatyczna -. Techniki zabezpieczeń. Zarządzanie kluczami - Mechanizmy z zastosowaniem technik symetrycznych	53/98	1998.12.28
17.	**PN-ISO/IEC 11770-3:2000** Technika informatyczna -. Techniki zabezpieczeń. Zarządzanie kluczami - Mechanizmy z zastosowaniem technik asymetrycznych	13/2000	2000.04.25
18.	**PN-ISO/IEC 13888-1:1999** Technika informatyczna - Techniki zabezpieczeń. Niezaprzeczalność - Model ogólny	47/99	1999.12.09
19.	**PN-ISO/IEC 13888-2:1999** Technika informatyczna - Techniki zabezpieczeń. Niezaprzeczalność - Mechanizmy wykorzystujące techniki symetryczne	47/99	1999.12.09
20.	**PN-ISO/IEC 13888-3:1999** Technika informatyczna - Techniki zabezpieczeń. Niezaprzeczalność - Mechanizmy wykorzystujące techniki asymetryczne	47/99	1999.12.09
21.	**PN-ISO/IEC 14888-1:2000** Technika informatyczna - Techniki zabezpieczeń. Podpisy cyfrowe z załącznikiem – Opis ogólny	28/2000	2000.09.21

Stan na 27 lutego 2001

Standardy międzynarodowe

1. ISO-15408 - Wspólne kryteria).
2. ISO-17799 - Technika informatyczna – Praktyczne zasady zarządzania bezpieczeństwem informacji.

Bibliografia

1. Adamski A.: Prawo karne komputerowe.
2. Adamski A.: Przestępstwa komputerowe w nowym kodeksie karnym.
3. Denning D. E.: Wojna informacyjna i bezpieczeństwo informacji.
4. Dudek A.: Nie tylko wirusy.
5. Garfinkel S., G. Spafford: Bezpieczeństwo w Unixie i Internecie.
6. Kaeo M.: Tworzenie bezpiecznych sieci.
7. Kifner T.: Polityka bezpieczeństwa i ochrony informacji.
8. Liderman K.: Bezpieczeństwo informacji w systemach komputerowych.
9. Stallings W.: Ochrona danych w sieci i intersieci.

1.7. WARTOŚĆ INFORMACJI W SYTUACJACH KRYZYSOWYCH I KONFLIKTOWYCH

Jak dotychczas nie powstała pełna jakościowa teoria informacji i można wyrazić wątpliwość, czy istnieją szanse na jej stworzenie. Jest to spowodowane wielością i różnorodnością funkcji, które informacja spełnia, zwłaszcza między ludźmi[1].

Istnieje wiele modeli odwzorowujących jakościowe aspekty informacji, przy czym modele te stanowią mniej lub bardziej wyspecjalizowane ujęcia informacji, a w ramach tych ujęć - różne sposoby ich opisu. Jednym z tych ujęć - modeli jest **infologia**[2].

Obszar zainteresowań infologii obejmuje[3]:

- wyjaśnianie znaczenia[4] (wartości) informacji w aspekcie użytkowym;
- badanie i wyjaśnianie własności informacji;
- analizę żądań użytkownika, kierowanych pod adresem informacji;
- poszukiwanie metod i sposobów zapewnienia przez informację żądań, formułowanych przez użytkownika.

Przy tak sprecyzowanych obszarach zainteresowań infologii należy zwrócić uwagę na dwa problemy:

1. Badanie czynników, od których zależy nadawanie przez człowieka znaczenia informacji w momencie jej stosowania.
2. Rozróżnienie pewnych klas tych czynników (a że tylko człowiek postrzega i generuje informacje oraz decyduje, czynniki te dotyczą):
   - osobowości człowieka i jej wpływu na kształtowanie znaczenia informacji (*psychologiczne czynniki znaczenia informacji*);
   - rodzaju, siły i kierunku interakcji między ludźmi i wpływu tych interakcji na kształtowanie się znaczenia informacji (*socjologiczne uwarunkowania znaczenia informacji*);
   - języka, w którym wyrażana jest informacja, co wprowadza ograniczenia poznawcze, tkwiące w samej konstrukcji języka używanego do przedstawienia informacji (*językowe uwarunkowania znaczenia informacji*);

---

[1] *Flakiewicz W., Informacyjne systemy zarządzania, PWE 1990, s. 15.*
[2] *Za jej twórców uważani są B. Sundgren i B. Langefors, którzy rozwijali ją w latach -pięćdziesiątych.*
[3] *Stefanowicz B., Jakość informacji w ujęciu infologicznym, "Wiadomości Statystyczne" 1987, nr 1.*
[4] *termin ten można utożsamiać z takimi pojęciami, jak: sens, wartość, istotność, walor, waga danej informacji. W tej pracy będziemy używać pojęcia wartości i znaczenia.*

- znaczenia informacji jako procesu nadania (określenia) jej sensu i istotności dla człowieka (*semantyczne uwarunkowania znaczenia informacji*);
- organizacji informacji w postaci ich strumieni i systemów informacyjnych (*systemowy punkt widzenia na rolę informacji odgrywaną przez nią w ramach systemu, w którym funkcjonuje*).

Wszystkie te czynniki występują łącznie, w różnych interakcjach, które wyznaczają znaczenie informacji nadawanej jej przez człowieka.

Wydaje się zatem, że tak pojęte wieloaspektowe ujęcie znaczenia informacji nie może być wyjaśnione całkowicie i jednoznacznie. Albowiem informacja i jej własności muszą być rozważane na tle nieskończonej różnorodności możliwych stanów rzeczywistości, do której się one odnoszą. Nadto złożoności tej rzeczywistości, w której wykrycie nowych związków może w sposób istotny zmienić znaczenie informacji. Niemniej za pomocą informacji możemy odwzorować (*homomorficznie*) interesujące nas stany świata i na podstawie tego odwzorowania oraz opartego na nim wnioskowania (decydowania[5]) wyznaczyć kierunek, siłę i treść podejmowanych przedsięwzięć.

Zasadne zatem będzie sformułowanie, że: **znaczenie (wartość) informacji oznacza zawsze znaczenie (wartość) dla określonego podmiotu**.

---

[5] *Z punktu widzenia podejmowania decyzji w różnych matematycznych modelach decyzyjnych E. Kofler określa wartość informacji jako wartość przejścia z jednej sytuacji decyzyjnej do drugiej sytuacji decyzyjnej. Patrz E. Kofler, O wartości informacji, Rozprawy UW, PWN, 1968. W szczególności rozważa problemy decyzyjne w warunkach niepewności, ryzyka i konfliktowych. Uważa, że "*każda gra z naturą - to także gra o informację. Fakt ten znajduje pełne odbicie w naszej rzeczywistości. Cała nasza cywilizacja, cała nasza kultura materialna i duchowa - to wynik ciągłych gier ludzkości z naturą, a na każdym etapie rozwoju ludzkości - poziom cywilizacji jest funkcją posiadanych na tym etapie przez ludzkość informacji o strategiach natury.*" E. Kofler, Gry w N.N. Worobiew, E. Kofler, H. Greniewski, Strategia gier, KiW, 1969, s. 73.*

1.7.1. Informacja i jej własności

W literaturze przedmiotu znajdujemy wiele prób definiowania pojęcia ***informacji***. Wszystkie one nie są jednak zadowalające. Dla konkretyzacji przytoczymy najważniejsze[6]:

"**Informacja** - zbiór wiadomości o faktach, zdarzeniach, cechach przedmiotów itp. ujęty i podany w takiej formie, że pozwala odbiorcy (człowiek, maszyna) ustosunkować się do zaistniałej sytuacji i podjąć odpowiednie działanie".[7]

"**Informacja** określa znaczenie (treść), jakie przy zastosowaniu odpowiedniej interpretacji [...] przypisuje się wiadomościom [...]. Wiadomością będzie każdy przekaz o określonym znaczeniu, wysłany i odbierany w świecie materii ożywionej i nieożywionej"[8].

"**Informację** utożsamia się ze znaczeniem (treścią), jakie, przy odpowiedniej konwencji, przyporządkowuje danym [...] każdy czynnik, który może być subiektywnie wykorzystany do celowego działania. Informacje to dane wykorzystywane do celowego działania"[9].

"**Informacja** - myśl, którą reprezentują dane"[10].

"**Informacja** - to wiadomość mająca formę danych"[11].

"**Informacja** to znaczenie (treść), jakie przy zastosowaniu odpowiednich konwencji przyporządkowuje się danym"[12].

I jeszcze inna, (nieoczekiwanie odmienna)[13]: "***informacja*** *to materialne odwzorowanie porcji energii, zewnętrznej w stosunku do podmiotu walki zbrojnej, przybliżające ów podmiot do jednego ze stanów końcowych tej walki*"[14].

---

[6] *Obszerny przegląd definicji pojęcia informacji znajdziemy w: Stefanowicz B., Informacyjne Systemy Zarządzania, wyd. SGH, 1998.*
[7] *Poradnik ekonomistów. Informatyka, wyd.2 PWE,1982, s. 589*
[8] *Zarys informatyki dla ekonomistów, pr. zb. p. red. A. Nowickiego, 1985, s. 17.*
[9] *Kierzkowski Z., Elementy informatyki, PWN, 1976, s. 15.*
[10] *Naur P., Zarys metod informatyki, WNT, 1979, s. 16.*
[11] *Wstęp do informatyki w zarządzaniu, pr. zb. p. red. T. Wierzbickiego, PWN, 1976, s. 10.*
[12] *Informatyka w zarządzaniu, pr. zb. p. red. T. Wierzbickiego, PWN, 1986, s.9.*
[13] *Nieoczekiwana, albowiem Wiener w swoim podstawowym dziele (*Cybernetics or Control and Communication in the Animal and the Machine, *New York, Wiley 1948) nie wypowiada się na temat czym jest informacja, ograniczając się jedynie do wyrażenia poglądu, czym informacja nie jest. "*Mechaniczny mózg nie wydziela myśli, jak wątroba wydziela żółć, zdaniem dawniejszych materialistów, ani też nie wydaje jej w postaci energii, jak robi to mięsień w swoim działaniu. Informacja jest informacją, a nie materia ani energią"
[14] *R. Kwećka, Informacja w walce zbrojnej, AON, 2001, s. 28.*

Można zatem powiedzieć, że informacja to treść komunikatu:

$$K = <O, X, x, t>$$

gdzie: **K** – komunikat;

O – obiekt;

X - cecha (atrybut) obiektu **O**;

x - wartość (realizacja) cechy **X**;

t - czas w którym cecha **X** obiektu **O** przyjmuje wartość **x**.

Informacja cechuje się następującymi własnościami:

- jest obiektywna (tzn. niezależna od obserwatora);
- jest synergiczna (tzn. przejawia cechy współdziałania z innymi informacjami);
- jest różnorodna;
- jest zasobem niewyczerpywalnym;
- może być powielana i przenoszona w czasie i przestrzeni;
- może być przetwarzana bez jej zatarcia (zniszczenia);
- ta sama informacja może mieć różne znaczenie dla różnych odbiorców (subiektywność odbioru);
- każda jednostkowa informacja opisuje tylko jedną cechę obiektu.

Informacja spełnia wiele różnorodnych funkcji w życiu społeczeństw i jednostek. Można wymienić następujące zasadnicze jej funkcje:[15]

- ***modelowania (opisywania)***, może być obrazem rzeczywistości, miarą złożoności i różnorodności badanego wycinka rzeczywistości;
- ***decyzyjna***, może motywować do działania, a więc osiągania pewnych celów;
- ***sterująca***: buduje się systemy informatyczne (bazy wiedzy i bazy danych) stanowiące podstawę planowania i podejmowania optymalnych lub racjonalnych decyzji;
- ***rozwoju wiedzy (cywilizacji)***: dane → informacja → wiedza → mądrość,
- ***kapitałotwórcza*** obok ziemi, kapitału i pracy;
- jest ***towarem;***
- pełni rolę ***kulturotwórczą***.

Wśród wielu propozycji formalnej definicji informacji warto zauważyć ujęcie Langerfors'a[16], który zaproponował podejście umożliwiające formalne zdefiniowanie informacji w postaci:

$$I = i(D, S, t)$$

gdzie:

D - reprezentacja informacji I w postaci danych (e- lub z- układu)[17];

S - układ informacyjny człowieka, który postrzega lub generuje informację **I**;

t - czas dostępny dla interpretacji i wnioskowania przez człowieka postrzegającego (generującego informację);

I - informacja przenoszona przez **D**;

i - funkcja informacyjna.

Zatem **informacja jest zindywidualizowaną interpretacja i zindywidualizowanym wnioskowaniem, odnoszącymi się do takiej konfiguracji danych, które tworzą łącznie ich e-układ**. Wynika stad, że ponieważ:

- **S** jest układem dynamicznym, a więc ta sama **D** może nieść różne **I** dla podmiotu w różnych momentach czasu;
- ze względu na zróżnicowanie **S**, te same **D** mogą przy stałym momencie czasu **t** nieść różne **I** dla różnych podmiotów;
- nie ma możliwości projektowania **I**[18], a jedynie można projektować **D**, zgodnie z celem i programem obserwacji rzeczywistości pozajęzykowej jako reprezentację informacji odwzorowującej tę rzeczywistość wyrażona w języku danych;
- nie ma możliwości takiego badania **I**, aby w oparciu o definiowane czynniki można było jednoznacznie opisać zarówno samą **I**, jak też tworzone przez nią *strumienie informacyjne* i w konsekwencji *systemy informacyjne*.

---

[15] *Dlatego ocena jej wartości z punktu widzenia decyzyjnego jest jedynie oceną jednoaspektową, a nie oceną w ogóle.*

[16] *Langefors B., Infological Models and Information User Views, "Information Systems" 1980, vol. 5.*

[17] *e-układ jest elementarnym układem danych, tj. takim doborem danych, że traktowany jako całość staje się źródłem informacji. Formalnie oznacza to, że jeżeli* ***x*** *stanowi n - krotność obiektów (n=1, 2, 3, ...),* ***y*** *jest własnością lub relacją, a* ***z*** *jest czasem, wtedy trójka* ***<x, y, z>*** *nazwana jest* elementarnym układem, e-układem.

[18] *Informacja jest zawsze* ***czyjąś*** *informacją. Należy zauważyć, że przetwarzanie informacji jest wyłączną domeną człowieka. Dlatego w systemach informatycznych mamy do czynienia tylko z przetwarzaniem* ***danych****, a nie przetwarzaniem informacji.*

Ponieważ samo pojęcie informacji jest pojęciem względnym, tym bardziej charakterystyka tego pojęcia będzie mocno utrudniona. Dlatego pojęcie jakości informacji jest tak ogólne, że na ogół nie próbuje się go nawet określać wprost, lecz pośrednio - przez cechy przynależące temu pojęciu oraz wielokryterialne - przez co enumeracja tych cech jest na ogół różnorodna (co do proponowanego nazewnictwa i poziomu abstrakcji). Oto lista cech informacji determinujących jej jakość[19]:

- agregacja (poziom syntezy informacji);
- aktualność (zgodność treści informacji z rzeczywistym stanem procesu w danym momencie czasu);
- celowość (zdolność do wyznaczania norm sterujących w procesie sterowania);
- cenność (wartość) (spowodowanie zmiany cenności sytuacji decyzyjnej);
- decyzyjność (stopień wpływu na przebieg procesu decyzyjnego);
- dokładność (stopień uwzględnienia szczegółów w treści informacji);
- dostępność (możliwość korzystania z informacji w odpowiednim miejscu i czasie przez jej odbiorcę);
- efektywność (zdolność do wywołania określonych, istotnych dla użytkownika efektów);
- elastyczność (zdolność do zaspokojenia różnych potrzeb użytkownika);
- ilość (zmniejszenie niepewności w sytuacji decyzyjnej);
- jednoznaczność (stosowanie jednoznacznego języka i precyzyjnie określonych pojęć);
- kompletność (użytkownik nie jest zmuszony sięgać po informacje dodatkowe);
- komunikatywność (ilość pracy niezbędnej dla nadania jej przez odbiorcę formy umożliwiającej wnioskowanie i podjęcie decyzji);
- kosztowność (poziom nakładów finansowych na zdobycie lub sukcesywne uzyskiwanie informacji);
- objętość (wielkość obszaru niezbędnego do zapisania informacji w pamięci komputera lub na nośniku);
- opłacalność (różnica między cennością i kosztem informacji);

[19] *M. Niedźwiedziński, Cechy informacji - próba systematyzacji, "Systemy Informatyczne", 1987, nr 1.*

- pełność (stopień likwidacji niepewności decydenta w procesie zarządzania);
- porównywalność (możliwość porównania informacji z innymi informacjami);
- pracochłonność (wielkość nakładów pracy poniesionych na uzyskanie i wykorzystanie informacji);
- prawdziwość (zgodność treści informacji z rzeczywistym przebiegiem opisywanego przez nią zdarzenia);
- precyzyjność (stopień jednoznaczności terminologii użytej przez informację);
- prospektywność (stopień antycypacji przebiegu planowanych zdarzeń),
- przydatność (zmiana prawdopodobieństwa osiągnięcia celu, wynikła z dysponowania informacją);
- przyswajalność (objętościowy zakres informacji, który jest w stanie efektywnie wykorzystać decydent),
- redundancja (stopień nadmiarowości informacji nie wpływający na jej wzbogacenie);
- retrospektywność (informacja zwrotna o warunkach uprzednio podjętych decyzji);
- rozwlekłość (możliwość dodatkowego uzupełnienia informacji np. o walorach dydaktycznych);
- rzetelność (brak zniekształceń intencjonalnych w treści informacji);
- sensowność (ograniczenie różnorodności zachowania się systemu);
- szybkość (odstęp czasu od momentu zaistnienia zdarzenia do momentu otrzymania informacji o tym zdarzeniu);
- wiarygodność (brak deformacji informacji);
- wiek (odstęp czasu między momentem zaistnienia zdarzenia a momentem wykorzystania informacji);
- wierność (informacja o zbiorze oryginałów jest taka sama, jak w zbiorze obrazów);
- źródłowość (pochodzenie informacji z (bezpośredniej lub pośredniej) obserwacji).

J. Kisielnicki[20], dla porównania, wymienia następujące cechy informacji, wyodrębnione ze względu na kryteria:

- kryteria minimalne: dyspozycyjność(dostępność do każdej informacji istniejącej w systemie), aktualność (prawdziwość - informacja powinna dotyczyć obecnego stanu rzeczywistości), rzetelność (informacja nie powinna być półprawdą lub wprowadzać użytkownika w błąd), straty informacyjne (ilościowe różnice między informacja pierwotną a otrzymywaną przez użytkownika), porównywalność (możliwość przeprowadzenia analiz porównawczych);
- kryteria optymalizujące: niezawodność (każdy element systemu informatycznego należy tak projektować, aby zwiększyć niezawodność), przetwarzalność (określenie funkcji postaci danych i form ich przetwarzania), elastyczność (zdolność systemu informatycznego do reagowania na zmiany), wydajność (zdolność systemu informatycznego do przesyłania i przetwarzania w sensie fizycznym określonej ilości informacji w danej jednostce czasu), koszt (koszty finansowe systemu informatycznego), czas reakcji (czas oczekiwania na informację lub terminowość), szczegółowość (stopień uszczegółowienia informacji), stabilność (stopień odporności na zakłócenia), aktywność (częstość korzystania z informacji), priorytetowość (zdolność zajmowania się informacjami o różnym priorytecie), poufność (dostępność różnych grup użytkowników), łatwość użytkowania (przezwyciężalność barier psychofizycznych przez użytkowników), bezpieczeństwo informacji (możliwość całkowitego lub częściowego odtworzenia informacji), wymagania specjalne (różne, w zależności od bieżących potrzeb i decyzji).

Z przedstawionych treści wynika, że sposób doboru oraz rozumienia treści każdej wyróżnionej cechy jakości informacji jest pod wpływem zarówno cech osobowościowych użytkownika, jak i celu badawczego danej rzeczywistości pozajęzykowej. Dlatego **jakość** (najszerzej rozumiane określenie nie ilościowe, ale jakościowe) **informacji jest pojęciem względnym**.

---

[20] *Kisielnicki J., Kryteria jakości systemów informatycznych funkcjonujących w gospodarce narodowej, "Systemy Informatyczne", 1987, nr 1.*

1.7.2. Badania ilościowe informacji

Z przedstawionych powyżej treści wynika, że poprawne określenie ilościowych miar wartości (znaczenia) informacji w ogóle jest raczej niemożliwe. Można natomiast próbować identyfikować i operacjonalizować zależności pomiędzy efektywnością systemu działania a jakością jego podsystemu zarządzania. Aby wyrazić je *explicite* należy skłonić się do refleksji nad jakościowymi cechami informacji. Uważa się, że badanie procesów informacyjnych w systemach działania (ogólniej - w systemach socjotechnicznych) powinno obejmować przede wszystkim pragmatyczne problemy informacji, a więc ich **wartość**, **użyteczność i jakość**. Warunkiem ilościowego wyrażania powyższych cech jest określenie systemu aksjologicznego, zaś ocena powinna być zrelatywizowana do konkretnego użytkownika (odbiorcy) informacji. Rozpatrywanie informacji w ten sposób jest po prostu, konsekwencją przyjętych informacyjnych uwarunkowań procesu decyzyjnego.

Ogólnie biorąc pojęcie wartości informacji wiąże się z możliwością jej wykorzystania przez celowo działającego odbiorcę. Informacje *„uzyskują"* swą wartość w procesach praktyki społecznej (praktyki informacyjnej).

Badania naukowe wartości (jakości, użyteczności) informacji rozpoczęły się znacznie później niż badania ilości informacji zapoczątkowane matematyczną teorią informacji C. Shannona, jednakże w ostatnim okresie stały się od nich rozleglejsze i bardziej zróżnicowane. Nie oznacza to jednak, że w chwili obecnej istnieje jedna jakościowa teoria informacji porównywalna pod względem kompletności, spójności itp. z teorią ilościową. Stan omawianych badań jest mianowicie taki, że istnieje wiele koncepcji i teorii, posługujących się bardzo zróżnicowaną terminologią i różnym aparatem formalnym, różnie interpretujących to samo pojęcie wartości, użyteczności i jakości informacji [1]. Interesujący w kontekście niniejszych rozważań wydaje się być następujący pogląd [2]: *„Komunikaty, jakie otrzymuje osobnik, można rozpatrywać z punktu widzenia ich wartości obiektywnej i ich wartości emocjonalnej. Wartość obiektywna jest miarą tego, w jakim stopniu informacje zawarte w komunikacie wzbogacają wiedzę osobnika. Wartość emocjonalna jest miarą tego, w jakim stopniu informacje zawarte w komunikacie są potrzebne osobnikowi, odpowiadają zapotrzebowaniom. Wyrazem zapotrzebowania na informacje zwarte w komunikacie jest reakcja emocjonalna towarzysząca recepcji komunikatu ... im uboższymi informacjami*

o świecie dysponuje osobnik, tym większą rolę w jego działaniu odgrywa aspekt emocjonalny komunikatu".

Dla rozważań nad efektywnością systemów zarządzania istotne znaczenie mieć będzie następujące sformułowanie ogólnego pragmatycznego problemu informacji: **jak skutecznie otrzymywane informacje wpływają na efektywność zarządzania, a w konsekwencji i efektywność systemu działania. Zatem rozpatrywać będziemy pojęcia użyteczności i jakości informacji, aby przejść do zdefiniowania pojęcia wartości informacji**.

1.7.3. Użyteczność informacji

Jedno z pierwszych i najpopularniejszych ujęć zagadnienia użyteczności (przydatności) informacji w procesie podejmowania decyzji jest ujęcie A. Charkiewicza[21]. Zgodnie z tą propozycją użyteczność ***U*** informacji ***J*** określa zależność:

$$U(J) = \log_2 \frac{P_1}{P_0}$$

gdzie:

P_0 – prawdopodobieństwo osiągnięcia celu działania przed otrzymaniem ocenianej informacji ***J***;

P_1 – prawdopodobieństwo osiągnięcia celu po otrzymaniu informacji ***J***.

Ujęcie powyższe w pełni oddaje pragmatyczny sens informacji wykorzystywanej w procesie działania.

Określenie 1. **UŻYTECZNOŚCIĄ INFORMACJI** NAZYWA SIĘ WŁAŚCIWOŚĆ WYRAŻAJĄCĄ WPŁYW INFORMACJI NA TRAFNOŚĆ PODEJMOWANYCH DECYZJI (SKUTECZNOŚĆ ZARZĄDZANIA).

Cecha informacji zwana użytecznością związana jest z problem decyzyjnym, rozpatrywanym np. w konwencji tzw. psychologicznej teorii decyzji [4] przyjmuje się bowiem, że wszelka informacja, która niewiedzę decydenta częściowo lub całkowicie redukuje jest z jego punktu widzenia pożądana, czyli użyteczna, zaś jej znaczenie

---

[21] *A. Charkiewicz*, O ciennosti informacii, *[w:] Izbrannyje trudy, t.3, nauka, Moskwa 1973. Zob. także L. Kuleszyński [3] gdzie przedstawiono bardzo interesujący przykład wojskowego zastosowania wzoru Charkiewicza.*

zależy od konkretnego problemu decyzyjnego[22]. Z pewnością mniej użyteczna jest informacja wówczas, gdy przy każdym stanie rzeczy skutki działania niewiele się między sobą różnią co do efektywności, niż – gdy są one pod tym względem drastycznie zróżnicowane.

W rozważaniach o użyteczności informacji można przyjąć następujący ogólny model (Sienkiewicz [7]):

Niech obiekt zarządzania charakteryzowany jest za pomocą:

a) funkcji działania:

$$G: X \times D \rightarrow Y$$

b) funkcji efektywności:

$$F: X \times Y \times D \rightarrow E$$

funkcjonowanie systemu decyzyjnego opisuje przekształcenie:

$$P: V \times J \rightarrow D$$

zaś systemu informacyjnego:

$$H: S \rightarrow J$$

oraz:

$$\eta: X \times Y \times Z \rightarrow S$$

Zakłada się, że decydent podejmować może decyzje w dwóch skrajnych sytuacjach:

- w sytuacji dysponowania określonymi informacjami, czyli zgodnie z funkcją ***P***;
- w sytuacji braku tych informacji, a więc zgodnie z funkcją:

$$\pi: W \rightarrow D', \; J = \phi.$$

Użyteczność informacji ***J*** osiągnięta dzięki decyzji $d \in D$, gdy zachodzi stan rzeczy $s \in S$ taki, że $H(s) = i \in J$, zaś koszty związane z realizacją procesów informacyjnych wynoszą χ, określa się w sposób następujący:

$$U(d,s) = \sum_{s \in S} F[s, P(v, H(s))] p_s(i) - \chi,$$

gdzie: $p_s(i)$ – prawdopodobieństwo otrzymania przez system decyzyjny informacji $i \in J$, gdy zachodzi stan $s \in S$.

Dla drugiej z wyróżnionych sytuacji użyteczność określa funkcja:

---

[22] *Zatem użyteczność informacji jest pojęciem względnym. Jego względność polega na tym, że musimy wiązać informację z określonym układem odniesienia np. określoną sytuacją decyzyjną.*

$$U(d',s)=\sum_{s\in S}F[s,\pi(v)]p_s(v)$$

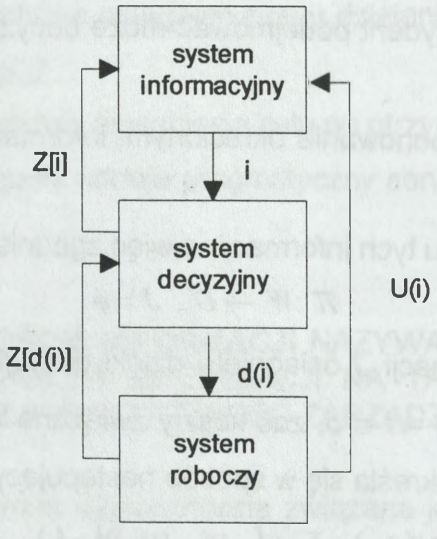
gdzie: $p_s(v)$ – prawdopodobieństwo decyzji nadrzędnej (nadrzędnego systemu decyzyjnego) $v \in V$ przy stanie rzeczy $s \in S$.

Wtedy, można mówić o względnej użyteczności informacji np. w sensie maksymalizacji minimalnej użyteczności bezwzględnej (kryterium maxmin Walda):

$$U(i)=\max_{d}\min_{s}U(d,s)-\max_{d'}\min_{s}U(d',s)$$

Powyższe ujęcie użyteczności informacji posiada sens tylko wtedy, gdy istnieją warunki niepewności. W przypadku, gdy $J \equiv S$ mamy do czynienia z tzw. informacją doskonałą.

Użyteczność informacji (rysunek 7.1) może być wyrażana poprzez efektywność systemu. Zakłada się, że efektywność uzyskana wskutek podjęcia przez system decyzyjny decyzji $d(i)$ na podstawie informacji i otrzymanej z systemu informacyjnego wyniesie $E[d(i)]$, natomiast w przypadku jej nie otrzymania wyniesie $E(d)$. Użyteczność i-tej informacji z punktu widzenia systemu decyzyjnego wyniesie wtedy $E_i = E[d(i)] - E[d]$.



Rysunek 7.1. Schemat analizy użyteczności informacji w systemie zarządzania.

Ponadto przyjmuje się, że system informacyjny uzyskuje pewien zysk $Z[i]$ po udostępnieniu i-tej informacji, który wyniesie $Z_0[i]$, gdy ta informacja nie zostanie udostępniona. Wtedy użyteczność "brutto" informacji i z punktu widzenia systemu informacyjnego wyniesie:

$$Z_i = Z[i] - Z_0[i]$$

Jeżeli koszty przesyłania i przetwarzania informacji ***i*** wynoszą ***K[i]***, zaś koszty systemu bez przetwarzania tej informacji - ***K₀[i]***, to można określić zysk "netto" systemu informacyjnego po udostępnieniu ***i***-tej informacji, jako różnicę: ***Z[i]*** - ***K[i]***, natomiast zysk ten wyniesie ***Z₀[i]*** - ***K₀[i]***, gdy informacja ta nie zostanie udostępniona.

Z punktu widzenia systemu informacyjnego użyteczność informacji ***i***-tej wyniesie:

$$U'(i) = (Z[i] - K(i)) - (Z_0[i] - K_0[i])$$

natomiast z punktu widzenia systemu decyzyjnego:

$$U^D(i) = (E[d(i)] - Z(i)) - (E[i] - \chi_0)$$

gdzie: χ_0 – stałe koszty funkcjonowania systemu decyzyjnego.

Ogólną użyteczność i-tej informacji określa się jako *„wartość dodatkową"* wytworzoną przez system informacyjny:

$$U(i) = U'(i) - U^D(i)$$

Jeżeli ***J*** oznacza zbiór typów informacji udostępnionych w danym okresie czasu, a λ_i - intensywność udostępniania informacji typu ***i*** (***i*** $\in$ ***J***), to wtedy średnia całkowita użyteczność informacji udostępniana przez system informacyjny w okresie czasu **T** wyniesie:

$$\overline{U} = \sum_{i \in J} \lambda_i \overline{U}(i) T$$

Jeżeli znana jest pożądana użyteczność informacji dla danego systemu zarządzania, np. U^* to wtedy najprostszy sposób oceny użyteczności informacji jest następujący:

$$\Xi[U] = \begin{cases} 1 \quad (aprobata), & gdy \quad U \geq U^*, \\ 0 \quad (dezaprobata), & gdy \quad U < U^*. \end{cases}$$

Ogólnie, użyteczność informacji ***J*** uzależniona jest od organizacji procesów decyzyjnych (funkcja ***P***) i organizacji procesów informacyjnych (funkcja η), czyli:

$$U(J) \equiv U_J(P, \eta),$$

a w związku z tym, użyteczność informacji służyć może jako kryterium wyboru wariantu organizacji procesów decyzyjnych i informacyjnych. Zakłada się przy tym, że istnieje taki wariant P^* i η^*, dla którego spełniony jest warunek:

$$U_J(P^*, \eta^*) \geq U_J(P, \eta),$$

gdzie: $P \subset \{P\}$ i $\eta \subset \{\eta\}$ ($\{P\}, \{\eta\}$ – odpowiednie rodziny funkcji).

Posługując się funkcją $U_J(P, \eta)$ można np. powiedzieć, że proces η_1 jest skuteczniejszy od procesu η_2 tylko wtedy, gdy:

$$U_J(P, \eta_1) > U_J(P, \eta_2).$$

W podobny sposób można porównywać warianty organizacji procesu decyzyjnego (P).

Ocena systemu zarządzania, który charakteryzują funkcje P^0 i ,η^0 może więc być dokonana w następujący sposób (w sensie kryterium maksymalnej użyteczności informacji):

$$\Xi[U(J)] = \begin{cases} 1 \quad (aprobata), & gdy \quad \left[U_J(P^*, \eta^*) - U_J(P^0, \eta^0)\right] \leq \Delta U_J, \\ 0 \quad (dezaprobata), & gdy \quad U_J(P^*, \eta^*) - U_J(P^0, \eta^0) > \Delta U_J. \end{cases}$$

Posługując się funkcją użyteczności informacji można określić warunki wprowadzania do systemu dodatkowej informacji ΔJ. Jeżeli np. system decyzyjny dysponuje pewną informacją J o użyteczności $U(J)$, to problem polega na określeniu takiej informacji dodatkowej, że spełnione zostaną następujące warunki:

$$U(J + \Delta J) > U(J)$$

oraz:

$$U(J + \Delta J) - U(J) > K(\Delta J)$$

gdzie $K(\Delta J)$ - koszt uzyskania informacji dodatkowej ΔJ.

Zgodnie z proponowanym ujęciem, użyteczność informacji ustala się ze względu na problem decyzji oraz kryterium decyzji. Wyraża to tym samym pragmatyczny aspekt informacji. Relatywizacja informacji do kryterium decyzji oznacza, że dla dwóch decydentów stojących wobec tego samego problemu dana informacja może mieć różną użyteczność, jeśli posługują się oni odmiennymi kryteriami podejmowania decyzji, lub też odmiennie oceniają szanse realizacji poszczególnych stanów rzeczy. Decyzja wymaga pewnej dozy arbitralności. I tę jej cechę musi odziedziczyć wszelki sposób wartościowania informacji ze względu na jej pragmatyczną przydatność.

1.7.4. Jakość informacji

Określenie 2. **JAKOŚCIĄ INFORMACJI** NAZWA SIĘ CECHĘ INFORMACJI WYRAŻAJĄCĄ STOPIEŃ SPEŁNIENIA WYMAGAŃ STAWIANYCH PRZEZ SYSTEM DECYZYJNY W ZAKRESIE:

- ✓ AKTUALNOŚCI (TERMINOWOŚCI);
- ✓ PEŁNOŚCI (KOMPLETNOŚCI);
- ✓ NIEZAWODNOŚCI (BEZBŁĘDNOŚCI).

Mówiąc o użyteczności informacji rozpatrywany był wpływ informacji (ściślej jej ilości i/lub znaczenia) na skuteczność decydowania, a więc i na efektywność działania. Obszarem zainteresowań było głównie to, jak zachowuje się decydent w przypadku posiadania określonej informacji i jej braku oraz jakie będą skutki takiego zachowania. Istnieją jednakże czynniki uwarunkowane organizacją systemu informacyjnego, charakterystykami techniczno-eksploatacyjnymi jego elementów (węzłów i kanałów) itp., które w zasadniczy sposób wpływają na określone cechy informacji udostępnionych systemowi decyzyjnemu. Do nich zaliczyliśmy aktualność (α), pełność (β) i niezawodność (γ). Przyjmuje się więc, że jakość informacji $Q(J)$ jest funkcją tych elementów:

$$Q(J) = Q[\alpha(J), \beta(J), \gamma(J)]$$

czyli istnieje przekształcenie:

$$Q : J \rightarrow \Re^{+} \cup \{0\}$$

albo:

$$Q : 2^{J} \rightarrow \Re^{+} \cup \{0\}.$$

Oznacza to, że każdej informacji udostępnionej decydentom można przyporządkować pewną wartość, wyrażającą stopień spełnienia określonych wymagań.

Określenie 3. **AKTUALNOŚĆ** (TERMINOWOŚĆ) JEST CECHĄ INFORMACJI, WYRAŻAJĄCĄ FAKT OTRZYMANIA PRZEZ DECYDENTA INFORMACJI W POŻĄDANYM (WYMAGANYM) CZASIE.

Ogólnie aktualność jako cecha informacji zależy od takich charakterystyk systemu informacyjnego, jak:

- metody zdobywania (zbierania) informacji;
- konfiguracja sieci przesyłania informacji;
- charakterystyki kanałów łączności;
- niezawodność sieci;

- intensywność przepływów informacji (obciążenie elementów systemu).

Niech dla każdej wiadomości (komunikatu) określony jest czas pomiędzy momentem t^0 wystąpienia wiadomości (w źródle informacji) a momentem t^x otrzymania wiadomości przez użytkownika (decydenta), czyli dana jest zmienna losowa $\tau = t^x - t^0$ o znanej funkcji gęstości prawdopodobieństwa $f(t)$, Dla takiego przypadku aktualność informacji określana jest jako prawdopodobieństwo terminowego dostarczenia wiadomości:

$$\alpha(\tau) = P_r\{\tau \le Tg\} = \int_0^{Tg} f(t)dt$$

gdzie ***Tg*** - dopuszczalny (wymagany) czas przebywania wiadomości w systemie informacyjnym.

Jeżeli założy się jednorodność wiadomości przesyłanych, to dla uproszczonego modelu sieci (model Kleinrocka [5]) z pojedynczym kanałem, czas przesyłania wiadomości wyrażany jest w postaci zależności:

$$\tau = [\mu C - \lambda]^{-1}$$

gdzie: **C** – przepustowość kanału;

μ^{-1} – przeciętna długość wiadomości napływających do systemu z prędkością λ.

W tych okolicznościach prostym oszacowaniem aktualności informacji jest wskaźnik:

$$\alpha = \begin{cases} 1, & dla \quad \tau \le Tg, \\ \tau / Tg, & dla \quad \tau > Tg \end{cases}$$

W związku z powyższym:

$$\tau = \tau(\mu, C, \lambda)$$

Rozszerzając ten model o charakterystyki techniczno-eksploatacyjne sieci otrzyma się następującą funkcję:

$$\alpha = \frac{\mu K_g - \lambda}{\frac{1}{T_g}\left(1 + \frac{\mu K_g K_p}{\frac{K_g}{T_g} + \eta}\right) + \mu K_g - \lambda}$$

dla $\frac{\lambda}{\mu K_g} < 1$,

gdzie: K_g - współczynnik gotowości kanału;

K_p - współczynnik przestoju kanału;

η - intensywność odnowy kanału.

Dla złożonego wielofazowego procesu informacyjnego czas τ składa się z następujących odcinków czasu:

1) τ_1 - czas zbierania informacji;
2) τ_2 - czas przesyłania informacji ze źródła do ośrodka przetwarzania;
3) τ_3 - czas przetwarzania informacji;
4) τ_4 - czas przechowywania informacji;
5) τ_5 - czas nawiązywania łączności;
6) τ_6 - czas przesyłania informacji do systemu decyzyjnego;

czyli $\tau = \sum_{i=1}^{6} \tau_i$, przy czym informacja posiadać będzie cechę aktualności, gdy $\tau \le T_g$.

Wyznaczenie zmiennej τ dla tego przypadku jest zadaniem bardzo trudnym, gdyż ma się tu do czynienia z wielofazowym systemem obsługi masowej o zawodnych elementach i nietrywialnych dyscyplinach obsługi (priorytety). Dla oszacowania wskaźnika aktualności α konieczne jest, bądź przeprowadzenie eksperymentów symulacyjnych, bądź oszacowanie poszczególnych czasów, zakładając „z góry" wystąpienie poważnych uproszczeń.

Niekiedy dla określenia aktualności informacji celowym jest wykorzystanie następującej funkcji:

$$\alpha(\tau) = \begin{cases} 1, & dla \quad \tau \le T_{g1}, \\ \dfrac{\tau}{\dfrac{T_{g1}}{T_{g2}}} + \dfrac{T_{g2}}{\dfrac{T_{g2}}{T_{g1}}}, & dla \quad T_{g1} < \tau < T_{g2}, \\ 0, & dla \quad \tau > T_{g2}. \end{cases}$$

gdzie: T_{g1} - maksymalny dopuszczalny czas przebywania informacji w systemie informacyjnym, T_{g2} - minimalny czas przebywania, powyżej którego decydent nie może wykorzystać już otrzymanych informacji.

Dla innego przypadku można wykorzystać funkcję nieliniową, jak np.:

$$\alpha(\tau)=\begin{cases}1, & dla \quad \tau \le T_{g1},\\ \dfrac{\ln\tau}{\ln\dfrac{T_{g1}}{T_{g2}}}+\dfrac{\ln T_{g2}}{\ln\dfrac{T_{g2}}{T_{g1}}}, & dla \quad T_{g1}<\tau<T_{g2},\\ 0, & dla \quad \tau > T_{g2}.\end{cases}$$

Określenie 4. **PEŁNOŚCIĄ** INFORMACJI NAZYWAMY CECHĘ INFORMACJI, WYRAŻAJĄCĄ ZAWARTOŚĆ RZECZYWISTYCH INFORMACJI O STANIE RZECZY W DANEJ WIADOMOŚCI.

