16

AKADEMIA OBRONY NARODOWEJ

Kpt. mgr inż. Adam ŻACH

SYMULACJE KOMPUTEROWE W MODELOWANIU BEZPIECZEŃSTWA INFORMACYJNEGO W SIŁACH ZBROJNYCH

Rozprawa doktorska

WARSZAWA

AKADEMIA OBRONY NARODOWEJ
WYDZIAŁ WOJSK LĄDOWYCH

Kpt. mgr inż. Adam ŻACH

SYMULACJE KOMPUTEROWE W MODELOWANIU BEZPIECZEŃSTWA INFORMACYJNEGO W SIŁACH ZBROJNYCH

Rozprawa doktorska

Opracowana
pod kierownictwem naukowym

płk. dr. hab. Henryka SPUSTKA

WARSZAWA **2008**

Spis treści

WPROWADZENIE

Problematyka ochrony informacji niejawnych jest bardzo rozległa oraz niezwykle trudna pod względem poznawczym. Dlatego też w niniejszej dysertacji przedmiot badań został ograniczonych wyłącznie do ochrony informacji niejawnych w obszarze Sił Zbrojnych RP. Potrzeba ochrony informacji niejawnych, a w tym przewidywanie możliwych zagrożeń, jest problemem, który został dostrzeżony i podjęty zarówno w obszarze cywilnym jak i wojskowym. Nie jest możliwe dokonanie wyraźnego podziału pomiędzy zagrożeniami tylko w cywilnych lub tylko w wojskowych systemach informacyjnych. Przedstawiony w dysertacji model zagrożeń informacyjnych Sił Zbrojnych RP może być podwaliną do dalszych badań, szczególnie w kierunku jego wykorzystania w symulacjach z wykorzystaniem narzędzi i aplikacji komputerowych.

Dysertacja składa się z wprowadzenia, czterech rozdziałów oraz zakończenia, bibliografii i załączników.

Wprowadzenie obejmuje metodologiczne podstawy przeprowadzonych badań. Przedstawiono w nim tok procedury badawczej: od koncepcji do sformułowanego problemu badawczego, treść problemu i cel badań, hipotezy robocze, założenia i ograniczenia badawcze oraz procedurę weryfikacji hipotez wraz z metodami, technikami i narzędziami badawczymi.

Rozdział pierwszy zawiera metodologiczne podstawy modelowania i symulacji. Główny nacisk został położony na teoretyczne podstawy tworzenia modeli matematycznych i symulacji komputerowych.

Rozdział drugi prezentuje analizę możliwych zagrożeń dla bezpieczeństwa informacyjnego Sił Zbrojnych RP.

W **rozdziale trzecim** scharakteryzowano zasadnicze sposoby zapewnienia bezpieczeństwa informacyjnego w Siłach Zbrojnych RP. Rozdział zawiera aktualne prawne, techniczne oraz organizacyjne rozwiązania stosowane w tym zakresie w Siłach Zbrojnych RP.

W **rozdziale czwartym** zawarto zbudowany model bezpieczeństwa informacyjnego Sił Zbrojnych RP oraz podjęto próbę określenia możliwości jego wykorzystania w symulacjach komputerowych.

Podstawy badawcze rozprawy

W warunkach postępującej globalizacji informacyjnej, w świecie gdzie informacja jest podstawą biznesu i rozwoju gospodarki, konieczna staje się znajomość zagrożeń mogących wpłynąć na integralność informacji. Jesteśmy społeczeństwem uzależnionym od informacji. Nowoczesne techniki przekazu umożliwiają nam łatwe jej przenoszenie na praktycznie dowolną odległość. Działalność niemal każdej instytucji związana jest z przetwarzaniem informacji. Realnym staje się zagrożenie działań destrukcyjnych oraz zakłócających działanie instytucji, zarówno cywilnych jak i wojskowych, polegające na próbach ingerencji w przepływ i przetwarzanie informacji.

Coraz powszechniejsze zastosowanie w wojskowych systemach łączności urządzeń opartych na najnowszych rozwiązaniach technicznych powoduje, że stają się one również celem takiego ataku. W nowoczesnych siłach zbrojnych wykonanie precyzyjnych uderzeń ogniowych oparto całkowicie na skomputeryzowanym uzbrojeniu, a poczta elektroniczna weszła na stałe do wojskowych systemów łączności.

Wykorzystując ogólnodostępne sieci połączeń internetowych możliwe jest koordynowanie akcji terrorystycznych prowadzonych w różnych częściach świata. Internet stwarza możliwości komunikowania pomiędzy członkami i grupami terrorystycznymi znajdującymi się w różnych państwach, czy kontynentach oraz ich szkolenie bez konieczności bezpośrednich spotkań.

Ataki informacyjne mogą, i zapewne będą, połączone z innymi atakami, najczęściej o charakterze terrorystycznym. Uderzenia te mogą być skierowane w żywotnie ważne systemy, takie jak obsługa ruchu lotniczego czy dystrybucji energii elektrycznej.

Biorąc pod uwagę rosnącą skalę zjawiska i coraz poważniejsze jego skutki, brak podjęcia dobrze zaplanowanego, usystematyzowanego procesu jego zwalczania może mieć bardzo poważne konsekwencje. W Polsce już dzisiaj istnieje wiele systemów informatycznych (PESEL – NET, ZUS, systemy bankowe), których zakłócenie zawsze odbije się negatywnie na funkcjonowaniu państwa oraz poczuciu bezpieczeństwa jego obywateli. Jeszcze poważniejsze są potencjalne zagrożenia dla systemów działających w sektorze energetycznym, gazociągowym czy w służbach ratunkowych.

Do zasadniczych zagrożeń informacyjnych mogących oddziaływać również na działania sił zbrojnych możemy zaliczyć:

- zrywanie procedur wymiany informacji,
- manipulowanie informacją (dezinformacja, zatajanie, zniekształcanie),
- nieautoryzowane korzystanie z zasobów informacyjnych (baz danych) oraz kopiowanie i niszczenie zgromadzonych danych,
- masowe niszczenie oprogramowania systemowego[1].

Kompleksowe zastosowanie takich form ataku może doprowadzić do skutecznego zablokowania systemów kierujących użyciem broni, zarówno masowego rażenia, jak i konwencjonalnej. Dlatego też nie możemy mówić o bezpiecznym państwie w przypadku, gdy zagrożony będzie system informacyjny sił zbrojnych.

W fazie pokoju najwrażliwsze na oddziaływanie są stacjonarne elementy łączności i informatyki. Istnieją możliwości „paraliżu" wojskowych systemów informacyjnych poprzez celowe niszczenie czy uszkodzenie central oraz (w większości dzierżawionych od operatorów cywilnych) linii transmisyjnych.