Jako wskaźnik oceny pełności informacji może zostać przyjęty stosunek rzeczywistej ilości informacji zawartej w udostępnianych wiadomościach do maksymalnej ilości informacji, jaka może być w nich zawarta. Ilość informacyjna wyrażana jest w postaci przyrostu entropii [6]. Do wyrażenia stopnia pełności informacji można posłużyć się pewnym ogólnym modelem. Zakłada się, że informacje zawarte w danej wiadomości dotyczą pewnej sytuacji:

$$<\boldsymbol{A}(t), \boldsymbol{B}(t), \boldsymbol{P}(t)>$$

gdzie:

$\boldsymbol{A}(t) = \{a_i : i = 1, 2, ..., N(t)\}$ - zbiór możliwych skutków (działań, decyzji) *„dedukowanych"* przez odbiorców wiadomości na podstawie informacji w niej zawartych;

$\boldsymbol{B}(t) = \{b_j : j = 1, 2, ..., M(t)\}$ - zbiór przyczyn – zaobserwowanych stanów rzeczy;

$\boldsymbol{P}(t) = [p_{ij}(t)]_{N(t)*M(t)}$ – macierz prawdopodobieństw powiązań (zależności) skutków i przyczyn.

Ilość informacji zawartej w wiadomości możemy określić jako przyrost entropii, czyli:

$$I(t)=H(t_0) - H(t_k)$$

gdzie: $\boldsymbol{H}(t_0)$ – entropia dla sytuacji początkowej;

$\boldsymbol{H}(t_k)$ – entropia w badanej chwili t_k, w której odbiorca (decydent) otrzymał wiadomość przy czym:

$$H(t_k)=-\sum_{i=1}^{N(t_k)}\sum_{j=1}^{M(t_k)} p_{ij}(t_k)\log p_{ij}(t_k).$$

Dla oceny pełności informacji w pojedynczej wiadomości można zastosować następujący wskaźnik:

$$i(t)=\begin{cases} I(t), & \text{dla } H(t_0)>H(t) \\ 0, & \text{dla } H(t_0)\le H(t) \end{cases}$$

a wtedy:

$$\beta(t)=\frac{i(t)}{H(t_0)}=\begin{cases} 1-\dfrac{H(t)}{H(t_0)}, & \text{dla } i(t_0)=I(t), \\ 0, & \text{dla } i(t)=0. \end{cases}$$

Dla oceny pełności informacji zawartych w **N** różnych wiadomościach wykorzystuje się wskaźnik ważony:

$$\beta(t)=\frac{\sum_{n=1}^{N}\omega_n i_n(t_n)}{\sum_{n=1}^{N}\omega_n H_n(t_0)}$$

gdzie:

$$t_0 \le \min\{t_n\}, \qquad \max\{t_n\}\le t,$$

$$\sum_{n=1}^{N}\omega_n = 1, \qquad 0\le\omega_n\le 1.$$

Tak określony wskaźnik oceny pełności informacji spełnia również warunek:

$$0 \le \beta(t) \le 1, \quad t \in [t_0, T].$$

Uważa się, że ocena pełności informacji należy do najtrudniejszych zadań w procesie oceny jakości informacji. Przedstawiona metoda oceny opiera się na ilościowych charakterystykach informacji, wykorzystując znajomość prawdopodobieństwa związków między przyczynami i skutkami. Istnieją oczywiście trudności z identyfikacja poszczególnych czynników określających sytuację informacyjną.

Aby uwolnić się od konieczności stosowania pojęcia entropii można posłużyć się następującym modelem: niech system decyzyjny podejmuje decyzje określone zbiorem ***D***, przy czym z każdą decyzja **d** ∈ **D** związany jest pewien zbiór zagadnień dotyczących stanu rzeczy **S** ⊂ **X** × **X** × **Y**:

$$Z^d = \{z_j^d : j \in J^d\},$$

$$\bigcup_{d\in D} Z^d = Z.$$

W szczególności zbiór zagadnień identyfikowany jest ze zbiorem pytań ***Q*** ≡ ***Z***, skierowanych do systemu informacyjnego. Każde pytanie ***q*** ∈ ***Q*** wymaga odpowiedzi

zawierającej określone informacje J_q. Wielkość J_q nazywać się będzie, odpowiedzią systemu informacyjnego na pytanie $q \in Q$. Ponadto, niech dla każdego pytania q istnieje taki podzbiór $S_q \subset S$, który nazywany będzie podzbiorem obiektów relewantnych. Na podstawie powyższych pojęć można skonstruować następujące wskaźniki:

a) wskaźnik kompletności odpowiedzi:

$$\beta_{Kq} = \frac{\operatorname{card}(S_q \cap J_q)}{\operatorname{card} S_q}$$

b) wskaźnik dokładności odpowiedzi:

$$\beta_{Dq} = \frac{\operatorname{card}(S_q \cap J_q)}{\operatorname{card} J_q}$$

Zamiast wskaźnikami dla danego pytania (odpowiedzi) posługiwać się można wskaźnikami uogólnionymi β_K i β_D (dla *"uogólnionego pytania"* i *"uogólnionej odpowiedzi"*). W związku z powyższym wprowadza się miarę pełności informacji w postaci funkcji nieliniowej:

$$\beta = \frac{(\kappa^2 + 1)\beta_K \beta_D}{\kappa^2 \beta_K + \beta_D}$$

spełniającej następujące warunki:

- ✓ $\beta \in [0,1]$;
- ✓ $\beta_K = 0 \rightarrow \beta = 0$;
- ✓ $\beta_K = 0 \leftrightarrow \beta_D = 0$;
- ✓ $\beta_K = 1 \wedge \beta_D = 1 \Rightarrow \beta = 1$;
- ✓ β jest funkcją rosnącą β_K i β_D;

jeżeli $\kappa = \frac{\beta_K}{\beta_D}$, to $\left(\frac{\partial \beta}{\partial \beta_D}\right)_{\beta_K} = \left(\frac{\partial \beta}{\partial \beta_K}\right)_{\beta_D}$.

Określenie 5. NIEZAWODNOŚCIĄ (PRAWIDŁOWOŚCIĄ) INFORMACJI NAZYWA SIĘ CECHĘ, WYRAŻAJĄCĄ STOPIEŃ WPŁYWU ZNIEKSZTAŁCEŃ I ZAKŁÓCEŃ NA INFORMACJE DOSTARCZANE PRZEZ SYSTEM INFORMACYJNY ICH ODBIORCOM (DECYDENTOM).

W celu określenia wskaźnika oceny niezawodności informacji $\gamma(t)$ konieczne jest uwzględnienie szczegółowych charakterystyk systemu informacyjnego, takich jak np.: własności zbioru sygnałów wejściowych, które mogą być przykładane na wejście kanału, czy własności zbioru sygnałów wyjściowych, gdy ustalony jest sygnał wej-

ściowy, a w szczególności: charakterystyki kanałów łączności, kodów i reguł decyzyjnych realizowanych w odbiorniku. W analizie najczęściej przyjmowane założenia dotyczą: ziarnistości kanałów (zbiory sygnałów wejściowych i wyjściowych zawierają skończoną liczbę elementów) oraz binarności (na wejściu i wyjściu pojawiają się ciągi sygnałów binarnych). Dla poszczególnych przesyłanych wiadomości określa się prawdopodobieństwa błędu przy stosowaniu np. kodu wykrywającego (korygującego) jeden błąd.

Dla uproszczenia rozważań, którym w literaturze specjalistycznej (z telekomunikacji i teleinformatyki) poświęcono wiele uwagi, przyjmuje się następujący wskaźnik oceny niezawodności informacji:

$$\gamma(t) = \prod_{i=1}^{3} P_i(t)$$

gdzie: $P_1(t)$ - prawdopodobieństwo tego, że podczas przesyłania wiadomości do chwili t nie wystąpią błędy elementarne;

$P_2(t)$ - prawdopodobieństwo tego, że do chwili t nie nastąpi zablokowanie sieci przesyłania informacji;

$P_3(t)$ - prawdopodobieństwo tego, że do chwili t nie nastąpi zerwanie łączności.

W szczególności wygodnie jest posługiwać się pewnym uproszczonym wyrażeniem, pozwalającym wyznaczyć prawdopodobieństwo wystąpienia w przesyłanej sieci błędu. Zakłada się, że przesyłane są w kanale z zakłóceniami symbole binarne. Przyjmuje się, że symbole binarne przesyłane są w postaci **n**-elementowych wiadomości, zaś błędy występują w postaci m-elementowych ciągów. Dla tego modelu prawdopodobieństwo wystąpienia błędu w wiadomości określone jest wyrażeniem:

$$P_0 = \frac{p}{q}\left(1 + \frac{n-1}{\overline{m}}\right)$$

gdzie: $p = \lim \frac{N_1}{N}$ dla $N \to \infty$,

N_1 - liczba zakłóconych wiadomości;

N - liczba przesyłanych symbolów binarnych;

q - gęstość błędów w pojedynczym pakiecie;

$\overline{m} = \sum_{m=1}^{M_{max}} mP_m$ - wartość oczekiwana liczby błędów,

P_m – prawdopodobieństwo wystąpienia m-elementowej "paczki" błędów w wiadomości.

Dla wartości P_0 określa się następujące oszacowanie m-elementowej „paczki" błędów w wiadomości:

$$\left[\frac{p}{q}\left(1+\frac{n-1}{\overline{m}}\right)\right]^2 < \Delta P_0 < \frac{p^2}{q}\left(1+\frac{n-1}{\overline{m}}\right)\frac{(\overline{m}-1)}{(q\overline{m}-p\overline{m}+p)}.$$

Wyznaczoną w powyższy sposób wielkość wykorzystuje się do oceny niezawodności informacji:

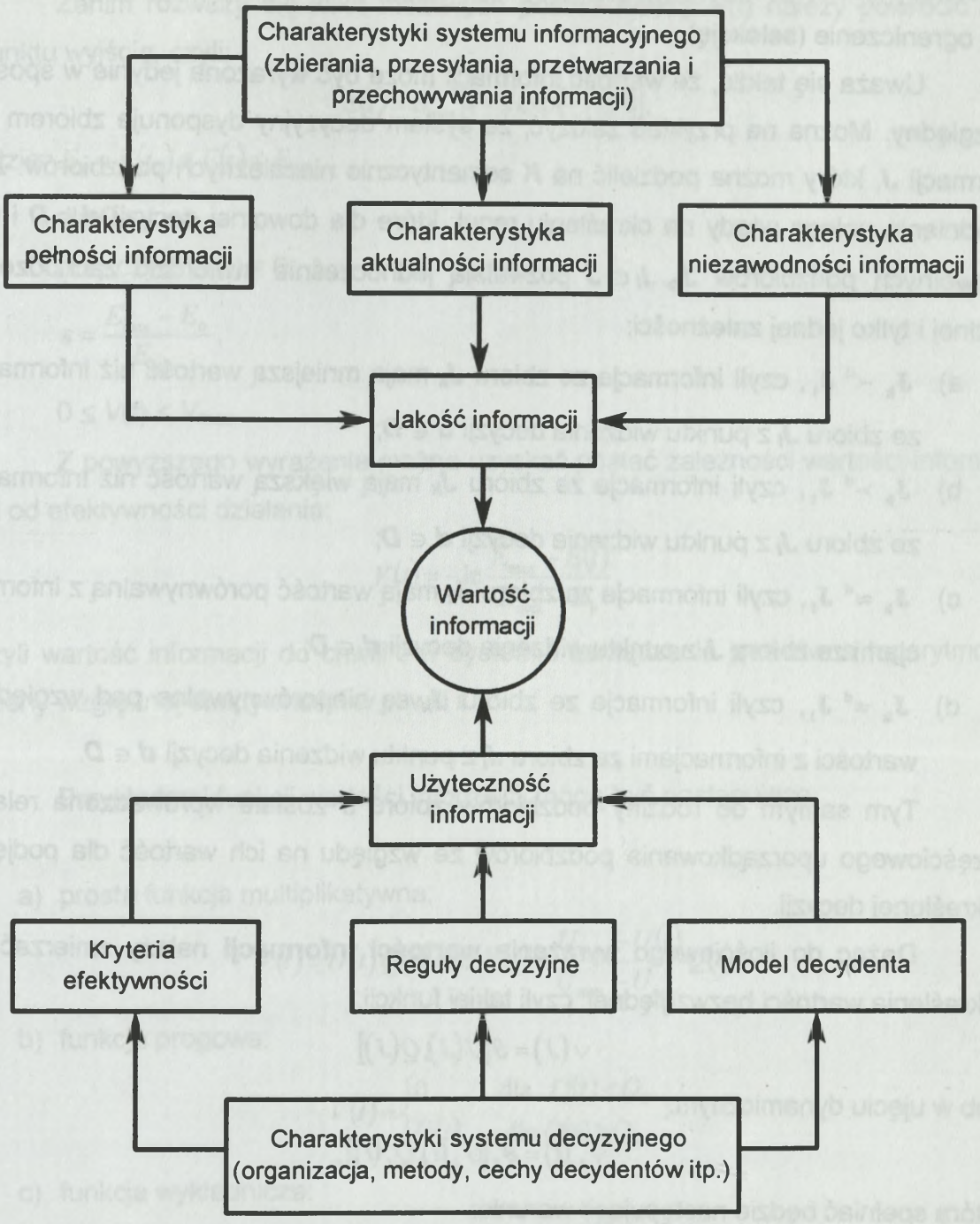
$$\gamma = 1 - P_0.$$

1.7.5. Wartość informacji

Określenie 6. **WARTOŚCIĄ INFORMACJI** NAZYWA SIĘ CECHĘ KOMPLEKSOWĄ, WYRAŻAJĄCĄ ZWIĄZKI MIĘDZY UŻYTECZNOŚCIĄ I JAKOŚCIA ROZPATRYWANE Z PUNKTU WIDZENIA WPŁYWU INFORMACJI NA EFEKTYWNOŚĆ DZIAŁANIA.

Określenie 7. **WARTOŚCIĄ INFORMACJI** NAZYWA SIĘ WŁASNOŚĆ INFORMACJI, WYRAŻAJĄCĄ STOPIEŃ SPEŁNIENIA POTRZEB I WYMAGAŃ UŻYTKOWNIKÓW INFORMACJI W PROCESIE DZIAŁANIA.

O ile użyteczność informacji określała jej wpływ na skuteczność podejmowanych decyzji, a jakość – stopień spełnienia określonych wymagań, o tyle wartość informacji (rysunek 7.2.), jako własność wiążąca obie wymienione cechy powinna określać bezwzględną wartość uzyskaną przez informacje w procesie działania, a więc jej niejako wartość społeczną [7].



Rysunek 7.2. Schemat analizy czynników determinujących wartość informacji. Źródło: Sienkiewicz P [7]

Należy także podkreślić względną niezależność ilości informacji zawartej w określonej wiadomości i jej wartości. Zależność wartości od ilości informacji ma dość często postać krzywej jednomodalnej: wartość wzrasta w funkcji ilości informacji do pewnego maksimum, po czym może wykazać tendencję malejącą. Wynika to z faktu, że użytkownik informacji ma ograniczone możliwości efektywnego wykorzystania zbyt dużej ilości informacji dostarczonej w jednostce czasu, dlatego zadaniem

systemu informacyjnego może być niekiedy zwiększenie wartości informacji poprzez jej ograniczenie (selekcję).

Uważa się także, że wartość informacji może być wyrażona jedynie w sposób względny. Można na przykład założyć, że system decyzyjny dysponuje zbiorem informacji ***J***, który można podzielić na ***K*** semantycznie niezależnych podzbiorów. Zagadnienie polega wtedy na określeniu reguł, które dla dowolnej decyzji $d \in D$ i dla dowolnych podzbiorów $J_k, J_l \subset J$ pozwalają jednocześnie stwierdzić zachodzenie jednej i tylko jednej zależności:

a) $\mathbf{J}_k \prec^d \mathbf{J}_l$, czyli informacje ze zbioru J_k mają mniejszą wartość niż informacje ze zbioru J_l z punktu widzenia decyzji $d \in D$;

b) $\mathbf{J}_k \succ^d \mathbf{J}_l$, czyli informacje ze zbioru J_k mają większą wartość niż informacje ze zbioru J_l z punktu widzenia decyzji $d \in D$;

c) $\mathbf{J}_k \approx^d \mathbf{J}_l$, czyli informacje ze zbioru J_k mają wartość porównywalną z informacjami ze zbioru J_l z punktu widzenia decyzji $d \in D$;

d) $\mathbf{J}_k \neq^d \mathbf{J}_l$, czyli informacje ze zbioru J_k są nieporównywalne pod względem wartości z informacjami ze zbioru J_l z punktu widzenia decyzji $d \in D$.

Tym samym do rodziny podzbiorów zbioru ***J*** została wprowadzona relacja częściowego uporządkowania podzbiorów ze względu na ich wartość dla podjęcia określonej decyzji.

Dążąc do ilościowego wyrażenia **wartości informacji** należy zmierzać do określenia wartości bezwzględnej, czyli takiej funkcji:

$$\vee(J) = \vartheta[U(J), Q(J)]$$

lub w ujęciu dynamicznym:

$$\vee_J(t) = \vartheta_J[U_J(t), Q_J(t)],$$

która spełniać będzie następujące warunki:

a) $U \to U_{\max} \wedge Q \to 1 \Rightarrow V \to V_{\max}$;

b) $U \to U_{\min} \wedge Q \to 0 \Rightarrow V \to V_{\min}$;

c) $U = 0 \wedge Q = 0 \Rightarrow V = 0$;

d) $\left(\frac{\partial V}{\partial U}\right)_Q > \left(\frac{\partial V}{\partial U}\right)_U$

czyli wzrost funkcji ***V*** względem zmiennej ***U*** jest szybszy niż względem zmiennej ***Q***.

Zanim rozważy się kilka możliwych postaci funkcji ***V(t)*** należy powrócić do punktu wyjścia, czyli:

$$E(t) = E_{\max}\left[1 - \varepsilon \exp(-V(t))\right],$$

gdzie: $E_0 = E(t_0) \le E(t) \le E_{\max}$

dla $0 \le t < \infty$

przy czym E(0) = 0

$$\varepsilon = \frac{E_{\max} - E_0}{E_{\max}},$$

$0 \le V(t) \le V_{\max}$.

Z powyższego wyrażenia można uzyskać postać zależności wartości informacji od efektywności działania:

$$V(t) = -\ln \frac{E_{\max} - E(t)}{E_{\max} - E_0},$$

czyli wartość informacji do chwili ***t*** w systemie zarządzania jest równa logarytmowi oceny względnej efektywności w chwili ***t***.

Przykładami funkcji wartości informacji mogą być następujące:

a) prosta funkcja multiplikatywna:

$$V(t) = U(t)\,Q(t) \text{ lub } V(t) = \frac{U_{\max} - U(t)}{U_{\max} - U_{\min}} Q(t);$$

b) funkcja progowa:

$$V(t) = \begin{cases} 0, & \text{dla } Q(t) < Q_0, \\ U(t), & \text{dla } Q(t) \ge Q_0 \end{cases};$$

c) funkcja wykładnicza:

$$\mathbf{V(t) = 1 - [1 - U(t)]^{Q(t)}};$$

d) funkcja „przedziałowa":

$$\mathbf{V(t)} = \begin{cases} 0, & \text{dla } \mathbf{Q(t) \le Q_0 - \Delta Q}, \\ \mathbf{U(t)} \dfrac{\mathbf{Q(t) - Q_0 + \Delta Q}}{2\Delta \mathbf{Q}}, & \text{dla } \mathbf{Q(t) \in [Q_0 - \Delta Q, Q_0 + \Delta Q]}, \\ \mathbf{U(t)}, & \text{dla } \mathbf{Q(t) \ge Q_0 + \Delta Q}; \end{cases}$$

e) funkcja logarytmiczna:

$$V(t)=\begin{cases}0, & \text{dla } Q(t)\le Q_0-\Delta Q,\\ U(t)\left[\dfrac{\ln Q(t)}{\ln\dfrac{Q_0+\Delta Q}{Q_0-\Delta Q}}+\dfrac{\ln Q_0-\Delta Q}{\ln\dfrac{Q_0-\Delta Q}{Q_0+\Delta Q}}\right], & \text{dla } Q(t)\in[Q_0-\Delta Q,Q_0+\Delta Q],\\ U(t), & \text{dla } Q(t)\ge Q_0+\Delta Q;\end{cases}$$

f) funkcja eksponencjalna:

$$\mathbf{V(t)=U(t)\left[1-\frac{U_{max}-U(t)}{U_{max}}e^{-Q(t)}\right]}$$

lub:

$$V(t)=U(t)\left[1-e^{-Q(t)}\right]$$

g) funkcja logistyczna:

$$V(t)=\frac{U(t)}{1+a\exp\left[-bQ(t)\right]}$$

1.7.6. Degradacja wartości informacji

Z punktu widzenia problemu decyzyjnego istotny jest taki komunikat, w którym występujący strumień informacyjny awizuje problem lub prawdopodobieństwo jego wystąpienia oraz strumień informacyjny dotyczący problemu i możliwości jego rozwiązania przez decydenta. Aby określony strumień informacyjny był użyteczny dla decydenta powinien zawierać dane umożliwiające precyzację:

- na czym polega istota problemu (analiza merytoryczna);
- gdzie powstał problem (lokalizacja przestrzenna);
- kiedy powstał problem (lokalizacja w czasie);
- jakie są najistotniejsze przyczyny powstania problemu;
- jakie skutki wywołuje (wywołać może) problem;
- stopień powtarzalności problemu, stopień zrutynizowania problemu.

Tak określone potrzeby informacyjne decydenta są wyjątkowo wszechstronne (wynikają z racjonalnych przesłanek decyzyjnych) i stanowić powinny punkt odniesienia do badania wartości informacji (poprzez zawartość informacyjną komunikatów)

w każdej konkretnej sytuacji decyzyjnej dla określonego decydenta przy określonym problemie decyzyjnym.

Jak zatem widać względność jakiegokolwiek ujęcia formalnego jest wyjątkowo duża, w zasadzie pozbawiająca sensu czynienia jakichkolwiek prób uogólniających.

Konceptualizacja spójnego kompleksu komunikatów, który w sposób wystarczający (pełny, a więc o maksymalnej wartości) mógłby stać się źródłem informacji na temat powstałego problemu, czyli preparacja informacyjnego modelu problemu jest niezwykle skomplikowana. Komunikat (zbiór komunikatów) o problemie musiałby zatem spełniać zarówno funkcję komunikatu pojęciowego (ustalającego sens problemu), jak i komunikatu - źródła informacji (istotność problemu). Ponadto zawierać musi opis przyczynowo - skutkowy problemu stanowiąc podstawę wyobrażeń co do stanu pożądanego (celu), a także informację o sposobie rozwiązania problemu. Model taki uwzględniać powinien wizje świata użytkownika. A wszystko powinno być skorelowane z sytuacja na tle której problem został spostrzeżony.

Powróćmy jednak do pewnych propozycji ujęć ilościowych przedstawionych powyżej. Jeżeli zatem za podstawę oceny ilościowej zmian wartości informacji w procesie jej dezaktualizacji (czasowej)[23] przyjmiemy zaproponowane powyżej postacie funkcji wartości informacji, to możliwa jest analiza zmian ich wartości poprzez wszechstronne badanie przebiegu zmian tych funkcji.

Na przykład, jeżeli funkcja wartości informacji będzie krzywą logistyczną, to wówczas przyjmując jako argument wartości – jakość, określić można punkt przegięcia wykresu funkcji o współrzędnych:

$$Q(t)=\frac{1}{b}\ln a,$$

$$V(t)=\frac{1}{2}U(t).$$

Jeżeli natomiast ustali się użyteczność informacji $U(t) = U$, to można wyznaczyć „czas połowicznego rozkładu informacji", czyli czas po upływie którego wartość informacji ulegnie zmniejszeniu o połowę:

$$T_{0,5}=\left\{\tau : V(\tau)=\frac{1}{2}V_J\right\}$$

---

[23] *Rozpatrywanie degradacji wartości informacji ze względu na przestrzeń (zmienne: długości, szerokości i wysokości), choć wydaje się być uzasadnione, to nie jest możliwe. W przedstawionych bowiem modelach zmienne te nie występują (należy konceptualizować inne modele), a więc różniczki kierunkowe nie mogą być obliczane.*

Uważa się, że podstawowym czynnikiem, który powoduje zmniejszenie wartości informacji jest jakość informacji a więc:

$$Q(T_{0,5}) = -\frac{1}{b}\ln\left[\frac{U_J - \frac{1}{2}U_J}{\frac{a}{2}V_J}\right].$$

Wykorzystując wartość $V(t) = -\ln\frac{E_{\max} - E(t)}{E_{\max} - E_0}$ $V(t)$ otrzyma się następujący związek:

$$U_J(t) = -\ln\frac{E_{\max} - E(t)}{E_{\max} - E_0}\left[1 - ae^{-bQ_J(t)}\right],$$

dla którego równoważna jest postać:

$$E(t) = E_{\max}\left[1 - \frac{E_{\max} - E_0}{E_{\max}}\exp\left(\frac{U_J(t)}{1 - a\exp(-bQ_J(t))}\right)\right].$$

W ten sposób można prześledzić wpływ wartości informacji oraz poszczególnych jej komponentów: użyteczności i jakości na efektywność działania. Umożliwia to dokonanie analizy wpływu funkcjonowania systemu zarządzania na efektywność systemu działania.

Uzupełnieniem powyższych rozważań jest model[24], w którym przedmiotem badań są relacje zachodzące pomiędzy rzeczywistą informacją zawartą w danym obiekcie, a informacją odebraną przez użytkownika za pośrednictwem systemu informacyjnego. Zakłada się, że cecha $a_j(t)$ charakteryzująca obiekt może przyjmować dyskretne wartości: $\alpha_1,...,\alpha_{L_j}$, zaś cecha ta w odebranej wiadomości jako $b_j(t)$ przyjmuje wartości: $\beta_1,...,\beta_{M_j}$. W przypadku, gdy $a_j(t) = \alpha_l$ oraz $b_j(t) = b_m$ uzyska się pewien efekt γ_{lm}. Przyjmuje się ponadto, że znane są: prawdopodobieństwo tego, że jeśli $a_j(t_0) = \alpha_k$, to odbiorca otrzyma $b_j(t) = \beta_m$ - $\zeta_{km}(t)$ oraz $\rho_a(k)$ – prawdopodobieństwo, że $a_j(t_0) = \alpha_k$. Dane jest także prawdopodobieństwo $\pi_{kl}(t)$ tego, że cecha przyjmująca w chwili wartość α_k przyjmie w chwili t wartość α_l. Wtedy jakość informacji określa wyrażenie:

$$Q(t) = \sum_{l,m}\left[\gamma_{lm}\sum_{k=1}^{L}\rho_a(k)\pi_{kl}(t)\zeta_{km}(t)\right]$$

[24] *Model Rogińskiego, na podstawie Rogucki A., Analiza systemowa w planowaniu obrony, MON, 1976.*

Powyższy model uwzględnia ocenę informacji w pewnych szczególnych przypadkach:

a) gdy obiekt nie zmienia się, to jest $a_i(t) = a_i(t_0) = \alpha_k$:

$$Q(t) = \sum_{l=1}^{L} \sum_{k=1}^{L} \rho_a(k) \pi_{kl}(t) \gamma_{lk}$$

b) gdy system informacyjny nie wnosi zniekształceń, tj. $b_i(t) = a_i(t_0) = \alpha_k$

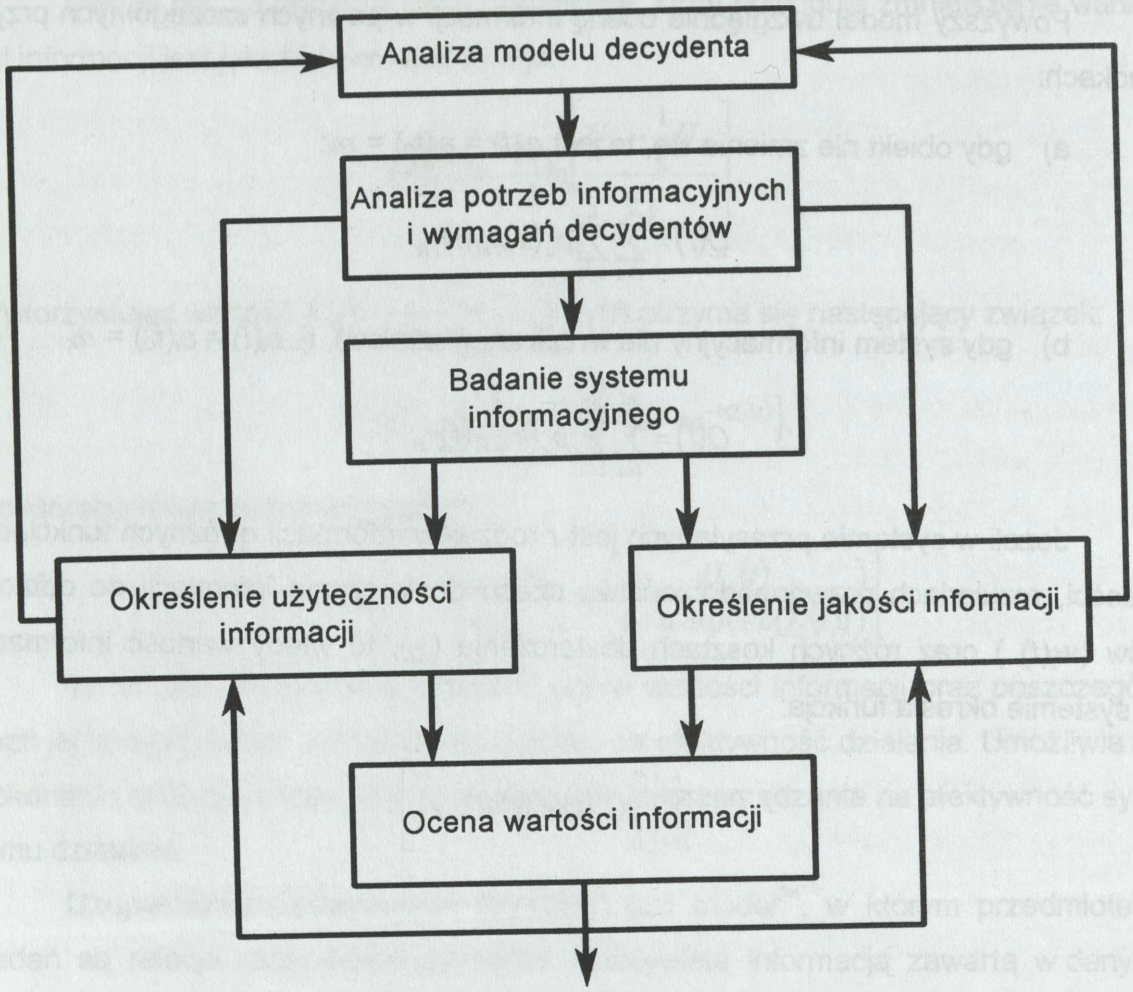
$$Q(t) = \sum_{l=1}^{L} \sum_{k=1}^{L} \rho_a(k) \gamma_{kl}(t) \gamma_{kl}$$

Jeżeli w systemie przesyłanych jest ***r*** rodzajów informacji o różnych funkcjach jakości, rozkładach prawdopodobieństwa czasu dostarczania informacji do odbiorców ($w_j(t)$) oraz różnych kosztach dostarczenia (χ_j), to wtedy wartość informacji w systemie określa funkcja:

$$V = \sum_{j=1}^{r} \left[\int_0^{\infty} Q_j(t) w_j(t) dt - \chi_j \right].$$

Podsumowanie

Zagadnienie oceny informacji wykorzystywanych w dowolnym procesie zarządzania jest niewątpliwie jednym z ważniejszych problemów badawczych, a to z dwóch powodów, po pierwsze - pragmatyczny aspekt informacji, to podstawa oceny efektywności obserwacji rzeczywistości w badaniach, a więc jest to także problem *stricte* metodologiczny; po drugie – ocena (prowadzona w kategoriach jakościowych) informacji, to podstawa efektywności samego systemu zarządzania, bądź systemu informacyjnego a więc jest to także problem praktyczny rozpatrywany w ramach inżynierii systemów, a inżynierii systemów zarządzania (systemów informacyjnych) w szczególności. Z tych to powodów, abstrahując od klasycznego ilościowego („Shannowskiego") ujęcia informacji, warto zwrócić uwagę na jakościowe ujęciu informacji. W przedstawionej propozycji (rysunek 7.3), dostrzegamy znaczne możliwości i perspektywy rozwoju, które mogą się okazać tak wartościowe dla teorii (efektywności) systemów zarządzania, jak wartościową dla rozwoju telekomunikacji okazała się teoria informacji C. Shannona.



Rysunek 7.3. Schemat analizy wartości informacji w systemie zarządzania.

Źródło: Sienkiewicz P. [7]

Bibliografia:

1. Mazur M.: Cybernetyka i charakter, PIW, Warszawa 1975.
2. Obuchowski K.: Kody orientacji i struktura procesów emocjonalnych, PWN, Warszawa 1970.
3. Kuleszyński L.: Dowodzenie wojskami a cybernetyka, MON, Warszawa 1967.
4. Kozielecki J.: Problemy psychologii matematycznej, PWN, Warszawa 1971.
5. Kleinrock L.: Comunication Nets, MC Graw-Hill Book Co., New York 1964.
6. Tiemnikow F.: Afonin W., Dimitrijew W., Podstawy techniki informacyjnej, WNT, Warszawa 1974.
7. Sienkiewicz P.: Teoria efektywności systemów kierowania, ASG WP, Warszawa 1979.

1.8. MODELOWANIE WALKI INFORMACYJNEJ

W przedstawionym materiale przyjęto następujący schemat postępowania:

Na wstępie podano fizyczną interpretację entropii na prostym przykładzie tasowania kart do gry. Wskazano przy tym na podstawowe problemy opisu zjawisk nieodwracalnych. Następnie, bazując na analizie literatury traktującej o problemach pomiaru i wartościowania informacji, omówiono założenia probabilistycznego modelu przewagi informacyjnej. Jednocześnie, zaproponowano użycie symulacyjnej metody Monte Carlo na etapie generacji wartości poszczególnych stanów w macierzy wariantów działania stron.

Przykłady procesów nieodwracalnych znajdujemy między innymi na kartach książek traktujących o zjawiskach fizycznych. Przykładowo: kawałek kredy spadając ze stołu na podłogę podlegając prawom mechaniki klasycznej przechodzi do innego stanu z którego powrót do stanu pierwotnego, chociaż teoretycznie możliwy, nigdy nie zachodzi. Kawałek kredy mógłby wznieść się z podłogi do góry i osiąść z powrotem na stole. Proces ten nigdy jednak nie zachodzi, a wiemy to z codziennego doświadczenia i z prawa wzrostu entropii.

1.8.1. O entropii i prawie wzrostu entropii

Przykład:

Rozpatrzmy talię kart ułożonych rosnąco od dwójki trefl do asa pik. Talia znajduje się w stanie, który oznaczymy umownie przez **A**. Każdy inny stan kart, po dowolnym ich przetasowaniu, oznaczymy przez **B**. Przejście od stanu **A** do stanu **B** jest procesem nieodwracalnym. Wiemy, że przejście to jest teoretycznie możliwe, lecz bardzo mało prawdopodobne[1].

[1] *Przykład zaczerpnięto z K. Zalewski, Wykłady z termodynamiki fenomenologicznej i statystycznej, PWN Warszawa 1978, s.50.*

Stany mikro i makroskopowe

Powracamy do poprzedniego przykładu z talią kart. Stany **A** i **B** nazywamy makroskopowymi. Stan mikroskopowy stanowi konkretne ułożenie kart.

Przez $\Delta\Gamma$ oznaczymy liczbę stanów mikroskopowych.

Obliczymy ile stanów mikroskopowych odpowiada stanom makroskopowym **A** i **B**.

Stanowi **A** odpowiada tylko jeden stan, więc: $\Delta\Gamma(A)=1$.

Zaś dla stanu **B** mamy: $\Delta\Gamma(B)=52!-1\approx 8\cdot 10^{67}$.

Wniosek:

Zakładając, że tasowanie kart jest idealne, tzn. że każdy stan mikroskopowy jest wytwarzany z równym prawdopodobieństwem, startując z jakiegokolwiek stanu, mamy $8\cdot 10^{67}$ razy większe prawdopodobieństwo przejścia do stanu **B** niż do stanu **A**.

Z punktu widzenia praw tasowania możliwe są przejścia zarówno ze stanu **A** do **B** jak i z **B** do **A**. Praktycznie jednak, tylko przejścia z **A** do **B** są realizowane. Jeśli układ raz znajdzie się w stanie **B**, to już go nie opuści.

Podane wyżej rozumowanie stosuje się bez zmian jakościowych do wyjaśnienia procesów nieodwracalnych w praktycznie spotykanych układach makroskopowych.

Wielkość $\Delta\Gamma$ gwałtownie rośnie wraz ze wzrostem liczby składników układu. Przykładowo, gdyby do talii kart dodać jedną kartę, to liczba $\Delta\Gamma(B)$ wzrosłaby 53–krotnie. Stąd, wygodniej jest zamiast liczby $\Delta\Gamma$ wprowadzić entropię S zdefiniowaną jako:

$$S = k\cdot \ln \Delta\Gamma ,$$

gdzie k jest stałą.

Powyższy wzór, zwany wzorem Boltzmanna, stosuje się do **układów izolowanych w równowadze pełnej bądź niepełnej**.

W praktyce, **każdy układ można interpretować jako część jakiegoś większego układu izolowanego**. Dzięki temu, teoria entropii pozwala na wyjaśnienie natury wszystkich procesów nieodwracalnych[2].

Wracamy do przykładu z uporządkowaną talią kart. Obliczymy entropię stanów **A** i **B**.

$$S(A)=0, \qquad S(B)=k\cdot \ln\left(8\cdot 10^{67}\right)=156\cdot k .$$

Zatem, wyjaśnienie procesów nieodwracalnych sprowadza się do twierdzenia, że **w procesach nieodwracalnych, zachodzących w układzie izolowanym, entropia rośnie**. Jest to jedna z postaci prawa wzrostu entropii.

Stan układu izolowanego, w którym układ posiada maksymalną entropię jaką można osiągnąć w danych warunkach, nazywany jest **stanem równowagi pełnej**.

Porównanie entropii układu w stanie pełnej równowagi z entropią układu w innych stanach jest wykonalne tylko wtedy, gdy te inne stany są **stanami równowagi niepełnej**.

Prawdopodobieństwo makrostanu

Dany stan makroskopowy realizuje się za pośrednictwem dużej ilości mikrostanów. Znając cechy charakteryzujące dany makrostan, można obliczyć wszystkie mikrostany, zgodnie z tymi cechami.[3]

Prawdopodobieństwo wystąpienia makrostanu definiuje się poprzez stosunek liczby mikrostanów odpowiadających danemu makrostanowi, do całkowitej liczby stanów osiąganych przez dany układ. Przykładowo dla makrostanu **A** mamy:

$$p_A = \frac{\Delta\Gamma(A)}{\Delta\Gamma}.$$

W naszym przykładzie z talią kart: $p_A = \frac{1}{52!} \approx \frac{1}{8 \cdot 10^{67}} \to 0$, $p_B \approx 1$.

Liczbę mikrostanów $\Delta\Gamma(A)$ nazywa się także prawdopodobieństwem stanu makroskopowego. Liczba ta nie jest prawdopodobieństwem w sensie matematycznym, gdyż to ostatnie musi być mniejsze lub równe jedności, a liczba $\Delta\Gamma(A)$ jest bardzo duża. Nazwa „prawdopodobieństwo stanu" wzięła się stąd, że wzór: $p_A = \frac{\Delta\Gamma(A)}{\Delta\Gamma}$ pozwala znajdować prawdopodobieństwo makrostanu.[4] Wychodząc

---

[2] *tamże s.52.*

[3] *A.M.Matwiejew, Fizyka cząsteczkowa, PWN, Warszawa 1989, s.49.*

[4] *Bezpośrednie policzenie stanów przeważnie jest niemożliwe. Stąd, teoria znajdowania ilości stanów powinna być tak skonstruowana by uniknąć konieczności ich liczenia. Najkorzystniej byłoby znaleźć od razu prawdopodobieństwa p_A bez znajomości liczby stanów $\Delta\Gamma(A)$. Metodami bezpośredniego obliczania liczby mikrostanów są metody kombinatoryczne. Wykorzystujemy zależności na liczbę możliwych kombinacji lub wariacji, zależnie od natury rozpatrywanego zjawiska:*

$$C(n,m) = \binom{n}{m} = \frac{n!}{m!(n-m)!},\ V(n,m) = \frac{n!}{(n-m)!},\ \overline{V(n,m)} = n^m.$$

z rozważań kombinatorycznych, wykorzystując wzór Stirlinga[5] możliwym staje się obliczenie prawdopodobieństwa makrostanu.

1.8.2. Model prawdopodobieństwa wiedzy

Analizując dostępną literaturę, zwrócono uwagę na opracowanie poświęcone teoretycznym podstawom przewagi informacyjnej. Stworzono tam pewien model prawdopodobieństwa wiedzy, który posłużył jako podstawa rozważań teoretycznych. Następnie odwołano się do teorii gier i równań Lanchester'a. Do dalszych rozważań wykorzystano model prawdopodobieństwa wiedzy wraz ze zdefiniowanymi miarami informacji, celem stworzenia zależności analitycznych opisujących przewagę informacyjną nad przeciwnikiem. Zdefiniowano pewną nową Miarę Efektywności (MOE) opartą na wiedzy, jaką jest kontrola przestrzeni bojowej dla koncepcji manewru dominującego. Zbadano także możliwość opracowania nowych Miar Efektywności dla poszczególnych rodzajów operacji[6].

Prace nad miarami efektywności i związanymi z nimi wielkościami wymiernymi zdecydowanie sugerują, że informacja - w szczególności przewaga informacyjna, może mieć silny wpływ na wyniki operacji militarnych. Pomiar stopnia przewagi informacyjnej, jaki mogłaby osiągnąć, jedna strona nad drugą, jest czymś najbardziej pożądanym w wieku informacyjnym. W raporcie, o którym tu mowa, skupiono się na miarach relatywnych, poczynając od wiedzy względnej, dla której opracowano jednostkę miary wiedzy.