Przy rozpatrywaniu możliwości przeciwdziałania zagrożeniom informacyjnym w siłach zbrojnych RP istotna jest identyfikacja zagrożeń. Należy odpowiedzieć na pytanie: ***W jaki sposób mogą być przeprowadzone ataki na infrastrukturę oraz zasoby informacyjne sił zbrojnych oraz które z tych ataków mogą być najgroźniejsze?***

Złożoność problematyki zagrożeń, ich mnogość oraz różny poziom niesionego niebezpieczeństwa nie pozwala odpowiedzieć w prosty sposób na tak postawione pytanie. W związku z tym konieczne staje się odnalezienie metod nakreślenia scenariuszy ewentualnych ataków, bądź przeprowadzenie ich symulacji.

Wynikiem podjętych prac w ramach dysertacji doktorskiej jest model zagrożeń informacyjnych w Siłach Zbrojnych RP oraz jego wykorzystania w eksperymentach symulacyjnych przeprowadzonych przy użyciu techniki komputerowej.

---

[1] P. Gawliczek, J. Pawłowski, *Zagrożenia asymetryczne*, Akademia Obrony Narodowej, Warszawa 2003.

Modelowanie bezpieczeństwa informacyjnego – bieżący stan badań

Potrzeba symulacji zagrożeń związanych z atakami informacyjnymi została zauważona już przed wieloma laty, przez instytucje zajmujące się bezpieczeństwem. Pierwsze prace nad analizą zagrożeń związanych z atakami z cyberprzestrzeni przeprowadzono w roku 1996 przez naukowców skupionych wokół RAND Corporation. Przeprowadzono wówczas symulację, której nadano nazwę „The Day After ... in Cyberspace" [2]. Jej scenariusz obejmował symulację zdarzeń mogących wystąpić w obszarze zagrożeń informacyjnych i w większości mających już w przeszłości swoje miejsce.

Scenariusz gry obejmował ataki informacyjne na takie obiekty jak systemy transportowe, systemy telekomunikacyjne, źródła zasilania, systemy finansowe, siły zbrojne oraz systemy polityczne. W jej trakcie, przeprowadzone w cyberprzestrzeni ataki doprowadziły do katastrof w ruchu lotniczym i kolejowym, zakłóceń pracy operatorów telekomunikacyjnych (w tym sieci komórkowych), zniszczenia rafinerii w Arabii Saudyjskiej, paraliżu światowego rynku finansowego, zakłóceń w działaniu wojskowych systemów telekomunikacyjnych, co w efekcie doprowadziło do demonstracji oraz zamieszek na tle politycznym.

Zdarzenia w trakcie gry były symulowane z wykorzystaniem ataków poprzez zastosowanie[3]:

a) bomb logicznych:
   - przerwa w zasilaniu w energię elektryczną w Kairze (przerwa w zasilaniu przez kilka godzin około 90% odbiorców),
   - wybuch w rafinerii ARAMCO w Arabii Saudyjskiej poprzez doprowadzenia do awarii systemu kierowania i sterowania,
   - katastrofa szybkiego pociągu pasażerskiego jadącego po torze, na którym znajdował się skład towarowy,
   - zablokowanie bankomatów w dwóch największych sieciach bankowych w Georgii,

---

[2] Opis symulacji można odlaneźć w: R. C. Molander, A. S. Riddile, S. A. Wilson *Strategic Information Warfare: A New Face of War*, Santa Monica 1996. http://rand.org/pubs/monograph_reports/2007/MR797.pdf.

[3] Na podstawie: *Modelowanie zagrożeń dla bezpieczeństwa informacyjnego państwa: teoria walki informacyjnej: projekt badawczy 0500A 01923/oprac. zespół aut.: Tadeusz Jemioło [i in.]; Akademia Obrony Narodowej.*

- zainfekowanie pokładowego oprogramowania samolotów pasażerskich, co doprowadziło do katastrofy, w której zginęło 30 osób a 100 zostało rannych,
- uszkodzenie Publicznej Sieci Telekomunikacyjnej w Arabii Saudyjskiej,
- awaria całej sieci telefonicznej, włączając telefonię komórkową, w regionie Waszyngton/Baltimore,
- elektroniczna ingerencja w działanie Giełdy Papierów Wartościowych w Chicago.

b) spoofing[4]:
- przejęcie na 7 minut transmisji wiadomości nadawanych przez stacje CBS celem wezwania do obywatelskiego nieposłuszeństwa oraz wystąpienia przeciwko rządzącym.

c) przeciążenie informacyjne:
- zablokowanie systemu łączności telefonicznej wojskowej bazy w Waszyngtonie poprzez zmasowane wybieranie numerów telefonicznych z wykorzystaniem komputerów.

d) detektory[5]:
- wykrycie w Banku Anglii urządzeń wykrywających (detektorów) służących najprawdopodobniej do nieautoryzowanego włączenia się w system transakcyjny banku.

e) wirusy komputerowe:
- zmiany w danych dotyczących dyslokacji jednostek wojskowych Sił Zbrojnych USA.

f) robaki komputerowe:
- zakłócenia w pracy systemu stacji radiolokacyjnych działających rejonie Zatoki Perskiej i odpowiedzialnych za obserwację przestrzeni powietrznej oraz obserwację atakowanego celu.

---

[4] **Spoofing** – to termin określający fałszowanie źródłowego adresu IP w wysyłanym przez komputer pakiecie sieciowym. Takie działanie może służyć ukryciu tożsamości atakującego (np. w przypadku ataków DoS), podszyciu się pod innego użytkownika sieci i ingerowanie w jego aktywność sieciową, lub wykorzystaniu uprawnień posiadanych przez inny adres.

[5] **Detektory** – programy zaprojektowane do analizy sieci łączności. Wykorzystywane przez administratorów do nadzoru nad siecią i detekcji uszkodzeń i problemów. Mogą być również wykorzystywane do wykrywania zbiorów danych niejawnych np. haseł, podsłuchu transmisji oraz wprowadzania celowych błędów i uszkodzeń.

g) spamming:
   - przejęcie głównej rządowej sieci informacyjnej w Arabii Saudyjskiej. Spreparowane informacje doprowadziły do demonstracji przeciwko panującej w tym kraju monarchii.

h) próby wielokanałowe:
   - skomasowany atak informacyjny z nieznanego źródła prowadzony przeciwko prawie wszystkim bazom wojskowym w USA i Europie, a zaangażowanym militarnie w Arabii Saudyjskiej.

Przeprowadzona gra pokazała, że wysocy urzędnicy państwowi są nieprzygotowani do właściwej oceny zagrożeń generowanych w jej trakcie. Nie potrafili oni podjąć jednoznacznej i właściwej decyzji mogącej być reakcją na bieżącą sytuację. Dodatkowo gra pokazała słabe punkty amerykańskiej infrastruktury informacyjnej.