Ta wymierna wielkość, wyraża zależność między wiedzą idealną i rzeczywistą w operacjach militarnych, dla obu stron. Skupiono się także na potrzebie posiadania nowych miar efektywności do oceny nowych koncepcji operacji aktualnie przyjmowanych przez Armię, jak również na wpływie, jaki na te operacje może wywierać informacja.

Tradycyjne miary efektywności (wciąż „zakorzenione" w modelach opracowywanych dla każdego indywidualnego układu sił), wyliczają efektywność na bazie wskaźników zmian zdominowanych przez główne systemy uzbrojenia. Mierzą one jedynie pewną część zdolności bojowej dowolnej jednostki wojskowej. Ponadto,

---

[5] *Dla dużych n spełniona jest równości:* $n! \approx (n/e)^n$, $\ln n! \approx \ln\left[(n/e)^n\right] = n\ln(n/e) = n\ln n - n$.

[6] *R. Darilek i inni, Miary efektywności dla armii wieku informacyjnego, Centrum Rand Arroyo, 2002 – tłumaczenie z języka angielskiego, źrdło: http//www.rand.org/organization/ard/*

tradycyjne miary efektywności nie spełniają swojego zadania, gdy dochodzi do przygotowywania operacji stabilizujących i zachowania bezpieczeństwa - operacji znanych wcześniej jako operacje militarne inne niż wojna (MOOTW), które mogą zdominować przyszłe operacje militarne.

Dwa warianty prawa Lanchestera (wariant liniowy i kwadratowy), zostały uzupełnione przez tzw. wariant mieszany - prawo Lanchestera zmodyfikowane wiedzą.

W omawianym tu podejściu probabilistycznym, widoczny staje się pewien mechanizm zwany *„fizykalizacją zjawisk"*[7]. Mechanizm ten jest naturalną konsekwencją stosowania aparatu matematycznego do opisu różnych zjawisk analogicznie do tych, występujących w fizyce klasycznej. Tego typu podejście wynika z chęci zastosowania „eleganckich" w sensie analitycznym metod analiz zjawisk z jakimi mamy do czynienia w fizyce. Stąd zastosowanie *„hamiltonianów"* i koncepcji entropowego modelu informacji w połączeniu z prawem Lanchestera zmodyfikowanym wiedzą.

Kolejne modyfikacje równań Lanchestera dowodzą, ograniczonej ich przydatności do opisu rzeczywistych zjawisk pola walki. Nie można odmówić tym równaniom *„elegancji"* w zapisie, jednakże pozostaną one jedynie narzędziem dociekań akademickich. Prawdziwych rozwiązań należy poszukiwać w symulacjach komputerowych.

1.8.3. Metoda Monte Carlo w probabilistycznym modelu przewagi

Metoda Monte Carlo polega na przedstawieniu rozwiązania podstawowego problemu w postaci parametru pewnej hipotetycznej populacji i używaniu losowej sekwencji liczb do tworzenia próbki tej populacji, na podstawie, której można dokonać statystycznego oszacowania wartości badanego parametru[8].

---

[7] *patrz H. Spustek, Przewaga w walce i operacji, rozprawa habilitacyjna AON, Warszawa 2002 r.*
[8] *Dieter W.Heermann, Podstawy symulacji komputerowych w fizyce, WNT Warszawa 1997 s.80.*

Algorytm metody Monte Carlo[9]

Dwanaście kroków postępowania w metodzie Monte Carlo:

1. Określamy parametr stanowiący podstawowy miernik danego, rozwiązywanego problemu.
2. Budujemy model analityczny danego problemu, wykorzystując matematyczne zależności pomiędzy najważniejszymi zmiennymi. Zmienne w modelu mogą mieć charakter deterministyczny lub losowy Zmienne deterministyczne mogą przyjmować tylko jedną wartość, podczas gdy zmienne losowe mogą przybierać wiele wartości.
3. Dla każdej zmiennej losowej musi być określony odpowiadający jej rozkład prawdopodobieństwa.
4. Rozkład prawdopodobieństwa każdej zmiennej losowej musi być przetworzony do postaci skumulowanego rozkładu prawdopodobieństwa.
5. Każdej możliwej wartości zmiennej losowej musi być przypisana odpowiednia wartość losowa, ze skumulowanego rozkładu prawdopodobieństwa tej zmiennej.
6. Dla każdej zmiennej losowej musi istnieć możliwość wygenerowania liczby losowej.
7. Każdej liczbie losowej musi być przypisana odpowiednia wartość zmiennej losowej.
8. Odpowiednia wartość zmiennej losowej, określona w poprzednim kroku, musi być wykorzystana do wyznaczania podstawowego miernika danego problemu zgodnie z krokiem drugim niniejszego algorytmu.
9. Wartość wyznaczona dla podstawowego miernika w kroku ósmym (poprzednim) musi zostać zapamiętana.
10. Kroki od sześć do dziewięć muszą być powtarzane wymaganą ilość razy (zazwyczaj od 100 do 1000 razy).
11. Wartości podstawowego miernika, zapamiętane zgodnie z punktem dziewiątym, stają się podstawą do określania jego rozkładu prawdopodobieństwa i skumulowanego rozkładu prawdopodobieństwa.

[9] *F.Fabozzi, Fixed income mathematics, Probus Publishing Co., 1997.*

12. Skumulowany rozkład prawdopodobieństwa utworzony w punkcie jedenastym musi zostać przeanalizowany. Podczas analizy wyznaczane są wybrane parametry statystyki opisowej.

Metoda Monte Carlo w zastosowaniu do generacji wartości stanów w macierzy wariantów działania stron

„Zmodyfikujemy" dwanaście kroków postępowania do poniższych sześciu:

1. Określ punkt początkowy x_0 w przestrzeni fazowej.
2. Wygeneruj nowy stan x'.
3. Oblicz prawdopodobieństwo przejścia $W(x, x')$.
4. Wygeneruj liczbę losową $R \in [0,1]$ (rozkład równomierny).
5. Jeżeli prawdopodobieństwo przejścia W jest mniejsze niż liczba losowa R, to potraktuj stary stan jako nowy i wróć do kroku drugiego.
6. W przeciwnym razie, zaakceptuj nowy stan i wróć do kroku drugiego.

W metodzie Monte Carlo (wariant opisany powyżej) milcząco założono, że przyjęty wymiar prawdopodobieństw przejść spełnia **wymóg ergodyczności**. Termin **ergodyczność** oznacza, że każdy stan jest osiągalny z każdego innego stanu. Ściślej mówiąc, każdy stan musi być dostępny z każdego innego stanu w skończonej liczbie przejść. W innych przypadkach, stany układu są podzielone na różne klasy ergodyczności i nie jest możliwe przejście między tymi klasami[10].

Przykład

Dana jest macierz stochastyczna:

$$\begin{bmatrix} 1/2 & 1/4 & 0 & 1/4 \\ 0 & 1/3 & 2/3 & 0 \\ 0 & 1 & 0 & 0 \\ 1/2 & 0 & 1/2 & 0 \end{bmatrix},$$

zawierająca prawdopodobieństwa przejścia pomiędzy czterema stanami: 1, 2, 3 i 4[11].

Przejście ze stanu nr 1 do stanu nr 4 jest możliwe z prawdopodobieństwem $1/4$, podczas gdy przejście ze stanu nr 4 do stanu nr 1 dokonuje się

[10] *Dieter W.Heermann, Podstawy symulacji komputerowych w fizyce, WNT Warszawa 1997 s.88.*
[11] *tamże s.71.*

z prawdopodobieństwem $1/2$. Macierz powyższa jest nieredukowalna. Nie ma tu możliwości przejścia ze stanu nr 2 do stanu nr 1 lub stanu nr 4. Ponadto, jeżeli stanami początkowymi są stany nr 2 lub nr 3, to wszystkimi następnymi stanami są albo stan nr 2 albo stan nr 3. Sytuację tą przedstawia diagram na rysunku niżej. Na diagramie zaznaczono jedynie prawdopodobieństwa przejść z poszczególnych stanów, pominięto prawdopodobieństwa pozostawania w danych stanach.

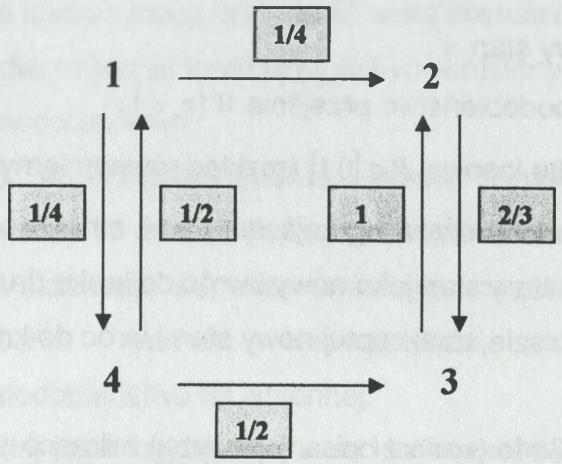


Diagram prawdopodobieństw przejść pomiędzy stanami 1, 2, 3 i 4.

Źródło: Dieter W.Heermann, Podstawy symulacji komputerowych w fizyce, WNT Warszawa 1997 s.71.

1.8.4. Entropowy model przewagi

Informacja ma dwa istotne atrybuty: wartość i jakość. Informacja przedstawia sobą wartość jeśli informuje dowódcę i dodaje nowe elementy do wiedzy posiadanej przez niego o sytuacji bojowej. Konsekwencją tego jest to, że jeżeli odwołuje się on do *"wiedzy"* to oznacza to, że jest ona istotna. Jakość informacji zależy od jej precyzji, dokładności, aktualności i kompletności.

W trakcie gromadzenia informacji z różnych źródeł, dowódca poszukuje takich informacji, które posiadają wartość (są one określane terminem CEI – critical elements of information). Problem polega na tym, że rzadko jesteśmy w stanie trafnie ocenić jakość informacji jaką właśnie otrzymujemy. W konsekwencji tego, dowódca musi zdawać sobie sprawę z tego, że część *"wiedzy"* może być zbyteczna. Przypuśćmy, że przeciwnik używając zaawansowanych technik maskowania i imitacji

spowodował, że nasz dowódca zna rzeczywiście położenie połowy obiektów, spośród tych, których sądzi, że zna. Powoduje to powstanie kilku dodatkowych kwestii, które musi uwzględnić dowódca w trakcie podejmowania decyzji. Jeśli podejrzewa on, że jest wprowadzony w błąd, może zdecydować, że należy poczekać do momentu, w którym dotrą do niego pewniejsze informacje. Jeśli zaś nic nie podejrzewa, to może postąpić ponownie jak przedtem, otrzymując inny i prawdopodobnie mniej imponujący wynik. Powyższe rozważanie sugeruje konieczność zastosowania użytecznej metody oceny informacji.

Wiedza dowódcy zmienia się w miarę nadchodzących analiz pola walki. Zmienia się zatem rozkład prawdopodobieństwa $P_i(U|V=v)$, możliwych do osiągnięcia *„mikrostanów"* o których była mowa na początku rozważań, tam gdzie rozważaliśmy entropię układu. Do bieżącej oceny posiadanej wiedzy wygodnie jest użyć wielkość entropię informacji określonej zależnością Shannon'a[12]. Entropia informacji jest miarą średniej ilości informacji w danym rozkładzie prawdopodobieństwa, zdefiniowana następująco:

$$S\left[P_i(U|V=v)\right] = H_i(U|V=v) = -\sum_{u=0}^{n} P_i(U=u|V=v)\ln\left[P_i(U=u|V=v)\right].$$

Funkcja entropii informacji przyjmuje wartość maksymalną, gdy dana informacja przy danym rozkładzie prawdopodobieństwa jest najmniej prawdopodobna (osiąga najwyższy poziom niepewności). Z operacyjnego punktu widzenia, ma to miejsce wówczas, gdy dowódca nie posiada żadnej wiedzy o rozmieszczeniu jakiegokolwiek spośród n celów przeciwnika. W takim przypadku mamy: $P_i(U=u)=\frac{1}{n+1}$. Można łatwo sprawdzić, że entropia w tym rozkładzie wynosi $S_0(U)=\ln(n+1)$. Z drugiej strony, jeśli dowódca posiada potwierdzenie,

---

[12] *Rozumowanie Shannon'a bazuje na entropii zdefiniowanej w termodynamice statystycznej.*
Przykład: (M.Cichy, J.Nimańczuk, S.Szpakowicz, Zbiór zadań z propedeutyki informatyki, PWN Warszawa 1977, s.7)
Źródło nadaje n komunikatów z prawdopodobieństwami odpowiednio: p_1, p_2, p_3, ..., p_n.
Obliczyć ilość informacji zawartą w każdym z komunikatów i entropię źródła.
Ilość informacji zawartej w komunikacie o prawdopodobieństwie p jest określona wzorem:

$$k = \log_2 \frac{1}{p} = -\log_2 p.$$

Entropię informacyjną źródła można obliczyć ze wzoru: $H = \sum_{i=1}^{n} p_i \cdot \log_2 \frac{1}{p_i}$.

o rozmieszczeniu μ jednostek w promieniu kontrolowanym, wówczas:

$$P_i(U=\mu|V=\nu)=1 \quad i \quad P_i(U\neq\mu|V=\nu)=0.$$

Łatwo też można sprawdzić, że entropia w tym rozkładzie jest równa zeru (porównaj rozważania na temat entropii rozkładu kart do gry, prowadzone na początku).

Zatem, mając informację o rozmieszczeniu μ jednostek w promieniu kontrolowanym, stopień pewności wynosi: $\ln(n+1)-S_i(U|V=\nu)$.

Wówczas możemy podać miarę wiedzy w postaci:

$$S_i(U|V=\nu)=\frac{n(n+1)-S_i(U|V=\nu)}{\ln(n+1)}.$$

Przykład:

Niech **K** będzie miarą wartości informacji lub wiedzy dostępnej dla dowódcy. W niektórych przypadkach **K** może być wartością liczbową, przykładowo: jeśli przeciwnik posiada **N** oddziałów, jednostek, wówczas **K=0.3 N**. Oznacza to że dowódca zna położenia **0.3N** wrogich oddziałów. Dla obu stron **K** zawiera dwa komponenty: wiedzę o wiedzy wysokiej jakości i wiedzę o wiedzy niskiej jakości lub bezwartościowej wiedzy $\mathbf{K = K_C + K_i}$.

W przykładzie: $\mathbf{K_C = K_i = 0{,}15\ N}$. W typowych przypadkach **K** jest wielowymiarowe, zawiera wiele informacji takich jak wolę walki przeciwnika, identyfikację jednostek itp. Warto odnotować że w większości przypadków dowódcy nie wiedzą że są częściowo w błędzie, wyprowadzeni w pole, przez działania przeciwnika.

W walce, obszar działania (AO- area of operation), wiedza i manewr współdziałają ze sobą, tak aby zapewnić efektywne wykorzystanie siły ognia. Kiedy jednostka pojawia się w obszarze działań możemy oczekiwać, że będzie zorientowana na działania ofensywne bądź też defensywne. Przeciwnik jest wówczas pełnym graczem, chcącym w aktywny sposób osiągnąć postawione sobie cele. Jednocześnie, stara się on uniemożliwić realizację naszych celów.

Kilka definicji

Definicja:

Oddział kontroluje obszar jeśli jest w stanie operować w nim bez przeszkód. To nie oznacza, że nieprzyjaciel jest wyeliminowany z tego obszaru, a jedynie, że zaprzyjaźnione oddziały są w stanie wywierać wpływ na wszystkie punkty w danym obszarze przez cały czas.

Definicja:

Promień kontroli oddziału jest to minimum z: maksymalnego efektywnego zasięgu ognia danego oddziału i ognia systemów broni wsparcia w_i, maksymalny efektywny zasięg lokalnych systemów rozpoznania s_i i skojarzonego promienia operacji c_i.

$$r_i = \min\{w_i, s_i, c_i\}$$

Definicja:

Wiedza jest to stopień w jakim dowódca jednostki zna położenie jednostek przeciwnika i naszych w swoim promieniu kontroli.

Oznaczmy wiedzę jednostek niebieskich i oraz czerwonych j jako $K_{B,\,i}$ oraz $K_{R,\,j}$.

Świadomość sytuacyjna określona w powyższych definicjach może zostać porównana do wiedzy o CEI i może zawierać tak trudne elementy jak ocena postawy bojowej przeciwnika oraz jego intencje. CEI lub istotny element informacji są składnikami informacji koniecznymi do wyznaczenia wspólnego obrazu przestrzeni bojowej i stopnia w jakim ten obraz jest jasny dla dowódcy jednostki, oceniającego swoją świadomość sytuacyjną lub wiedzę.

W naszych rozważaniach, bardziej istotnym jest liczba obcych celi w j–tym celu zainteresowania (TAI – target area of interest), niż wiedza o położeniu n celi w obszarze promienia kontroli.

W przypadku gdy liczba obcych celi w każdym kontrolowanym obszarze jest równa μ_j, wówczas mamy $\sum_j \mu_j \le n$.

Przykład:

Dla uproszczenia zakładamy, że TAIs nie nakładają się na siebie, wobec czego suma wiedzy walczących ze sobą dowódców jest w przybliżeniu równa całkowitej liczbie celów przeciwnika w TAIs. Dla n=3 mamy: $K = \sum_{j=1}^{3} \omega_j K_j$, gdzie K_j jest wiedzą o lokalizacji celi w TAI_j i ω_j jest względną ważnością TAI_j obu dowódców $\left(\sum_{j=1}^{3} \omega_j = 1 \right)$. Średnia wiedza wynosi $K = \frac{1}{3} \cdot \sum_{j=1}^{3} K_j$. Metryka wiedzy w tym przypadku jest średnią wiedzą ważoną nad TAIs i przedstawia poziom sytuacyjnej świadomości dowódcy.

Wiedza jest wartością średnią wiedzy oddziału $K_B = \frac{1}{m} \sum_{i=1}^{m} K_{B,i}$ i $K_R = \frac{1}{s} \sum_{i=1}^{s} K_{R,i}$.

Wiedza relatywna lub relatywna świadomość sytuacyjna jest definiowana jako iloraz:

$$\Gamma = \frac{K_B}{K_R}, \; K_R \neq 0.$$

Uwaga:

K_B jest nieograniczone z góry, zaś K_R jest ograniczone z dołu przez 0.

Przewaga informacyjna

Oczekuje się, że armia wieku informacyjnego będzie w stanie w pełni wykorzystać możliwości jakie drzemią w przewadze informacyjnej. Rodzi się nowe pytanie – jaki wpływ może wywołać przewaga informacyjna na sposób dowodzenia w przyszłości? Amerykańska wizja armii (dokument Army Vision 2010) opiera się na pojęciu przewagi informacyjnej. Przewaga informacyjna definiowana jest jako zdolność do gromadzenia, przetwarzania i rozpowszechniania nieprzerwanego potoku informacji, przy pozbawieniu tych samych możliwości przeciwnika. Zdefiniowanie pojęcia wiedzy relatywnej umożliwia nam dokonanie oceny przewagi informacyjnej pomiędzy Czerwonymi (**R**) i Niebieskimi (**B**).

Możliwe reakcje

Jeśli	*Wtedy*	*I*
$K_B > K_R$	$\Gamma > 1$	Niebiescy posiadają przewagę informacyjną
$K_B < K_R$	$\Gamma < 1$	Czerwoni posiadają przewagę informacyjną
$K_B = K_R$	$\Gamma = 1$	Brak przewagi informacyjnej

Źródło: R. Darilek i inni, Miary efektywności dla armii wieku informacyjnego, Centrum Rand Arroyo, 2002 – tłumaczenie z języka angielskiego, http//www.rand.org/organization/ard/

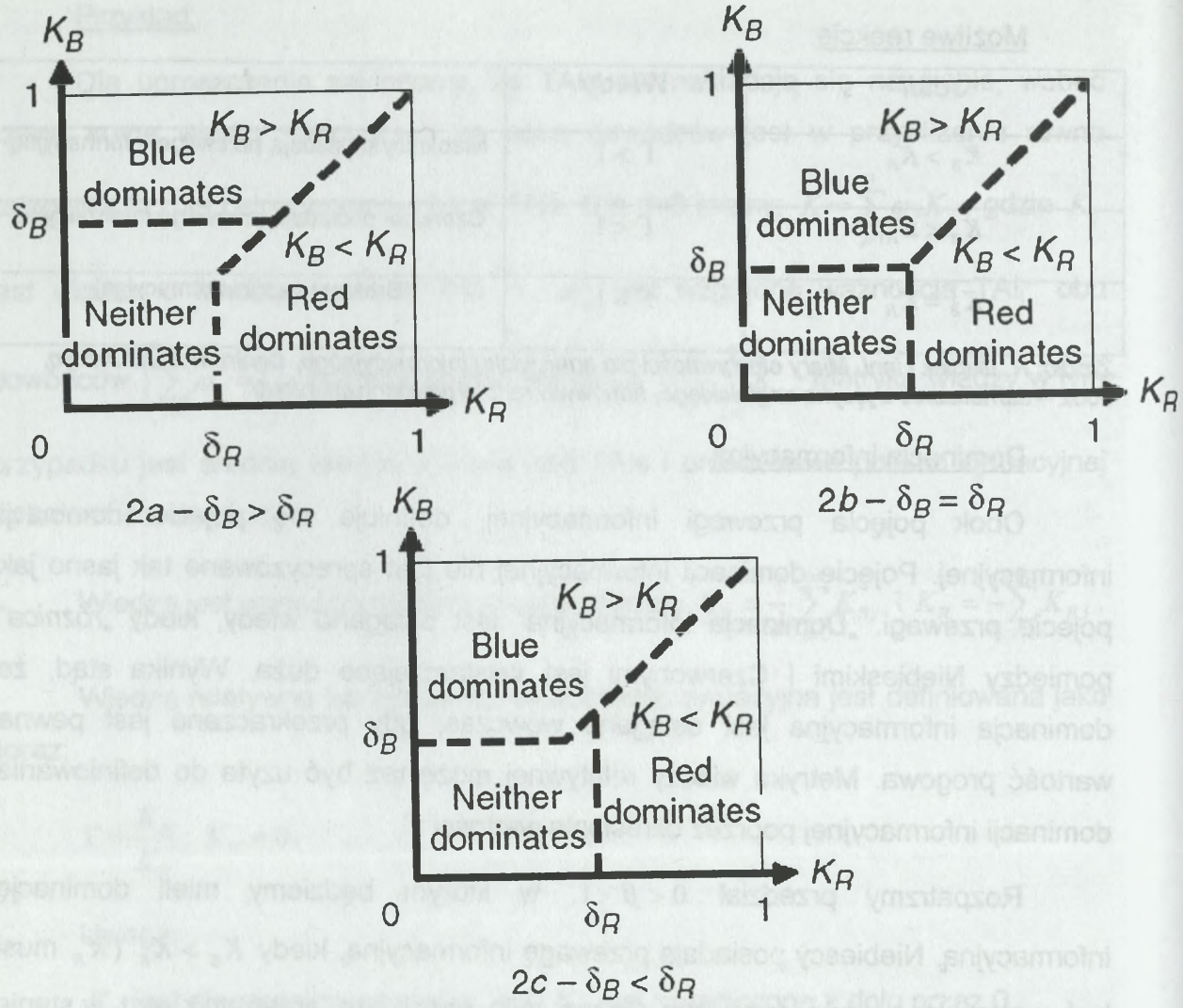
Dominacja informacyjna

Obok pojęcia przewagi informacyjnej, definiuje się pojęcie dominacji informacyjnej. Pojęcie dominacji informacyjnej nie jest sprecyzowane tak jasno jak pojecie przewagi. „Dominacja informacyjna" jest osiągana wtedy, kiedy *„różnica"* pomiędzy Niebieskimi i Czerwonymi jest wystarczająco duża. Wynika stąd, że dominacja informacyjna jest osiągana wówczas, gdy przekraczana jest pewna wartość progowa. Metryka wiedzy relatywnej może też być użyta do definiowania dominacji informacyjnej poprzez określenie wartości Γ.

Rozpatrzmy przedział $0 < \beta < 1$, w którym będziemy mieli dominację informacyjną. Niebiescy posiadają przewagę informacyjną, kiedy $K_B > K_R$ (K_R musi być wartością na tyle dużą aby można było uznać, że przeciwnik jest w stanie osiągnąć przewagę informacyjną)[13], wtedy $1 \geq K_B - K_R \geq \beta$. Dzieląc obie strony przez K_R otrzymujemy:

$$\frac{1}{K_R} \geq \Gamma - 1 \geq \frac{\beta}{K_R}.$$

[13] *Jeśli K_R jest bardzo małe, to nie można mówić o przewadze informacyjnej a w konsekwencji nie można mówić o uzyskaniu dominacji informacyjnej.*



Dominacja informacyjna

Źródło: R. Darilek i inni, Miary efektywności dla armii wieku informacyjnego, Centrum Rand Arroyo, 2002 – tłumaczenie z języka angielskiego, http//www.rand.org/organization/ard/

Daje to ograniczenie Γ do przedziału:

$$1+\frac{\beta}{K_R} \le \Gamma \le 1+\frac{1}{K_R}.$$

Jeśli interesowałyby nas warunki, przy których czerwoni uzyskaliby przewagę informacyjną, konieczne byłoby przeprowadzenie podobnego rozumowania.

Graficzne zobrazowanie dominacji informacyjnej przedstawia powyższy rysunek. Zobrazowanie to pozwala zrozumieć różnicę pomiędzy przewagą informacyjną a dominacja informacyjną. Na uwagę zasługuje fakt, że pomimo

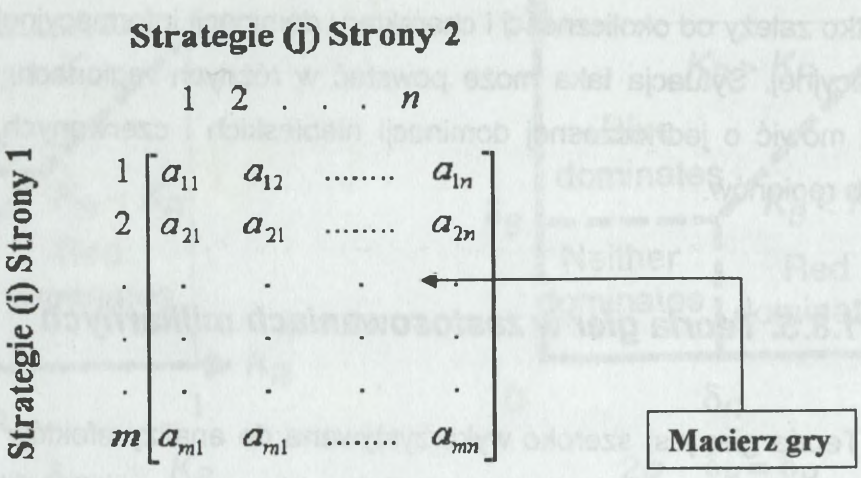
dominacji jednej ze stron, możliwa jest nadal przewaga informacyjna drugiej strony. Wszystko zależy od okoliczności i charakteru dominacji informacyjnej, bądź przewagi informacyjnej. Sytuacja taka może powstać w różnych regionach. Oznacza to, że można mówić o jednoczesnej dominacji niebieskich i czerwonych, ale dla dwóch różnych regionów.

1.8.5. Teoria gier w zastosowaniach militarnych

Teoria gier jest szeroko wykorzystywana do analizy efektów wyboru strategii alternatywnych celem osiągnięcia założonych celów militarnych. W przypadku dwuosobowych gier z zerową sumą, tzn. gdy wygrana jednego gracza jest stratą gracza drugiego, obaj gracze mają kilka alternatywnych strategii, które mogą realizować, a chociaż każdy jest świadom strategii dostępnych swojemu przeciwnikowi, żaden z nich nie jest pewny, jaką strategię wybierze przeciwnik. Każdy gracz wybiera taką strategię, która maksymalizuje jego zysk. Jednocześnie każdy gracz zabezpiecza się przed wyborem takiej strategii jego przeciwnika, która może przyczynić się do zmniejszenia zysku.
W działaniach obu graczy widać siłę oddziaływania informacji na wynik walki. Każdy z graczy reprezentuje stronę w walce.

Wszystkie gry mają strukturę taką, jak niżej. Strony: 1 i 2, mogą wybrać odpowiednio strategie i = 1, 2, 3, ..., m oraz j = 1, 2, 3, ..., n. Dla każdej pary strategii istnieje pewien zysk a_{ij}. Zysk a_{ij} jednej strony, jest jednocześnie stratą a_{ij} strony drugiej.

Podczas gdy strona pierwsza maksymalizuje swój zysk, strona druga minimalizuje swoje straty.



Przypadki zmiennej wiedzy

Przykład:

O wojnie moglibyśmy myśleć abstrakcyjnie w następujący sposób. W dowolnej walce wybór strategii Strony 1 będzie miał zasadniczy wpływ na wynik, podobnie jak dla Strony 2. W zależności od warunków walki (stosunki sił, teren, itp.), możliwe strategie mogą powodować większe lub mniejsze różnice.

Podobnie do powszechnie uwzględnianych (wyżej wymienionych) warunków walki, należy uwzględnić wartość informacji. Można rozważyć pewne abstrakcyjne przypadki, w których wybór strategii ma bardzo zróżnicowane konsekwencje w odniesieniu do uzyskanych wyników.

Możliwe są cztery przypadki:

- **Gra I:** dla armii współczesnej – przypadek klasyczny (obie strony posiadają prawidłową wiedzę). Strona pierwsza i Strona druga mają wspólną i prawidłową wiedzę w postaci wszystkich wartości z macierzy zysków **A**. Obie strony mają tę samą informację o zyskach, ale nie są świadome, jakich wyborów dokonuje przeciwnik. Żadna ze stron nie posiada przewagi wiedzy.
- **Gra 2:** Armia XXI wieku (Strona pierwsza posiada prawidłową informację, a Strona druga informację nieprawidłową). Strona pierwsza posiada prawidłową wiedzę o wszystkich wartościach **A** = $\mathbf{A}_1$, a Strona druga dysponuje całkowicie *nieprawidłowym* rozumieniem macierzy zysków. Symulacja tego stanu odbywa

się poprzez dostarczenie Stronie drugiej macierzy zysków **A** = $\mathbf{A_2}$ złożonej z pewnego zestawu liczb losowych z przedziału od 0 do 100. Dlatego też Strona druga podejmować będzie decyzje oparte na informacji fałszywej. Mimo całkowitej abstrakcji, pozwala to na opis pewnej sytuacji, w której Armia XXI wieku posiadająca luksusową informację walczy z przeciwnikiem, który nie tylko nie posiada ważnej informacji, ale także jest całkowicie wprowadzony w błąd. Sytuacja ta może być traktowana jako przypadek, w którym Niebiescy (Stroma pierwsza) posiadają przewagę informacyjną.

- **Gra 3:** AAN (Strona pierwsza posiada prawidłową informację. Strona druga posiada prawidłową informację. Strona pierwsza zna wybór Strony drugiej). Strona pierwsza i Strona druga posiadają prawidłową wiedzę o wartościach **A**, podobnie jak w Grze 1. Strona druga wybiera swoją strategię minimax j* z prawidłowej macierzy **A**. Jednakże, Strona pierwsza zna wybór Strony drugiej, i zamiast dokonywać wyboru swojej strategii maximin (i), skupia się raczej, jedynie na zyskach odpowiadających wyborowi minimax Strony drugiej i maksymalizuje swój zysk. Symuluje to przypadek, w którym Strona pierwsza posiada perfekcyjny wywiad, a w wyniku, inny rodzaj lub wyższy poziom przewagi informacyjnej. Mimo, że informacja bazowa Strony drugiej w tym przypadku (w przeciwieństwie do Gry 2) nie jest zła, to jest ona wyraźnie gorsza w porównaniu do Strony pierwszej.
- **Gra 4:** AAN (Strona pierwsza posiada informację prawidłową. Strona druga posiada informację nieprawidłową, Strona pierwsza zna wybór Strony drugiej). W grze czwartej Strona pierwsza posiada prawidłową wiedzę o wszystkich wartościach A = A_1, a Strona druga dysponuje całkowicie niepoprawną macierzą zysków A = A_2, złożoną z drugiego zestawu liczb losowych z przedziału między 0 i 100, jak w Grze 2. Strona druga wybiera swoją strategię minimax.j* w oparciu o nieprawidłową informację z A_2. Strona pierwsza zna wybór Strony drugiej. Zamiast wykorzystywać swoją strategię maximin, skupia się ona jedynie na zyskach odpowiadających wyborowi minimax Strony drugiej dokonanym w oparciu o nieprawidłową informację i dokonuje swojego wyboru z prawidłowej macierzy A_1. Strona pierwsza posiada informację perfekcyjną (wiedza maksymalna). Może ona nawet tworzyć swoją pozycję (wykorzystując ofensywne operacje informacyjne) przez aktywną znajomość faktu, że Strona druga posiada

złą informację. Zatem Strona pierwsza posiada nie tylko przewagę informacyjną ale także dominację informacyjną.

Z gier tych wynika wyraźny wniosek, że przewaga i dominacja informacyjna pochodzi z dynamicznych interakcji między obu stronami. Mogą się one zmieniać w czasie - np. w trakcie trwania konfliktu. Stąd też powinniśmy myśleć o przewadze i dominacji informacyjnej w kategoriach dynamicznych.

Macierze gier

Porządkując możliwe wybory jednej strony w poziomie a drugiej w pionie, uzyskujemy macierz w układzie Strona 1 – Strona 2. Wpisy w tej macierzy stanowią zyski obu stron (zysk Strony 1 stanowi jednocześnie stratę strony 2). Zawartość macierzy stanowią liczby będące wynikiem symulacji działań obu stron, zależnie od przyjętego wariantu postępowania. W pierwszym uproszczeniu, liczby te mogą być przyjęte jako stałe. Następnie, w oparciu o zastosowany model walki, generowane są kolejne wartości będące rozwiązaniami układu równań różniczkowych. Modelowe równania różniczkowe mogą mieć postać deterministyczną, bądź też mogą być *„uzupełnione"* o czynniki losowe, stając się równaniami stochastycznymi.

Strona 1 ↓

Strona 2 ↑	Opcja 1	Opcja 2	Opcja 3	Opcja 4
Opcja 1	7	4	7	2
Opcja 2	8	12	16	13
Opcja 3	1	0	4	6

Przykładowa macierz gry – punkt widzenia Strony 1.
Źródło: opracowanie własne.

Stochastyczne równania różniczkowe są naturalnym uogólnieniem równań różniczkowych zwyczajnych. Rozwiązując układy stochastycznych równań różniczkowych otrzymujemy tzw. „portrety fazowe". Analiza obserwowanych

atraktorów przedstawiających graficzną reprezentację n - rozwiązań danego układu równań, pozwala na wyciągnięcie wniosków co do rozwiązań osobliwych oraz roli atraktorów.

1.8.6. Stochastyczne równanie logistyczne

Funkcja logistyczna jest jedną z podstawowych funkcji trendu i zajmuje wyjątkowo uprzywilejowane miejsce wśród bardzo wielu różnych postaci funkcji używanych do opisu zjawisk ekonomicznych i przyrodniczych. Wynika to stąd, że wzrost organizmów zwierzęcych i roślinnych, liczebność organizmów żywych bytujących wokreślonych warunkach, jak i produkcja całych gałęzi przemysłu, przebiegają wsposób dający się opisać krzywą logistyczną. Jej równanie można uzyskać na drodze dedukcyjnej wychodząc z rozważań fizykalnych. Równaniem krzywej logistycznej możemy opisać wszystkie zjawiska, których prędkość rozwoju jest wprost proporcjonalna do iloczynu osiągniętego wzrostu nazywanego czynnikiem rozpędu, oraz do odległości tego wzrostu od poziomu nasycenia (a-y), który możemy nazwać czynnikiem hamowania, gdyż z upływem czasu wartość tego czynnika maleje.

Otrzymujemy równanie różniczkowe noszące nazwę prawa wzrostu Robertsona:

$$\frac{dy}{dx} = ky(a-y),$$

gdzie: k > 0 jest współczynnikiem proporcjonalności,

a jest poziomem nasycenia (rzędną asymptoty krzywej logistycznej).

Postać funkcji logistycznej (zależna od wartości jej parametrów) wykorzystywana jest między innymi w ekonometrii do wyznaczania trendu logistycznego.

Rozdzielając zmienne w powyższym równaniu otrzymujemy:

$$\left(\frac{1}{y} + \frac{1}{a-y}\right)dy = akdx,$$

co po rozwiązaniu względem y prowadzi do wzoru:

$$y = \frac{a}{1+e^{-akx-C_1}},$$

gdzie C_1 jest dowolną stałą[14].

Podstawiając $c = ak$ oraz $b = e^{-C_1}$ otrzymujemy równoważną postać krzywej logistycznej[15]:

$$y = \frac{a}{1 + be^{-\alpha x}}.$$

Powyższa funkcja jest nieliniową funkcją trzech parametrów a, b, c[16]. Można wykazać, że funkcja jest stale rosnąca, najpierw w tempie coraz bardziej przyspieszonym $(y' > 0)$, a następnie w tempie malejącym $(y'' < 0)$, aż do niemal całkowitego zahamowania wzrostu, o czym świadczy fakt, że krzywa zbliża się asymptotycznie do prostej $y = a$, co określa się stwierdzeniem, że z biegiem czasu

---

[14] *S. Smolik, Wyznaczanie parametrów krzywej logistycznej, Przegląd statystyczny R.XXXII- zeszyt 4- 1985, s.365 – 373.*

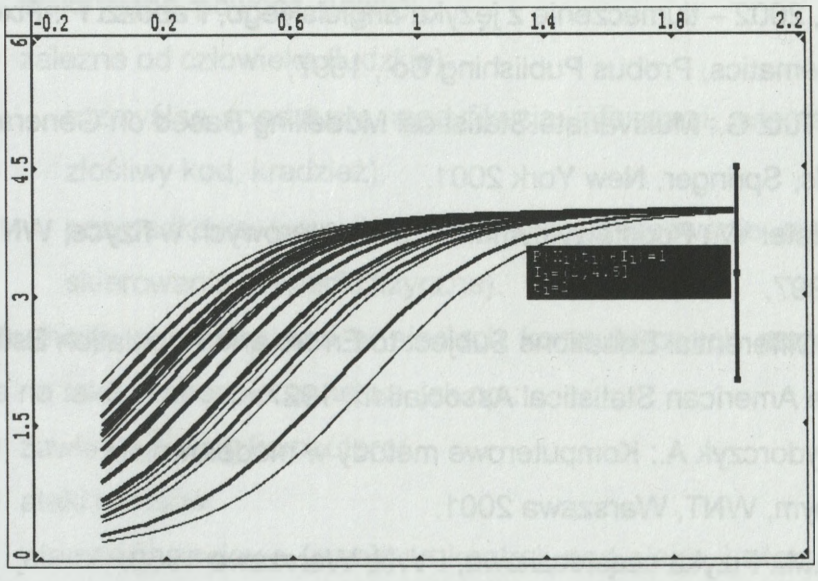
[15] *H.Hotelling, Differential Equations Subject to Errors and Population Estimates, Journal of the American Statistical Association, 1927 s. 283 –292.*

[16] *Zainteresowanie krzywą logistyczną sięga końca XIX wieku. Pionierem był P. F. Verhulst, a pierwszym propagatorem jej wykorzystania R. F. Pearl. To on nadał jej ostateczną postać stosowaną z dużym powodzeniem do dzisiaj. Demografowie (np. A.J. Lotka) i biolodzy jako pierwsi próbowali posłużyć się krzywą logistyczną do wyrażenia prawa rozwoju populacji. Krzywą logistyczną można dobrze dopasować do szeregu czasowego obrazującego ilościowy wzrost organizmów żywych w ustalonych warunkach (określony zapas żywności lub określony dopływ żywności). Krzywa ta może również dobrze opisywać wzrost ilościowy organizmów żywych wszędzie tam, gdzie nie nastąpiła jeszcze ingerencja człowieka w ich życie, np. w rezerwatach ścisłych czy niedostępnych obszarach. Wzrost populacji ludzkiej nie rozwija się dokładnie według tej krzywej. Wpływa na to wiele warunków społeczno-ekonomicznych oddziałujących na zasoby żywności. Podważyło to możliwość wykorzystania krzywej logistycznej jako uniwersalnego prawa rozwoju populacji. Wykazano, że rozwój ludności Szwecji przebiegał zgodnie z krzywą logistyczną. Rozwój ten w ciągu ostatnich dwóch stuleci odbywał się prawie w izolacji (nie oddziaływały na niego w znacznym stopniu czynniki zewnętrzne).Funkcja logistyczna dobrze opisuje popyt na dobra trwałego użytku, np. na samochody w krajach wysoko rozwiniętych, na telewizory, na motocykle i motorowery, na motocykle i skutery, na radioodbiorniki; dobrze obrazuje również wzrost liczby abonentów telefonicznych w Polsce. W Polsce zastosowano funkcję logistyczną do badania popytu na dobra trwałego użytku. Na podstawie danych dotyczących stanu posiadania motocykli i rowerów w gospodarstwach wiejskich w Polsce w latach 1951-1962 dokonano ekstrapolacji powstałej funkcji na lata 1963-1966. Podkreślono przy tym, że funkcja logistyczna może dawać dobre prognozy krótkoterminowe i średnioterminowe, natomiast prognozy długoterminowe są ryzykowne. Za pomocą funkcji logistycznej możemy opisać zależność wydajności pracy od stażu pracy na ustalonym stanowisku w przypadku pracowników, którzy nie przekroczyli wieku 50 lat (po przekroczeniu tej granicy wieku wydajność spada). Warto podkreślić, że przy powyższej aproksymacji pomijamy wpływ postępu technologicznego. Krzywa logistyczna dobrze opisuje zmiany szybkości pewnych zjawisk chemicznych, np. szybkości rozpuszczania się soli w wodzie. Podobnie, zależność wielu reakcji od czasu ich trwania, zwłaszcza reakcji syntezy, np. reakcji wody z karbidem, w wyniku, której otrzymujemy acetylen. W. Winkler zaproponował użycie krzywej logistycznej do opisu zmian gęstości sieci dróg kolejowych na określonym terenie. Funkcję logistyczną zastosowano w medycynie (np. rozwój pewnych chorób w organizmie) i farmakologii (sposób dawkowania niektórych leków). Podjęto również próby wykorzystania krzywej logistycznej w rehabilitacji i antropologii.*

krzywa logistyczna gaśnie. Wynika stąd, że obserwowany gasnący wzrost badanego procesu zmierza do stanu stagnacji[17].