Kolejną symulację przeprowadził Komitet Połączonych Sztabów armii amerykańskiej w roku 1997. W ramach gry wojennej pod kryptonimem „Eligible Receiver" ponownie udowodniono, że możliwe jest poprzez walkę informacyjną oraz cyberataki, wyłączenie systemów zasilania miast, wstrzymanie pracy rafinerii ropy naftowej czy przejęcie kontroli nad systemami lotów[6].

Problematyka modelowania i symulacji zagrożeń informacyjnych została zauważona także w Polsce. Pracownicy naukowi Akademii Obrony Narodowej pod kierownictwem prof. Tadeusza Jemioło zrealizowali w latach 2003 - 2004 projekt badawczy pod tytułem „Modelowanie zagrożeń dla bezpieczeństwa informacyjnego państwa". Jego efektem jest 3 tomowe opracowanie obejmujące problematykę identyfikacji i analizy zagrożeń[7], modelowania walki informacyjnej[8] oraz wspomagania wyboru strategii przeciwdziałania zagrożeniom informacyjnym[9].

Wynikiem podjętych prac w omawianym opracowaniu stał się ekspertowy system wspomagania strategii przeciwdziałania zagrożeniom informacyjnym opracowany z wykorzystaniem pakietu sztucznej inteligencji Sphinx. Po przeprowadzonych przez autorów testach stwierdzono, że system ten spełnia wymagania stawiane

---

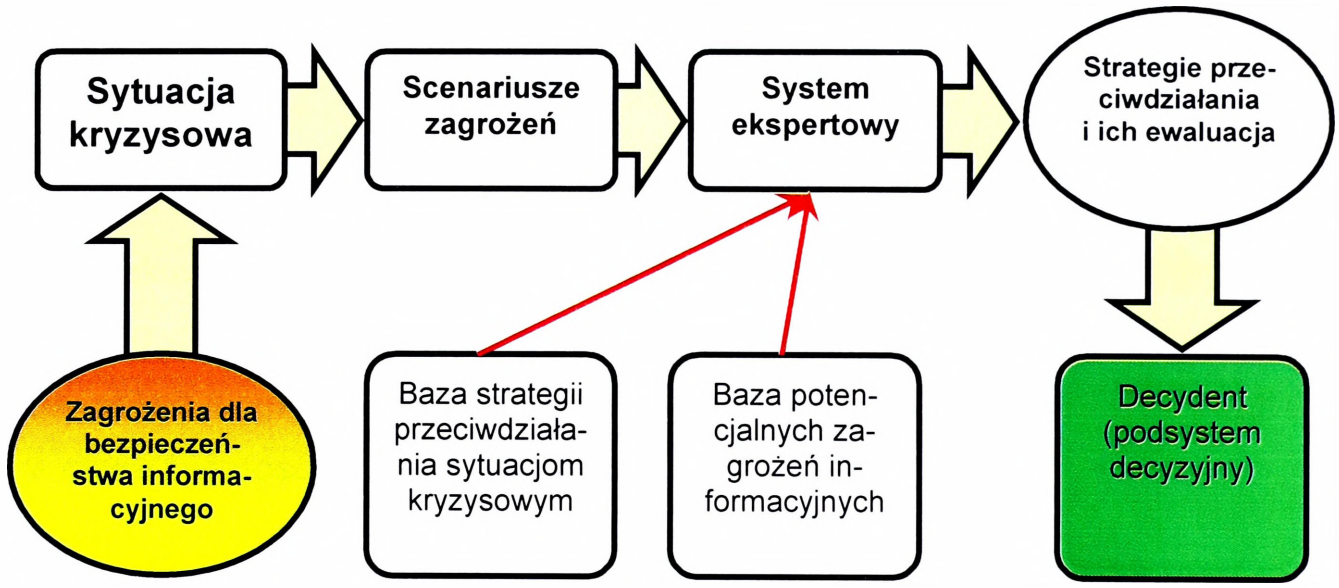
[6] B. Gert, *Hacker Can Shut Down the Power Grid, Military Admits*, Washington Times 16.04.1998 r.

[7] Praca naukowo badawcza wykonana pod kierownictwem T. Jemioło, *Modelowanie zagrożeń dla bezpieczeństwa informacyjnego państwa: teoria walki informacyjnej*: projekt badawczy 0500A 01923, T.1. Zagrożenia dla bezpieczeństwa informacyjnego państwa: (identyfikacja, analiza zagrożeń i ryzyka) Warszawa Akademia Obrony Narodowej 2004.

[8] Tamże, T. 2. *Modelowanie walki informacyjnej: (podstawy, scenariusze, modele).*

[9] Tamże, T. 3. *Wspomaganie wyboru strategii przeciwdziałania zagrożeniom informacyjnym: (koncepcja systemu ekspertowego): raport z badań.*

przed tego rodzaju narzędziem gdyż pozwala na pozyskiwanie wiedzy, jej gromadzenie, przetwarzanie oraz wizualizację. Do zasadniczych jego zalet zaliczono możliwość łatwego przygotowania raportów i analiz, łatwy i czytelny opis wspomaganego zagadnienia, możliwość monitorowania sytuacji wraz z wariantami jej rozwiązania, możliwość wprowadzania sugestii analityka do możliwych scenariuszy, możliwość definiowania własnych kryteriów oceny zdarzeń oraz przyjazny użytkownikowi interfejs w języku polskim.



Rys.1. System ekspertowy w procesie decyzyjnym w zakresie bezpieczeństwa informacyjnego.

Źródło: Praca naukowo-badawcza wykonana pod kierownictwem T. Jemioło, Modelowanie zagrożeń dla bezpieczeństwa informacyjnego państwa: teoria walki informacyjnej: projekt badawczy 0500A 01923, T. 3. Wspomaganie wyboru strategii przeciwdziałania zagrożeniom informacyjnym: (koncepcja systemu ekspertowego): Warszawa Akademia Obrony Narodowej, Warszawa 2004.

Zgodnie z przedstawionym powyżej schematem, newralgicznymi dla właściwego przeciwdziałania zagrożeniom informacyjnym elementami w procesie decyzyjnym są jak najpełniejsze bazy informacji dotyczących zagrożeń i scenariuszy ich występowania oraz strategii przeciwdziałania zagrożeniom. Jednym z elementów tych baz mogą być również modele zagrożeń oraz przeprowadzone na ich bazie symulacje potencjalnych sytuacji kryzysowych.

Stąd w procesie budowania opisanego powyżej systemu ekspertowego, autorzy przedstawili szereg modeli mogących być podstawą do badań nad bezpieczeństwem informacyjnym. Wśród nich znalazły się modele zagrożenia, bezpieczeństwa, ryzyka i zabezpieczenia jak również model walki oraz walki cybernetycznej.