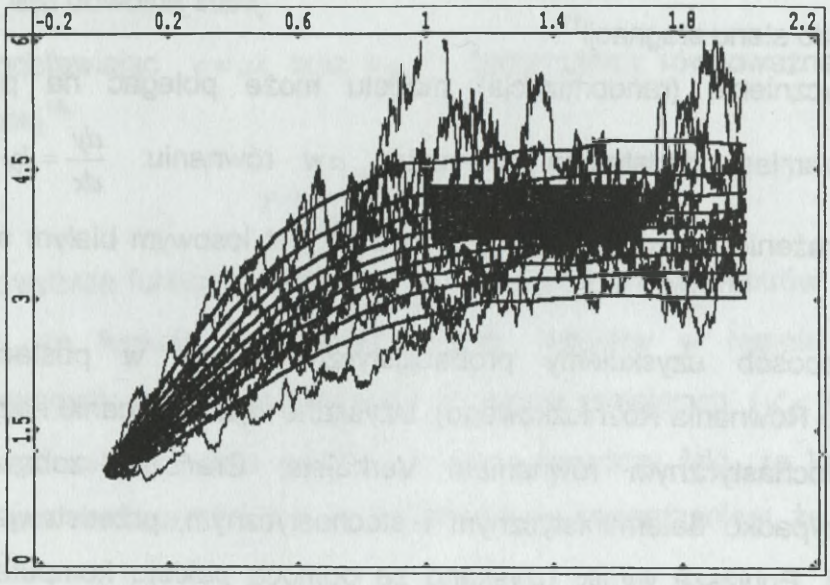
Ustochastycznienie (randomizacja) modelu może polegać na przyjęciu założenia, że zamiast dodatniego parametru a w równaniu: $\frac{dy}{dx} = ky(a-y)$, uwzględnimy wyrażenie $a+\sigma\cdot\xi_t$, gdzie $\{\xi_t : t \geq 0\}$ jest losowym białym szumem gaussowskim.

W ten sposób uzyskujemy probabilistyczny model w postaci **SRR** (**S**tochastycznego **R**ównania **R**óżniczkowego). Uzyskane wyżej równanie nazywa się gaussowskim stochastycznym równaniem Verhulsta. Graficzne zobrazowanie problemu, w przypadku deterministycznym i stochastycznym, przedstawiają dwa poniższe rysunki. Poniższe wyniki uzyskano za pomocą pakietu komputerowego SDE-SOLVER[18]. W przyszłości możliwe będzie wykorzystanie tego pakietu do prac badawczych nad postacią stochastycznego modelu przewagi informacyjnej.



[17] *L.Fahrmeir, G.Tutz, Multivariate Statistical Modelling Based on Generalized Linear Models, Springer, New York 2001, s.403-404.*

[18] *A.Janicki, A.Izydorczyk, Komputerowe metody w modelowaniu stochastycznym, WNT, Warszawa 2001.*



Bibliografia:

1. Cichy M., Nimańczuk J., Szpakowicz S.: Zbiór zadań z propedeutyki informatyki, PWN Warszawa 1977.
2. Darilek R. i inni: Miary efektywności dla armii wieku informacyjnego, Centrum Rand Arroyo, 2002 – tłumaczenie z języka angielskiego, Fabozzi F.: Fixed income mathematics, Probus Publishing Co., 1997.
3. Fahrmeir L., Tutz G.: Multivariate Statistical Modelling Based on Generalized Linear Models, Springer, New York 2001.
4. Heermann Dieter W.: Podstawy symulacji komputerowych w fizyce, WNT Warszawa 1997.
5. Hotelling H.: Differential Equations Subject to Errors and Population Estimates, Journal of the American Statistical Association, 1927.
6. Janicki A., Izydorczyk A.: Komputerowe metody w modelowaniu stochastycznym, WNT, Warszawa 2001.
7. Matwiejew A.M.: Fizyka cząsteczkowa, PWN, Warszawa 1989.
8. Smolik S.: Wyznaczanie parametrów krzywej logistycznej, Przegląd statystyczny R.XXXII- zeszyt 4-1985.
9. Spustek H.: Przewaga w walce i operacji, rozprawa habilitacyjna AON, Warszawa 2002.
10. Zalewski: Wykłady z termodynamiki fenomenologicznej i statystycznej, PWN Warszawa 1978.

1.9. METODYKA OCENY ZAGROŻEŃ INFORMACYJNYCH

1.9.1. Analiza możliwych i dopuszczalnych zagrożeń informacyjnych

W dobie dynamicznego rozwoju techniki komputerowej i systemów informatycznych zintegrowanych z telekomunikacją, gdy efektywność każdej organizacji, zależy od ich systemów informacyjnych stanowiących podstawę systemów informatycznych, informacja występująca jako towar i zasób jest narażona na bardzo różne zagrożenia. Obok zagadnienia bezpieczeństwa systemów komputerowych i zawartej w nim informacji występuje także zagadnienie bezpieczeństwa użytkownika w aspekcie odpowiedzialności prawnej za naruszenie praw autorskich i własności intelektualnej. Polska norma PN-I-13335-1 - *"Wytyczne do zarządzania bezpieczeństwem systemów informatycznych"* wyróżnia m.in. następujące rodzaje zagrożeń:

a) środowiskowe - niezależne od człowieka (trzęsienie ziemi, wyładowania elektryczne, powódź, pożar);
b) zależne od człowieka (ludzkie):
   - rozmyślne (podsłuch, modyfikacja informacji, włamania do systemu, złośliwy kod, kradzież);
   - przypadkowe (pomyłki i pominięcia, skasowanie pliku, nieprawidłowe skierowanie, wypadki fizyczne).

Informacja przekazywana w sieciach komputerowych może być dodatkowo narażona na takie niebezpieczeństwa, jak np.:

a) zawieszenie się komputera;
b) ataki wirusów;
c) włamania sieciowe (przejęcie kontroli nad siecią i włamania do kolejnych komputerów pracujących w sieci), np.:
d) sniffing to wykorzystanie interfejsu sieciowego do odbierania danych nie przeznaczonych dla komputera, w którym ten interfejs jest zainstalowany. Możliwość taką ma wiele różnorodnych maszyn (np. sniffery). Sniffery, czyli „węszyciele" są programami do analizy ruchu w sieci. Dla administratorów są znakomitymi narzędziami diagnostycznymi. Pozwalają

podejrzeć każdy pakiet przesyłany łączami. Dzięki nim można rozwiązać wiele skomplikowanych problemów w sieciach komputerowych:

- spoofing (omijanie przez hackera zabezpieczeń wprowadzonych do sieci przez jej administratora, podszywanie i udawanie innego komputera);
- hijacking (przechwycenie transmisji pomiędzy dwoma zdalnymi komputerami).

W ostatnim czasie odnotowuje się gwałtowny wzrost włamań i innych naruszeń bezpieczeństwa systemów komunikacyjnych. Wprowadzenie nowych typów usług przez operatorów sieci, jak np. audioteks, telekonferencje, obsługa kart kredytowych i telefonicznych do opłat otwiera duże możliwości nadużyć i nielegalnego wykorzystania zasobów telekomunikacyjnych. Oszustwa telekomunikacyjne stały się niezwykle dochodowym międzynarodowym procederem. Szacuje się np., że straty ponoszone przez operatorów telekomunikacyjnych wskutek oszustw i nadużyć wynoszą od 2 do 5%, a w niektórych przypadkach do 20% całości obrotu danego operatora.

Przytoczone wyżej zagrożenia powodują, iż informacja musi być chroniona. Ochrona informacji ściśle powiązana jest z polityką bezpieczeństwa poszczególnych instytucji. Cytowana już wyżej polska norma PN-I-3335-1, definiuje politykę bezpieczeństwa instytucji w zakresie systemów informatycznych (ang. *IT security policy*) jako: zasady, procedury zarządzania, które określają, jakie zasoby (włącznie z informacjami wrażliwymi) są zarządzane, chronione i dystrybuowane w danej instytucji i jej systemach informatycznych.

Celem polityki bezpieczeństwa informacyjnego jest stworzenie podstaw, procedur i wymagań niezbędnych dla zapewnienia właściwej ochrony przetwarzanym informacjom. Obejmuje ona bezpieczeństwo środków łączności i informatyki, a także bezpieczeństwo osobowe, fizyczne, przemysłowe i emisyjne. Głównym założeniem polityki bezpieczeństwa jest określenie:

- jakie grupy informacji będą chronione;
- w jakich systemach informacje te mogą być przetwarzane;
- kto i na jakich zasadach ma mieć do nich dostęp;
- kto jest odpowiedzialny za zarządzanie informacją;
- kto jest odpowiedzialny za zarządzanie bezpieczeństwem informacji;

- jakie warunki należy spełnić aby uzyskać poświadczenia, świadectwa i certyfikaty.

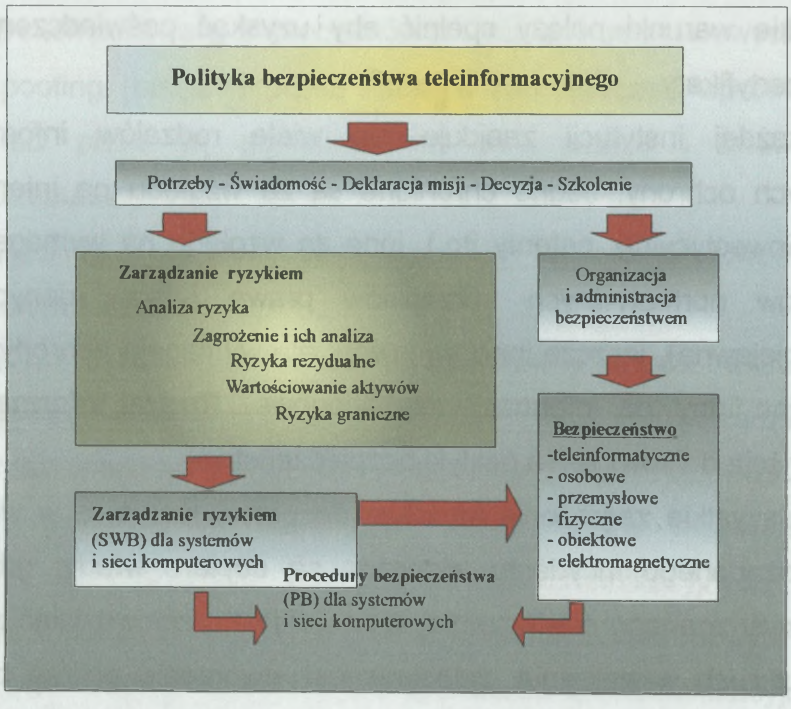
W każdej instytucji znajduje się wiele rodzajów informacji (danych) wymagających ochrony. Jedne chronione są ze względu na interes firmy (dane finansowe, inwestycyjne, patenty itp.), inne ze względu na wymagania wynikające z dokumentów normatywnych i przepisów prawa (zbiory danych osobowych, informacje niejawne), jeszcze inne są jawne, ale wymagają ochrony ze względu na konkurencyjne firmy (np. informacje marketingowe). **Rodzaj informacji (grupa)** jest punktem wyjścia do stworzenia polityki bezpieczeństwa!

Nie wszystkie zagrożenia są łatwe do przewidzenia, a w wielu wypadkach skutki niepożądanego incydentu widoczne są dopiero wtedy, gdy nastąpiła już szkoda, w myśl znanego powiedzenia, iż łatwiej jest przeciwdziałać zagrożeniom niż usuwać skutki ich wystąpienia, zalecane jest stworzenie polityki bezpieczeństwa, odzwierciedlającej cele i strategie danej instytucji z uwzględnieniem środowiska, w jakim się znajduje.

Można wyróżnić wiele elementów wchodzących w skład polityki bezpieczeństwa:

- potrzeb, świadomość, deklaracja misji, decyzje, szkolenie;
- analiza i zarządzanie ryzykiem;
- organizacja i administracja bezpieczeństwem;
- INFOSEC (bezpieczeństwo teleinformatyczne, osobowe, przemysłowe, fizyczne, obiektowe, elektromagnetyczne,...);
- itd.

Opracowanie spójnej polityki bezpieczeństwa jest w obecnej sytuacji rozwoju rynku usług elektronicznych swoistą koniecznością. Praktycznie większość firm powołuje w swoich strukturach komórki odpowiedzialne wyłącznie za bezpieczeństwo i ochronę gromadzonej i przesyłanej informacji. Specjalizacja jest dobrą praktyką, ponieważ należy oddzielać funkcje i role administracji zasobami teleinformatycznymi firmy od czynności i procedur związanych z podwyższeniem ich bezpieczeństwa.



Rysunek 9.1. Polityka bezpieczeństwa teleinformacyjnego.

Przyjmuje się, że polityka bezpieczeństwa systemów teleinformatycznych musi być podporządkowana ogólnej polityce bezpieczeństwa firmy a w konsekwencji bezpieczeństwa informacyjnego państwa. Ogólna polityka określa bowiem, zakres prac oraz obszary szczególnej ochrony. Opracowanie ogólnej polityki bezpieczeństwa rozpoczyna się od określenia zasobów podlegających ochronie. Zasoby należy zidentyfikować, sklasyfikować oraz pogrupować. Wiedza nt. rodzaju ochranianych zasobów jest kluczowa, co do dalszego zakresu czynności. Kolejnym krokiem jest oszacowanie wartości chronionych zasobów. Może to być bardzo trudne do jednoznacznego określenia, jednakże nawet zgrubna estymacja może pozwolić później trafnie wybrać lub odrzucić techniki ochrony.

Zastosowany system ochrony powinien być skuteczny, a koszt jego zastosowania powinien być równy lub wyższy niż strata w wartości informacji poniesiona przy ewentualnym ataku. Wybór właściwego systemu ochrony jest tym prostszy, im analiza zagrożeń oraz stopnia ryzyka pełniejsza. Administrator bezpieczeństwa podczas opracowywania zasad powinien uwzględnić m.in. takie elementy jak:

- logiczny nadzór bezpieczeństwa;
- fizyczny nadzór bezpieczeństwa;
- integralność systemu oraz informacji;

- poufność informacji;
- opracowanie zasad oraz procedur dla personelu odpowiedzialnego za sieć;
- opracowanie zasad oraz procedur dla użytkowników wewnętrznych oraz zewnętrznych zasobów sieciowych;
- zorganizowanie szkolenia w zakresie polityki bezpieczeństwa.

Opracowana polityka bezpieczeństwa w miarę rozwoju systemu teleinformatycznego ulega zmianie, modyfikowana jest również, jeżeli wykryte zostają w jej funkcjonowaniu luki.

Problem ochrony zasobów informacyjnych dotyczy również systemów wojskowych. Wynika to przede wszystkim z samej specyfiki wojska, gdzie duży nacisk kładzie się na szeroko rozumianą ochronę informacji. Dotyczy to w szczególności takich dziedzin, jak (wg poglądów państw sojuszniczych NATO, w kolejności priorytetów):

- operacje związane z procesem walki;
- obraz wspólnych działań operacyjnych;
- rozpoznanie wojskowe;
- logistyka / transport;
- informacje o obiektach wojskowych;
- systemy łączności oraz systemy informatyczne;
- zbieranie informacji, koordynacja działań, zarządzanie procesem obiegu informacji;
- logistyka / dostawy;
- logistyka / wsparcie medyczne;
- utrzymanie stanu osobowego;
- logistyka / utrzymanie sprzętu, konserwacja;
- plany operacyjne;
- prowadzona polityka;
- 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 całego społeczeństwa;
- zabezpieczenie zasobów informacyjnych wymaga połączenia wysiłków wszystkich korporacji (w tym czynników rządowych) w zakresie integracji osiągnięć naukowych oraz władz odpowiedzialnych za bezpieczeństwo.

1.9.2. Analiza ryzyka a analiza zagrożeń

Istnieje kilka definicji analizy ryzyka. Najprościej ujmując, ***Analiza ryzyka*** *(dla potrzeb bezpieczeństwa teleinformatycznego) jest procesem identyfikacji (jakościowej i ilościowej) ryzyka utraty bezpieczeństwa teleinformatycznego.* Prowadzenie analizy ryzyka jednocześnie identyfikuje obszary wymagające ochrony. Systematycznie wykonywany proces analizy ryzyka pozwala na wprowadzenie działań profilaktycznych.

W systemowym ujęciu analiza ryzyka składa się z następujących etapów[1]:

I. Szacowania ryzyka:

1. Identyfikacji zagrożeń;
2. Określeniu elementów systemu podatnych na zagrożenia;
3. Określeniu prawdopodobieństwa wystąpienia skutków zagrożeń w przypadku zajścia takich zagrożeń.

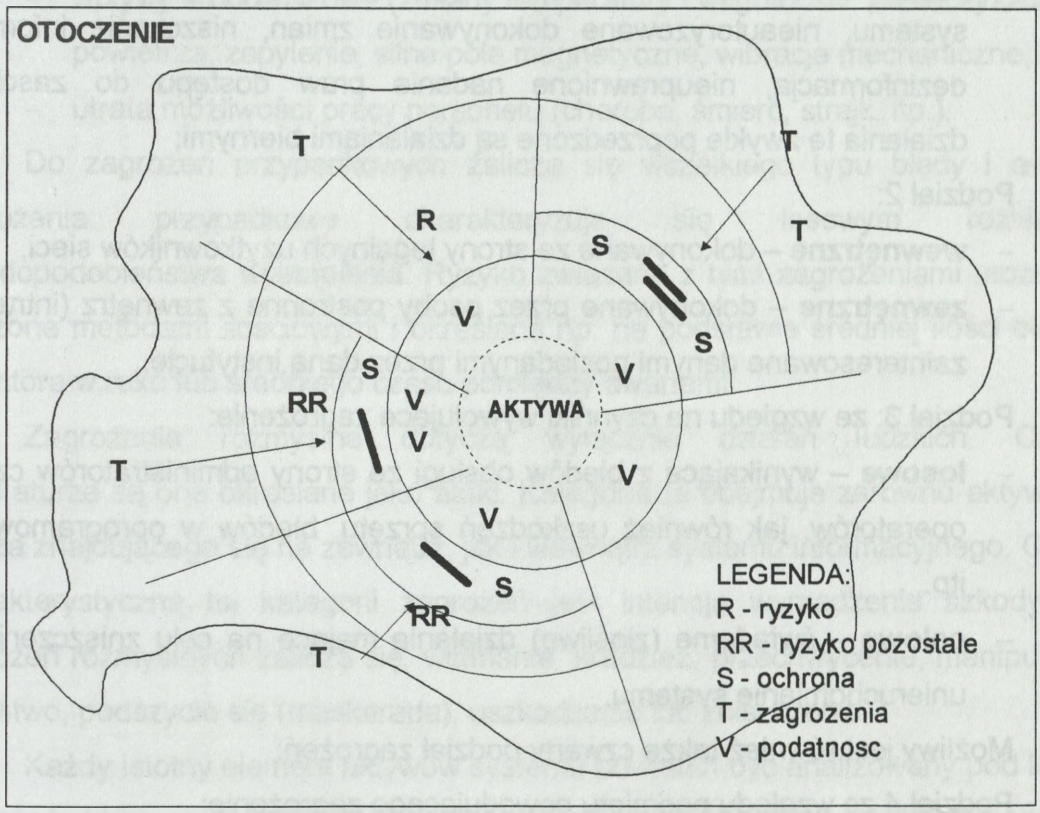
II. Oceny akceptowalności ryzyka:

1. Określeniu stopnia szkodliwości skutków zagrożenia (szacowanie kosztów poniesionych w wypadku realizacji zagrożenia)
2. Oszacowanie kosztów zabezpieczeń;
3. Analiza strat (liczonych w określonej walucie) – w przypadku realizacji zagrożenia i braku zabezpieczeń
4. Analiza zysków, gdy zainstalowane zabezpieczenia przeszkodzą w realizacji zagrożenia.

W projekcie polskiej normy Pr PN-I-02000 znajdujemy taką oto definicję: *„analiza ryzyka - systematyczna metoda identyfikowania aktywów systemu przetwarzania danych, zagrożeń tych aktywów i podatności systemu na te zagrożenia (risk analysis)".*

Norma podkreśla terminy: aktywa, zagrożenia i podatność. Należy się z tym zgodzić, zwłaszcza, że aktywa (programowe, fizyczne czy informatyczne) to przecież wszystko, co posiadamy, to nasze zasoby o ustalonej wrażliwości i podatności.

Do pewnego usystematyzowania pojęć, posłużymy się modelem graficznym elementów analizy ryzyka (ISO 13335-1). Niejako wartością dodaną z przeprowadzonej prawidłowo analizy ryzyka jest wzrost świadomości związanej z bezpieczeństwem informacji na wszystkich poziomach organizacji (firmy) począwszy od kierownictwa najwyższego szczebla, aż do personelu operacyjnego i pomocniczego.



Rysunek 9.2. Model elementów analizy ryzyka (PN-I- 13335-1)

Reasumując: analiza ryzyka polega na ocenie wszystkich negatywnych skutków badanego przedsięwzięcia i odpowiadających im prawdopodobieństw.

Stałym elementem polityki bezpieczeństwa jest prowadzenie analiz związanych z podatnością systemów informatycznych na zagrożenia, tzw. analiza zagrożeń. Analiza ta polega na gromadzeniu informacji o możliwych zagrożeniach

[1] *Liderman K., „Bezpieczeństwo teleinformatyczne", Instytut Automatyki i Robotyki, WAT, Warszawa 2001, s. 55-56.*

systemu przetwarzania informacji w taki sposób, aby nie pominąć żadnego z zagrożeń istotnych. Stąd też istotna staje się właściwa klasyfikacja zagrożeń oraz dobór stosownego kryterium klasyfikacji.

Poniżej przedstawiono przykładowe klasyfikacje wg różnych kryteriów podziału:

Podział 1: Czynnościowe:

- **bierne** – nieuprawnione ujawnienie informacji bez oddziaływania na pracę systemu (podsłuch, analiza ruchu w sieci, emisja ujawniająca);
- **czynne** – aktywne oddziaływanie na system (nieuprawniony dostęp do systemu, nieautoryzowane dokonywanie zmian, niszczenie informacji, dezinformacja, nieuprawnione nadanie praw dostępu do zasobów); działania te zwykle poprzedzone są działaniami biernymi;

Podział 2:

- **wewnętrzne** – dokonywane ze strony legalnych użytkowników sieci,
- **zewnętrzne** – dokonywane przez osoby postronne z zewnętrz (intruzów), zainteresowane danymi posiadanymi przez daną instytucję.

Podział 3: ze względu na czynniki wywołujące zagrożenie:

- **losowe** – wynikające z błędów obsługi ze strony administratorów czy też operatorów, jak również uszkodzeń sprzętu, błędów w oprogramowaniu, itp.,
- **celowe** – świadome (złośliwe) działania mające na celu zniszczenie lub unieruchomianie systemu.

Możliwy jest również także czwarty podział zagrożeń:

Podział 4 ze względu podmiotu powodującego zagrożenie:

- **sprzętowe** – powodowane przez sprzęt,
- **programowe** – powodowane poprzez oprogramowanie,
- **osobowe** – powodowane przez ludzi.

Przedstawiona klasyfikacja zagrożeń nie wyklucza wzajemnego przenikania i nakładania się na siebie poszczególnych elementów, co oznacza, iż zagrożenie może być np. jednocześnie czynne, wewnętrzne, celowe programowe lub jednocześnie przypadkowe i sprzętowe.

Skuteczny atak na system wymaga przełamania bariery, którą stanowią zasady dostępu do systemu. Wbrew powszechnemu mniemaniu, podkreślić należy,

że największego zagrożenia należy spodziewać się strony legalnych użytkowników systemu, przy czym zagrożenie to wzrasta wraz z liczbą użytkowników i zróżnicowaniem ich uprawnień.

Wymieniane wcześniej zagrożenia zewnętrzne mogą być całkowicie niezależne od działania ludzkiego (np. katastrofy żywiołowe) albo mogą powstać na skutek awarii innych systemów (np. pożar lub zalanie). Do kategorii zagrożeń zewnętrznych należy zaliczyć:

- wypadki i katastrofy spowodowane czynnikami naturalnymi (woda, ogień, wyładowania atmosferyczne, trzęsieniem ziemi, itp.),
- wpływy środowiskowe (zmiany temperatury i wilgotności, zanieczyszczenie powietrza, zapylenie, silne pola magnetyczne, wibracje mechaniczne, itp.),
- utrata możliwości pracy personelu (choroba, śmierć, strajk, itp.).

Do zagrożeń przypadkowych zalicza się wszelkiego typu błędy i awarie. Zagrożenia przypadkowe charakteryzują się losowym rozkładem prawdopodobieństwa wystąpienia. Ryzyko związane z tymi zagrożeniami może być mierzone metodami ilościowymi i określane np. na podstawie średniej ilości błędów operatora w roku lub średniego czasu pomiędzy awariami.

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.

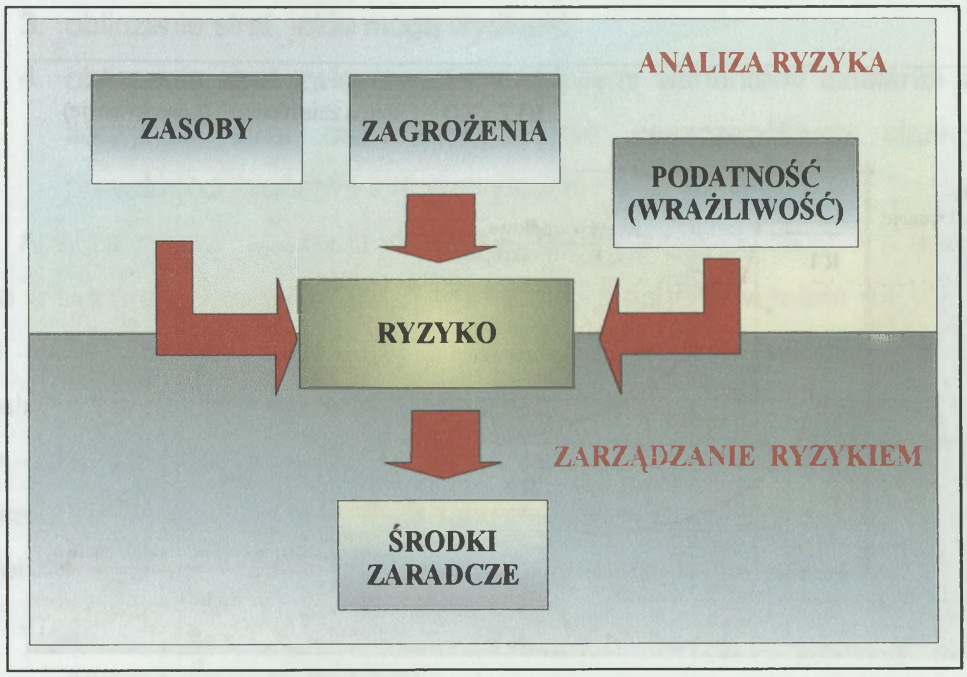
Każdy istotny element aktywów systemu powinien być analizowany pod kątem zagrożeń, które mogą przyczynić się do jego uszkodzenia lub utraty. Szczególną uwagę należy zwrócić na identyfikację sposobów, jakimi dane zagrożenie może się objawić. Przykładowo, działaniami, które mogą prowadzić do uzyskania nieupoważnionego dostępu może być podsłuch i odtworzenie (*playback)* zarejestrowanej sesji użytkownika, złamanie hasła, dołączenie nieautoryzowanych elementów do sieci, itp.

1.9.3. Zarządzanie ryzykiem

Z analizą ryzyka ściśle wiąże się pojęcie zarządzanie ryzykiem - dotyczy ono identyfikacji, kontrolowania i eliminacji lub minimalizowania prawdopodobieństwa zaistnienia niepewnych zdarzeń, które mogą mieć wpływ na decyzje informacyjne oraz zawierające skuteczny program zarządzania, obejmujący ocenę ryzyka, decyzje zarządzające, wdrożenie środków kontroli oraz sprawdzenie (przegląd) skuteczności. Jest to system metod i działań zmierzających do obniżenia stopnia oddziaływania ryzyka na funkcjonowanie systemu i do podejmowania w tym celu optymalnych decyzji. Szczegółowe poznanie charakteru i zakresu potencjalnego ryzyka pozwala na wybór w odpowiednim czasie czynności zapobiegawczych bądź też na minimalizację jego wpływu i skutków.

Kierownicy jednostek organizacyjnych oraz administratorzy muszą mieć stałą świadomość istnienia zagrożeń. Są sytuacje, w których nawet duże inwestycje i tak będą za małe i nie pozwolą na uniknięcie mało prawdopodobnych zagrożeń. Dlatego osoby funkcyjne muszą znaleźć odpowiedź na takie pytania, jak:

- co złego może się zdarzyć i z jakim prawdopodobieństwem;
- jakie będą konsekwencje zagrożenia, i w jaki sposób można je zminimalizować;
- jak duże ryzyko jest akceptowalne, i w jaki sposób można je zminimalizować,
- jakie będą koszty wprowadzenia zabezpieczeń;
- jakie mogą być straty w przypadku wystąpienia zagrożenia oraz czy koszty strat nie będą większe niż koszty zabezpieczeń.



Rysunek 9.3. Analiza ryzyka.

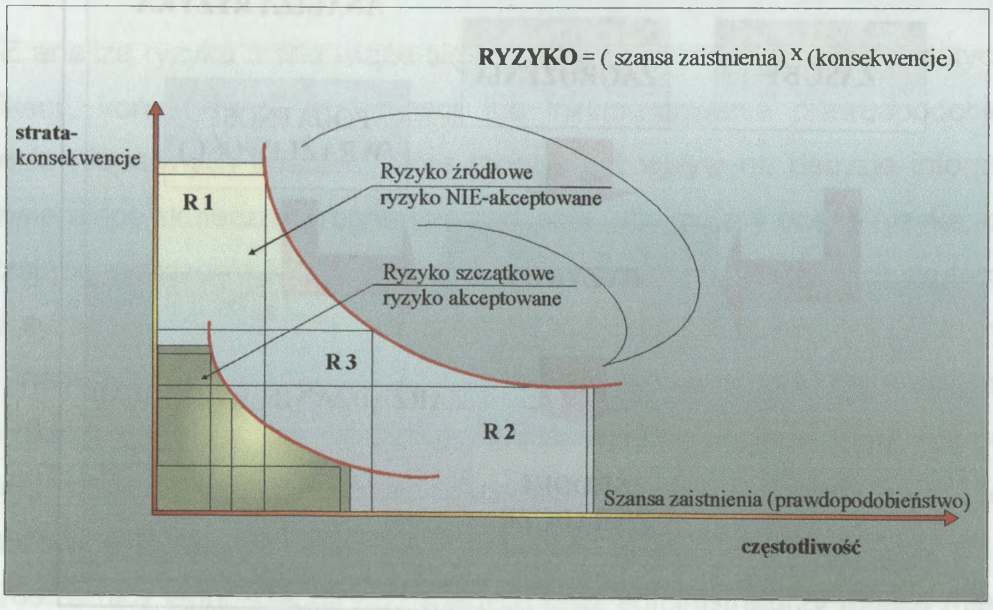
Zasadniczym celem zarządzania ryzykiem jest obniżenie ryzyka, gdyż całkowite jego wyeliminowanie nie jest możliwe. Istnieją różne definicje ryzyka. Polska norma PN-I-13335-1 – „*Wytyczne do zarządzania bezpieczeństwem systemów informatycznych*" definiuje tzw. pojęcie zarządzania ryzykiem (ang. *risk management*). Polega ono na „*porównywaniu określonego ryzyka z zyskami i/lub kosztami zabezpieczeń oraz tworzeniu strategii wdrożenia polityki bezpieczeństwa w zakresie systemów informatycznych zgodnej z celami działania danej instytucji*". Zgodnie z tą normą „*należy rozważyć różne rodzaje zabezpieczeń oraz wykonać analizę kosztów i/lub zysków. Zabezpieczenia są dobierane dla odpowiedniego ryzyka i potencjalnych następstw. Należy także wziąć pod uwagę poziom akceptowalnego ryzyka szczątkowego*".

Matematycznie można to określić jako iloczyn szansy zaistnienia danego zagrożenia i konsekwencji, jakie z tego mogą wyniknąć:

Ryzyko = (szansa zaistnienia) x konsekwencje (1)

Obniżenie ryzyka można uzyskać poprzez zastosowanie środków zabezpieczających, a obniżone w ten sposób ryzyko stanowi ryzyko szczątkowe (ang. *residual risk*). Istotnym problemem jest, do jakiego poziomu należy obniżać ryzyko, aby instytucja była zdolna ponieść koszty zabezpieczeń, a ryzyko szczątkowe

było akceptowalne. Występujące tutaj współzależności dobitnie obrazuje poniższy rysunek:



Rysunek 9.4. Zależności ryzyka.

Przy rozgraniczaniu ryzyka akceptowalnego od nieakceptowalnego niezbędna jest analiza maksymalnego dopuszczalnego ryzyka - MDR. Dopuszczalne maksymalne ryzyko rozumiane jest jako część środków własnych, jaką dana instytucja gotowa jest ponieść w przypadku „katastrofy", jak również tzw. zyski operacyjne („cash-flow") czy też gwarancje w formie odszkodowań uzyskane od firm ubezpieczeniowych. Matematycznie można to zapisać:

$$MDR = \alpha S_w + \beta Zysk + \gamma Gwarancje \quad (2)$$

gdzie:

S_w część środków własnych;

α część (procent) przeznaczony na środki własne;

β część (procent) rocznego zysku operacyjnego brutto;

γ szacunkowy wskaźnik odszkodowań.

Analiza ryzyka obejmuje cztery podstawowe etapy:

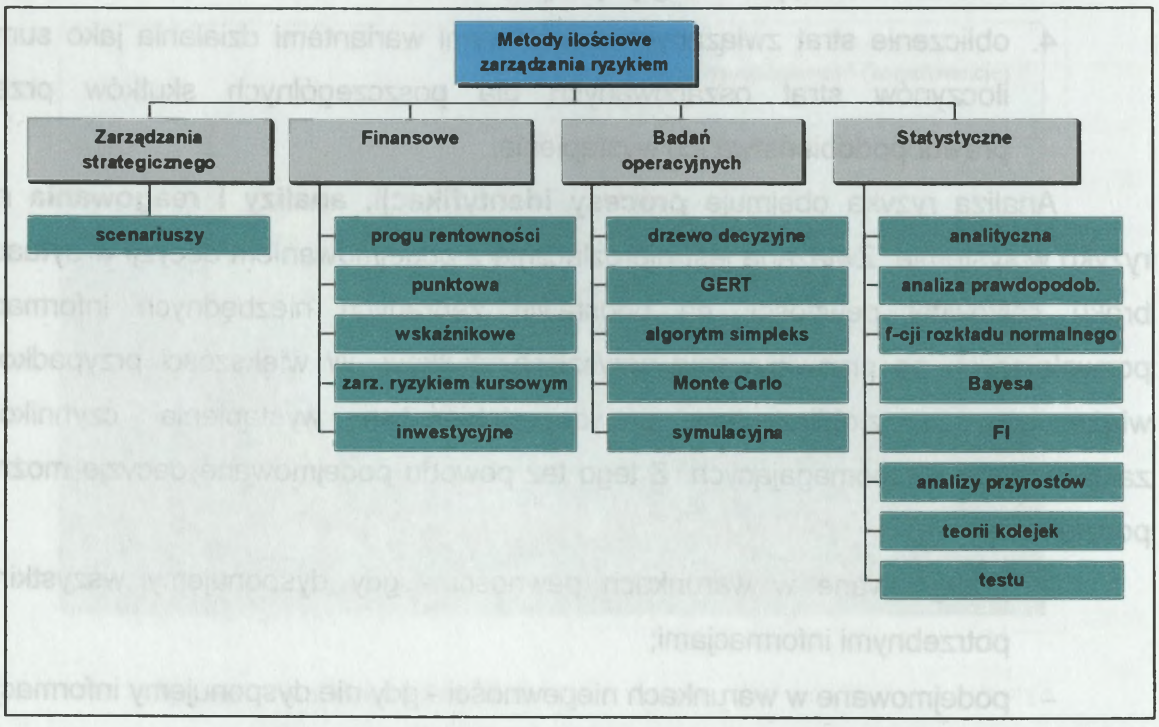
1. określenie wszystkich możliwych i prawdopodobnych niepożądanych skutków działania (bliższych i dalszych) dla każdego alternatywnego wariantu działania;

2. oszacowanie prawdopodobieństwa wystąpienia tych skutków;
3. obliczenie strat, jakie mogą wystąpić;
4. obliczenie strat związanych z możliwymi wariantami działania jako sumy iloczynów strat oszacowanych dla poszczególnych skutków przez prawdopodobieństwa ich wystąpienia.

Analiza ryzyka obejmuje **procesy identyfikacji, analizy i reagowania** na ryzyko w systemie. Związana jest nierozłącznie z podejmowaniem decyzji w sytuacji braku całkowitej pewności, na podstawie zebranych niezbędnych informacji pozwalających na przewidywanie przyszłych skutków. W większości przypadków wiąże się to z obliczeniem prawdopodobieństwa wystąpienia czynników zakłócających i wspomagających. Z tego też powodu podejmowane decyzje można podzielić na:

- podejmowane w warunkach pewności - gdy dysponujemy wszystkimi potrzebnymi informacjami;
- podejmowane w warunkach niepewności - gdy nie dysponujemy informacją o przyszłych stanach systemu i otoczenia;
- podejmowane w warunkach ryzyka - gdy na podstawie posiadanych informacji możemy ocenić prawdopodobieństwo wystąpienia różnych stanów otoczenia oraz systemu.

Ryzyko najczęściej rozumiane jest jako niebezpieczeństwo poniesienia straty, możliwość wystąpienia określonego zagrożenia lub nie osiągnięcia celu. Można je także określić jako taką sytuację, w której nie można przewidzieć przyszłych warunków eksploatacji systemu, natomiast znany jest natomiast rozkład prawdopodobieństwa ich wystąpienia. Ryzyko jest naturalnym zjawiskiem i nie można go wyeliminować. Można je natomiast ograniczać poprzez prowadzenie rozpoznania, kształtowanie, badania, kontrolę realizacji zadań.



Schemat 9.1. Metody ilościowe zarządzania ryzykiem.

W procesie zarządzania ryzykiem ważne jest, aby nie zostało pominięte żadne istotne zagrożenie, ponieważ może to wpłynąć na niewłaściwy dobór mechanizmów zabezpieczeń.

Sukces prowadzonych analiz zależy w głównej mierze od udziału zarządu najwyższego szczebla już na etapie projektu systemu teleinformatycznego.

W analizie należy uwzględnić:

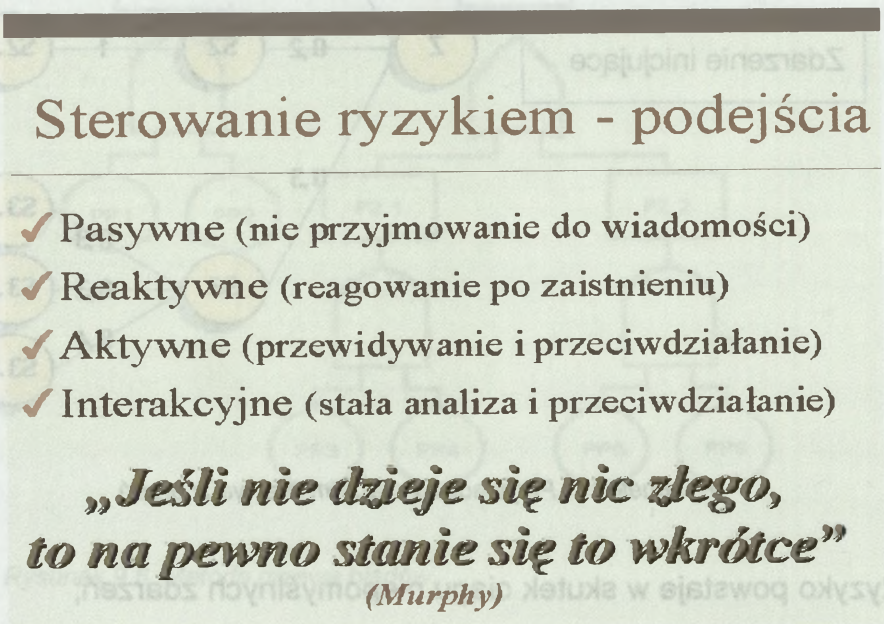
- wsparcie kierownictwa dla projektu, wyrażone na wszystkich poziomach organizacji;
- wyjaśnienie przez kierownictwo zamiarów i celów analizy ryzyka;
- wybranie przez kierownictwo wykwalifikowanego zespołu oraz formalne przekazanie pełnomocnictwa i odpowiedzialności;
- przegląd i aprobatę wyników pracy zespołu analizy ryzyka przez kierownictwo.