Modelem najbardziej związanym z treścią niniejszej dysertacji jest model zabezpieczenia. Zakłada on, że w chwili $t = 0$ wartość systemu wynosi $v_0 > 0$ i równa się sumie wartości poszczególnych elementów (podsystemów), czyli:

$$v_0 = \sum_{j=1}^{M} v_{jo} \tag{1}$$

Znany jest, zatem rozkład wartości o strukturze systemu S:

$$\langle u_{10}, u_{20}, u_{jo,}, \ldots, u_{jm} \rangle \tag{2}$$

gdzie:

$$u_{jo} = \frac{v_{jo}}{v_0} \tag{3}$$

Otoczenie generuje zagrożenia skierowane na system $Z \rightarrow S$, przy czym wartość oczekiwana strat w obiekcie $S_j \in S$ w wyniku wystąpienia zagrożenia $Z_i \in Z$ wynosi W_{ij}, $0 \leq W_{ij} \leq v_{ij}$. Jeżeli założymy, że od chwili t nastąpiło N zagrożeń oraz, że na każdy obiekt mogą byś skierowane wszystkie możliwe i prawdopodobne zagrożenia, to w chwili t wartość obiektu S_j wyniesie:

$$v_{jt} = v_{j0} - \sum_{i=1}^{N} W_{ij} \geq 0\,, \tag{4}$$

zaś wartość systemu po zmasowanym zagrożeniu wyniesie

$$v_t = \sum_{j=1}^{M} v_{jt} = \sum_{j=1}^{M} \left(v_{j0} - \sum_{i=1}^{N} W_{ij} \right), \tag{5}$$

przy czym straty systemu wyniosą: $v_0 - v_t \geq 0.$

Niech decyzję otoczenia – określa zmienna:

x_{ij}= 1, jeśli zagrożenie Z_i skierowane zostało na obiekt S_j,

x_{ij}= 0, w przeciwnym przypadku.

Czyli określa przedział poszczególnych zagrożeń do poszczególnych obiektów, przy czym spełnione muszą być warunki:

$$\sum_{j=1}^{M} x_{ij} = 1, i = 1, \ldots, N \tag{6}$$

$$\sum_{j=1}^{N} x_{ij} = 1, i = 1, \ldots, M \tag{7}$$

$$\sum_{j=1}^{N} \sum_{j=1}^{M} x_{ij} \leq M \leq N\,. \tag{8}$$

Wówczas funkcja wartości dla systemu w chwili *t* ma postać:

$$v_t(x) = \sum_{j=1}^{M} \left(v_{jo} - \sum_{j=1}^{N} W_{ij} X_{ij} \right). \qquad (9)$$

Kolejnym opracowaniem zajmującym się problematyką bezpieczeństwa informacyjnego w aspekcie jego modelowania i prognozowania jest opracowanie poświęcone wynikom badań zrealizowanych w Akademii Obrony Narodowej[10]. Jej głównym celem było opracowanie modelu „Cyberwar" pozwalającego modelować procesy walki informacyjnej. Zasadniczym elementem tej pracy były przeprowadzone w ramach Podyplomowych Studiów Bezpieczeństwa Informacyjnego gry symulacyjne oparte na scenariuszu „Cyberwar". Wnioski z przeprowadzonych gier z udziałem słuchaczy specjalistycznych studiów podyplomowych, są przekonywującym uzasadnieniem potrzeby prowadzenie badań w tym kierunku. Autorzy widzą potrzebę prowadzenia tego typu gier rozgrywanych z różną intensywnością, skalą i rodzajami zagrożeń ze względu na:

a) różnice w postrzeganiu poszczególnych zagrożeń nawet przy dużej i zbliżonej do siebie wiedzy teoretycznej z tej dziedziny przez biorących udział w grze uczestników,
b) możliwość konfrontacji poglądów oraz poznania innego niż własne postrzeganie tego samego problemu,
c) zmniejszanie się roli wszelkich form kontroli nad przepływem informacji, techniki, uzbrojenia i środków finansowych,
d) wzrost znaczenia niepaństwowych podmiotów życia społeczno - gospodarczego,
e) wzrost problemów na tle religijnym i przestępczości zorganizowanej,
f) wzrost zagrożeń ze strony ugrupowań terrorystycznych o niekonwencjonalnych metodach działania.

[10] Praca naukowo-badawcza wykonana pod kierownictwem Marka Kinasiewicza, *Modelowanie procesów walki informacyjnej: model "Cyberwar"*, Akademia Obrony Narodowej, Centrum Symulacji i Komputerowych Gier Wojennych, Warszawa 2006.

Założenia metodologiczne rozprawy

Głównym zadaniem badawczym niniejszej dysertacji było wykonanie modelu bezpieczeństwa informacyjnego Sił Zbrojnych RP oraz wskazanie na możliwości jego wykorzystania do przeprowadzenia symulacji komputerowych w tym zakresie.

Czynności procedury badawczej przeprowadzono wykorzystując właściwe dla ich realizacji metody, techniki i narzędzia badawcze w trzech głównych etapach: konceptualizacji, realizacji badań właściwych i ich finalizacji[11].

Literaturę przedmiotu badań podzielono na cztery grupy. Pierwsza obejmowała literaturę dającą metodologiczne podstawy podjęcia określonego problemu badawczego. Pozwoliła ona na zebranie wiedzy na temat metod, technik i narzędzi badawczych oraz etapów prowadzenia badań. Druga grupa obejmowała zbiór opracowań oraz publikacji zajmujących się opisem oraz charakteryzowaniem zagrożeń informacyjnych, zarówno w szerokim (ogólnym) jak i węższym (uwzględniającym specyfikę Sił Zbrojnych RP) aspekcie. Trzecia to dział obejmujący obowiązujące i dostępne akty prawne, unormowania instrukcyjne oraz opracowania i publikacje będące podstawą wiedzy na temat bezpieczeństwa informacyjnego w Siłach Zbrojnych RP. Ostatnia, czwarta grupa to literatura dotycząca modelowania i symulacji komputerowych.

Zakres zebranej literatury oraz jej podział i uporządkowanie współgra z podjętą w dysertacji problematyką badawczą.

Cel badań został zdefiniowany jako: ***Zastosowanie metod symulacji komputerowych w modelowaniu bezpieczeństwa informacyjnego w siłach zbrojnych***.

Stosownie do przyjętego celu badań, problem badawczy sprowadza się do odpowiedzi na pytanie: ***W jaki sposób można wykorzystać metody symulacji komputerowych w modelowaniu bezpieczeństwa informacyjnego w siłach zbrojnych?***

---

[11] M. Cieślarczyk, *Metody, techniki i narzędzia badawcze oraz elementy statystyki stosowane w pracach magisterskich i doktorskich,* Akademia Obrony Narodowej, Warszawa 2006, s. 22.