Dobranie składu zespołu analizy ryzyka jest sprawą krytyczną dla osiągnięcia sukcesu projektu. Rzeczą istotną jest zapewnienie reprezentacji personelu projektowego odpowiedzialnego za bezpieczeństwo:

- fizyczne;

- personelu;
- proceduralne;
- obiegu informacji i dokumentów;
- informatyki;
- łączności.

Obszary wymienione powyżej powinny być reprezentowane w zespole analiz ryzyka przez ludzi dobrze poruszających się w obszarze zarówno własnego zadania, jak i jego związkami z ogólnym zadaniem organizacji. Ważnym jest, aby kierownik zespołu lub przynajmniej któryś z członków zespołu posiadał doświadczenia w przeprowadzaniu analiz ryzyka.

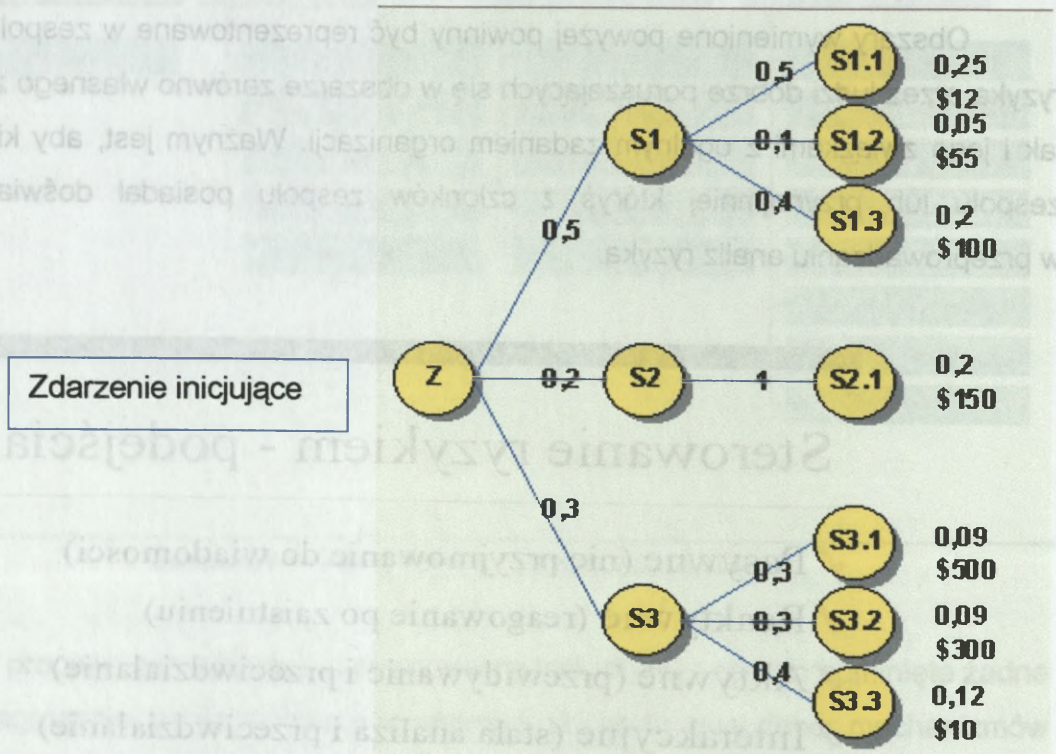


Metodyka oceny ryzyka

Przy ocenie ryzyka używa się metod modelowania przystosowanych do szacowania małych prawdopodobieństw – drzew zdarzeń i drzew błędów, bowiem częstości, dla których wystąpiły zdarzenia to tzw. zdarzenia rzadkie. Można stosować również szacowanie ryzyka bez dekompozycji zdarzeń (szacunki probabilistyczne, koncepcja najgroźniejszego wypadku wiarygodnego).

Metoda drzewa zdarzeń

Graficzny model zależności przyczynowo skutkowych występujących w rozpatrywanym przypadku. Budując drzewo *zdarzeń zakłada* się, że w wyniku pewnego ciągu zdarzeń powstaje określony skutek.



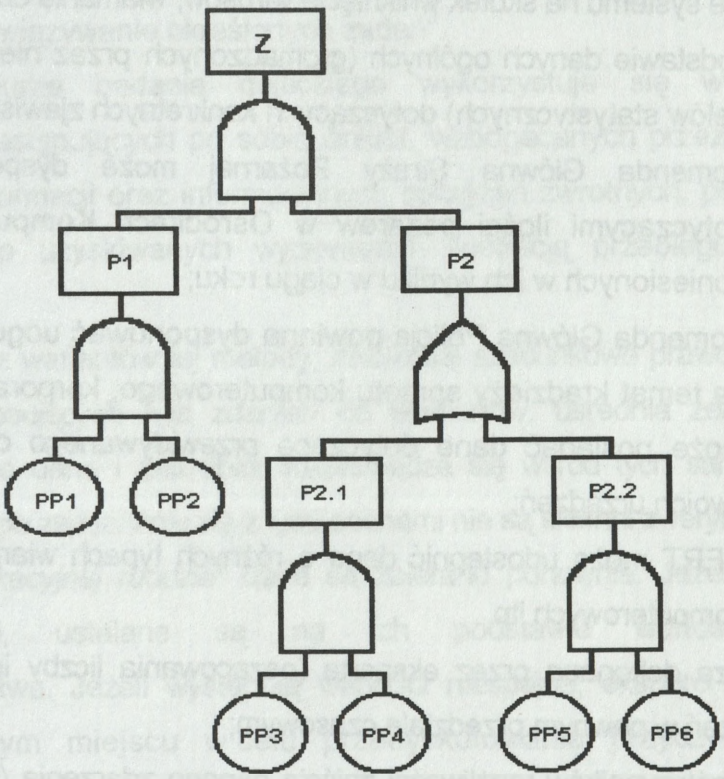
Rysunek 9.5. Przykładowy diagram drzewa zdarzeń

- Ryzyko powstaje w skutek ciągu niepomyślnych zdarzeń;
- Przyczyna - zdarzenie inicjujące;
- Skutek - możliwe inne zdarzenia (ścieżki, ciągi).

W różnych miejscach drzewa *zdarzeń* znajdują się punkty rozgałęzień ilustrujące fakt, że po pewnych zdarzeniach istnieje możliwość wystąpienia różnych innych zdarzeń. Prawdopodobieństwo określonego skutku otrzymuje się mnożąc przez siebie prawdopodobieństwa wszystkich *zdarzeń* składających się na ścieżkę w drzewie, po której dochodzimy do rozważanego skutku.

Metoda drzewa błędów

Graficzny model zależności przyczynowo-skutkowych budowany w przeciwnym kierunku niż drzewo zdarzeń. Rozpoczyna się określonym skutkiem i rozwija w kierunku zdarzeń poprzedzających, pokazując wszystkie możliwe kombinacje zdarzeń niepożądanych, które mogły doprowadzić do wyspecyfikowanego skutku.



Rysunek 9.6. Metoda drzewa błędów.

- Budowane jest w przeciwnym kierunku do drzewa zdarzeń;
- Początek - niepożądany skutek;
- Rozwinięcie na zdarzenia poprzedzające - przyczyny zdarzenia.

Drzewa zdarzeń i drzewa błędów wykorzystuje się zarówno do analizy jakościowej jak i ilościowej. Przeprowadzenie analizy jakościowej (gdy nie dokonujemy szacunków prawdopodobieństw) pomaga zorientować się w całym zakresie ryzyka i zrozumieć sytuację, której ryzyko dotyczy. Po przeprowadzeniu analizy ilościowej, drzewa zdarzeń i drzewa błędów pomagają w wyznaczeniu prawdopodobieństw pewnych ciągów zdarzeń lub pojedynczych zdarzeń.

Uzyskanie prawdopodobieństw zdarzeń elementarnych jest możliwe:

- na podstawie danych statystycznych o pracy określonego systemu teleinformatycznego (prawdopodobieństwa zajścia konkretnych zdarzeń). Warunkiem jest tutaj znalezienie takiego systemu teleinformatycznego, dla którego jest prowadzony dziennik eksploatacji obejmujący m.in. takie fakty jak: sprzętowe awarie systemu, nieudane próby logowania do systemu, awarie systemu na skutek wniknięcia wirusów, włamania do systemu itd.
- na podstawie danych ogólnych (gromadzonych przez niektóre organizacje dla celów statystycznych) dotyczących konkretnych zjawisk, np.:
  - Komenda Główna Straży Pożarnej może dysponować danymi dotyczącymi ilości pożarów w Ośrodkach Komputerowych i strat poniesionych w ich wyniku w ciągu roku;
  - Komenda Główna Policja powinna dysponować uogólnionymi danymi na temat kradzieży sprzętu komputerowego, korporacja przemysłowa może posiadać dane dotyczące przewidywanego czasu eksploatacji swoich urządzeń;
  - CERT może udostępnić dane o różnych typach włamań do systemów komputerowych itp.
- analiza dokonana przez eksperta (oszacowania liczby interesujących nas zdarzeń w pewnym przedziale czasowym;
- z współczynników możliwości zajścia danego zdarzenia (w konkretnej skali przez nas żądanej) a stworzonych przez eksperta;
- na podstawie metody delfickiej.

W większości przypadków w analizie ryzyka mamy do czynienia z oceną prawdopodobieństwa zdarzeń rzadkich (pożar lub trzęsienie ziemi). W przypadku braku danych empirycznych, korzystamy (jak wynika z przytoczonej wcześniej listy) z ocen ekspertów.

Praktyka wskazuje, ze oceny ekspertów, czyli subiektywne szacowanie prawdopodobieństw zdarzeń rzadkich, może być obciążone dużymi błędami. Przyczyn można się doszukiwać m.in. w osobniczej percepcji zagrożeń i ryzyka, dramatyzowaniu niektórych zdarzeń w środkach masowego przekazu.

Inną, wymienioną wcześniej metodą określania prawdopodobieństw zdarzeń rzadkich, jest ***metoda delficka.***

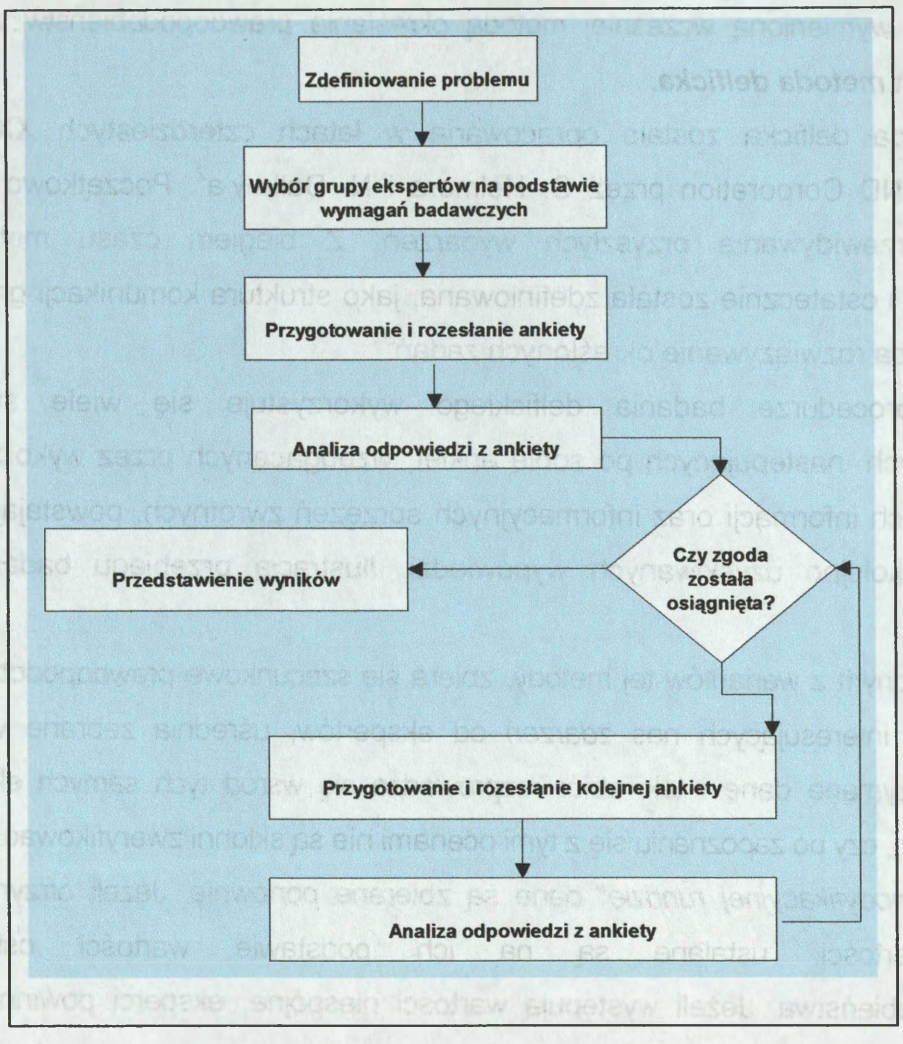
Metoda delficka została opracowana w latach czterdziestych XX wieku w firmie RAND Corporation przez O. Helmera i N. Dalkey'a[2]. Początkowo była to technika przewidywania przyszłych wydarzeń. Z biegiem czasu metoda ta ewoluowała i ostatecznie została zdefiniowana, jako struktura komunikacji grupowej, umożliwiająca rozwiązywanie określonych zadań[3].

W procedurze badania delfickiego wykorzystuje się wiele starannie opracowanych, następujących po sobie ankiet, wzbogacanych przez wykorzystanie zsumowanych informacji oraz informacyjnych sprzężeń zwrotnych, powstających na podstawie kolejno uzyskiwanych wypowiedzi. Ilustracją przebiegu badania jest rysunek 9.7.

W jednym z wariantów tej metody, zbiera się szacunkowe prawdopodobieństwa wystąpienia interesujących nas *zdarzeń* od ekspertów, uśrednia zebrane wartości, powiela otrzymane dane i taki zbiór rozprowadza się wśród tych samych ekspertów z zapytaniem, czy po zapoznaniu się z tymi ocenami nie są skłonni zweryfikować swojej. Po takiej *„modyfikacyjnej rundzie"* dane są zbierane ponownie. Jeżeli otrzymuje się spójne wartości, ustalane są na ich podstawie wartości ostateczne prawdopodobieństwa. Jeżeli występują wartości niespójne, eksperci powinni zostać zebrani w jednym miejscu w celu przedyskutowania przyczyn niespójność i wypracowania wartości końcowych prawdopodobieństw ocenianych *zdarzeń rzadkich.*

---

[2] *http://pespmc1.vub.ac.be/ASC/Delphi_metho.html. Delphi Method. Principia Cybernetica Web.*
[3] *C. Jones. Estimating Software Costs. McGraw-Hill, New York, 1998.*



Rysunek 9.7. Etapy postępowania w metodzie delfickiej.

Metody oceny akceptowalności ryzyka

W analizie ryzyka przy ocenie akceptowalności ryzyka, można stosować następujące formalne metody:

1. *preferencje ujawnione* - miarą akceptowalności nowego ryzyka związanego z danym przedsięwzięciem jest ryzyko już istniejące w społeczeństwie, tzn. trzeba posiadać informacje z nim związane i porównać z badanym ryzykiem;
2. *preferencje wyrażone* - różne osoby są pytane wprost o akceptowalność konkretnego ryzyka (musza być świadome zarówno ryzyka jak i korzyści przedsięwzięcia);
3. *analiza ryzyka i korzyści.*

Akceptowalność ryzyka (w szczególności w trzeciej z metod) napotyka na poważne trudności, gdy w grę wchodzi życie ludzkie (a więc głównie w systemach komputerowych wspomagających intensywną terapię, nawigację w samolotach, pracę reaktora jądrowego itp.), ponieważ **nie ma akceptowanych powszechnie metod oceniania wartości życia ludzkiego.**

W literaturze[4] można spotkać następujące podejścia do wyceny wartości życia ludzkiego:

- życie ludzkie jako kapitał - *wersja netto:* wartość osoby jako wartość straty dla reszty społeczeństwa - od dyskontowanych zarobków tej osoby odejmuje się dyskontowaną kwotę przeznaczoną przez nią w przyszłości na konsumpcję; *wersja brutto:* ocena wartości życia obejmuje również kwotę zarobków przeznaczonych przez daną osobę w przyszłości na konsumpcję, której to kwoty nie odejmuje się od dyskontowanej sumy przyszłych zarobków;
- orzeczenia sądowe w sprawach odszkodowań za utratę życia;
- ogólna suma odszkodowania, której zażądaliby członkowie grupy narażonej na ryzyko za zgodę na dodatkowe prawdopodobieństwo utraty życia wynikające z ocenianego przedsięwzięcia;

Poniższa tabela zawiera oceny akceptowalności ryzyka.

Tabela 9.1.

Prawdopodo-bieństwo / Straty	Mało prawdopodobne $p<0,3$	Prawdopodobne $0,3 \leq p \leq 0,7$	Wysoce prawdopodobne $0,7<p$
Marginalne	**niski**	**niski**	**średni**
Krytyczne	**średni**	**wysoki**	**wysoki**
Katastrofalne	**wysoki**	**niedopuszczalny**	**niedopuszczalny**

[4] *Findeisen W. (red): „Analiza systemowa - podstawy i metodologia". PWN. Warszawa. 1985.*

1.9.4. Zautomatyzowane systemy analizy ryzyka

Koszty przeprowadzenia analizy ryzyka są z reguły dosyć wysokie, jednak zautomatyzowana analiza ryzyka z reguły je rekompensuje.

Do szczególnych zalet takiej analizy należą:

- ustalone sposoby wprowadzania danych, a następnie łatwość dostępu i posługiwania się danymi zestawionymi w bazie niezbędnej do prowadzenia analizy;
- możliwość manipulowania danymi w celu zobrazowania wpływu i efektów różnych kombinacji zastosowania środków zabezpieczających i symulacji strat;
- możliwość szybkiego wprowadzania zmian do rozpoznawanego środowiska (aktywa i zasoby) oraz rozpoznanie wielkości ryzyka w organizacji.

Proces wyboru narzędzi może być składową zadania stawianego przy podstawowej analizie potrzeb. Przeprowadzić go można w kilku fazach poprzez:

- zdefiniowanie kryteriów wymagań;
- wybranie zespołu do oceny narzędzi;
- przygotowanie listy ocenianych punktów;
- przedstawienie propozycji oprogramowania wykorzystywanego w analizie ryzyka;
- ocenę i wybór programu.

Automatyczne narzędzie analizy ryzyka powinno zabezpieczyć pracę w następujących trzech obszarach:

- zbierania danych;
- procedur analitycznych;
- generowania (zobrazowania) wyników.

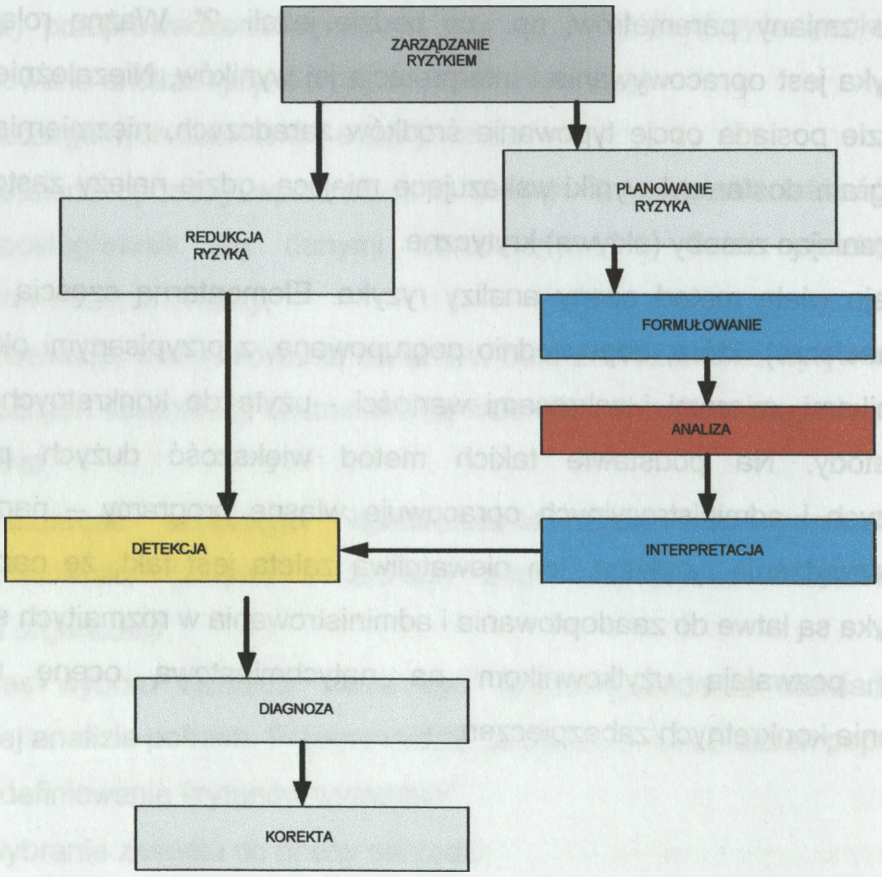
Zbieranie danych ma umożliwić wprowadzenie informacji tekstowych lub graficznych dotyczących wszystkich aspektów analizowanego systemu lub sieci.

Aktywa i zasoby opisane ilościowo, wartościowo lub jakościowo oraz informacje o zagrożeniach, słabych punktach i środkach zaradczych muszą tworzyć korelacyjną bazę danych jako podstawę do dalszej analizy.

Ważnym jest, by narzędzie (metodologia) bez względu na to, czy wykorzystuje podejście ilościowe, jakościowe, czy mieszane, reagowało w sposób interakcyjny na scenariusze zmiany parametrów, np. „co będzie jeżeli...?". Ważną rolą narzędzi analizy ryzyka jest opracowywanie i interpretacja jej wyników. Niezależnie od tego, czy narzędzie posiada opcję typowania środków zaradczych, niezmiernie ważnym jest by program dostarczył wyniki wskazujące miejsca, gdzie należy zastosować te środki, ochraniając zasoby (aktywa) krytyczne.

Istnieje wiele metod oceny analizy ryzyka. Elementarną częścią metod są matryce (macierze), które, odpowiednio pogrupowane, z przypisanymi określonymi współczynnikami, miarami i zakresami wartości - użyte do konkretnych zasobów tworzą metody. Na podstawie takich metod większość dużych podmiotów gospodarczych i administracyjnych opracowuje własne programy – narzędzia do analizy i zarządzania ryzykiem. Ich niewątpliwą zaletą jest fakt, że narzędzia do analizy ryzyka są łatwe do zaadoptowania i administrowania w rozmaitych systemach i zazwyczaj pozwalają użytkownikom na natychmiastową ocenę rezultatów wprowadzenia konkretnych zabezpieczeń.

Cykl zarządzania ryzykiem można ująć schematycznie w następujący sposób:



Rysunek 9.8. Cykl zarządzania ryzykiem zabezpieczeń.

Istnieją dwa podstawowe podejścia do procesu analizy ryzyka: *kwantyfikatywne* i *kwalifikatywne.*

Podejście *kwantyfikatywne* najczęściej oznacza analizę ryzyka i oszacowanie wspomagające matematyczne obliczenia wpływu zagrożenia, częstotliwości i prawdopodobieństwa. Podejście operuje wyłącznie na danych numerycznych, bierze pod uwagę dane ilościowe i statystyczne.

Najczęściej spotykanymi matrycami są:

- wartości mierzone;
- wartość procentowa;
- liczba wystąpień „*n*", gdzie *n*>0;
- prawdopodobieństwo wystąpienia;
- opis graniczny.

Najczęściej spotykanymi metodami przy podejściu *kwantyfikatywnym* są:

- określenie rocznej spodziewanej straty - ALE (*Annualized Loss Expectancy*);
- określenie straty pojedynczego wystąpienia - SOL (*Single Occurence Loss*);
- badanie progu opłacalności;
- formułowanie funkcji;
- ocena pozycji konkurencyjnej (*benchmarking*).

Podejście *kwalifikatywne* polega na prowadzeniu rankingu zagrożeń i zasobów. Bazuje na wiedzy i ocenie osób dokonujących analizy. Wynik jest najczęściej opisowy, pozwalający na późniejsze przełożenie słów na szereg wskaźników cyfrowych. Podejście takie jest znacznie prostsze do stosowania pod warunkiem ustalenia granic kryteriów. Przy stosowaniu *kwalifikatywnych* metod analizy ryzyka nie ma możliwości analizy efektywności kosztowej zabezpieczeń, chyba, że wcześniej *skwantyfikowano* wartości ryzyka. Metody *kwalifikatywne* często zwracają większą uwagę na opisy, a nie na wyliczenia. Z tego też powodu zarzuca się im nieobiektywność oraz wskazuje się, że interpretacja danych zależy tylko i wyłącznie od ich zrozumienia przez osobę badającą, co wiąże się z dużą subiektywnością oceny.

Najczęściej spotykanymi matrycami są:

- tablica „zero-jedynkowa";
- tablica wysokości ryzyka (LOW, MEDIUM, HIGH);
- tablica wag ryzyka HSE (*Vital, Critical, Important, Convinient*).

Większość narzędzi do analizy ryzyka stosuje rozdzielnie obydwie metody. Stosunkowo niewiele narzędzi potrafi je łączyć.

Do ciekawszych rozwiązań należą:

ALGORITHMISC - 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 kwantyfikatywne opracowane przez BIS. Jego moduł RiskWatch jest

narzędziem,które przy pomocy teoretycznych modeli jest w stanie obliczyć przyszłe wartości scenariuszy.

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. 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 i 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.

CORA (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). 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.

CRAMM (CCTA Risk Analysis & Management Methodology) - pakiet służący do analizy i zarządzania ryzykiem, którego podstawową metodą działania jest metoda *kwalifikatywna*. Pakiet składa się z 3 części, a dodatkowo jest wspierany dużą biblioteką ankiet, kwestionariuszy i zaleceń. Pakiet powstał przy współpracy brytyjskich specjalistów rządowych i firmy BIS Applied System Limited. Jest zabezpieczony przed nieuprawnionym dostępem oraz utratą poufności baz danych, które są tworzone w trakcie realizacji zadań.

VIR'94 - Metodologia VIR'94 - (*Voorschrift Infomatiebeyeiliging Rijkdienst*), łącznie z właściwym oprogramowaniem, zalecana jest przez oficjalne służby ochrony

informacji Holandii jako dyrektywa działania. Stosować ją można na wszystkich szczeblach zarządzania, od ministerstwa poprzez departamenty, agencje, aż do instytucji czy przedsiębiorstw.

Pakiet składa się z sześciu 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.

MARION – opiera się na bibliotece aktualnie znanych incydentów. Pakiet zawiera wiele ankiet i kwestionariuszy stosowanych do oceny rozwiązań w zakresie bezpieczeństwa. W analizie ryzyka przyjęto metodę *kwalifikatywno - kwantyfikatywną*. Oprogramowanie wylicza wyniki analizy dla 27 kategorii zasobów i zagrożeń. Umożliwia także prowadzenie analizy porównawczej wyników oraz utworzenie cenowej bazy danych dla elementów mających wpływ na bezpieczeństwo. Umożliwia to programowe oszacowanie kosztów ponoszonych w związku z poprawą systemu zabezpieczeń. Prezentacja wyników możliwa jest zarówno w formie numerycznej, jak i graficznej.

MAGERIT (Methodology of Risk Analysis and Management of Information Systems of Public Administrations) - metodologia zalecana jest dla instytucji administracji publicznej Hiszpanii. Zajmuje się w następującymi 3 dziedzinami:

1. opisem metodologii analizy i zarządzania ryzykiem;
2. przygotowaniem możliwie pełnej informacji i zgrupowaniem jej w bazie danych stanowiącej produkt wyjściowy do właściwej oceny ryzyka;
3. programowaniem narzędziowym wspomagającym implementację metody.

Produkt obejmuje wszystkie fazy przetwarzania, przesyłania i przechowywania informacji w systemach TI.

MASSIA (Methode d'Audit de la Securite des Systemes d'Information de l'Armement) - łącznie z oprogramowaniem narzędziowym obejmuje:

- przeprowadzenie badania podatności systemu informatycznego na zagrożenia;
- przeprowadzenie badania procedur operacyjnych, odpowiedzialnych za zapewnienie bezpieczeństwa.

W trakcie badania dokonuje się przeglądu stałej organizacji systemu, podsystemu działań zapobiegawczych, wewnętrznych i zewnętrznych, kontroli itd. Produkt stosuje przede wszystkim metodę *kwantyfikatywną*, prowadzącą do uzyskania pełnych danych dla wypracowania tzw. szczególnych wymagań bezpieczeństwa (SWB). Metoda stosowana jest głównie do prowadzenia procedur kontrolnych ITSEC.

IST/RAMP - (International Security Technology/Risk Anałysis Management) – w tym pakiecie zastosowano metodologię *kwantyfikatywną*. Wymaga on sprzętu typu "mainframe". Komputery klasy PC stosuje się jedynie do zobrazowania wyników. W trakcie działania program generuje zestawy potrzebnych ankiet i kwestionariuszy. Po ich uzyskaniu grupowane są one w pięciu kategoriach aktywów i zagrożeń. Pakiet dysponuje dużą biblioteką incydentów i ma możliwość przeprowadzenia analizy porównawczej.

RISKPAC - pakiet przygotowany jest do prowadzenia analizy ryzyka w agencjach rządowych. Zastosowano w nim metodę kwalifikacyjno-kwantyfikacyjną. Zestawy ankiet i kwestionariuszy pogrupowane są w cztery kategorie. Każda z nich tworzy oddzielny zbiór aktywów i zagrożeń, podlegających szczegółowej ocenie. Poziomy ryzyka przedstawiane są i monitorowane dla każdej kategorii oddzielnie. W systemie zawarto osobny moduł korekcji, który na podstawie przeprowadzonej analizy przedstawia zalecenia, których celem jest poprawienie stanu bezpieczeństwa.

Elementem pomocnym w przeprowadzaniu analizy zagrożeń sieci i systemów teleinformatycznych jest także zastosowanie zbioru narzędzi TQM. Powiązanie metod analizy ryzyka z nowoczesnym **narzędziem pomiaru i doskonalenia jakości TQM** (Total Quality Management - *Kompleksowe Zarządzanie Jakością)* pozwala nie tylko na wnikliwą analizę obiektu badań, ale również na ciągłe doskonalenie jakości wypracowanego modelu, w tym przypadku - systemu bezpieczeństwa informacyjnego.

Rdzeniem i jednocześnie siłą systemu *TQM* jest wzajemne powiązanie dwóch głównych celów jego zastosowania: pomiaru jakości (efektywności) działań idoskonalenia systemu, którego parametry podlegają pomiarowi. Narzędzia stosowane w procesach wspomaganych przez system *TQM* pozwalają na realizację obydwu celów.

Do narzędzi tych należy 7 narzędzi tradycyjnych (*Seven Tools*):

- ***pionowa 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.

Przykłady zastosowania zbioru narzędzi *TQM* w polityce bezpieczeństwa informacji przedstawiono w załącznikach 9.1 i 9.2 - pionowa sieć działań oraz diagram przyczynowo-skutkowy Ishikawy – pozwalające na systemowe podejście do omawianej problematyki.

Pionowa sieć działań w zastosowaniu polityki bezpieczeństwa informacji

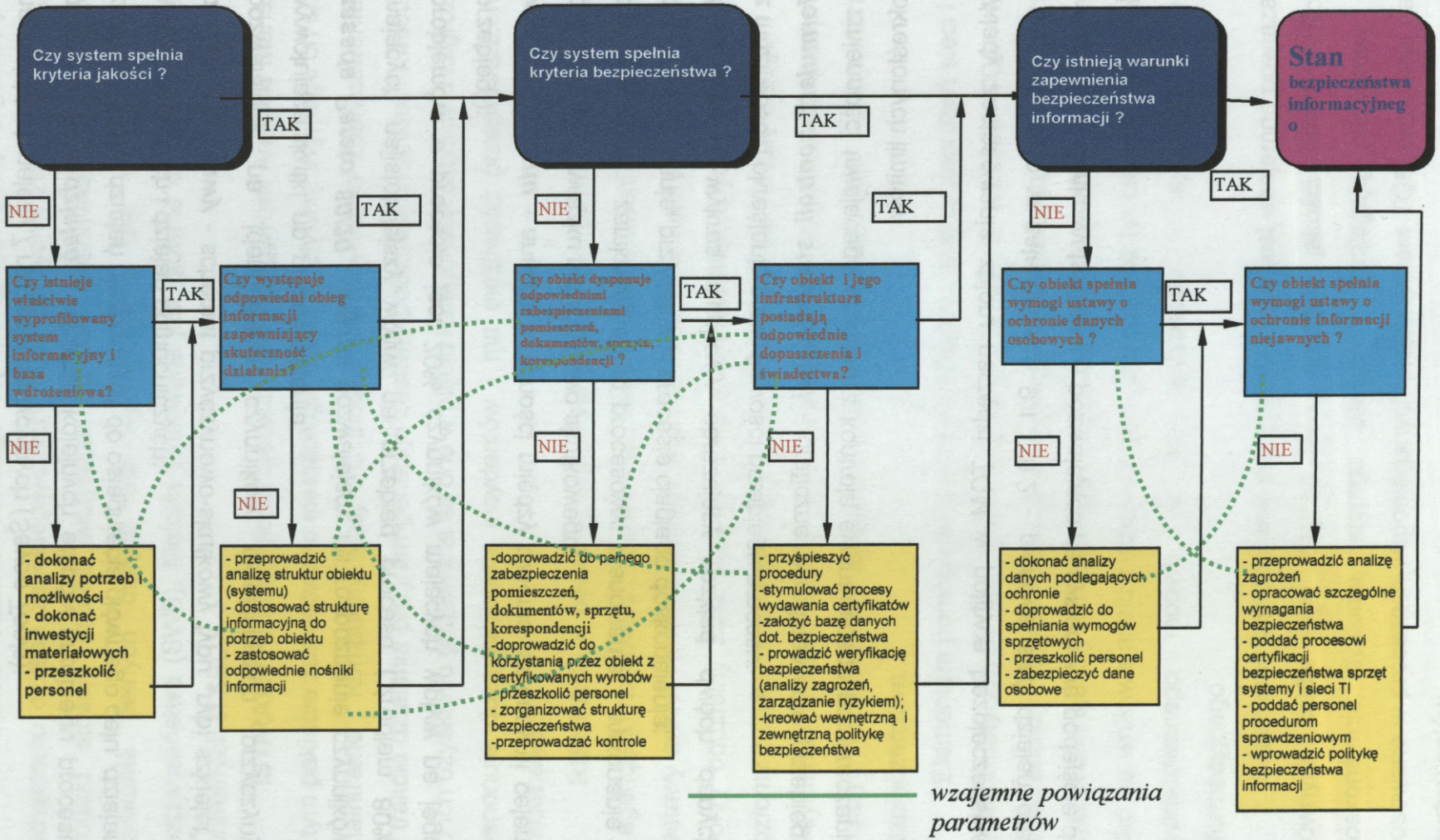
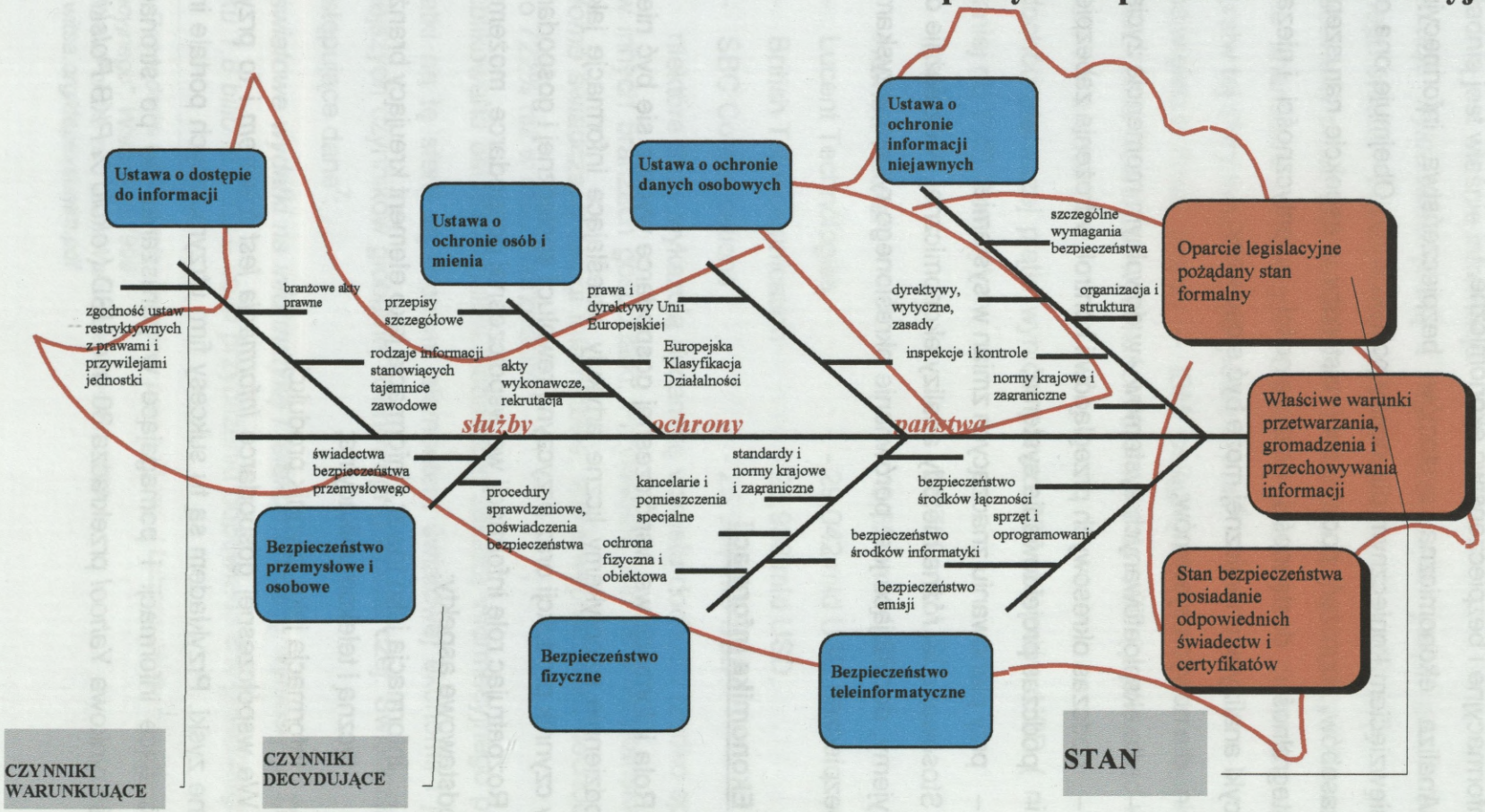


Diagram przycznowo-skutkowy Ishikawy typu "rybi szkielet" w odniesieniu do polityki bezpieczeństwa informacyjnego



1.9.5. Ekonomiczne aspekty bezpieczeństwa informacyjnego

Priorytetowymi aspektami bezpieczeństwa XX i XXI wieku jest bezpieczeństwo informacyjne i bezpieczeństwo ekonomiczne.

Analiza ekonomiczna systemów bezpieczeństwa informacyjnego jest przedsięwzięciem koniecznym dla oceny polityki firmy. Obejmuje ona ocenę wartości zasobów, zagrożeń, podatności i następstw w aspekcie naruszenia poufności, integralności, dostępności, rozliczalności, autentyczności i niezawodności. Pełny cykl analizy ekonomicznej może być stosowany:

- dla nowych systemów;
- dla eksploatowanych systemów - w dowolnym momencie życia systemu;
- podczas okresowych przeglądów i kontroli wdrożenia zabezpieczeń;
- podczas projektowania systemu;
- przy planowaniu znaczących zmian w systemie.

Stosowane są różne metody analizy ekonomicznej. Niezależnie od tego, jakiej użyjemy, decydujące jest porównanie określonego ryzyka z zyskami i kosztami zabezpieczeń.

Ekonomika informacii

Rola informacji we współczesnej gospodarce wydaje się być niepodważalna. Codziennie napotykamy liczne artykuły określające informację jako najważniejszy czynnik produkcji oraz przyczynę rewolucji społecznej i gospodarczej.

Rozpatrując rolę informacji we współczesnej gospodarce, możemy wyróżnić trzy podstawowe aspekty:

- informacja jako towar,; informacja jako element kreujący branżę informatyczną i telekomunikacyjną;
- informacja jako czynnik produkcji.

We współczesnej gospodarce *informacja jest towarem* i to przynoszącym ogromne zyski. Przykładem są tu sukcesy firm utrzymujących portale internetowe dostarczające informacji i pomagające w poruszaniu się po stronach WWW. Wartość rynkowa *Yahoo!* przekracza 30 mld USD (*około ¼ PKB Polski*), a *Excite*

został w styczniu 1999 roku kupiony za 6,7 mld USD[5]. Należy tu podkreślić, że obie te firmy jeszcze parę lat temu po prostu nie istniały.

Przykładów takich we współczesnej gospodarce jest znacznie więcej – rozwijające się coraz dynamiczniej firmy oferują produkty, których najistotniejszą i najdroższą składnią jest właśnie informacja.

Informacja wykreowała jedną z najpotężniejszych gałęzi gospodarczych współczesnego świata – branżę informatyczno-telekomunikacyjną (IT).