Aby rozwiązać powyższy problem badawczy należy odpowiedzieć na następujące pytania (problemy) szczegółowe:

1) ***Jakie są rodzaje zagrożeń bezpieczeństwa informacyjnego w siłach zbrojnych? Jakie zagrożenia są najbardziej prawdopodobne, a jakie najbardziej niebezpieczne?***
2) ***Jakimi metodami oraz przy zaangażowaniu jakich środków realizowane jest obecnie zapewnienie bezpieczeństwa informacyjnego w siłach zbrojnych?***
3) ***W jaki sposób prognozować zagrożenia oraz skutki ich wystąpienia?***
4) ***W jaki sposób można wykorzystać metody symulacji komputerowych do procesu prognozowania zagrożeń informacyjnych w siłach zbrojnych?***

Analiza literatury, a w tym wyników przeprowadzonych badań, pozwoliła na sformułowanie przyjętych do dalszych rozważań hipotez[12].

Hipoteza pierwsza. Złożoność problematyki zagrożeń informacyjnych, ciągłe ewoluowanie zagrożeń już rozpoznanych, oraz pojawianie się nowych zagrożeń, stawia przed organizacjami oraz ludźmi zajmującymi się bezpieczeństwem informacyjnym nowe wyzwania. Skuteczne zabezpieczenie informacji może mieć miejsce tylko wówczas, gdy będą określone w miarę jak najdokładniej zagrożenia i obszar ich występowania.

Nie jest możliwe zorganizowanie skutecznego systemu ochrony przed zagrożeniami informacyjnymi bez właściwej ich identyfikacji i skutków wystąpienia.

Hipoteza druga. Jakościowa zmiana zagrożeń informacyjnych, obszaru ich występowania oraz możliwych konsekwencji implikuje konieczność poszukiwania nowych, skuteczniejszych metod ich przewidywania, identyfikacji i skutecznego przed nimi zabezpieczania. Technologiczne zmiany narzędzi do wykonywania, przechowywania i przesyłania informacji powinny iść w parze ze zmianami w narzędziach do zapewnienia wszystkim tym czynnościom należytego poziomu bezpieczeństwa. Poszukiwanie w tym zakresie metod opartych na wyspecjalizowanych narzędziach oraz aplikacjach komputerowych może pozwolić osiągnąć ten stan.

---

[12] T. Majewski, *Miejsce celów, problemów i hipotez w procesie badań naukowych*, Akademia Obrony Narodowej, Warszawa 2006.

Metody symulacyjne, w tym metody symulacji komputerowych, pozwalają prognozować skutki wystąpienia zagrożeń informacyjnych.

Hipoteza trzecia. Symulacje, przeprowadzane na modelach będących uproszczeniem rzeczywistości, pomagają poznać i ją zrozumieć. Dane zebrane w toku przeprowadzania eksperymentów symulacyjnych, wraz z ich konfrontacją z danymi rzeczywistymi zebranymi z badanego systemu, mogą stanowić podstawę do określania możliwych scenariuszy przyszłości. W przypadku zagrożeń informacyjnych jest to niezwykle istotna właściwość i zaleta metod symulacji, gdyż jednym z najważniejszych zadań systemu ochrony informacji jest zabezpieczenie przed utratą informacji. Prognozowanie zagrożeń pozwala na zastosowanie odpowiedniej profilaktyki i działań wyprzedzających.

Wykorzystanie metod symulacji komputerowych do identyfikacji zagrożeń informacyjnych sił zbrojnych pozwoli na uzyskanie prognoz krótkoterminowych w tym zakresie.

Hipoteza czwarta. Konieczność prognozowania zagrożeń informacyjnych poprzez prowadzenie w tym zakresie symulacji wymusza konieczność opracowania modelu bezpieczeństwa informacyjnego. Właściwie opracowany model, uwzględniający wszystkie, albo prawie wszystkie, najważniejsze składowe procesu zabezpieczenia informacji, może stać się uniwersalnym narzędziem możliwym do wykorzystania zarówno w siłach zbrojnych jak i poza nimi.

Model bezpieczeństwa informacyjnego w siłach zbrojnych umożliwi dobór właściwych metod i środków ochrony przed zagrożeniami informacyjnymi poprzez wykonanie na jego bazie eksperymentów symulacyjnych.

Procedura badawcza

Szeroki obszar tematyczny badań zmusił autora rozprawy do zastosowania ograniczeń sprowadzających się do rozpatrzenia następujących obszarów:

- zagrożenia informacyjne Sił Zbrojnych RP,
- teoretyczne podstawy modelowania i symulacji komputerowych,
- zastosowanie symulacji komputerowych do modelowania zagrożeń informacyjnych w Siłach Zbrojnych RP.

Procedura badawcza, jak już wcześniej wspomniano, obejmowała trzy zasadnicze etapy: konceptualizację, badania właściwe oraz ich finalizację.

W etapie pierwszym – konceptualizacji, określono problem badawczy, cel i przedmiot badań, teren badań, sprecyzowano hipotezy robocze, metody i techniki badawcze oraz opracowano koncepcję dysertacji. Głównym zadaniem tego etapu było zebranie wiedzy teoretycznej na temat zagrożeń informacyjnych, sposobów zapewnienia bezpieczeństwa informacyjnego w Siłach Zbrojnych RP oraz teorii modelowania i symulacji komputerowych. Cel ten realizowano teoretycznymi metodami ogólnonaukowymi, takimi jak analiza i synteza[13] zabranej literatury, abstrahowanie[14] oraz uogólnianie[15].

Analiza jest oparta na zdolności umysłu ludzkiego do myślowego rozdzielenia na części: rzeczy, zjawisk, zdarzeń i złożonych procesów w celu lepszego poznania[16]. Spośród znanych rodzajów analizy, jako złożonej metody badawczej, kolejne etapy badań determinowały konieczność wykorzystania analizy elementarnej[17], analizy strukturalnej[18] oraz analizy pojęciowej[19]. Wszystkie wyszczególnione metody w etapie pierwszym stosowane były również w etapach kolejnych.

W etapie drugim – badań właściwych, dokonano wyboru terenu badań, sposobu ich przeprowadzenia i przeprowadzono badania. W celu zebrania danych empirycznych niezbędnych do opracowania modelu bezpieczeństwa informacyjnego Sił Zbrojnych RP, spośród znanych metod empirycznych, zastosowano metodę[20] ankie-

---

[13] **Synteza** – jest oparta na zdolności ludzkiego umysłu do myślowego łączenia w całość według określonej zasady rzeczy, zjawisk, zdarzeń itp. uprzednio rozdzielonych, podejmowana w celu lepszego ich poznania.

[14] **Abstrahowanie** – czynność myślowa polegająca na wyodrębnieniu określonych elementów przedmiotu badań, uznanych z pewnych względów za nieistotne czy drugorzędne oraz na uwzględnieniu w tych rozważaniach innych elementów, które są istotne.

[15] **Uogólnianie** – operacja myśowa przechodzenia od twierdzeń o pojedynczym zjawisku do twierdzeń bardziej ogólnych, dotyczących grupy lub klasy zjawisk, a następnie bardziej ogólnych.

[16] M. Cieślarczyk, *Metody, techniki i narzędzia badawcze oraz elementy statystyki stosowane w pracach magisterskich i doktorskich,* Akademia Obrony Narodowej, Warszawa 2006, s. 46.

[17] **Analiza elementarna –** polega na podzieleniu (rozkładaniu) badanego zjawiska (przedmiotu badań) na części bez dopatrywania się między nimi jakichkolwiek stosunków i powiązań. W niniejszej dysertacji analizie elementarnej poddano zagrożenia bezpieczeństwa informacyjnego oraz elementy składowe bezpieczeństwa.

[18] **Analiza strukturalna** – zmierza do zbadania składu i struktury obiektów (zjawisk, procesów).

[19] **Analiza pojęciowa** – zmierza do zdobycia jasności w rozumieniu terminów (pojęć).

[20] **Metoda** – zespół zabiegów koncepcyjnych i instrumentalnych obejmujących najogólniej całość postępowania badacza, zmierzające do rozwiązania określonego problemu naukowego.

tową. Wykorzystaną techniką[21] była technika ankiety indywidualnej z wykorzystaniem przygotowanego narzędzia[22], jakim był kwestionariusz ankiety[23].

Przeprowadzone badania pozwoliły na poznanie opinii ankietowanych ekspertów na temat prawdopodobieństwa wystąpienia wyszczególnionych w ankiecie zagrożeń dla bezpieczeństwa informacyjnego Sił Zbrojnych RP. Wyniki badań uzyskane tą drogą wzbogaciły wiedzę z zakresu rozpatrywanych zagadnień i stanowiły podstawę do opracowania modelu bezpieczeństwa informacyjnego Sił Zbrojnych RP oraz założeń do eksperymentu symulacyjnego. Badania przeprowadzono wśród specjalistów pracujących na szczeblu centralnym Sił Zbrojnych RP, a także szczeblu Sił Powietrznych i związków taktycznych wchodzących w skład Sił Powietrznych.

W następnej kolejności opracowano, w oparciu o techniki modelowania, model bezpieczeństwa informacyjnego Sił Zbrojnych RP oraz przeprowadzono eksperyment symulacyjny z wykorzystaniem techniki komputerowej.

Etap trzeci – finalizacja badań, objął takie czynności jak zebranie danych oraz przygotowanie ich do analizy i obliczeń statystycznych, analiza danych empirycznych a w tym wnioskowanie i weryfikacja hipotez roboczych oraz opracowanie dysertacji.

Przeprowadzenie opisanego powyżej procesu badawczego napotykało na wszystkich swoich etapach na utrudnienia związane głównie ze specyfiką obszaru badań. Specyfika Sił Zbrojnych RP oraz charakter opracowywanych, przetwarzanych oraz przesyłanych informacji wymusza często nadawanie im klauzul niejawności. Dotyczy to również dokumentacji organizacji systemów ochrony, organizacji obiegu informacji niejawnych, a także analiz potencjalnych zagrożeń. Z tego powodu nie powiodły się próby przeprowadzenia badań ankietowych w instytucjach kierunkowo delegowanych do zapewnienia bezpieczeństwa informacyjnego w Siłach Zbrojnych RP takich jak Służba Kontrwywiadu Wojskowego oraz Agencji Wywiadu. Szefowie tych instytucji, zasłaniając się niejawnym charakterem prowadzonych prac odmówili udziału w badaniach.

---

[21] **Technika** – sposób zbierania danych, jeden z możliwych sposobów realizacji danej metody.

[22] **Narzędzia badawcze** – wszelkie materialne środki pomocnicze badania naukowego.

[23] T. Majewski, *Ankieta i wywiad w badaniach wojskowych,* Akademia Obrony Narodowej, Warszawa 2002.

Rozdział 1 – Teoretyczne podstawy modelowania i symulacji

CEL BADAŃ

Celem badań zagadnień poruszanych w niniejszym rozdziale jest: **Przedstawienie teoretycznych podstaw modelowania matematycznego oraz wykorzystania modelu w symulacjach komputerowych.**

GŁÓWNY PROBLEM BADAWCZY

Stosownie do przyjętego celu badań, problem badawczy sprowadza się do odpowiedzi na pytanie: **W jaki sposób buduje się matematyczny model rzeczywistości oraz jakie są możliwości jego wykorzystania w eksperymentach symulacji komputerowych?**

HIPOTEZY ROBOCZE

Hipoteza pierwsza

Złożoność struktur, zjawisk i procesów będących przedmiotem badań naukowych jest w wielu przypadkach tak duża, że bez przyjęcia ich uproszczonej formy, przeprowadzenie badań staje się niemożliwe do realizacji.

Hipoteza druga

Skutecznym narzędziem do przedstawiania uproszczonych postaci rzeczywistości są modele. Pozwalają one prowadzić badania uwzględniające zmiany badanego fragmentu rzeczywistości, w tym prowadzić eksperymenty symulacyjne.

Hipoteza trzecia

Budowanie modelu w oparciu o język matematyki pozwala na odwzorowanie badanego fragmentu rzeczywistości w postaci umożliwiającej wykorzystanie go do prowadzenia symulacji komputerowych.

1.1. Rola modelu w procesie poznania naukowego

Celem nauki jest opisywanie, tłumaczenie i przewidywanie zachowania otaczającego nas świata[24]. Jedną z przeszkód stającą przed każdym naukowcem w procesie badawczym jest często rozległy obszar i duża złożoność obserwowanej i badanej rzeczywistości.

Badając otaczającą nas rzeczywistość musimy uświadomić sobie, że nie istnieją ani metodologiczne ani organizacyjne możliwości zbadania jej w całości. Musimy eksplorować interesujące nas wycinki. Przykładowo, badając ruch samochodu na pewnej, określonej trasie bierzemy pod uwagę tylko te czynniki, które mają wpływ na badane zjawisko, czyli wagę samochodu, jego przyczepność, długość drogi i prędkość. Poza obszarem zainteresowania znajdują się inne, nieistotne dla badań, ale nierozerwalnie związane z samochodem cechy, takie jak kolor czy marka.

W prawie każdej dziedzinie nauki, badania rozpoczyna się od poznania prawd rządzących obiektami prostymi. Na drodze tych badań możemy dojść do prawd i zachowań rządzących obiektami bardziej złożonymi.

Narzędzie, które pozwala na takie podejście w badaniach naukowych stanowią modele. Model oznacza reprezentację badanego obiektu w postaci innej, niż ta, w której występuje on w rzeczywistości[25].

Pojęcie modelu jest dalece niejednoznaczne i zależne od dziedziny, w jakiej jest używane.