Opracowany przez Business Week coroczny przegląd branży informacyjnej podaje dane finansowe pokazujące potencjał gospodarczy i dynamikę wzrostu przedsiębiorstw tej sfery światowej gospodarki. I tak[6]:

- największa firma branży – IBM osiągnęła w roku obrachunkowym 1997/1998 dochód w wysokości 78,8 miliarda USD (*jest to rząd wielkości PKB Irlandii*);
- dochód pierwszej piątki wyniósł ponad 207 miliardów USD (niewiele mniej niż PKB Szwecji);
  - IBM - 78,769 mld USD,
  - Hewlett-Packard - 46,624 mld USD,
  - Lucent Technologies - 29,042 mld USD,
  - British Telecomunication - 26,933 mld USD,
  - SBC Comunications - 25,944 mld USD,
- niektóre firmy wykazują dynamikę wzrostu dochodu rzadko spotykaną w innych branżach gospodarki. Przykładem jest tu amerykańska firma *At Home* świadcząca usługi internetowe, która wypracowała dochód większy o 722% niż w roku poprzednim.

Opublikowana ostatnio analiza globalnego sektora informacyjnego pokazuje, iż wydatki na tę sferę są istotnym elementem światowej ekonomii i jednym z najistotniejszych czynników globalnej równowagi gospodarczej. Świadczą o tym choćby następujące dane[7]:

- *światowe wydatki na informatykę i telekomunikację wyniosły w 1997 roku 1,8 biliona USD* – co w przybliżeniu odpowiada 6% globalnego świa-

---

[5] *M.Goliński: Gospodarka i informacja, Ze zbioru prac pod red. J.Lubicza „W drodze do społeczeństwa informacyjnego", Warszawa 1999*
[6] *Business Week/Polska, nr 1 (82), Warszawa, styczeń 1999*
[7] *http://www.witsa.org/depexsumm.pdf*

towego PKB. Jest to więcej niż PKB Francji i *prawie 15 razy tyle, ile PKB Polski*;

- w porównaniu do roku 1992 wielkość światowych wydatków na tę sferę wzrosła o prawie 40 %. Dynamika wzrostu była, więc o 27% wyższa niż w przypadku globalnego PKB;
- w okresie 1992 – 1997 wydatki na teleinformatykę najszybciej rosły w następujących regionach świata:
  - Azja/Pacyfik 14,5%;
  - Ameryka Łacińska 13,6%;
  - Europa Wschodnia 9,5%.

Wydatki na sferę teleinformatyczną są czynnikiem potęgującym wszelkie zjawiska społeczne i ekonomiczne. Inwestycje te mają korzystny wpływ na gospodarki narodowe i światowe poprzez:

- powstawanie nowych firm (*tylko w USA w ciągu ostatnich pięciu lat corocznie powstawało średnio 7200 nowych firm w sektorze teleinformatycznym);*
- tworzenie nowych miejsc pracy;
- zwiększenie efektywności gospodarki jako całości;
- łagodzenie przebiegu cyklów koniunkturalnych.

Informacja stała się jednym z najważniejszych czynników produkcji – czynnikiem o charakterze strategicznym. Dotychczasowe zastosowania teleinformatyczne służyły głównie zwiększeniu wewnętrznej efektywności i zmniejszeniu kosztów bezpośrednich przedsiębiorstwa w takich obszarach jak zarządzanie, finanse czy księgowość. Współczesne rozwiązania idą w kierunku zabezpieczenia pozycji przedsiębiorstwa na rynku i wypracowania przewagi nad konkurencją mają więc charakter strategiczny. Przykładami takiego rodzaju zastosowań teleinformatycznych mogą być:

- polepszenie komunikacji z dostawcami i klientami;
- skrócenie czasu przygotowania nowych produktów;
- wzmocnienie istotnych cech przedsiębiorstwa;
- korzystniejsze kształtowanie bariery wejścia na rynek;
- zdobywanie istniejących i tworzenie nowych, nieznanych dotychczas rynków;

- stworzenie nowych kanałów dystrybucji;
- polepszenie kooperacji z innymi firmami.

Cechą charakterystyczną zastosowań teleinformatycznych ostatnich lat jest także to, iż po objęciu swym działaniem wszystkich obszarów funkcjonalnych wewnątrz organizacji, coraz częściej techniki i technologie informacyjne przekraczają granice organizacyjne poszczególnych przedsiębiorstw. Dzieje się tak wtedy, gdy systemy informacyjne firmy zostają połączone z systemami dostawców, klientów lub pozostałymi podmiotami z gospodarczego otoczenia przedsiębiorstwa.

Coraz większa liczba firm wymienia informacje elektronicznie. Gospodarka elektroniczna to bazująca na technologii sieciowej koordynacja materiałów, procesów i ludzi ułatwiająca wymianę handlową. W jej skład wchodzą między innymi takie techniki jak:

- elektroniczna wymiana dokumentacji *(Electronic Data Interchange – EDI)*;
- elektroniczny transfer środków pieniężnych *(Electronic Funds Transfer – EFT)*;
- interaktywne systemy informacji głosowej (*Interactive Voice Respondense*);
- bankowość elektroniczna (*electronic banking*) i jej „domowa" odmiana (*home banking*);
- elektroniczne zakupy (*electronic shopping*);
- systemy rezerwacji.

Mówiąc o gospodarce elektronicznej nie można pominąć naturalnego środowiska dla tego typu rozwiązań, którym jest Internet. Abstrahując od codziennych jego zastosowań (*WWW, FTP, e-mail*), wyróżnić możemy takie formy wykorzystania Internetu w biznesie jak:

- *Intranet* – dla potrzeb wewnętrznej komunikacji w firmie;
- *Extranet* – dla tworzenia międzyorganizacyjnych systemów informacyjnych;
- *Internet* – powszechnie dostępne medium dla sfery elektronicznej gospodarki.

Mimo błyskawicznego rozwoju Internetu, wciąż nie ma dogodnych warunków do realizacji transakcji handlowych. Główną barierą rozwoju powszechnych

interaktywnych zakupów i usług bankowych są problemy związane z bezpieczeństwem transakcji w sieci. Aby systemy tego typu stały się powszechne, konieczne jest stworzenie bezpiecznych form elektronicznych płatności.

Zarządzanie bezpieczeństwem systemów informacyjnych

Nie można mówić o zarządzaniu bezpieczeństwem systemów informacyjnych bez próby określenia, czym jest samo pojęcie bezpieczeństwa.

Bezpieczeństwo informacyjne jest częścią składową zarządzania informacją w organizacji i obejmuje ochronę zarówno systemów komputerowych jak i informacji przed celowymi lub przypadkowymi zniszczeniami.

Program zabezpieczeń powinien zmierzać ku następującym celom:

- ustalenie procesu planowania zabezpieczeń;
- ustalenie funkcji zarządzania zabezpieczeniami;
- rozwój polityki zabezpieczeń;
- określenie procesu analizy nakładów i efektów;
- ustalenie procesu zarządzania ryzykiem;
- ustalenie formalnych procedur oceny zabezpieczeń;
- planowanie i realizacja działań naprawczych.

Drugie kluczowe pojęcie, które w tym miejscu należy przytoczyć, to *polityka bezpieczeństwa instytucji w zakresie systemów informacyjnych*. Obejmuje ona zasady, zarządzenia i procedury, które określają, jak zasoby są zarządzane, chronione i dystrybuowane w instytucji i jej systemach teleinformatycznych (teleinformacyjnych).

Zarządzanie bezpieczeństwem informacji (systemów informatycznych) obejmuje zespół procesów zmierzających do osiągnięcia i utrzymywania ustalonego poziomu bezpieczeństwa, tzn. poziomu poufności, integralności, dostępności, rozliczalności, autentyczności i niezawodności.

Jego realizacja obejmuje działania, takie jak:

- określenie celów (*co należy chronić*), strategii (*w jaki sposób*) i polityk bezpieczeństwa systemów informatycznych w instytucji (*jakie konkretne przedsięwzięcia należy podjąć*);

- identyfikowanie i analizowanie zagrożeń dla zasobów;
- identyfikowanie i analizowanie ryzyka;
- określenie adekwatnych zabezpieczeń;
- monitorowanie wdrożenia, eksploatacji (skuteczności) zabezpieczeń;
- opracowanie i wdrożenie programu szkoleniowo-uświadamiającego;
- wykrywanie incydentów i reakcja na nie.

Zarządzanie zabezpieczeniami wymaga opracowania strategii i dokonania analizy SWOT. Jest to szeroko stosowana metoda służąca do badania otoczenia organizacji oraz analizy jej wnętrza.

Nazwa SWOT jest akronimem angielskich słów:

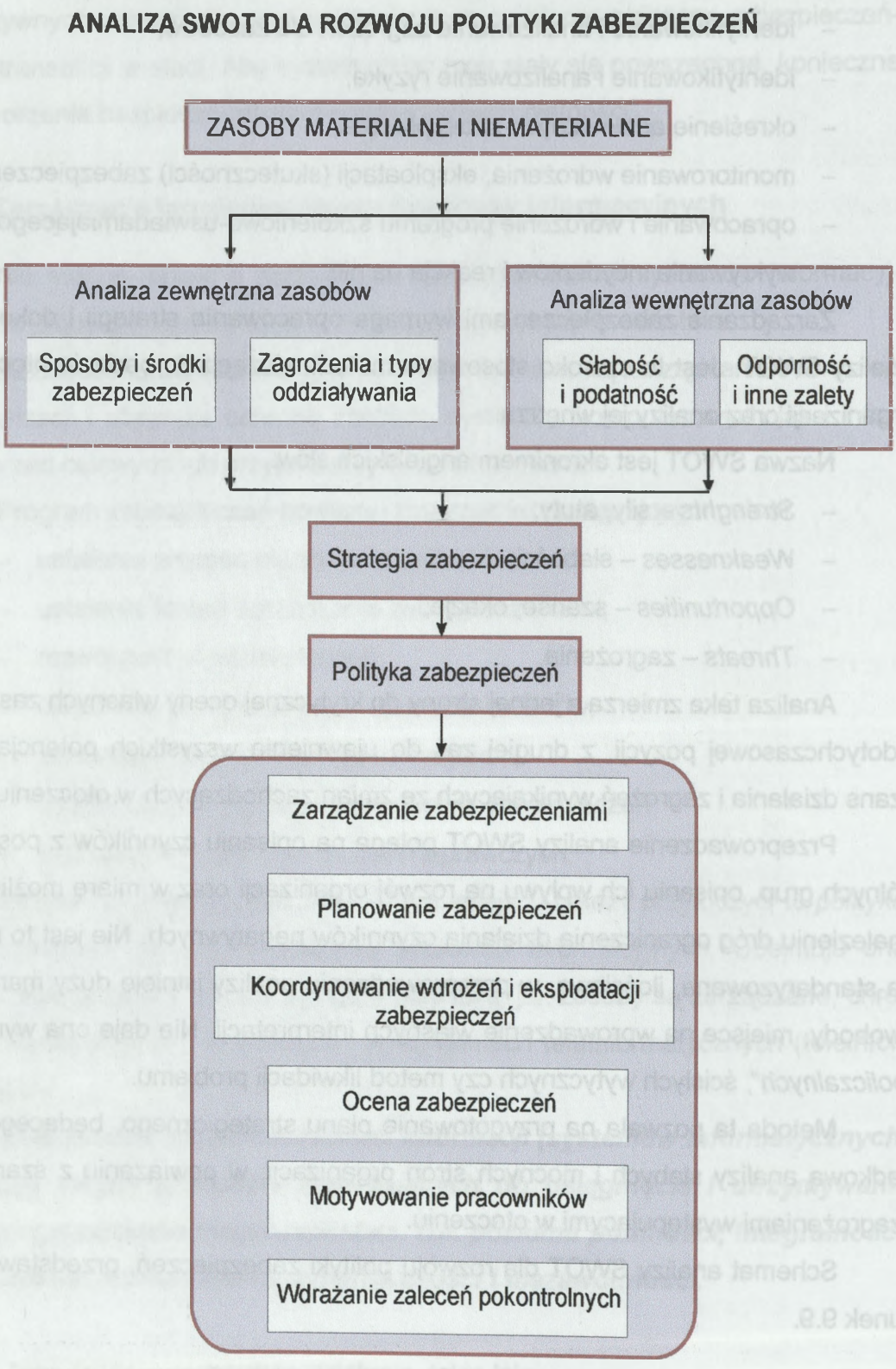
- *Strenghts* – siły, atuty;
- *Weaknesses* – słabości;
- *Opportunities* – szanse, okazje;
- *Threats* – zagrożenia.

Analiza taka zmierza z jednej strony do krytycznej oceny własnych zasobów i dotychczasowej pozycji, z drugiej zaś do ujawnienia wszystkich potencjalnych szans działania i zagrożeń wynikających ze zmian zachodzących w otoczeniu.

Przeprowadzenie analizy SWOT polega na opisaniu czynników z poszczególnych grup, opisaniu ich wpływu na rozwój organizacji oraz w miarę możliwości znalezieniu dróg ograniczenia działania czynników negatywnych. Nie jest to metoda standaryzowana, ilościowa, w przeprowadzeniu analizy istnieje duży margines swobody, miejsce na wprowadzenie własnych interpretacji. Nie daje ona wyników *„policzalnych”*, ścisłych wytycznych czy metod likwidacji problemu.

Metoda ta pozwala na przygotowanie planu strategicznego, będącego wypadkową analizy słabych i mocnych stron organizacji, w powiązaniu z szansami i zagrożeniami występującymi w otoczeniu.

Schemat analizy SWOT dla rozwoju polityki zabezpieczeń, przedstawia rysunek 9.9.



Rysunek 9.9. Analiza SWOT dla rozwoju polityki zabezpieczeń.

Pierwszy krok analizy SWOT obejmuje analizę zewnętrznych sił organizacji, które wywierają wpływ na strategię zabezpieczeń (zagrożenia, środki i sposoby zabezpieczeń). Krok drugi stanowi analiza wewnętrznych mocnych (*odporność zasobów*) i słabych *(podatność zasobów*) stron organizacji oraz jej kultury pracy. Krok trzeci to opracowanie strategii i polityki zabezpieczeń. Krok ostatni obejmuje zarządzanie zabezpieczeniami.

Zabezpieczenie systemów informatycznych wymaga analizy zasobów organizacji, przy czym istotna jest wartość każdego zasobu, która jest jego wewnętrznym atrybutem i wyrażana jest jako koszt nabycia i konserwacji.

W systemach informatycznych wyróżnia się cztery podstawowe kategorie zasobów:

- zasoby fizyczne (komputery, nośniki pamięci, urządzenia wprowadzania i wyprowadzania danych);
- zasoby intelektualne (oprogramowanie wraz z dokumentacją);
- zasoby kadrowe (użytkownicy, projektanci, programiści i administratorzy);
- usługi i transakcje dokonane przy użyciu oprogramowania aplikacyjnego, a także usługi operatorskie, administracji i oceny systemów informatycznych.

Zasoby wskutek oddziaływania zagrożeń narażone są na kradzież, zniszczenie lub uszkodzenie. Ponieważ nie wszystkie zagrożenia są jednakowo prawdopodobne, w związku z tym, nie wszystkie zasoby muszą być chronione.

Stopień ochrony informacji powinien zależeć od wartości i względnego znaczenia danego zasobu dla organizacji. Im zasób jest bardziej unikalny tym ma większą wartość i bardziej należy go chronić. Jednak o tym, które zasoby chronić, a które pozostawić niechronione i uwzględnić krańcowe ryzyko wynikłe z tej sytuacji, powinien decydować Zarząd firmy.

Tworzenie zabezpieczeń systemu teleinformacyjnego, jak już wcześniej wspomniałam, sprowadza się do opracowania i wdrożenia odpowiedniej polityki ochrony tego systemu oraz środków technicznych, organizacyjnych i prawnych, które wspomagają i uzupełniają przedsięwzięcia realizowanie w ramach przyjętej polityki.

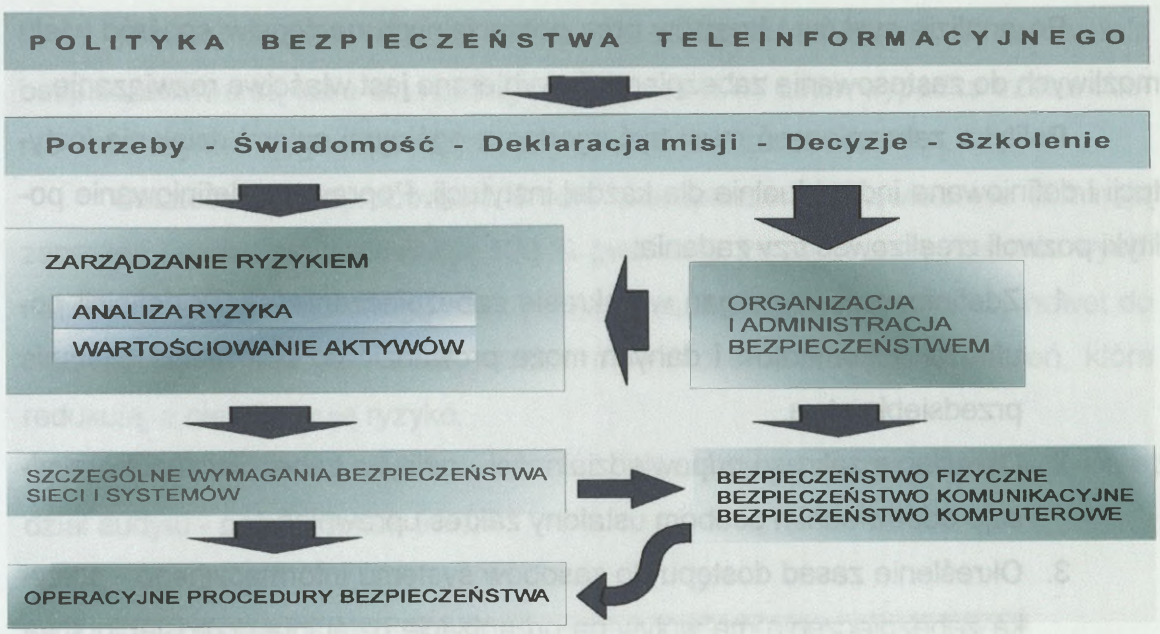
Wytycznymi dla polityki ochrony, która jest definiowana jako zbiór reguł i praktyk regulujących bezpieczeństwo systemów informacyjnych, są:

- *zgodność ze standardami*: dostawca zabezpieczeń definiuje zbiór standardów, których zachowanie deklaruje. Takie standardy powinny obejmować:
  - techniczne standardy dla formatów danych, protokołów i komunikatów;
  - techniczne standardy dla sprzętu i zabezpieczenia sprzętu;
  - standardy dotyczące zapewnienia zabezpieczenia;
- *zgodność z obowiązującym prawem*: wykaz przepisów prawnych i uregulowań z którymi zgodność pozostaje zachowana.

Podstawowym elementem polityki bezpieczeństwa jest dokument jasno określający zakres czynności i obowiązki użytkowników danego systemu. Ze względu na różnorodność zasobów zagrożeń i mnogość zagadnień związanych z ich ochroną, w organizacjach formułowane są polityki szczegółowe obejmujące następujące obszary:

- zabezpieczenie informacji;
- środki zabezpieczenia fizycznego (zabezpieczenie podstawowej infrastruktury, budynków, zabezpieczenie sprzętu informatycznego);
- zabezpieczenie oprogramowania aplikacyjnego i sieciowego;
- zabezpieczenie użytkowników, identyfikacja, uwierzytelnianie, kontrola dostępu do zasobów;
- ochrona przed złośliwym oprogramowaniem;
- zabezpieczenie poczty elektronicznej i informacji udostępnianych w Internecie, ochrona prywatności użytkowników Internetu;
- ochrona własności intelektualnej;
- zarządzanie zabezpieczeniami.

Etapy w procesie polityki bezpieczeństwa teleinformacyjnego, przedstawia rysunek 9.10.



Rysunek 9.10. Etapy w polityce bezpieczeństwa teleinformacyjnego[8]

Schemat ilustruje zbiór procesów polityki bezpieczeństwa teleinformacyjnego, zawierających inne procesy bezpośrednio lub pośrednio związane z bezpieczeństwem. *Kluczowym punktem jest tu proces zarządzania ryzykiem z* podprocesem analizy ryzyka. Proces zarządzania ryzykiem sprowadza się do porównywania określonego ryzyka z zyskami i kosztami zabezpieczeń oraz wypracowywania strategii ich wdrożenia i polityki bezpieczeństwa instytucji w zakresie systemów informatycznych.

W ramach tego procesu należy oszacować ewentualne straty, które mogą powstać w wyniku włamania się lub zniszczenia systemu. Przy szacowaniu strat należy brać pod uwagę następujące czynniki:

- obliczalność strat;
- możliwość ich udowodnienia;
- możliwość i koszty ich naprawy.

Należy też sprawdzić opłacalność poszczególnych elementów systemu traktując ją jako zagadnienie rozwiązywalne ekonomicznie.

Wyliczając ewentualne straty wynikające z włamania się do systemu należy zwrócić uwagę, aby koszty poniesione na ochronę nie były od nich większe.

---

[8] *B.Kusina : Informacja – towar chroniony, Konferencja e-Komputer Expo, Warszawa 23-24.01.2001*

Po analizie zysków i kosztów oraz potencjalnych następstw spośród wielu możliwych do zastosowania zabezpieczeń, wybierane jest właściwe rozwiązanie.

Polityka zabezpieczeń musi być zgodna z ogólnymi celami działania instytucji i definiowana indywidualnie dla każdej instytucji. Poprawne zdefiniowanie polityki pozwoli zrealizować trzy zadania:

1. Zdefiniowanie wymagań w zakresie zabezpieczenia - brak definicji poufności dokumentów i danych może prowadzić do ujawnienia tajemnic przedsiębiorstwa.
2. Określenie zakresu odpowiedzialności - polityka zabezpieczenia przypisuje odpowiednim osobom ustalony zakres uprawnień.
3. Określenie zasad dostępu do zasobów systemu informacyjnego - polityka zabezpieczenia ma wpływ na organizację działania przedsiębiorstwa tzn. zasady prowadzenia rekrutacji pracowników, bezpieczeństwo i kontrolę pracy.

Wdrożenie polityki bezpieczeństwa w przedsiębiorstwie kosztuje. Koszty te należy porównać z wartością chronionych zasobów.

Załóżmy, że posiadamy *zasób o wartości* ***A***. Jeżeli *koszt penetracji sieci i naruszenia zasobu wynosi* ***P***, to:

Współczynnik ryzyka (S) = A/P[9]

Współczynnik ryzyka wyrażany jest stosunkiem wartości zasobu, do kosztu penetracji sieci, która ma na celu naruszenie zasobu.

W sieci bezpiecznej wartość ***P*** *powinna być większa od wartości* ***A***, co oznacza, że koszt penetracji sieci i kradzieży lub uszkodzenia zasobu powinien być większy od wartości zasobu.

Załóżmy, że *koszt wdrożenia polityki bezpieczeństwa*, która ma chronić zasób, *wynosi,* ***N***. Jeżeli sieć jest dobrze zaprojektowana, to koszt ***N*** powinien być związany z wartością zasobu ***A*** *i wówczas:*

Współczynnik inwestycji (K)= N/A[10]

Należy dążyć do tego, żeby koszt wdrożenia zabezpieczeń był wyraźnie mniejszy niż wartość chronionego zasobu, zatem **N**, powinno być mniejsze niż **A**.

---

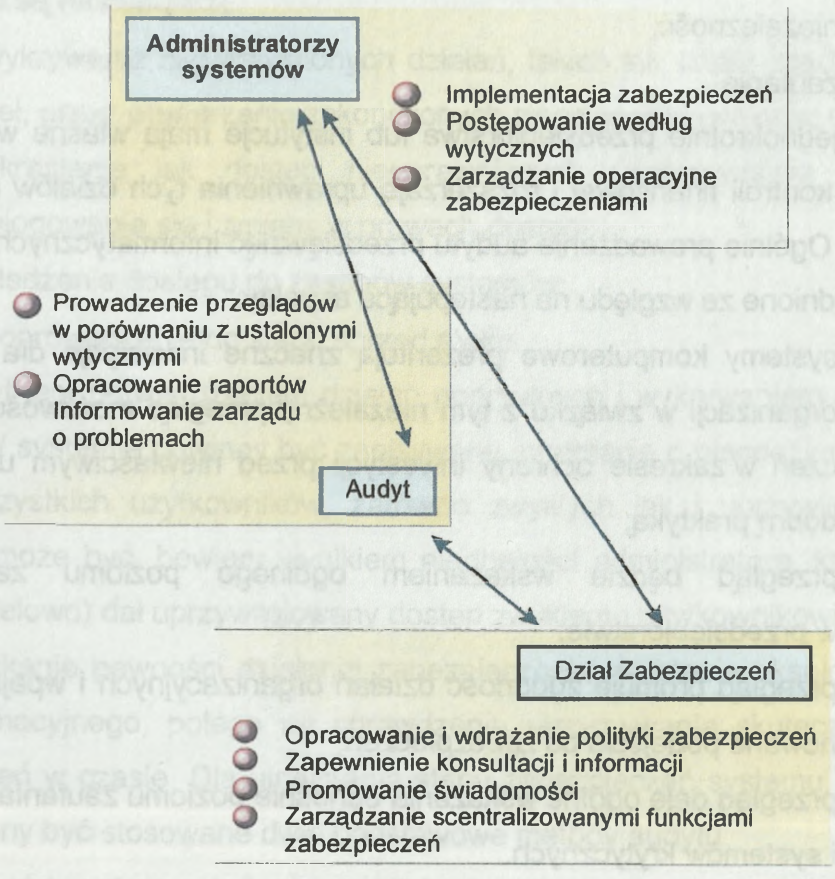
[9] *Ahuja V. :Bezpieczeństwo w sieciach, Mikom, Warszawa 1997*
[10] *Ahuja V.: Bezpieczeństwo w sieciach, Mikom, Warszawa 1997*

W wielu sieciach koszt ***N*** wdrożenia zabezpieczeń i koszt ***P*** naruszenia bezpieczeństwa są stałe dla każdego zasobu sieci. W takim wypadku trzeba ocenić współczynnik ryzyka dla najbardziej krytycznych zasobów.

Ostatecznie zaaprobowane środki zabezpieczeń całkowicie nie eliminują zagrożeń i nawet nie zapewniają 100 % gwarancji, że zagrożenie zostanie wyeliminowane. Biorąc pod uwagę koszty eliminowania zagrożeń nie należy nawet do tego dążyć. W praktyce należy, zatem mówić o środkach zabezpieczeń, które redukują, a nie eliminują ryzyko.

Ocena polityki zabezpieczeń zasobów informatycznych prowadzona jest przez dział audytu - *patrz rysunek 9.11.*

POWIĄZANIA INTRAORGANIZACYJNE DLA ZARZĄDZANIA ZABEZPIECZEŃ



Rysunek 9.11. Rola audytu w procesie zabezpieczeń systemów informatycznych[11].

[11] *M. Pańkowska: Audyt w zarządzaniu zabezpieczeniami systemów informatycznych, Enigma'2000 – IV Krajowa Konferencja Zastosowań Kryptografii, Warszawa 23-25.05.2000*

W literaturze przedmiotu do tej pory brak zgodności poglądów, czym jest audyt. Dla jednych audyt oznacza proces gromadzenia danych na temat działań i zasobów systemów komputerowych. Inni uważają, że audyt jest przeglądem istniejącej kontroli i wykrywaniem bezprawnych działań.

Podstawowym celem audytu w środowisku informatycznym jest niezależny przegląd aplikacji, systemu informatycznego i sieci dla oceny zgodności z ustaloną polityką, przyjętymi wytycznymi i standardami. Strona odpowiedzialna jest zobowiązana podjąć działania prewencyjne, zapobiegawcze, wdrożyć stosowne mechanizmy kontroli zabezpieczeń, co powinno prowadzić do ogólnie wyższego poziomu zabezpieczeń w organizacji.

Należy zwrócić uwagę na trzy konieczne cechy jakościowe jednostek, które powinny prowadzić audyt:

- wiedza;
- niezależność;
- zaufanie.

Niejednokrotnie przedsiębiorstwa lub instytucje mają własne wydziały wewnętrznej kontroli finansowej i rozszerzają uprawnienia tych działów na sferę informatyki. Ogólnie prowadzenie audytu przedsięwzięć informatycznych wydaje się być uzasadnione ze względu na następujące aspekty:

- systemy komputerowe prezentują znaczne inwestycje dla większości organizacji w związku z tym niezależny przegląd możliwości zabezpieczeń w zakresie ochrony inwestycji przed niewłaściwym użyciem jest dobrą praktyką;
- przegląd będzie wskazaniem ogólnego poziomu zabezpieczeń w przedsiębiorstwie;
- przegląd promuje zgodność działań organizacyjnych i wpaja zdyscyplinowane podejście do zabezpieczeń;
- przegląd daje ogólne wskazania odnośnie poziomu zaufania do aplikacji i systemów krytycznych.

W przedsiębiorstwach i instytucjach znajdują zastosowanie różne metody realizacji audytu. Należą do nich:

- zautomatyzowane narzędzia wyszukiwania słabości systemu zabezpieczenia (np. narzędzia weryfikacji integralności plików, wyszukiwania

słabych haseł, kontrola aktualności modyfikacji w systemach i aplikacjach);

- wewnętrzne mechanizmy audytu (w tej grupie mieszczą się badania, ankiety, obserwacje, testy zabezpieczeń i danych);
- testy penetracyjne (próby włamania się do systemu przy użyciu różnych metod, w tym nielegalne uzyskanie informacji od użytkowników). Z uwagi na potencjalne znaczne ryzyko wyrządzenia szkody w systemie informacyjnym, testy penetracyjne powinny być wykonywane tylko przez kompetentnych specjalistów pracujących pod nadzorem.

Tradycyjny audyt systemów komputerowych koncentruje swą uwagę na trzech obszarach zagadnień: przeglądzie zabezpieczeń, stwierdzeniu zgodności zabezpieczeń z polityką i badaniu śladu rewizyjnego. Ślad rewizyjny jest zbiorem danych, generowanych przez działania na systemie komputerowym. Cele śladu rewizyjnego są następujące:

- wykrywanie nieuprawnionych działań, takich jak próby zgadywania haseł, przez powtarzanie zakończonych niepowodzeniem prób dostępu;
- określenie jak dostęp nieuprawnionych urzeczywistnia się przez wlogowanie się i zmiany w prawach dostępu;
- śledzenie dostępu do zasobów systemów;
- doprowadzenie do stanu sprzed ataku.

Audyt jest potwierdzeniem działań poprawnych i wykrywaniem naruszenia systemu. W systemie powinny być zapisywane informacje o niecodziennych działaniach wszystkich użytkowników, zarówno zwykłych jak i uprzywilejowanych. Włamanie może być, bowiem wynikiem niedbałości administratora, który pomyłkowo (lub celowo) dał uprzywilejowany dostęp zwykłemu użytkownikowi.

Uzyskanie pewności działania zabezpieczenia na etapie eksploatacji systemu informacyjnego, polega na sprawdzeniu utrzymywania skuteczności tych zabezpieczeń w czasie. Dla utrzymania stanu zabezpieczeń systemu informacyjnego powinny być stosowane dwie podstawowe metody audytu:

- audyt systemu - jednorazowe lub okresowo powtarzające się całościowe szacowanie poziomu zabezpieczenia;

- monitorowanie systemu - działanie o charakterze ciągłym, mające na celu nadzór nad zmieniającym się systemem, jego użytkownikami oraz środowiskiem.

Obecnie audyt przestaje być tylko kontrolą zabezpieczeń i obejmuje ocenę wykonania i zarządzanie ryzykiem zniszczenia uszkodzenia zasobów informatycznych.

Testowaniem może być objęty pojedynczy system, aplikacja lub system sieciowy. Istotne jest by test był powtarzalny. Wiedza zdobyta podczas testowania, stosowna kontrola i środki zapobiegawcze mogą być użyte dla wyeliminowania słabości.

Podsumowanie

Analiza ekonomiczna systemów bezpieczeństwa informacyjnego jest kluczowym procesem zarządzania bezpieczeństwem.

Wdrożenie programu zarządzania bezpieczeństwem systemów informatycznych, jest najbardziej efektywnym pod względem kosztów, sposobem zoptymalizowania zwrotu wydatków instytucji na zakup sprzętu i oprogramowanie. Niemożność określenia, jakie zasoby posiada instytucja i gdzie się one znajdują, prowadzi do wielu problemów:

- zasoby firmy są uszczuplane przez straty, nadużycia i kradzieże;
- do środowiska komputerowego dostają się wirusy i inne elementy zagrażające bezpieczeństwu;
- koszty integracji rosną w wyniku niezgodności systemów i różnorodności wersji oprogramowania;
- rosną koszty szkoleń, pomocy technicznej i serwisu;
- w związku z łamaniem prawa autorskiego rośnie ryzyko grzywien i kar;
- rosną całkowite koszty eksploatacji.

Rozwój zabezpieczeń powinien uwzględniać dwa komplementarne punkty widzenia: jak wyeliminować lub zredukować prawdopodobieństwo szczególnych zagrożeń zasobów *(orientacja na zagrożenia)* lub, co należy zrobić, by chronić zasoby przed zagrożeniami *(orientacja na zasoby)*.

Formułowana polityka zabezpieczeń powinna w maksymalnym stopniu uwzględniać rozwiązania istniejące. W poszukiwaniu rozwiązań należy uwzględnić rozsądny kompromis między wyznaczonym poziomem zabezpieczenia, a poziomem nakładów finansowych, które instytucja gotowa jest ponieść.

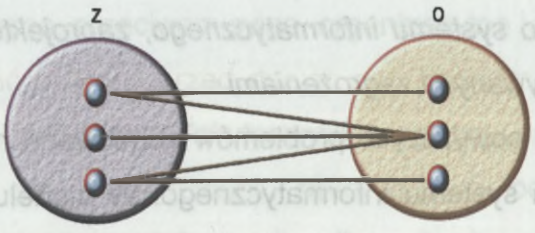
Kryteria oceny efektywności systemu bezpieczeństwa informacyjnego

Ocena efektywności systemów bezpieczeństwa informacyjnego stanowi centralne zagadnienie analizy ekonomicznej. Znaczenie oceny efektywności dla powodzenia analizy ekonomicznej wynika z faktu, że wybór parametrów, charakterystyk i kryteriów oceny systemu przesądza o trafności kolejnych wyborów, prowadzących do ostatecznej decyzji.

Przedstawiony poniżej matematyczny opis charakterystyk obiektów wymagających ochrony, występujących zagrożeń i metod przeciwdziałania względnie osłabienia skutków działania tych zagrożeń zobrazowany jest przykładem praktycznego zastosowania tego modelu.

Każdy system informatyczny składa się ze *zbioru **O** określonej liczby obiektów*, których skuteczna ochrona ma istotny wpływ na zapewnienie bezpieczeństwa całemu systemowi, a z każdym zdefiniowanym obiektem związana jest pewna liczba zagrożeń, które może podjąć potencjalny intruz, by uzyskać nieuprawniony dostęp do tego obiektu. Można wyliczyć wszystkie potencjalne działania skierowane przeciw wszystkim zabezpieczonym obiektom i utworzyć *zbiór zagrożeń **Z***. Cechą tego zbioru jest to, że z każdym zagrożeniem związane jest prawdopodobieństwo jego zaistnienia. W każdym rzeczywistym systemie informatycznym prawdopodobieństwa te można oszacować.

Relacje łączące obiekty z zagrożeniami zobrazowano na rysunek 9.12.

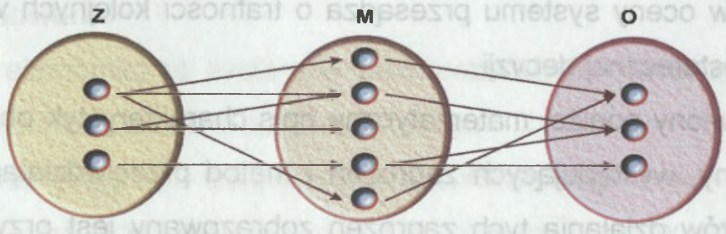


Rysunek 9.12. Związki między obiektami a zagrożeniami.

Jak widzimy, relacja między zagrożeniami a obiektami nie jest jednoznaczna – jedno zagrożenie może być niebezpieczne dla wielu obiektów, a jeden obiekt może podlegać wielu zagrożeniom.

Można także określić *zbiór metod bezpieczeństwa (ochrony)* ***M***, zawierający wszystkie znane środki ochrony (środki zabezpieczające). W idealnym przypadku każdy element zbioru **M** mógłby eliminować oddziaływanie jednego zagrożenia ze *zbioru zagrożeń* ***Z***, na jeden chroniony obiekt ze *zbioru obiektów* ***O***. W rzeczywistości jeden środek zabezpieczający może chronić kilka obiektów, przed więcej niż jednym zagrożeniem.

Relacje pomiędzy elementami zbiorów **Z, M** i **O** przedstawiono na rysunek 9.13.



Rysunek 9.13. Związki między obiektami, środkami ochrony a zagrożeniami.

W obszarze działań mających na celu zapewnienie właściwego poziomu bezpieczeństwa systemom informatycznym, można wyodrębnić dwa podstawowe zadania (problemy), które należy rozwiązać.

PROBLEM I

Sprawdzić czy wdrażany lub eksploatowany system informatyczny spełnia wymagania bezpieczeństwa jego użytkowania.

PROBLEM II

Dla budowanego systemu informatycznego, zaprojektować system zabezpieczeń przed przewidywanymi zagrożeniami.

Dla rozwiązania powyższych problemów zbudowano model matematyczny oceny bezpieczeństwa systemu informatycznego. W modelu tym przedstawiono także sposób pomiaru i postać uogólnionej miary poziomu bezpieczeństwa systemu informatycznego.

Model oceny bezpieczeństwa systemu informatycznego zbudowany został przy uwzględnieniu następujących założeń:

1. System informatyczny traktowany jest jako jeden obiekt, na który działają zagrożenia.
2. Występowanie zagrożenia ze zbioru zagrożeń **Z** jest zdarzeniem niezależnym tzn. wystąpienie jednego zagrożenia nie ma wpływu na wystąpienie innego zagrożenia.
3. *Zbiór zagrożeń dzieli się na trzy grupy związane z: utratą poufności, integralności, względnie dostępności danych.*
4. Ochronie podlegają wykorzystywane w systemie informatycznym informacje, które dzieli się na następujące *klasy: tajne specjalnego znaczenia, tajne, poufne, jawne.* Podział ten wynika bezpośrednio z obowiązujących w Rzeczpospolitej Polskiej przepisów o ochronie tajemnicy.
5. Zastosowany środek ochrony ze zbioru środków ochrony **M** jest zdarzeniem niezależnym, tzn. jeden środek ochronny nie wpływa na skuteczność ochrony innych środków.
6. Zastosowany środek ochrony może bronić przed skutkami wystąpienia dowolnej liczby zagrożeń.

Wpływ poszczególnych zagrożeń na bezpieczeństwo obiektu (systemu informatycznego) nie jest jednakowy. Charakteryzuje się go *współczynnikiem agresji* ***„a"***. Współczynnik ten można rozumieć jako subiektywną wagę znaczenia przypisywanego danemu zagrożeniu **z.** Współczynniki agresji przyjmują wartości:

$$a_i \geq 0$$

przy założeniu, że:

$$\sum_{i=1}^{I} a_i = I \quad \textit{gdzie: } I \textit{ – liczność zbioru zagrożeń}$$

7. *Środki ochrony podzielone są na sześć grup*: fizyczne, programowe, kryptograficzne, przeciwemisyjne, organizacyjne i personalne.
8. Skuteczność ochrony przed danym zagrożeniem, mierzona jest *współczynnikiem* ***„w"*** *jakości (skuteczności) ochrony obiektu* przed **z**-tym zagrożeniem przy zastosowaniu **m**-tej metody ochrony. *Współczynniki skuteczności ochrony informacji* ***„w"*** *przyjmują wartości:*

$$0 \leq W < 1$$

9. Dla wszystkich klas systemów informatycznych można określić minimalne poziomy bezpieczeństwa **„Wb_{min}"**, które przyjmują wartości z przedziału **< 0,1)** i wskazują, na jakim poziomie powinny być zwalczane poszczególne typy zagrożeń, aby można było uznać oceniany system za bezpieczny.

Mając powyższe na uwadze można określić macierze W^n_{InxJm}, gdzie:
In – liczność zbioru zagrożeń w ***n***-tej grupie;
Jm – liczność zbioru środków ochrony w ***m***-tej grupie, której elementami są współczynniki jakości (skuteczności) $w_{i,j}$ ochrony obiektu, przed z_i zagrożeniem przy zastosowaniu m_j środka ochrony

Współczynnik skuteczności ochrony przed wystąpieniem ***i***-tego zagrożenia w ***n***-tej grupie, przy zastosowaniu metod ochrony z ***m***-tej grupy obliczamy ze wzoru:

$$W_j^{n,m} = 1 - \prod_{j=1}^{J_m} (1 - w_{i,j})\, p_j^m \quad dla \;\; n \in (1,3) \;\; i \;\; m \in (1,6) \qquad (1)$$

gdzie $p_j^m = \begin{cases} 1 - jeśli\ stosuje\ się\ j\text{-}ty\ środek\ ochrony \\ 0 - w\ przeciwnym\ wypadku \end{cases}$

Jak już wcześniej stwierdzono, prawdopodobieństwo wystąpienia poszczególnych zagrożeń nie jest jednakowe. Ponadto skutki oddziaływania różnych zagrożeń na chroniony obiekt mają niejednakowy wpływ na zachowanie jego bezpieczeństwa. Biorąc to pod uwagę, poziom bezpieczeństwa obiektu dla określonej grupy zagrożeń przy zastosowaniu danej grupy metod ochrony, wyznaczamy z następującej zależności:

$$WB^{n,m} = \frac{1}{In} \sum_{i=1}^{In} W_i^{n,m} * a_i^n \quad dla\ n \in (1,3)\ i\ m \in (1,6) \qquad (2)$$

gdzie: a_i^n – współczynnik agresji ***i***-tego zagrożenia w ***n***-tej grupie, przy założeniu, że:

$$\sum_{i=1}^{In} a_i^n = In$$

natomiast całkowity (uogólniony) wskaźnik bezpieczeństwa obiektu (systemu informatycznego) dla danej grupy zagrożeń wyznaczamy z zależności:

$$WBC^n = 1 - \prod_{j=1}^{Jm} (1 - WB^{n,j}) \quad dla \ n \in (1,3) \tag{3}$$

Do rozwiązania przedstawionych problemów w zakresie bezpieczeństwa systemów informatycznych niezbędne są wskaźniki (współczynniki) liczbowe: jakości – ***„w"***, agresji – ***„a"*** oraz minimalnego poziomu ochrony – ***„WBC_{min}"***, które mogą być obecnie wyznaczone jedynie na podstawie doświadczeń w projektowaniu i eksploatacji systemów informatycznych przez ekspertów w dziedzinie bezpieczeństwa. Matematyczne wyznaczenie tych wskaźników (np. w postaci prawdopodobieństw) może być możliwe jedynie wtedy, jeśli dysponować będziemy odpowiednią liczbą danych statystycznych.