Po pierwsze ***modelem*** może być pierwowzór, egzemplarz eksperymentalny urządzeń, narzędzi czy budowli planowanych do wykonania. Mnożenie przykładów takiego rozumienia modelu jest ze względu na nieskończoną ilość możliwości mało racjonalne. W zasadzie wszystko, co jest tworzone mocą ludzkiej wytwórczości może mieć swój pierwotny kształt wizualizowany z pomocą modelu.

Pojęcie ***modelu*** może być również rozumiane i używane jako określenie wzorca, ideału, do jakiego dążymy, celu, jaki chcemy zrealizować w zamierzonym działaniu. To właśnie w takim rozumieniu tworzone są przez pracodawców modele (wzor-

---

[24] I. Białnicki – Birula. I. Białnicka – Birula, *Modelowanie rzeczywistości*, Wydawnictwo Naukowo – Techniczne, Warszawa 2007, s. 9.

[25] J. Gutenabum, *Modelowanie matematyczne systemów*, Akademicka Oficyna Wydawnicza EXIT, Warszawa 2003, s. 11.

ce) poszukiwanego pracownika czy np. idealnego nauczyciela. Model taki jest zbiorem cech, umiejętności i predyspozycji, jakie powinien posiadać kandydat.

Jeszcze innym rozumieniem tego pojęcia posługujemy się w przypadku, gdy tworzymy miniaturę przedmiotu występującego w postaci naturalnej w dużych rozmiarach. Modele takie powszechnie wykorzystywane są we wszelkich dziedzinach przemysłu i takie rozumienie przenika się z tym opisywanym jako pierwsze. Często, bowiem pierwowzory urządzeń czy budowli tworzone są jako ich miniatury. Modele takie budowane są z zachowaniem proporcji poszczególnych elementów, czyli mówiąc inaczej – w skali. Najpowszechniej znanymi modelami budowanymi w skali są modele ikonograficzne, czyli mapy, plany czy obrazy.

Nieco inne rozumienie ***modelu*** funkcjonuje w świecie artystycznym. W tym rozumieniu model to rzecz lub człowiek, który będzie malowany czy rzeźbiony.

Najbardziej abstrakcyjną formą modelu są modele stosowane do badań mających na celu wyjaśnianie pewnych złożonych zjawisk społecznych, czy mechanizmów działania struktur będących przedmiotem badań. Są to przykładowo modele społeczeństwa, bezpieczeństwa, organizacji, zachowań, ale również mózgu, komunikowania się i uczenia.

W działalności naukowej modelowanie jest w chwili obecnej jednym z podstawowych narzędzi poznania rzeczywistości, jej zrozumienia, a później kreowania[26].

W ujęciu naukowy model jest rozumiany jako uproszczona – przy czym umyślnie i celowo – reprezentacja rzeczywistości[27].

1.2. Klasyfikacja modeli

U podstaw wszystkich badań naukowych jest określenie, co chcemy badać oraz jakimi metodami, technikami i narzędziami zamierzamy badania przeprowadzić. Nie ma uniwersalnych metod badań. Planowanie każdego procesu badawczego to przede wszystkim wybór, spośród wielu znanych i dostępnych, tych metod, technik i narzędzi, które powinny zagwarantować jak najpełniejsze i najbardziej obiektywne przeprowadzenie badań.

---

[26] H. Spustek, *Wybrane zagadnienia badań operacyjnych i modelowania liniowego*, Akademia Obrony Narodowej, Warszawa 2002, s. 10.

[27] J. Gutenabum, *Modelowanie matematyczne systemów*, Akademicka Oficyna Wydawnicza EXIT, Warszawa 2003, s. 11.

Nie jest inaczej w przypadku badań związanych z modelowaniem zjawisk, procesów czy przebiegów pewnych zdarzeń oraz prowadzenia przy ich pomocy eksperymentów symulacyjnych. Złożoność badanej rzeczywistości wymusiła przez lata prac z i nad modelami takie ich zróżnicowanie, aby można było wykorzystać możliwości, jakie one dają w procesach badań naukowych. Podziałów i klasyfikacji, jak w wielu dziedzinach, może być wiele i mogą być one rozpatrywane według wielu kryteriów. Kryteriami takimi mogą być: forma związku między zmiennymi, charakter powiązań między zmiennymi, ilość branych pod uwagę zależności, zakres badań, występowanie lub brak zmiennej losowej między zmiennymi czy statystyczność zależności[28].

Biorąc pod uwagę powyższe, modele możemy podzielić na dwie zasadnicze grupy: modele opisowe i modele optymalizacyjne.

Modele opisowe pozwalają na opis stanu bieżącego badanego obiektu oraz prognozowania jego stanu przyszłego.

Natomiast zadaniem ***modeli optymalizacyjnych*** jest stworzenie w procesie podejmowania decyzji komfortu wyboru najlepszego rozwiązania spośród wielu dostępnych.

Kolejne kryterium pozwala na podział modeli w zależności od języka modelowania. Według tego kryterium, modele można podzielić na ***opisowe, formalne i matematyczne***. Modele opisowe wyrażane są za pomocą języka naturalnego. Formalne wyrażane są językiem logiki, ze szczególnym wykorzystaniem logiki matematycznej. Natomiast ostatnie, jak sama nazwa wskazuje, opisane są językiem matematyki.

Istnieje jeszcze wiele innych podziałów modeli[29], jednak ze względu na obszar zainteresowań niniejszej dysertacji szerzej opisane zostaną modele matematyczne. Ze względu na uniwersalizm języka, jakim one operują, stają się dziedziną interdyscyplinarną dążącą do jak największej ekspansji. Jest to skutkiem coraz szerszego wykorzystywania technik komputerowych w działaniach poznawczych. Sformułowanie modelu w postaci matematyczno – logicznej pozwala, ze względu na duży sto-

---

[28] H. Spustek, *Wybrane zagadnienia badań operacyjnych i modelowania liniowego*, Akademia Obrony Narodowej, Warszawa 2002, s. 11.

[29] Ich przykłady można znaleźć w: I. Białnicki – Birula. I. Białnicka – Birula, *Modelowanie rzeczywistości*, Wydawnictwo Naukowo – Techniczne, Warszawa 2007, J. Gutenabum, *Modelowanie matematyczne systemów*, Akademicka Oficyna Wydawnicza EXIT, Warszawa 2003, H. Spustek, *Wybrane zagadnienia badań operacyjnych i modelowania liniowego*, Akademia Obrony Narodowej, Warszawa 2002, M. Cieślak, *Prognozowanie gospodarcze. Metody i zastosowania*, Wydawnictwo Naukowe PWN, Warszawa 2004.

pień abstrakcji i operowanie symbolami, na wyciąganie wniosków jakościowych i dzięki tej postaci daje możliwości implementacji do komputerowych systemów symulacyjnych.