Ze względu na brak wymienionych wartości, dla zilustrowania działania modelu posłużono się współczynnikami wyznaczonymi przez grupę specjalistów mających dużą wiedzę w zakresie bezpieczeństwa oraz wieloletnie doświadczenie w projektowaniu i eksploatacji systemów informatycznych. I tak dla przykładu *tabela 9.2.* - zawiera wartości współczynników minimalnego poziomu bezpieczeństwa, *tabela 9.3.* – zawiera wartości współczynników agresji, natomiast *tabela 9.4.*– zawiera wartości współczynników skuteczności dla metod ochrony fizycznych. W podobnej formie ujęte zostały wartości współczynników skuteczności dla programowych, kryptograficznych, przeciwemisyjnych, organizacyjnych i personalnych metod ochrony.

Tabela 9.2.

Minimalne współczynniki bezpieczeństwa[12]

Typ zagrożenia	Klasa systemu	WBC_{min}
Utrata poufności	Tajne spec. znacz.	0,97
	Tajne	0,85
	Poufne	0,75
	Jawne	0,35
Utrata integralności	Tajne spec. znacz.	0,90
	Tajne	0,80
	Poufne	0,65
	Jawne	0,30
Utrata dostępności	Tajne spec. znacz.	0,90
	Tajne	0,80
	Poufne	0,70
	Jawne	0,45

[12] *Źródło: VI Miedzynarodowa Wojskowa Konferencja Telekomunikacji i Informatyki, Jabłonna 1997 – Materiały cz.I*

Tabela 9.3.

Współczynniki agresji[13]

Typ zagrożenia	Rodzaj zagrożenia	Współczynnik agresji
Utrata poufności	Nieuprawniony dostęp	1,5
	Kradzież informacji	1
	Kradzież sprzętu	0,5
	Nielegalne kopiowanie informacji	1
	Zagubienie nośników z zapisaną informacją	0,8
	Ujawnienie zabezpieczeń	2
	Emisja ujawniająca	0,6
	Podsłuch bierny	0,6
Utrata integralności	Modyfikacja danych	1,5
	Modyfikacja oprogramowania	1,5
	Błędy oprogramowania aplikacyjnego	1,2
	Podsłuch aktywny	0,8
	Szumy i przesłuchy	0,5
	Zakłócenia impulsowe	0,5
Utrata dostępności	Błędne działanie systemu operacyjnego	1,5
	Błędne działanie oprogramowania	1,5
	Błędne działanie sprzętu komputerowego	1,4
	Błędne działanie personelu	0,8
	Awaria zasilania	1,5
	Awaria sieci transmisji danych	0,6
	Klęski żywiołowe	0,6
	Oddziaływanie pola magnetycznego	0,5
	Sabotaż komputerowy	0,6

[13] *Źródło: VI Międzynarodowa Wojskowa Konferencja Telekomunikacji i Informatyki, Jabłonna 1997 – Materiały cz.I*

Tabela 9.4.

Współczynniki skuteczności dla fizycznych metod ochrony[14]

Typ zagrożenia	Środek ochrony / Zagrożenie	System kontroli dostępu do obiektu	System kontroli dostępu do urządzeń technicznych	System zapobiegania obserwacji elementów syst.	Syst. zapewnienia niezawod. Zasilania i klimat.	System zapewnienia niezawodności sprzętu	Syst. ochrony przed oddz. Pola elektromag.	Syst. zapobiegania skutkom klęsk żywiołowych	System składowania
Utrata poufności	Nieuprawniony dostęp	0,2	0,3	0,2	0	0	0	0	0
	Kradzież informacji	0,2	0,3	0,3	0	0	0	0	0
	Kradzież sprzętu	0,1	0,2	0	0	0	0	0	0
	Nielegalne kopiowanie informacji	0,2	0,3	0,1	0	0	0	0	0
	Zagubienie nośników z zapisaną informacją	0,1	0,1	0	0	0	0	0	0
	Ujawnienie zabezpieczeń	0,1	0,1	0,2	0	0	0	0	0
	Emisja ujawniająca	0	0	0	0,1	0,1	0	0	0
	Podsłuch bierny	0,2	0	0	0,1	0,1	0	0	0
Utrata integralności	Modyfikacja danych	0,1	0,3	0	0	0,3	0,2	0	0,2
	Modyfikacja oprogramowania	0,1	0,3	0	0	0,3	0,2	0	0,2
	Błędy oprogramowania aplikacyjnego	0	0	0	0	0,3	0,2	0	0
	Podsłuch aktywny	0,1	0,2	0	0,1	0,2	0	0	0
	Szumy i przesłuchy	0	0	0	0,1	0,1	0	0	0
	Zakłócenia impulsowe	0	0	0	0,1	0,1	0,1	0	0
Utrata dostępności	Błędne działanie systemu operacyjnego	0	0	0	0,1	0,2	0,2	0	0,2
	Błędne działanie oprogramowania	0	0	0	0,1	0,2	0,2	0	0,2
	Błędne działanie sprzętu komputerowego	0	0,1	0	0,2	0,3	0,2	0,2	0
	Błędne działanie personelu	0,1	0,2	0,1	0,1	0	0	0	0,2
	Awaria zasilania	0	0	0	0,3	0,3	0,3	0,2	0,2
	Awaria sieci transmisji danych	0	0	0	0,2	0,2	0,3	0,2	0
	Klęski żywiołowe	0	0	0	0	0,1	0	0,3	0,2
	Oddziaływanie pola magnetycznego	0,1	0	0	0,2	0,2	0,3	0	0
	Sabotaż komputerowy	0,1	0,2	0,3	0	0	0,2	0	0,2
Wektor wyboru środków ochrony		1	1	1	0	0	1	0	1

[14] *Źródło: VI Międzynarodowa Wojskowa Konferencja Telekomunikacji i Informatyki, Jabłonna 1997 – Materiały cz.I*

W celu sprawdzenia czy wdrażany lub eksploatowany system informatyczny spełnia wymagania bezpieczeństwa jego użytkowania należy:

- dla wszystkich zagrożeń – w ramach poszczególnych grup zagrożeń – wyliczyć wg wzoru (1) współczynniki skuteczności ochrony;
- dla wszystkich grup zagrożeń, wyliczyć wg wzoru (2) współczynniki bezpieczeństwa obiektu przy zastosowaniu danej grupy metod ochrony;
- dla wszystkich grup zagrożeń wyliczyć wg wzoru (3) całkowite wskaźniki bezpieczeństwa obiektu.

System uznajemy za bezpieczny, jeśli wyliczone całkowite wskaźniki bezpieczeństwa są równe lub większe od minimalnych całkowitych wskaźników bezpieczeństwa dla danej klasy systemu, tzn. gdy:

$$WBC^n \geq WBC^n_{\min} \quad dla\,każ\,\deg o \quad n \in (1,3)$$

PRZYKŁAD:

Sprawdzić czy eksploatowany system informatyczny przetwarzający informacje o klauzuli TAJNE spełnia wymagania w zakresie bezpieczeństwa jego użytkowania.

Zakładamy, że zgodnie z dokumentacją systemu oraz stanem faktycznym, system posiada następujące zabezpieczenia:

- w grupie fizycznych metod ochrony: system organizacji kontroli dostępu do obiektu, system zapobiegania obserwacji elementów systemu, system ochrony przed oddziaływaniem pola elektromagnetycznego;
- w grupie programowych metod ochrony: system haseł dostępu, dziennik zdarzeń w systemie, oprogramowanie antywirusowe;
- w grupie organizacyjnych metod ochrony: regulacje prawne, przepisy organizacyjne;
- w grupie personalnych metod ochrony: system doboru kadr, szkolenia i samokształcenie.

W celu wykonania niezbędnych obliczeń opracowano arkusz obliczeniowy przy użyciu pakietu EXCEL. Wyniki obliczeń przedstawione są w tabeli 9.5.

Tabela 9.5.

Arkusz obliczeń[15]

Typ zagrożenia	Środek ochrony / Zagrożenie	Fizyczne (m=1)	Programowe (m=2)	Kryptograficzne (m=3)	Przeciwemisyjne (m=4)	Organizacyjne (m=5)	Personalne (m=6)	Uogólnione wskaźniki bezpieczeństwa WBC[n]
Utrata poufności n=1	Nieuprawniony dostęp	0,552	0,765	0,2	0	0,36	0,539	
	Kradzież informacji	0,608	0,482	0,4	0	0,36	0,539	
	Kradzież sprzętu	0,28	0	0	0	0,36	0,539	
	Nielegalne kopiowanie informacji	0,496	0,417	0,3	0	0,36	0,539	
	Zagubienie nośników z zapisaną informacją	0,19	0	0,4	0	0,36	0,539	
	Ujawnienie zabezpieczeń	0,352	0,546	0,5	0,352	0,36	0,539	
	Emisja ujawniająca	0	0	0,4	0,552	0	0	
	Podsłuch bierny	0,2	0	0,4	0,496	0	0	
Poziomy bezpieczeństwa WB [1,m]		**0,38**	**0,39**	**0,32**	**0,13**	**0,31**	**0,46**	**0,92**
Utrata integralności n=2	Modyfikacja danych	0,597	0,585	0	0	0,36	0,539	
	Modyfikacja oprogramowania	0,597	0,585	0	0	0,36	0,539	
	Błędy oprogramowania aplikacyjnego	0,2	0	0	0	0,36	0,539	
	Podsłuch aktywny	0,28	0	0,4	0,552	0	0	
	Szumy i przesłuchy	0	0	0,2	0	0	0	
	Zakłócenia impulsowe	0,1	0	0	0	0	0	
Poziomy bezpieczeństwa WB [2,m]		**0,38**	**0,29**	**0,07**	**0,07**	**0,25**	**0,38**	**0,83**
Utrata dostępności n=3	Błędne działanie systemu operacyjnego	0,36	0,2	0	0	0,488	0,344	
	Błędne działanie oprogramowania	0,36	0,1	0	0	0,488	0,344	
	Błędne działanie sprzętu komputerowego	0,28	0,2	0	0	0,552	0,344	
	Błędne działanie personelu	0,482	0,482	0	0	0,488	0,76	
	Awaria zasilania	0,44	0	0	0	0,433	0	
	Awaria sieci transmisji danych	0,3	0	0	0	0,2	0	
	Klęski żywiołowe	0,2	0	0	0	0,3	0	
	Oddziaływanie pola magnetycznego	0,37	0	0	0	0,2	0	
	Sabotaż	0,677	0,533	0,4	0	0,552	0,59	
Poziomy bezpieczeństwa WB [3,m]		**0,38**	**0,16**	**0,03**	**0,00**	**0,45**	**0,28**	**0,80**

[15] *Źródło: VI Międzynarodowa Wojskowa Konferencja Telekomunikacji i Informatyki, Jabłonna 1997 – Materiały cz.I*

REZULTAT:

Na podstawie otrzymanych wyników obliczeń możemy stwierdzić, że oceniany system informatyczny nie spełnia wymagań w zakresie bezpieczeństwa, ponieważ całkowite wskaźniki bezpieczeństwa systemu są mniejsze od minimalnych wymaganych dla systemów tej klasy tzn:

$$WBC^{1} = 0,73 < WBC^{1}_{min} = 0,85$$
$$WBC^{2} = 0,65 < WBC^{2}_{min} = 0,80$$
$$WBC^{3} = 0,59 < WBC^{3}_{min} = 0,80$$

Optymalizacja systemu bezpieczeństwa informacyjnego

Rozwój techniki i technologii wzmaga zapotrzebowanie na metody analizy i obiektywnej oceny decyzji podejmowanych w szeroko rozumianym planowaniu i zarządzaniu. Każda bowiem działalność, w tym również zarządzanie bezpieczeństwem systemów informacyjnych, związana jest z określonymi celami, których osiągnięcie wymaga posiadania określonych środków.

Środki te bardzo często są ograniczone i mogą być użyte w różny sposób, o czym przesądzają konkretne warunki techniczne, organizacyjne, prawne i ekonomiczne, w jakich prowadzona jest działalność firmy (organizacji, państwa).

W działalności przedsiębiorstwa powstaje zatem problem podjęcia optymalnej decyzji dotyczącej sposobu zastosowania rozporządzalnych środków i zasobów oraz realizacji zamierzonego celu.

Analiza i ocena efektywności systemów rzeczywistych, w szczególności takich jak systemy bezpieczeństwa systemów informatycznych, stanowi centralne zagadnienie analizy systemowej. Znaczenie oceny efektywności dla powodzenia analizy systemowej dowolnego złożonego obiektu wynika z faktu, że wybór cech systemowych – parametrów, charakterystyk i kryteriów oceny systemu przesądza o trafności kolejnych wyborów, prowadzących do ostatecznej decyzji.

Względy praktyczne przemawiają za tym, aby w analizie systemowej nie było zbyt wielu kryteriów oceny, gdyż analiza powinna uwzględniać najistotniejsze cechy problemu i jego otoczenia, a także umożliwiać konstruowanie kompleksowego wskaźnika oceny efektywności systemu.

Znaczenie analizy efektywności w procesie analizy systemowej polega przede wszystkim na tym, że przygotowanie rzetelnych informacji jako przesłanek podejmowanych decyzji wymaga szczególnie wnikliwego rozpatrzenia różnych przejawów efektywności obiektów (systemów), użyteczności i jakości. Właśnie analiza systemowa ma uchronić niejako przed popełnieniem błędów inwestycyjnych, popełnieniem omyłek podczas zakupów licencyjnych i wyborów systemów bezpieczeństwa informacyjnego.

W analizie efektywności obiektów szczególne znaczenie należy przypisać następującym przedsięwzięciom:

- określenie cech głównych obiektu, istotnych z punktu widzenia zidentyfikowanych potrzeb i celów;
- wybór kryteriów efektywności (jakości);
- określenie wskaźników efektywności;
- opracowanie metod wyznaczania wartości efektywności (jakości) obiektów;
- określenie reguł wnioskowania – formułowania sądów ocenowych, porównawczych itp.

Na podstawie danych przedstawionych w tabeli 9.6., do których opracowania posłużyły dane zawarte w tabelach 9.2., 9.3. i 9.4. oraz eksperymentalne dane pozyskane ze źródeł firmy **X** dokonamy klasyfikacji wariantów systemu bezpieczeństwa danych wg różnych kryteriów.

Tabela 9.6.

Klasyfikacja wariantów systemu bezpieczeństwa danych wg różnych kryteriów

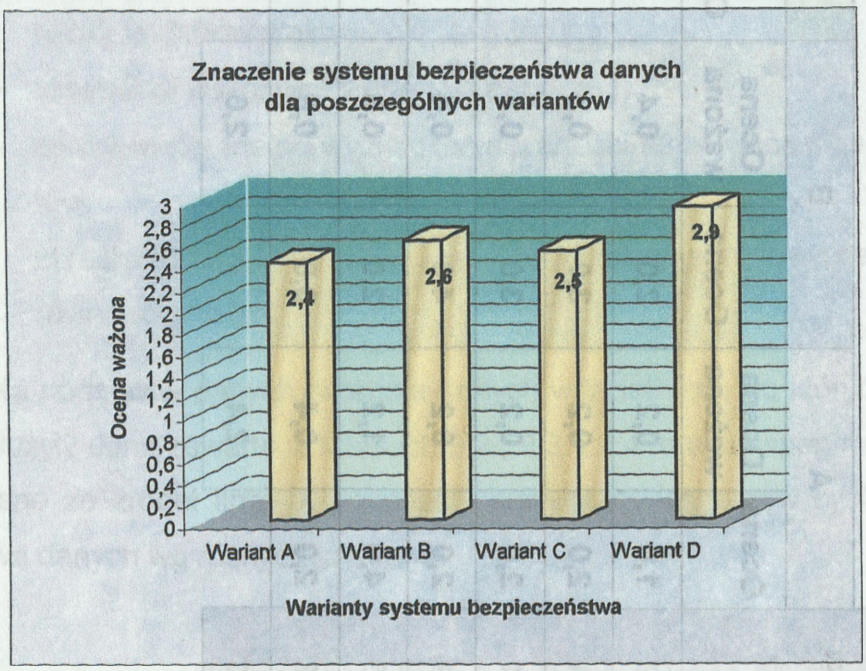
Kryterium oceny wariantu systemu bezpieczeństwa danych	Wagi	Warianty systemu bezpieczeństwa danych							
		A		B		C		D	
		Ocena	Ocena ważona	Ocena	Ocena ważona	Ocena	Ocena ważona	Ocena	Ocena ważona
Poufność danych	0,2	1,0	0,2	2,0	0,4	2,0	0,4	3,0	0,6
Dostępność danych	0,1	2,0	0,2	3,0	0,3	3,0	0,3	4,0	0,4
Integralność danych	0,1	2,0	0,2	3,0	0,3	2,0	0,2	3,0	0,3
Koszt	0,1	2,0	0,2	4,0	0,4	3,0	0,3	5,0	0,5
Ryzyko	0,3	4,0	1,2	2,0	0,6	3,0	0,9	1,0	0,3
Niezawodność	0,2	2,0	0,4	3,0	0,6	2,0	0,4	4,0	0,8
	1,0		2,4		2,6		2,5		2,9

$0 \leq \text{wagi} \leq 1$

$1 \leq \text{ocena} \leq 5$

Metody stosowane podczas optymalizacji zadań, skupiają się na porównaniu efektywności różnych sposobów rozwiązywania zagadnień i poszukiwania rozwiązania optymalnego. Pozwalają również, przeanalizować wybrany wycinek rzeczywistości oraz ocenić ilościowo rezultaty możliwych do podjęcia decyzji. Przy analizie możliwych skutków podejmowanych decyzji, uwzględniane są takie czynniki jak koszt, zysk, niezawodność i ryzyko. Jak ważne znaczenie mają te czynniki przy ocenie poszczególnych wariantów bezpieczeństwa danych, przedstawiają *wykres 9.1* i *wykres 9.2.*

Wykres 9.1. Znaczenie systemu bezpieczeństwa danych dla poszczególnych wariantów bezpieczeństwa (źródło: opracowanie własne)



Bezpieczeństwo systemów informacyjnych, jak wcześniej wspomniano, obejmuje zbiór procesów zawierających inne procesy bezpośrednio lub pośrednio związane z bezpieczeństwem. Kluczowym jest tu proces zarządzania ryzykiem.

Proces zarządzania ryzykiem sprowadza się do porównywania określonego ryzyka z zyskami i kosztami zabezpieczeń oraz wypracowywania strategii ich wdrożenia oraz polityki bezpieczeństwa instytucji w zakresie systemów informatycznych.

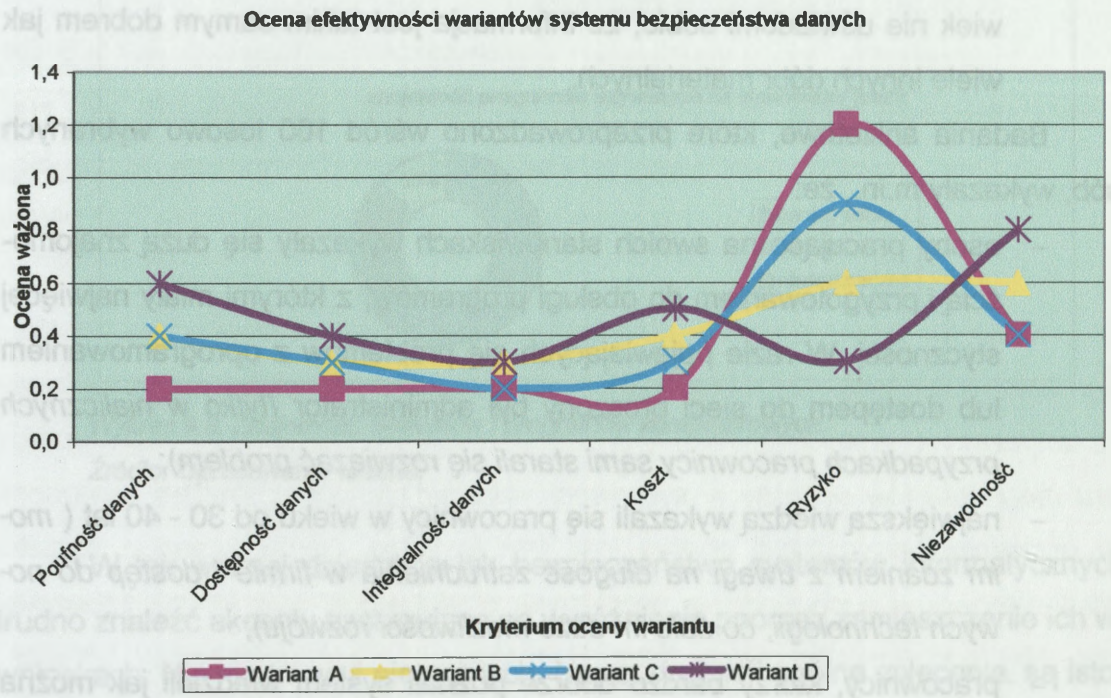
W ramach tego procesu należy oszacować ewentualne straty, które mogą powstać w wyniku włamania się lub zniszczenia systemu. Przy szacowaniu strat należy brać pod uwagę następujące czynniki:

- obliczalność strat;
- możliwość ich udowodnienia;
- możliwość i koszty ich naprawy;
- potencjalną możliwość ich ubezpieczenia.

Wyliczając ewentualne straty wynikające z włamania się do systemu należy zwrócić uwagę, aby koszty poniesione na ochronę nie były od nich większe.

Po analizie zysków i kosztów oraz potencjalnych następstw spośród wielu możliwych do zastosowania zabezpieczeń, wybierane jest właściwe rozwiązanie.

Wykres 9.2. Ocena efektywności wariantów systemu bezpieczeństwa danych



WNIOSKI

Wchodząc w erę społeczeństwa informacyjnego - instytucje rządowe i komercyjne, a nawet poszczególne jednostki stają się coraz bardziej uzależnione od szybkiego, niezawodnego, a przede wszystkim bezpiecznego przetworzenia ogromnych ilości informacji. Rosnąca wartość informacji powoduje wzrost zagrożeń dla nich, stąd niezwykłej wagi problemem stała się ochrona systemów teleinformatycznych i przetwarzanych w nich informacji.

By podkreślić wagę ochrony informacji należy jednoznacznie stwierdzić, że:

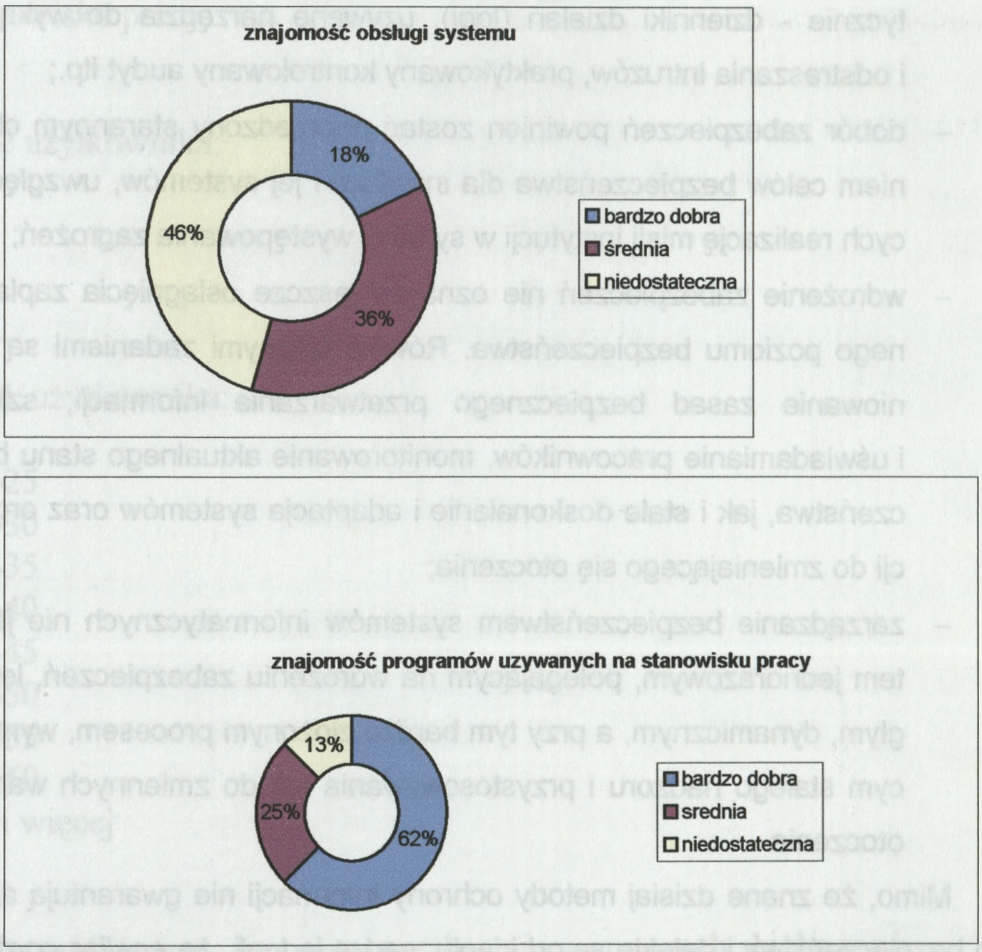
- system ochrony informacji to długi i dynamiczny proces polegający na stworzeniu odpowiednich struktur i instrukcji;
- w systemie bezpieczeństwa bezsprzecznie najważniejszy jest człowiek. Od jego kwalifikacji zawodowych oraz zachowań etycznych i moralnych zależy bardzo dużo. Niewiele pomoże wysokiej klasy sprzęt, jeśli człowiek nie uświadomi sobie, że informacja jest takim samym dobrem jak wiele innych dóbr materialnych.

Badania ankietowe, które przeprowadzono wśród 100 losowo wybranych osób, wykazały m.in., że:

- osoby pracujące na swoich stanowiskach wykazały się dużą znajomością i przygotowaniem do obsługi programów, z którymi miały najwięcej styczności. W razie pojawiających się problemów z oprogramowaniem lub dostępem do sieci proszony był administrator *(tylko w nielicznych przypadkach pracownicy sami starali się rozwiązać problem);*
- największą wiedzą wykazali się pracownicy w wieku od 30 - 40 lat (*moim zdaniem z uwagi na długość zatrudnienia w firmie i dostęp do nowych technologii, co dało im duże możliwości rozwoju);*
- pracownicy, którzy bardzo dobrze poznali system wiedzieli jak można dostać się do danych i mogli wykorzystać to w sposób niepowołany (*chodzi tu przeważnie o zabezpieczenia, kody oraz typy programów zabezpieczających*).

Dopełnieniem analizy są wyniki ankiety pokazujące znajomość obsługi systemów oraz programów używanych na stanowisku pracy, które prezentuje wykres

kołowy 9.3. zaś pytania na które odpowiadali respondenci zawiera wzór ankiety przedstawionej poniżej.



Wykres 9.3. Znajomość systemów i programów komputerowych.
Źródło: Opracowanie własne.

W tak ważnej dziedzinie jak bezpieczeństwo systemów informatycznych, trudno znaleźć akcenty zasługujące na wyróżnienie poprzez zamieszczenie ich we wnioskach. Nie ma kwestii nieważnych. Nawet drobne i ogólne zalecenia, są istotnie ważne.

Reasumując:

- *bezpieczeństwo musi być rozpatrywane w aspekcie organizacyjnym, technicznym, prawnym oraz ekonomicznym*. Wiąże się to z zapewnieniem gwarantowanego poziomu jakości informacji - informacje muszą być poprawne, dostępne tylko dla uprawnionych podmiotów, w odpowiednim czasie i tylko na odpowiednich stanowiskach instytucji;

- bezpieczeństwo musi być utrzymywane, a więc również monitorowane. Analizowany powinien być wpływ zmian na bezpieczeństwo, kontrolowana permanentnie rozliczalność, sprawdzane - coraz częściej automatycznie - dzienniki działań (logi), używane narzędzia do wykrywania i odstraszania intruzów, praktykowany kontrolowany audyt itp.;
- dobór zabezpieczeń powinien zostać poprzedzony starannym określeniem celów bezpieczeństwa dla instytucji i jej systemów, uwzględniających realizację misji instytucji w sytuacji występowania zagrożeń;
- wdrożenie zabezpieczeń nie oznacza jeszcze osiągnięcia zaplanowanego poziomu bezpieczeństwa. Równie ważnymi zadaniami są: zdefiniowanie zasad bezpiecznego przetwarzania informacji, szkolenie i uświadamianie pracowników, monitorowanie aktualnego stanu bezpieczeństwa, jak i stałe doskonalenie i adaptacja systemów oraz organizacji do zmieniającego się otoczenia;
- zarządzanie bezpieczeństwem systemów informatycznych nie jest aktem jednorazowym, polegającym na wdrożeniu zabezpieczeń, lecz ciągłym, dynamicznym, a przy tym bardzo złożonym procesem, wymagającym stałego nadzoru i przystosowywania się do zmiennych warunków otoczenia.

Mimo, że znane dzisiaj metody ochrony informacji nie gwarantują absolutnego bezpieczeństwa i dalekie są od ideału, sądzę jednak, że *analiza porównawcza dotycząca zagadnień prawno – ekonomicznych jest metodą optymalnego doboru mechanizmów ochrony w systemach informatycznych.* Głównym powodem dla przeprowadzenia takiej analizy jest fakt istnienia zróżnicowanego sprzętu i oprogramowania pochodzących od różnych producentów oraz koszty zabezpieczeń. Aby móc określić poziomy bezpieczeństwa w sposób unifikowany, konieczna jest znajomość ujednoliconych kryteriów bezpieczeństwa systemów informatycznych.

Analiza prawno – ekonomiczna powinna w maksymalnym stopniu uwzględniać rozwiązania istniejące i wyznaczać rozsądny kompromis między wyznaczonym poziomem zabezpieczenia, a poziomem nakładów finansowych, które instytucja (państwo) gotowa jest ponieść.

ANKIETA DOTYCZĄCA ZABEZPIECZEŃ W FIRMIE X

1. Stanowisko pracy: .....

2. Płeć użytkownika:

- ◻ M
- ◻ K

3. Wiek użytkownika:

- ◻ 18-25
- ◻ 26-30
- ◻ 31-35
- ◻ 36-40
- ◻ 41-45
- ◻ 46-50
- ◻ 51-55
- ◻ 56-60
- ◻ 60 i więcej

4. Czy pan(i) używa komputera wyłącznie w sprawach służbowych w miejscu pracy?

- ◻ TAK
- ◻ NIE

5. Ilu użytkowników korzysta z tego samego komputera ? .....

6. Czy inni użytkownicy mają inne kody dostępu ?

- ◻ TAK
- ◻ NIE

7. Czy istnieje jasna, sprecyzowana polityka działania i odpowiedzialności?

- ▫ TAK
- ▫ NIE

8. Czy wszystkie zbiory i dokumentacje, bez wyjątku podlegają wystarczającej kontroli?

- ▫ TAK
- ▫ NIE

9. Czy podczas pracy w firmie X przestrzegana jest surowa dyscyplina porządkowa?

- ▫ TAK
- ▫ NIE

10. W przypadku wpisania złego hasła lub braku dostępu do bazy danych:

- ▫ stara się Pan(i) sam(a) rozwiązać problem
- ▫ wzywany jest administrator
- ▫ inne jakie .....

11. Czy ochronie podlega?

- ▫ cała sieć
- ▫ poszczególne stacje robocze

12. Kto nadzoruje system?

.....

13. Jaka firma zabezpiecza dane w Pana(i) firmie?

.....

14. W jakiej formie są zapisywane dane?

.....

15. Czy udało się uniknąć podejścia do spraw bezpieczeństwa informacji opartego na urządzeniach, które często zawodzą?

- ▫ TAK
- ▫ NIE

16. Na ile zabezpieczenia według Pana(i) są skuteczne (podać w %)?

10 20 30 40 50 60 70 80 90 100

17. Jak Pan(i) ocenia zabezpieczenia?

- ▫ skuteczne
- ▫ nieskuteczne

1.9.6. Standardy normalizacyjne oraz akty prawne w zakresie bezpieczeństwa systemów informatycznych

Rozwój technologii informatycznych spowodował z jednej strony znaczny skok cywilizacyjny współczesnych społeczeństw – powodując powstanie społeczeństw informacyjnych – z drugiej zaś, spowodował pojawienie się nowych zjawisk związanych z nielegalnym wykorzystywaniem lub dostępem do informacji. Sytuacja ta znalazła swoje odbicie w działaniach wielu państw i grup państw, których efektem było opracowanie kryteriów oceny zabezpieczeń produktów teleinformatycznych.

Międzynarodowe standardy normalizacyjne

Próby ustandardowienia zagadnień związanych z ochroną i oceną bezpieczeństwa systemów informatycznych, były podejmowane w praktyce od połowy lat sześćdziesiątych, gdy zaczęły wchodzić do powszechnego użytku systemy wielodostępne oraz pojawiły się pierwsze sieci komputerowe.

Pierwszymi udanymi zaleceniami, które wywarły istotny wpływ na sposób rozumienia problematyki bezpieczeństwa w systemach informatycznych i na wiele lat stały się podstawą do opracowania lokalnych standardów, były zalecenia wydane w USA, w 1983 roku w postaci tzw. *„Pomarańczowej księgi"*.

W zarysie, historia prób opracowania standardów bezpieczeństwa informacji w systemach informatycznych, przedstawia się następująco:

- początek lat 80-tych, USA:
  Trusted Computer System Evaluation Criteria (TCSEC) „Orange Book";
- rok 1990:
  w ramach ISO[16] rozpoczęto prace nad opracowaniem międzynarodowego standardu kryteriów oceny bezpieczeństwa systemów informatycznych
  (Working Group 3/Subcommittee 27/Joint Technical Committee 1);

[16] *International Standards Organization – Międzynarodowa Organizacja Standardów*

- rok 1991, Europa:
  pod patronatem Komisji Europejskiej opublikowano przygotowany przez Francję, Niemcy, Holandię i Wielką Brytanię projekt: *Information Technology Security Evaluation Criteria v. 1.2 (ITSEC);*
- czerwiec 1993, Kanada:
  opublikowano *Canadian Trusted Computer Product Evaluation Criteria v. 3.0 (CTCPEC)* łączący cechy ITSEC i TCSEC;
- początek 1993, USA:
  opublikowano *Federal Criteria for Information Technology Security v. 1.0 - draft (FC)* jako konkurencyjną do kanadyjskiej próbę połączenia standardów USA i Europy;
- czerwiec 1993:
  organizacje, które opracowały CTCPEC, FC, TCSEC oraz ITSEC, podjęły wspólną pracę w ramach projektu o nazwie *Common Criteria (CC)*, nad połączeniem w/w standardów w jedną spójną całość;
- styczeń 1996:
  wersja 1.0 Common Criteria zaaprobowana w kwietniu 1996 roku przez ISO *(Committee Draft);*
- październik 1997:
  wersja „beta" Common Criteria v.2.0 stanowiąca podstawę do opracowania normy ISO/IEC 15408 o nazwie *„Evaluation Criteria for Information Technology Security";*
- 5.10.1998:
  podpisanie umowy pomiędzy organizacjami (z państw uczestniczących w projekcie CC) certyfikującymi produkty informatyczne o wzajemnym uznawaniu certyfikatów bezpieczeństwa wydawanych na podstawie Common Criteria.

Kryteria bezpieczeństwa systemów informatycznych wg TCSEC („Pomarańczowej księgi")

Departament Ministerstwa Obrony USA oraz Narodowe Biuro Standaryzacji przez ponad sześć lat pracowały nad stworzeniem ujednoliconych podstaw budowy, oceny i weryfikacji bezpiecznych systemów komputerowych. W efekcie, w 1983 roku powstały „Kryteria oceny zaufania systemów komputerowych" - TCSEC (*ang. Trusted Computer System Evaluation Criteria*) znane także pod nazwą *„Pomarańczowej księgi"* (*ang. Orange Book*).

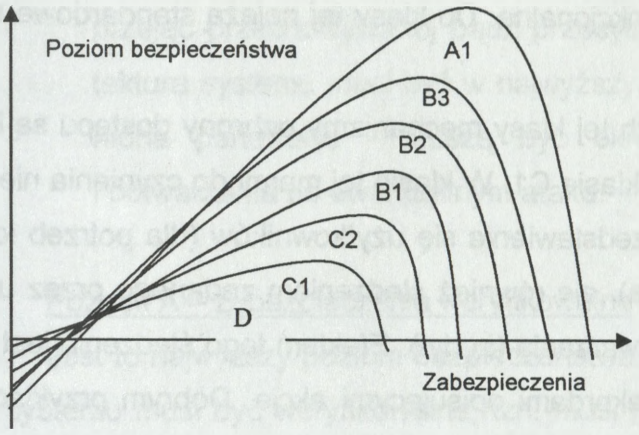
TCSEC definiuje *cztery poziomy bezpieczeństwa* oznaczone odpowiednio ***D, C, B, A.*** Do każdego z nich przydzielono pewną liczbę *klas oceny*, przy czym zachowano hierarchiczny porządek narastania możliwości ochrony danych. Najmniejsze możliwości odpowiadają poziomowi **D,** największe poziomowi **A.** Każdy wzrost możliwości oznacza jednocześnie zmniejszenie ryzyka penetracji systemu. Obowiązuje tu tzw. *zasada kumulacji możliwości*, zgodnie, z którą środki ochrony danych spełniające wymagania wyższego poziomu spełniać muszą wymagania niższego poziomu. Przejście do kolejnej klasy, a tym bardziej następnego poziomu, oznacza wydatne zwiększenie możliwości ochronnych.

W standardzie TCSEC, każdy poziom i klasa są charakteryzowane czterema głównymi elementami:[17]

- polityką bezpieczeństwa (*ang. security policy*);
- zdolnością rozliczania *(ang. accountability)* - identyfikacja, kontrola i sprawdzanie podmiotu, czyli jego odpowiedzialność;
- gwarancją działania mechanizmów zabezpieczających (*ang. assurance*);
- wymaganą dokumentacją (*ang. documentation)* - testy sprawdzające system i opis idei bezpieczeństwa systemu.

Struktura systematycznego podziału kryteriów na poziomy i klasy przedstawia się następująco: *(patrz rysunek 9.14).*

[17] *V. Ahuja: Bezpieczeństwo w sieciach, Mikom, Warszawa 1997*



Rysunek 9.14. Kryteria bezpieczeństwa systemów ochrony[18]

Poziom D – minimalne zabezpieczenia

Poziom ten posiada tylko klasę D. *Systemy należące do tego poziomu nie zawierają mechanizmów zabezpieczających* i zapewniają minimalną ochronę. Do tej grupy można zakwalifikować komputery klasy PC pracujące pod kontrolą systemu operacyjnego DOS.

Poziom C – zabezpieczenia dyskrecjonalne

W skład tego poziomu bezpieczeństwa wchodzą systemy, w których bezpieczeństwo opiera się na dyskrecjonalnej kontroli dostępu. Polega to na tym, że *dostęp użytkownika do obiektu systemu, wymaga sprawdzenia uprawnień użytkownika do tego obiektu*. Jeżeli użytkownik je posiada, to system zezwala mu na dostęp do obiektu, natomiast w przeciwnym razie następuje odmowa.

Poziom ten posiada dwie klasy - C1 i C2

- *Klasa C1 – jest najniższą klasą* poziomu C *i jednocześnie pierwszą, w której system zapewnia pewien stopień bezpieczeństwa*. System operacyjny kontroluje uprawnienia użytkowników do odczytu i zapisu plików i kartotek oraz dysponuje mechanizmem autoryzacji dostępu (dostęp możliwy tylko po podaniu hasła na wejściu do systemu ochrony). Klasa ta nie posiada mechanizmów rejestracji zdarzeń.

Aktualnie prawie każdy z większych systemów komercyjnych spełnia wymagania tego poziomu. Jednakże, aby się o tym przekonać, należy przeprowa-

[18] *B. Fischer: Przestępstwa komputerowe i ochrona informacji, Zakamycze 2000, Kraków 2000*

dzić odpowiednie testowanie funkcjonalne. Do klasy tej należą standardowe systemy UNIX.

- *Klasa C2* -w systemach tej klasy mechanizmy ochrony dostępu są bardziej precyzyjne niż w klasie C1. W klasie tej mamy do czynienia nie tylko z koniecznością przedstawienia się użytkowników (dla potrzeb identyfikacji i upoważnienia), ale również śledzeniem zadanego przez użytkownika procesu przetwarzania (audyt). Efektem tego śledzenia jest odpowiednia kronika z rekordami opisującymi akcje. Dobrym przykładem systemu tej klasy jest system operacyjny IBM MVS z pakietami ochrony zasobów systemu.

Poziom B – zabezpieczenia obowiązkowe

W skład tego poziomu bezpieczeństwa wchodzą systemy, w których bezpieczeństwo opiera się na obowiązkowej kontroli dostępu. Polega to na tym, że stosuje się klasyfikację informacji uwzględniającą różne poziomy jej bezpieczeństwa (np. jawna, poufna, tajna). Istotne jest tu utrudnienie w komunikacji użytkowników, np. użytkownik mający wyższe uprawnienia musi uzyskać uprawnienia niższe chcąc np. przesłać pocztę elektroniczną podwładnemu. Poziom ten posiada klasy B1, B2 i B3.

- *Klasa B1* – posiada wymagania jak dla klasy C2 tylko wzbogacone o mechanizm etykietowania (klauzule tajności); obsługuje bezpieczeństwo na kilku poziomach typu *„tajne"* i *„ściśle tajne"*. Ma zamontowane mechanizmy uznaniowej kontroli dostępu do plików i kartotek, co może spowodować zablokowanie dostępu do danych przez określonego użytkownika.
- *Klasa B2* – posiada mechanizmy zabezpieczeń zdefiniowane jeszcze precyzyjniej niż w klasie B1 (zabezpieczenia strukturalne). Polega to na tym, że każdy obiekt w systemie komputerowym musi mieć przypisaną etykietę bezpieczeństwa określającą jego status, np., jeżeli obiekt *„użytkownik"* żąda dostępu do obiektu *„plik"*, system ochrony na podstawie etykiet bezpieczeństwa akceptuje lub odrzuca żądanie.
- *Klasa B3* – problem bezpieczeństwa przenosi się tutaj na sprzęt komputerowy, który musi nam zagwarantować, że nikt nie będzie w stanie

przejąć przechowywanej bądź przesyłanej przez nas informacji. Architektura systemu musi być w najwyższym stopniu odporna na nieuprawniona penetrację - muszą być określone procedury alarmowania i odtwarzania po ewentualnym ataku.

Poziom A – zabezpieczenia weryfikowalne

Jest to najwyższy poziom bezpieczeństwa. Na tym poziomie cała konstrukcja systemu musi być weryfikowalna, tzn. musi poddać się ocenie formalnej, czy i jak obowiązujące mechanizmy (w zasadzie takie jak w klasie B3) są realizowane w praktyce - wymagana jest obszerna dokumentacja, której celem jest wykazanie, że baza bezpieczeństwa odpowiada wszelkim wymaganiom bezpieczeństwa na etapach projektu, wdrożenia i rozwoju. Poziom ten posiada tylko klasę A1.

Jak zatem widzimy, kolejne poziomy reprezentują istotne jakościowo różnice w zdolności systemu do spełniania kryteriów ochrony danych. Natomiast klasy wewnątrz poziomów oznaczają sukcesywne, lecz umiarkowane wzmocnienie skuteczności środków ochrony danego poziomu. Tak, więc jeśli pierwotnie zaliczono system do klasy C1, to istnieje możliwość stosunkowo łatwego spełnienia wymagań klasy C2. Jednakże osiągnięcie właściwości klasy np. B1 bez dużych i kosztownych zmian systemu ochrony oraz konstrukcji samego ochranianego systemu, jest niemożliwe.

Pod adresem *„Pomarańczowej księgi"* opracowanej przez specjalistów z kręgów wojskowych kierowano wiele zarzutów. Najważniejszy z nich dotyczył tego, ze przy opracowaniu uwzględniono bezpieczeństwo przechowywania (poufność) danych, a mniejszą uwagę zwracano na integralność danych i niezawodność systemu, co jest istotne dla firm komercyjnych. Ponoć większość firm zadowala poziom bezpieczeństwa z klasy C2.

„Pomarańczowa księga" koncentrowała swoją uwagę na współdzielonych systemach scentralizowanych, dominujących w latach siedemdziesiątych i nie uwzględniała zmian, które nastąpiły później, a polegały na szerokim stosowaniu stacji roboczych, serwerów i sieci komputerowych.

Z tego powodu w 1987 roku opublikowano zmodyfikowany zestaw kryteriów *„Trusted Network Interpretation of the TCSEC"* znany pod nazwą *„Księgi czerwonej"* *(ang. Red Book)*. Dodatkowo w roku 1991 opracowano dokument o nazwie

„Trusted Database Interpretation", który uwzględniał potrzebę oceny systemów aplikacyjnych niemieszczących się w pojedynczej klasie bezpieczeństwa widzianej z poziomu systemu operacyjnego.

Kryteria bezpieczeństwa systemów informatycznych wg ITSEC

W Europie wysiłki mające na celu ustalenie międzynarodowych kryteriów oceny bezpieczeństwa systemów informatycznych podjęte zostały w drugiej połowie lat osiemdziesiątych. Eksperci z Francji, Niemiec, Holandii i Wielkiej Brytanii opracowali w 1991 roku zestaw *„Kryteriów oceny bezpieczeństwa technologii informacyjnej"* – ITSEC (*ang. Information Technology Security Evaluation Criteria*). ITSEC stanowi próbę rozszerzenia *„Pomarańczowej księgi"*.

Zaleca on następujące mechanizmy ochronne[19]:

- identyfikacja i uwierzytelnianie użytkowników (*ang. identification and authentication);*
- kontrola dostępu do zasobów (*ang. access control*);
- możliwość rozliczania wykonywanych czynności (*ang.* accountability);
- śledzenie zdarzeń związanych z bezpieczeństwem (*ang.* audit);
- niemożność ponownego wykorzystania obiektów (*ang. object reuse*);
- nienaruszalność danych (*ang. accuracy*);
- niezawodność usług (*ang. reliability of service*);
- bezpieczna wymiana danych (*ang. data exchange*).

Skala ocen bezpieczeństwa w klasyfikacji ITSEC jest – podobnie jak w klasyfikacji TCSEC – siedmiopoziomowa, od E0 do E6, gdzie E0 oznacza poziom najmniej bezpieczny. Na każdy wyższy poziom tutaj też składają się wymagania niższego poziomu i pewne wymagania dodatkowe.

W porównaniu z *„Pomarańczową księgą"* w ITSEC funkcjonalność systemu jest dodatkowo cechowana takimi ocenami jak:

- wierność – rozszerzona funkcja integralności, obejmuje wykrywanie i prewencję;

[19] *V. Ahuja: Bezpieczeństwo w sieciach, Mikom, Warszawa 1997*

- niezawodność pracy – gwarantuje dostęp do zasobów systemu w wymaganym czasie (np. dla systemów pracujących w czasie rzeczywistym);
- wymiana danych – usługi związane z zabezpieczeniem kanałów transmisyjnych.

Porównanie poziomów zabezpieczeń według kryteriów ITSEC i TCSEC (*„Pomarańczowej księgi"*) przedstawiono w tabeli 9.7.

Tabela 9.7.

Klasy równorzędne według ITSEC i TCSEC[20]

ITSEC	TCSEC
E0	D
F-C1, E1	C1
F-C2, E2	C2
F-B1, E3	B1
F-B2, E4	B2
F-B3, E5	B3
F-B3, E6	A1

Dokumenty ITSEC zostały uzupełnione ostatnio o dokument przeznaczony dla osób dokonujących oceny bezpieczeństwa, nazwany ITSEM (*ang. Information Technology Security Evaluation Manual*). Dokument ten jest instrukcją postępowania w trakcie procesu oceny. ITSEM znany jest także pod nazwą *„Białej księgi"*.

Wspólne Kryteria – Common Criteria

Wspólne Kryteria – Common Criteria (CC) są wysiłkiem Kanady, Francji, Niemiec, Holandii, Stanów Zjednoczonych i Wielkiej Brytanii. Kraje te w październiku 1999 roku uzgodniły obowiązującą obecnie wersję 2.1, która stała się podstawą opracowania międzynarodowego standardu ISO/IEC 15408.

[20] *M. Molski: Podstawy bezpieczeństwa systemów informatycznych, MSG-Media, Bydgoszcz 1998*

Common Criteria stanowią podstawę do oceny poziomu zabezpieczeń urządzeń i systemów teleinformatycznych.

W Common Criteria wykorzystano model bezpieczeństwa, w którym zawarto takie elementy jak aktywa (informacyjne, materialne i kadrowe), zagrożenia i ich źródła, podatności i ryzyka, zabezpieczenia i właścicieli aktywów.

Charakterystyczne cechy zaleceń sformułowanych w Common Criteria są następujące[21]:

- CC są zaleceniami mającymi na celu wprowadzenie ujednoliconego sposobu oceny systemów informatycznych pod względem szeroko rozumianego bezpieczeństwa; *mówią tylko o tym, co należy zrobić*, aby osiągnąć zadane cele, *nie mówią natomiast nic o tym jak to zrealizować*;
- *CC są katalogiem* (wyrażonym w kategoriach klas, rodzin, komponentów schematów elementów) schematów konstrukcji wymagań związanych z ochroną informacji w systemach informatycznych;
- CC mogą być stosowane zarówno do produktów programowych jak i sprzętowych stosowanych w informatyce;
- CC nie zalecają ani nie wspierają żadnej ze znanych metod projektowania informatycznych wytwarzania systemów informatycznych oraz nie mówią nic na temat metodyki oceny systemów informatycznych (tzn. podają jak np. skonstruować profil ochrony, ale nie podają jak go wykorzystać);
- CC są przeznaczone zarówno dla użytkowników *(customers)* systemów projektantów (*developers*) systemów informatycznych, jak i osób oceniających te systemy i produkty (*evaluators*).

Wynikiem oceny systemu informatycznego według zaleceń CC jest dokument stwierdzający:

- zgodność tego systemu z określonym *profilem ochrony*, lub
- spełnienie wymagań bezpieczeństwa określonych w *przedsięwzięciach bezpieczeństwa,* lub
- przypisanie do konkretnego *poziomu bezpieczeństwa* (EAL – *Evaluation Assurance Level*). Jest 7 poziomów bezpieczeństwa: od EAL1 do EAL7.

---

[21] *K. Liderman: Bezpieczeństwo informacji w systemach informatycznych, Seria: Skrypty Wyższej Szkoły Informatyki Stosowanej i Zarządzania, Warszawa 2000*

Wyższy poziom zawiera wymagania o wyższym stopniu rygoryzmu lub bardziej formalne.

Jednym z celów opracowania Common Criteria była możliwość uznawania wyników badań i wystawianych certyfikatów przez kraje, które posiadają własne systemy oceny i certyfikacji lub takie, które nie posiadając takiego systemu są gotowe oficjalnie uznawać dokumenty wystawiane przez podmioty funkcjonujące zgodnie z metodyką zdefiniowaną w Common Criteria.

W tym celu kraje założycielskie, utworzyły jednolite porozumienie certyfikatów wzajemnym uznawaniu certyfikatów - *Common Criteria Recognition Arrangement (CCRA)*, dające podstawy do automatycznego wzajemnego uznawania wyników badań dla poziomów uzasadnionego zaufania EAL1-EAL4 z 7 poziomów zdefiniowanych we wspólnych kryteriach CC.

Porozumienie to:

- weszło w życie 23.05.2000 r.;
- jego członkami jest obecnie 14 państw (Australia, Nowa Zelandia, Kanada, Finlandia, Francja, RFN, Grecja, Włochy, Holandia, Norwegia, Hiszpania, Wielka Brytana, USA, Izrael);
- kraje członkowskie mogą być wystawcami i/lub konsumentami certyfikatów;
- obejmuje uznawanie certyfikatów dla poziomów uzasadnionego zaufania EAL1 – EAL4;
- określa wymagania dla jednostek certyfikujących oraz zawartość raportów z oceny i certyfikacji.

W tym miejscu należy podkreślić, że do tej pory[22] (*stan na początek kwietnia 2001 r.*) oceniono na świecie wg Common Criteria 47 produktów teleinformatycznych, w tym stosunkowo dużo systemów zaporowych (*ang. firewall*), do czego poprzednie kryteria TCSEC czy też ITSEC były mało przydane. W trakcie badań znajduje się 15 dalszych produktów teleinformatycznych.

[22] *R. Kośla, J.Cendrowski: Rola kryteriów oceny zabezpieczeń teleinformatyki dla bezpieczeństwa teleinformatycznego polskiej administracji publicznej w XXI wieku - Materiały II Sympozjum Bezpieczeństwa Systemów Informacyjnych, 22-23.05.2001*

Przykłady zastosowań międzynarodowych standardów normalizacyjnych

Jedną z możliwości podniesienia bezpieczeństwa informacji, jest projektowanie i wytwarzanie systemów komputerowych o wysokiej jakości. Sposób projektowania i wytwarzania takich systemów jest regulowany szeregiem zaleceń międzynarodowych organizacji normujących np. ISO - *International Standards Organization* .

Niektóre firmy wdrażają już praktycznie pewne rozwiązania sprzętowe i programowe bezpieczeństwa systemowego. Przykładowo: firma Hewlett–Packard realizuje w swoich wyrobach trzy funkcje – poufność, wiarygodność i dostępność usług.

Poufność jest realizowana przez szyfrowanie przechowywanych i przesyłanych informacji za pomocą sprzętowego modułu kryptograficznego w postaci standardowej karty rozszerzenia.

Wiarygodność jest realizowana przez system operacyjny HP-UX dostarczany w dwóch wersjach – standardowej (klasa C2) oraz BLS (klasa B1 z elementami B2).

Dostępność usług zapewniona jest przez ochronę przed:

- zanikiem zasilania (UPS, bateryjne podtrzymanie jednostki centralnej);
- awarią systemu dyskowego (macierze dyskowe RAID 1);
- utratą zgromadzonych danych (urządzenia archiwizujące taśmowe i magnetooptyczne);
- uszkodzeniem jednostki centralnej (konfiguracje z systemem rezerwowym).

Również Międzynarodowa Unia Telekomunikacyjna– ITU (*ang. International Telecommunication Union*), ujmuje w swoich opracowaniach zagadnienia związane z bezpieczeństwem systemów informatycznych (X.400, X.435, X.500, X.800). Wybrane normy z dziedziny ochrony informacji przedstawiono w tabeli 9.8.

Tabela 9.8.

Wybrane normy i projekty norm z dziedziny ochrony informacji[23]

Dziedzina	Norma
Podpisy cyfrowe	ISO 9796
Funkcje kompresji	ISO DIS 10118
Uwierzytelnienie	ISO DIS 9797, ISO 9798
Kryptosystemy	ANSI X.3.2 (DES)
Tryby pracy szyfru blokowego	ISO 10116
Dystrybucja kluczy	ISO CD 11166
Architektura bezpieczeństwa dla systemów otwartych	X.800 (kontynuacja ISO 7498-2)
Poczta elektroniczna, elektroniczna wymiana dokumentów EDI	X.400, X.435
Elektroniczna książka telefoniczna	X.500

1.9.7. Stan prawny w Europie

Problematyką prawną komputeryzacji, w tym także ochroną informacji, zajmuje się utworzona w 1948 roku Rada Europy. Jest to najstarsza w Europie instytucja, która proponuje międzynarodową i parlamentarną współpracę między innymi w zakresie tworzenia prawa. Jej uchwały, zalecenia i rezolucje są wprowadzane w życie we wszystkich krajach członkowskich.

W dziedzinie prawa chroniącego informację w systemach informatycznych Komitet Rady Europy przyjął następujące uchwały:

1. Rezolucję 73/22 o ochronie danych osobowych w sektorze prywatnym (1973 r.).
2. Rezolucję 74/22 o ochronie danych osobowych w sektorze publicznym (1974 r.).
3. Konwencję nr 108 o ochronie osób w związku z automatycznym przetwarzaniem danych o charakterze osobowym (1981 r.)
4. Zalecenie nr R/89/9, które dotyczy przede wszystkim uwzględnienia w ustawodawstwie poszczególnych państw tzw. listy minimalnej przestępstw komputerowych (1989 r.).

[23] *M. Molski: Podstawy bezpieczeństwa systemów informatycznych, MSG-Media, Bydgoszcz 1998*

Krajem, w którym dokonano całościowej regulacji ustawowej według wskazań Komisji Ekspertów Rady Europy, jest Francja. Zdaniem specjalistów, uregulowania prawne we Francji dotyczące przestępstw komputerowych są kompletne, spójne i dostosowane do specyfiki tej przestępczości.

Tworzą je:

1. Ustawa z 06.01.1978 roku dotycząca informatyki, karotek i wolności.
2. Ustawa z 03.07.1985 roku dotycząca ochrony praw autorskich do programów komputerowych.
3. Ustawa z 05.01.1988 roku o fałszerstwach komputerowych.

W Wielkiej Brytanii, w sierpniu 1990 roku weszła w życie *„Ustawa o nadużyciach komputerowych"*, która określa trzy kategorie przestępstw w informatyce:

1. niedozwolone wejście do systemu, włączając w to włamanie;
2. niedozwolone wejście do systemu z zamiarem popełnienia przestępstwa na zlecenie, w rodzaju oszustwa i kradzieży danych lub pomocy w wykonaniu takich czynności;
3. niedozwolone zmiany w danych komputerowych, włączając użycie wirusów, bomb logicznych itp..

Brytyjczycy przewidują surowe kary za te przestępstwa:

- za przestępstwa określone w pkt. 1 przewiduje się grzywnę do 2 tys. funtów szterlingów oraz pozbawienie wolności do 6 miesięcy;
- za przestępstwa określone w pkt. 2 i 3 przewiduje się karę pozbawienia wolności do 5 lat i grzywnę w nieograniczonej wysokości.

Omawiana ustawa, w odróżnieniu od innych chroni swym zasięgiem całe Zjednoczone Królestwo.

W Szwecji w1973 roku wydano pierwszą na świecie ustawę o danych, w której wprowadzono pojęcie przestępstwa przeciw danym.

W 1976 roku *w RFN* uchwalono federalną ustawę o ochronie danych.

1.9.8. Uregulowania prawne w Polsce

W ciągu ostatnich kilku lat można zaobserwować w Polsce wyraźny wzrost zaleceń oraz aktów prawnych zawierających wytyczne w zakresie ochrony informacji przechowywanych w systemach informatycznych. Dokumenty tego typu, opracowane w sposób dość szczegółowy, stanowią cenne źródło problematyki zarządzania bezpieczeństwem informacji.

Normy standaryzacyjne

Jednym ze skutków standaryzacji, jak już wcześniej wspomniałam, jest dążenie do jednoznacznej globalnej identyfikacji obiektów. Obiekty mogą być definiowane przez takie organizacje jak:

- ISO (*International Standards Organization*);
- IEC (*International Electrotechnical Commission*);
- ITU-T (*International Telecommunication Union;*
- *Telecommunication Standardization Sector*);
- organizacje komercyjne i rządowe.

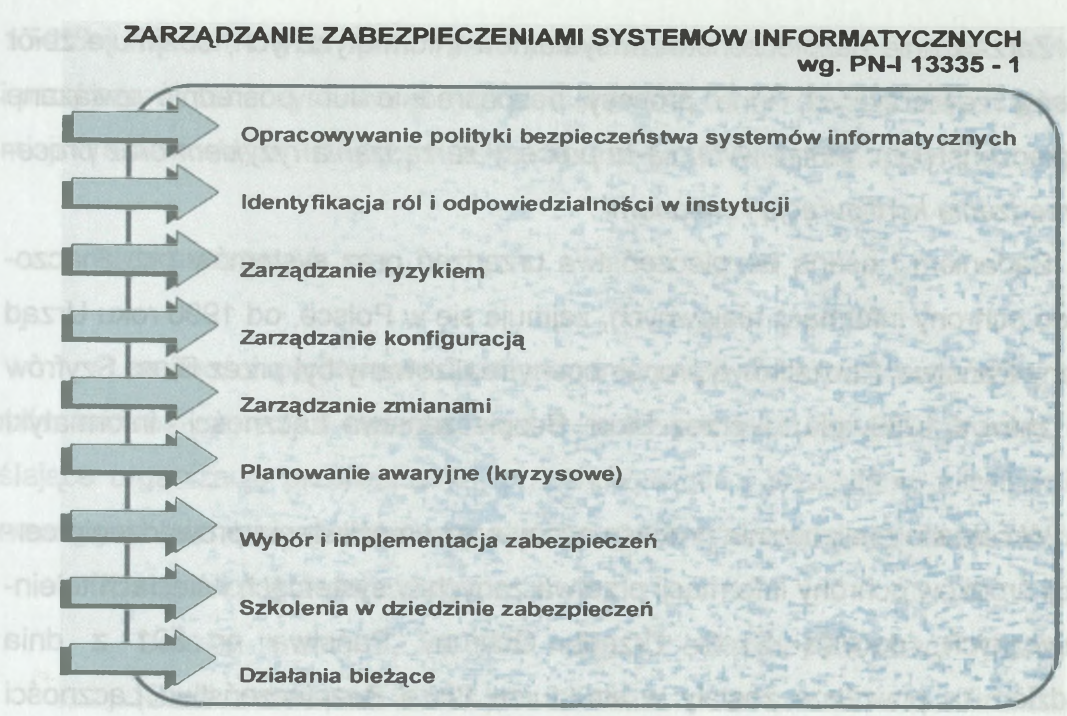
Kluczowym dla zarządzania bezpieczeństwem informacji jest *Raport Techniczny – ISO/IEC TR 13335,* składający się z 5 części, z których pierwsza obowiązuje od 2000 roku jako Polska Norma (pozostałe części są w różnym stadium przygotowania).

Poszczególne części raportu zawierają następujące informacje:

- ISO/IEC/TR 13335-1: Wytyczne do zarządzania bezpieczeństwem systemów informatycznych (jest to *Polska Norma PN-I-13335-1*);
  - terminologia, związki między pojęciami;
  - podstawowe modele;
- ISO/IEC/TR 13335-2: Planowanie i zarządzanie bezpieczeństwem systemów informatycznych;
  - różne podejścia do prowadzenia analizy ryzyka;
  - plany zabezpieczeń;
  - rola szkoleń i działań uświadamiających;

- stanowiska pracy w instytucji związane z bezpieczeństwem;
- ISO/IEC/TR 13335-3: Techniki zarządzania bezpieczeństwem systemów informatycznych;
  - formułowanie trójpoziomowej polityki bezpieczeństwa;
  - rozwinięcie problematyki analizy ryzyka;
  - rozwinięcie problematyki implementacji planu zabezpieczeń;
  - reagowanie na incydenty.
- ISO/IEC/TR 13335-4: Wybór zabezpieczeń;
  - klasyfikacja i charakterystyka różnych form zabezpieczeń;
  - dobór zabezpieczeń ze względu na rodzaj zagrożenia i rodzaj systemu.
- ISO/IEC/WD 13335-5: Zabezpieczenie dla połączeń z sieciami zewnętrznymi;
  - dobór zabezpieczeń stosowanych do ochrony styku systemu z siecią zewnętrzną.

Podstawową normą dla zarządzania bezpieczeństwem informacji w naszym kraju jest Polska Norma PN-I-13335-1. Zawiera ona ogólne wytyczne związane z polityką bezpieczeństwa systemów teleinformatycznych. Wytyczne te przedstawia rys 9.15.



Rysunek 9.15. Wytyczne dotyczące zarządzania zabezpieczeniami systemów informatycznych wg PN I 13335-1[24]

Według Polskiej Normy PN-I 13335-1, *zarządzanie bezpieczeństwem systemów informatycznych obejmuje zespół procesów zmierzających do osiągnięcia i utrzymywania ustalonego poziomu bezpieczeństwa, tzn. poziomu poufności, integralności, dostępności, rozliczalności, autentyczności i niezawodności.* Jego realizacja obejmuje działania, takie jak:

- określenie celów (*co należy chronić*), strategii (*w jaki sposób*) i polityk bezpieczeństwa systemów informatycznych w instytucji (*jakie konkretne przedsięwzięcia należy podjąć*);
- identyfikowanie i analizowanie zagrożeń dla zasobów;
- identyfikowanie i analizowanie ryzyka;
- określenie adekwatnych zabezpieczeń;
- monitorowanie wdrożenia, eksploatacji (skuteczności) zabezpieczeń;
- opracowanie i wdrożenie programu szkoleniowo-uświadamiającego;
- wykrywanie incydentów i reakcja na nie.

[24] *B.Kusina : Informacja – towar chroniony, Konferencja e-Komputer Expo, Warszawa 23 24.01.2001*

Zarządzanie bezpieczeństwem systemów informatycznych, obejmuje zbiór procesów zawierających inne procesy bezpośrednio lub pośrednio związane z bezpieczeństwem. *Kluczowymi są tu procesy zarządzania ryzykiem oraz procesy zarządzania konfiguracją i zmianami.*

Badaniem i oceną bezpieczeństwa urządzeń oraz systemów przeznaczonych do ochrony informacji niejawnych, zajmuje się w Polsce, od 1990 roku Urząd Ochrony Państwa. Początkowo proces oceny realizowany był przez Biuro Szyfrów UOP, zaś od 1996 roku – przez Biuro Bezpieczeństwa Łączności i Informatyki UOP.

W celu sformalizowania procesu oceny oraz umożliwienia prowadzenia certyfikacji środków ochrony informacji przetwarzanych w systemach i sieciach teleinformatycznych, decyzją Szefa Urzędu Ochrony Państwa nr 301 z dnia 7 października powołane zostały w strukturze Biura Bezpieczeństwa Łączności i Informatyki UOP:

- Jednostka Certyfikująca;
- Laboratorium Badawcze Urządzeń i Systemów Kryptograficznych;
- Laboratorium Badawcze Kompatybilności Elektromagnetycznej i Emisji Ujawniającej.

Jednostka Certyfikująca BBŁiI UOP odpowiedzialna jest za zlecanie badań laboratoriom badawczym i prowadzenie merytorycznego oraz formalnego nadzoru nad prowadzonymi badaniami. Sprawozdania z badań są weryfikowane i zatwierdzane przez Jednostkę Certyfikującą BBŁiI UOP. Fakt poprawnego zakończenia procesu badań i certyfikacji potwierdzany jest wydaniem stosownego certyfikatu. *Certyfikaty wystawiane są na czas określony.*

W badaniach środków ochrony, wykorzystywana jest metodyka oparta o kryteria oceny zabezpieczeń teleinformatyki wg zaleceń ITSEC.

Do marca 2001 roku BBŁiI UOP przeprowadziło badania i wydało certyfikaty bezpieczeństwa teleinformatycznego 25 produktom. Wart podkreślenia jest fakt, że większość z certyfikowanych produktów została opracowana w Polsce, a uzyskane certyfikaty poświadczają uzyskanie poziomu pewności E3 wg kryteriów ITSEC.

W roku 2000 BBŁiI UOP rozpoczęło prace zmierzające do przyjęcia międzynarodowych kryteriów *Common Criteria*, które uzyskały status normy *ISO/IEC*

15408. Efektem tych prac jest przetłumaczenie trzech części kryteriów i przekazanie roboczych wersji tych dokumentów do prac w Normalizacyjnej Komisji Problemowej nr 182 przy Polskim Komitecie Normalizacyjnym.

Akty prawne

O ważności problematyki ochrony informacji oraz bezpieczeństwa systemów informatycznych w naszym kraju, świadczą również regulacje prawne, określające organizację przetwarzania, przechowywania i przesyłania informacji stanowiących tajemnicę państwową, służbową lub przetwarzającą dane osobowe. Do regulacji tych zaliczamy:

- Ustawę z dnia 22.01.1999 roku „*O ochronie informacji niejawnych*" (Dz.U. z dn.08.02.1999 r.);
- Rozporządzenie Prezesa Rady Ministrów z dnia 25.02.1999 roku „*W sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych*" (Dz.U. z dn.05.03.1999 r.);
- Ustawę z dnia 29.08.1997 roku „*O ochronie danych osobowych*" (Dz.U. z dn.29.10.1997 r.);
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 03.06.1998 roku „*W sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych*" (Dz.U. z dn.30.06.1998 r.).

Zgodnie z definicją zawartą w Rozporządzeniu Prezesa Rady Ministrów z dn. 25.021999r. „*W sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych*", koncepcja bezpieczeństwa systemu teleinformatycznego wymaga zastosowania następujących rodzajów bezpieczeństwa: *(patrz rysunek 9.16).*



Rysunek 9.16. Bezpieczeństwo teleinformatyczne w świetle Rozporządzenia Prezesa Rady Ministrów z dn. 25.02.1999r.[25]

- *bezpieczeństwa fizycznego* – odpowiednia lokalizacja pomieszczeń, zabezpieczenia materialne (odpowiednie materiały budowlane na ściany i drzwi; kraty, zamki szyfrowe), zapewnienie odpowiedniej jakości źródeł zasilania, czytniki kart identyfikacyjnych, instalacje alarmowe (czujniki podczerwieni, ruchu, kamery, świetlne i dźwiękowe sygnalizatory włamań);
- *bezpieczeństwa kryptograficznego* – stosowanie szyfrowania i innych mechanizmów kryptograficznych gwarantujących integralność, uwierzytelnianie i zabezpieczenie przed ujawnieniem;
- *bezpieczeństwa elektromagnetycznego*- umieszczanie urządzeń w strefach gwarantujących bezpieczeństwo elektromagnetyczne; zastosowanie urządzeń o obniżonym poziomie emisji;

[25] *B.Kusina : Informacja – towar chroniony, Konferencja e-Komputer Expo, Warszawa 23-24.01.2001*

- *bezpieczeństwa transmisji* – określenie głównych i awaryjnych dróg transmisyjnych z zaznaczeniem kroków postępowania w przypadku awarii i metod odtworzenia utraconych połączeń;
- *bezpieczeństwa dostępu do urządzeń* – formalne przydzielanie uprawnień, kont, haseł oraz ograniczenie dostępu do wszystkich zasobów systemu teleinformatycznego.

Przestępstwa komputerowe w Kodeksie Karnym

Istotną rolę w zakresie ochrony i bezpieczeństwa systemów informatycznych oprócz omawianych już standardów i ustaw, odgrywają przepisy karnoprawne. Reguluje je Kodeks Karny Ustawą z dnia 06.06.1997 roku (Dz.U. nr 88, poz.553).

A oto niektóre z przepisów dotyczące przestępczości komputerowej regulowane przez Kodeks Karny:

Przestępstwa przeciwko ochronie informacji:

- Art.267 § 1 k.k. – hacking komputerowy:

kara grzywny, ograniczenie wolności albo jej pozbawienie do lat 2;

- Art.267 § 2 k.k. – podsłuch komputerowy (nieuprawnione przechwycenie informacji):

kara grzywny, ograniczenie wolności albo jej pozbawienie do lat 2;

- Art.268 § 2 k.k. – bezprawne niszczenie informacji:

kara pozbawienia wolności od 3 miesięcy do lat 5;

- Art.269 § 1 i 2 k.k. – sabotaż komputerowy:

kara pozbawienia wolności od 6 miesięcy do lat 8;

Przestępstwa z art.267 i 268 k.k. są ścigane na wniosek pokrzywdzonego.

Przestępstwa przeciwko mieniu:

- Art.278 § 2 k.k. – nielegalne uzyskanie programu komputerowego:

kara pozbawienia wolności od 3 miesięcy do lat 5, a przy mieniu znacznej wartości od 1 roku do lat 10;

- Art.293 § 1 k.k. – paserstwo programu komputerowego:

kara pozbawienia wolności od 3 miesięcy do lat 5;

- Art.287 § 1 k.k. – oszustwo komputerowe:

kara pozbawienia wolności od 3 miesięcy do lat 5;

- Art.287 § 1 k.k. – oszustwo telekomunikacyjne:

kara pozbawienia wolności do lat 3;

Przestępstwa przeciwko bezpieczeństwu powszechnemu:

- Art.165 § 1 ust. 4 k.k. – sprowadzenie niebezpieczeństwa dla życia lub zdrowia wielu osób albo mienia w znacznych rozmiarach:

kara pozbawienia wolności od 6 miesięcy do lat 8, przy skutkach śmiertelnych od 2 do lat 12;

- Art.165 § 2 k.k. – nieumyślne zakłócenie automatycznego przetwarzania informacji związane ze sprowadzeniem niebezpieczeństwa powszechnego:

kara pozbawienia wolności do lat 3, przy skutkach śmiertelnych od 6 miesięcy do lat 8;

Przestępstwa przeciwko Rzeczypospolitej Polskiej:

- Art.130 § 2 i 3 k.k. – szpiegostwo komputerowe albo wywiad komputerowy:

kara pozbawienia wolności powyżej lat 3 lub (§ 3)od 6 miesięcy do lat 8;

Przestępstwa przeciwko wiarygodności dokumentów:

- Art.270 § 1 k.k. – fałszerstwo komputerowe:

kara grzywny, kara ograniczenia wolności albo kara jej pozbawienia od 3 miesięcy do lat 5.

Prawo autorskie a ochrona programów komputerowych

Problematyka prawnej ochrony programów komputerowych zawarta jest w „*Ustawie o prawie autorskim i prawach pokrewnych*" z 04.02.1994 roku (Dziennik Ustaw nr 24, z dn. 23.02.1994 r.). Stwierdza się tam, że programy te podlegają ochronie takiej, jak utwory literackie. Ustawa przewiduje, przykładowo, następujące kary:

- za przywłaszczenie sobie autorstwa lub rozpowszechnianie dzieła bez podania nazwiska autora – do 2 lat pozbawienia wolności lub kara grzywny,

- za przywłaszczenie sobie autorstwa lub rozpowszechnianie dzieła dla uzyskania korzyści materialnych - do 3 lat pozbawienia wolności.

Uregulowania prawne niższej rangi

W wielu firmach, uwzględnia się wymogi dotyczące ochrony informacji na każdym szczeblu biorąc pod uwagę uregulowania dotyczące tajemnicy państwowej lub służbowej. Organy kierownicze wielu firm wydają dokumenty w formie zarządzeń lub uchwał poruszające zasady postępowania w zakresie bezpieczeństwa systemów informatycznych.

Na krajowym rynku pozytywnym przykładem może być TP S.A., która wydała m.in. następujące dokumenty:

- Zarządzenie nr 37 Prezesa Zarządu TP S.A. z dnia 28.10.1993 roku, wprowadzające wytyczne w sprawie ochrony tajemnicy państwowej i służbowej w systemie przetwarzania informacji przy wykorzystaniu komputerów,
- Uchwałę nr 158/95 z dnia 14.11.1995 roku, w sprawie przedsięwzięć organizacyjnych w zakresie bezpieczeństwa i ochrony informacji w systemach informatycznych TP S.A.

Obowiązuje ponadto *Zarządzenie nr 60/83 Ministra Spraw Wewnętrznych* z dnia 20.06.1998 roku, rozdział VII „Zabezpieczenia pomieszczeń" (dotyczy to sfery fizycznej zabezpieczeń systemów – m.in. informatycznych).

Podsumowanie

Rozwój technologiczny i wzrost zapotrzebowania na efektywne i przy tym bezpieczne produkty teleinformatyczne doprowadził do sytuacji, w której na rynku znajduje się wiele produktów, przez ich sprzedawców przedstawianych jako najlepszych, najszybszych i w 100% bezpiecznych.

Ta bogata oferta oraz duża złożoność technologiczna oferowanych produktów, wymagająca bardzo dużej wiedzy specjalistycznej do dokonania właściwego wyboru, doprowadziły do momentu, w którym niezbędne stało się opracowanie kryteriów oceny oferowanych produktów teleinformatycznych. Wytycznym dla tych kryteriów są standardy normalizacyjne i akty prawne.

Akty prawne i standardy powinny być dla producentów i użytkowników swoistą „biblią informatyczną" – szczególnie przy tworzeniu systemów, w których poufność, integralność informacji i niezawodność mają znaczenie specjalne.

Bibliografia:

1. Ahuja V.: Bezpieczeństwo w sieciach, Mikom, Warszawa 1997.
2. Biuletyn Wojskowego Instytutu Łączności, Zegrze 2001.
3. Czechowski R., Sienkiewicz P.: Przestępcze oblicza komputerów. PWN, Warszawa 1993.
4. Fischer B.: Przestępstwa komputerowe i ochrona informacji, Zakamycze 2000, Kraków 2000.
5. Gallagher Brian P.: Software acquisition. Risk management. Key Process Area (KPA) - A guidebook 1999.
6. Goban-Klas T., Sienkiewicz P.: Społeczeństwo informacyjne: Szanse, Zagrożenia, Wyzwania, Wyd. Postępu Telekomunikacyjnego, Kraków 1993.
7. Golat K., Golat R.: Prawo komputerowe (zagadnienia podstawowe), Wydawnictwo Prawnicze Sp. z O.O, Warszawa 1998.
8. Goliński M.: Gospodarka i informacja, Ze zbioru prac pod red. J. Lubacza: W drodze do społeczeństwa informacyjnego, Warszawa 1999.
9. Górski J.: Inżynieria oprogramowania w projekcie informatycznym, Mikom, Warszawa 1999.
10. Kifner T. : Polityka bezpieczeństwa i ochrony informacji, Helion, Gliwice 1999
11. Kośla R., Cendrowski J.: Rola kryteriów oceny zabezpieczeń teleinformatyki dla bezpieczeństwa teleinformatycznego polskiej administracji publicznej w XXI wieku - Materiały II Sympozjum.
12. Kusina B. : Informacja – towar chroniony, Konferencja e-Komputer Expo, Warszawa 23-24.01.2001.
13. Liderman K.: Bezpieczeństwo informacji w systemach informatycznych, Seria: Skrypty Wyższej Szkoły Informatyki Stosowanej i Zarządzania, Warszawa 2000.
14. Molski M.: Podstawy bezpieczeństwa systemów informatycznych, MSG-Media, Bydgoszcz 1998.

15. Polska norma PN-I-13335-1 - Wytyczne do zarządzania bezpieczeństwem systemów informatycznych. Pojęcia i modele bezpieczeństwa systemów informatycznych, cz. 1.
16. Rączkiewicz M.: Bezpieczeństwo sieci komputerowych, wyd. Fundacji Postępu Telekomunikacji.
17. Sadowski A.: Wybrane zagadnienia kryptologii i ochrony informacji, Helion, Gliwice 1999.
18. Sienkiewicz P.: Analiza systemowa, Bellona 2000.
19. Sienkiewicz P.: 5 Wykładów, Akademia Obrony Narodowej, Warszawa 2000.
20. Syta J.: Metodyki analizy ryzyka ze szczególnym uwzględnieniem bezpieczeństwa systemów informatycznych, Politechnika Warszawska, Wydział Inżynierii Produkcji 2001.
21. Stawowski M.: Ochrona informacji w sieciach komputerowych, ArsKom, Warszawa 1998.
22. Struś B: Analiza występujących i możliwych zagrożeń w systemach informatycznych. Koncepcje bezpieczeństwa informatycznego i stosowane rozwiązania, Praca studyjna, Akademia Obrony Narodowej – Centrum Informatyki, Warszawa 1995.
23. Materiały z Konferencji e-Komputer Expo: Informacja – towar chroniony, Warszawa 23-24.01.2001.
24. Materiały z II Sympozjum Bezpieczeństwa Systemów Informacyjnych, 22-23.05.2001.
25. Materiały z III Kongresu Administratorów Bezpieczeństwa Informacji, Zakopane 2000.
26. Materiały z IV Krajowej Konferencji Zastosowań Kryptografii, Warszawa 23-25.05.2000.
27. Materiały cz. I z VI Międzynarodowej Wojskowej Konferencji Telekomunikacji i Informatyki - Jabłonna 1997, wyd. Wojskowy Instytut Łączności.
28. Weierbach R.: „Vulnerability assessments", INFS 762, 2000.
29. Wiśniewski A.: Analiza ryzyka. Wytyczne dla administratorów systemów, AZW 2000.

Publikacje:

1. Computerworld - Raport: Bezpieczeństwo, Kwiecień 2001.
2. Computerworld – nr 46/1995.
3. Net World nr 7/2000 (61).
4. NetWorld, Czerwiec 1997.
5. Security Magazine, nr 1 (2) Październik 1999.
6. Przegląd Telekomunikacyjny, Nr 10/1998.
7. Vademecum Teleinformatyka Nr 1.
8. Vademecum Teleinformatyka Nr 2.

1.10. WNIOSKI

Przyjęty w badaniach wariant analizy systemowej obejmuje następujące problemy:

(1) model bezpieczeństwa informacyjnego systemu;

(2) analiza identyfikacyjna zagrożeń informacyjnych (źródła, symptomy, przyczyny, możliwe skutki);

(3) zarządzanie ryzykiem (ewaluacja ryzyka, kontrola i metody minimalizacji ryzyka);

(4) opracowanie scenariuszy możliwych i prawdopodobnych sytuacji zagrożeń dla bezpieczeństwa informacyjnego;

(5) generowanie dopuszczalnych strategii przeciwdziałania sytuacjom zagrożeń dla bezpieczeństwa informacyjnego.

Przyjęto, że powyższy wariant analizy systemowej odpowiada wymaganiom wynikającym z ogólnej sytuacji problemowej wynikającej z obecnego i przyszłego stanu realnych zjawisk w bliższym i dalszym otoczeniu systemowym państwa.

Analizując wpływ wydarzeń z 11 września na technikę informacyjną wybitny specjalista z zakresu IT – Edward Yourdon formułuje następujące *„przemiany paradygmatyczne"*[1]

- Systemy IT stanowią immanentną część (podsystemu) *„krytycznej infrastruktury"*.
- Źródłem zagrożeń są *„gracze"* należący do wielu kategorii (użytkownicy finalni, tzw. *„script kiddies"*, bezpaństwowi terroryści)/
- Bezpieczeństwo musi być obecnie uwzględniane zarówno podczas tworzenia, jak i eksploatowania systemów oprogramowania.
- Bezpieczeństwo zmieniło się w wyniku miniaturyzacji systemów komputerowych.
- Bezpieczeństwo uległo zmianie, ponieważ Internet jest obecnie używany jako pośrednia broń wspierająca terroryzm.

BIBLIOTEKA GŁÓWNA - ARCHIWUM
Nr ewid. 68716
Akademii Obrony Narodowej

[1] *E. Yourdon, Wojna na bity. WNT, Warszawa 2004.*