Model matematyczny jest zbiorem symboli i relacji matematycznych oraz bezwzględnie ścisłych zasad operowania nimi, przy czym zawarte w modelu symbole i relacje mają interpretację odnoszącą się do konkretnych elementów modelowanego wycinka rzeczywistości[30].

Obecnie modele matematyczne wykorzystywane są nie tylko w dziedzinach ściśle powiązanych z matematyką, takich jak geometria, fizyka czy ekonomia. Wykorzystywane są one również do badania i wyjaśniania zjawisk biologicznych, społecznych a nawet medycznych.

Wśród modeli matematycznych wyróżniamy następujące ich kategorie[31]:

a) modele deterministyczne, stochastyczne i probabilistyczne,
b) modele korelacyjne i przyczynowe,
c) modele dynamiczne i statyczne,
d) modele systemów o parametrach rozłożonych w przestrzeni,
e) modele ciągłe i dyskretne,
f) modele całkowitoliczbowe i binarne,
g) chaos.

Pierwszy podział dokonany jest według kryterium posiadania, lub nie, zmiennej losowej. W przypadku, gdy w modelu występują dokładne związki funkcjonalne i żadna ze zmiennych nie jest losowa jest to ***model deterministyczny,*** natomiast występowanie w modelu zmiennej losowej powoduje, że staje się on modelem stochastycznym. Szczególnymi odmianami modeli stochastycznych są modele ***probabilistyczny*** i ***statystyczny***. Różnią się one tym, że w pierwszym znany jest rozkład funkcji gęstości prawdopodobieństwa występujących tam zmiennych losowych natomiast w drugim, funkcja ta nie jest znana.

Kolejną wyszczególnioną kategorią modeli stanowią ***modele korelacyjne i przyczynowe***. Pierwsze (korelacyjne) tworzone są na podstawie obserwacji i doświadczeń zebranych na ich podstawie. Najczęściej stosowane są jako modele prognostyczne, mające wyjaśniać następstwa pewnych zdarzeń i weryfikowania zależ-

---

[30] J. Gutenabum, *Modelowanie matematyczne systemów*, Akademicka Oficyna Wydawnicza EXIT, Warszawa 2003, s. 14.

[31] Tamże, s. 63 ÷ 98.

ności przyczynowo – skutkowych. Niestety zdarza się, że ich wartość jako swoistej „przepowiedni" jest mierna ze względu na zbyt małą ilość obserwowanych zmiennych oraz braku realnego ich powiązania z prognozowanymi skutkami.

Błąd nietrafnej prognozy pozwala zminimalizować zastosowanie modelu przyczynowego. Jego budowa oparta jest, podobnie jak modelu korelacyjnego, na obserwacji zjawisk przyczynowo – skutkowych, z tą jednak różnicą, że uwzględnia wyłącznie rzeczywiste, a nie domniemane zależności obserwowalnych zmiennych. Modele te wykorzystywane są często jako ***modele decyzyjne.***

Kolejną kategorią modeli są ***modele dynamiczne i statyczne***. Podjęcie decyzji o wyborze, którego z tej kategorii modelu należy użyć w badaniach, zależy od tego jakie stany rzeczywistości zostały ujęte w planie badań. Modele statyczne wykorzystywane są do badania fragmentów rzeczywistości, w których interesują nas tylko pewne stany równowagi lub do badania zagadnień, w których problem dynamiki nie występuje. Modele te, to najczęściej modele przeznaczone do badań operacyjnych, modele zależności między wartościami uśrednionymi oraz modele systemów o wejściach wolnozmiennych[32]. Natomiast, gdy badaniami mają być objęte na przykład: analiza stabilności systemu w czasie, zmienność parametrów systemu w czasie oraz systemów niestabilnych, zastosowanie mają modele dynamiczne. Pozwalają one na badanie zarówno stanów równowagi, ale również stanów nieustalonych tj. takich, w jakich znajduje się system zachowujący się niestabilnie lub system wytrącony ze stanu równowagi.

Modele systemów o parametrach rozłożonych w przestrzeni to bardziej złożone narzędzie pozwalające na odwzorowywanie i badanie systemów rzeczywistych, w których zmiany zachodzą w funkcji czasu, jednak niejednorodnie na całej jego powierzchni. Tego rodzaje modele stosowane są na przykład do badania zanieczyszczeń powietrza czy wody, rozkładu temperatur czy rozkładu natężenia siły w konstrukcjach budowlanych.

W zależności od charakteru występujących w modelu zmiennych, możliwy jest podział modeli na ***ciągłe i dyskretne***. W pierwszym przypadku wartości zmiennej są

---

[32] Szczegółowy ich opis znajduję się w J. Gutenabum, *Modelowanie matematyczne systemów*, Akademicka Oficyna Wydawnicza EXIT, Warszawa 2003, s. 75÷80.

określane w każdym momencie czasu, w drugim w sposób dyskretny. Dla zmiennych dyskretnych przedziały czasu mogą mieć wartość stałą lub zmienną[33].

Kolejny podział modeli matematycznych to podział ze względu na przyjmowane przez zmienne wartości. W przypadku, gdy przyjmują one jedynie wartości ze zbioru liczb całkowitych, noszą nazwę ***modeli całkowitoliczbowych***, natomiast, gdy ich wartości to *0* lub *1,* nazywane są ***modelami binarnymi***. Ze względu na charakter modeli binarnych, a dokładnie na charakter zmiennych, które mogą przyjmować wyłącznie dwie wartości wykorzystywane one są w procesach podejmowania decyzji (tak lub nie, prawda lub fałsz) oraz w teorii informacji i telekomunikacji.

Ostatnią wyszczególnioną przez J. Gutenbauma kategorią modeli matematycznych jest ***chaos.*** Modele tego typu wykorzystywane są do badań nad zjawiskami i procesami, których efekt końcowy (wyjście) jest niezwykle wrażliwy na niewielkie nawet zmiany stanu początkowego (wejście) oraz zaburzenia współczynników równań. Rozwiązania tego typu równań (modeli matematycznych) mają cechy procesów losowych. Wykorzystywane są na przykład do badania przepływów hydrodynamicznych w meteorologii.

Inną klasyfikacją modeli jest ich podział ze względu na rezultat modelowania, język modelowania oraz aspekty badań.

W zależności od rezultatu modelowania wyróżniamy modele ***wyjaśniające, ocenowe i opisowe***[34]. Modele wyjaśniające mają na celu wyjaśnienie istoty cech systemu i zależności między nimi, modele ocenowe pozwalają na dokonanie oceny zarówno stanu bieżącego jak również przeszłego i przyszłego. Ostatnim modelem wyszczególnionym w ramach tej klasyfikacji są modele pozwalające na podjęcie decyzji prowadzących do osiągnięcia pożądanego stanu końcowego.

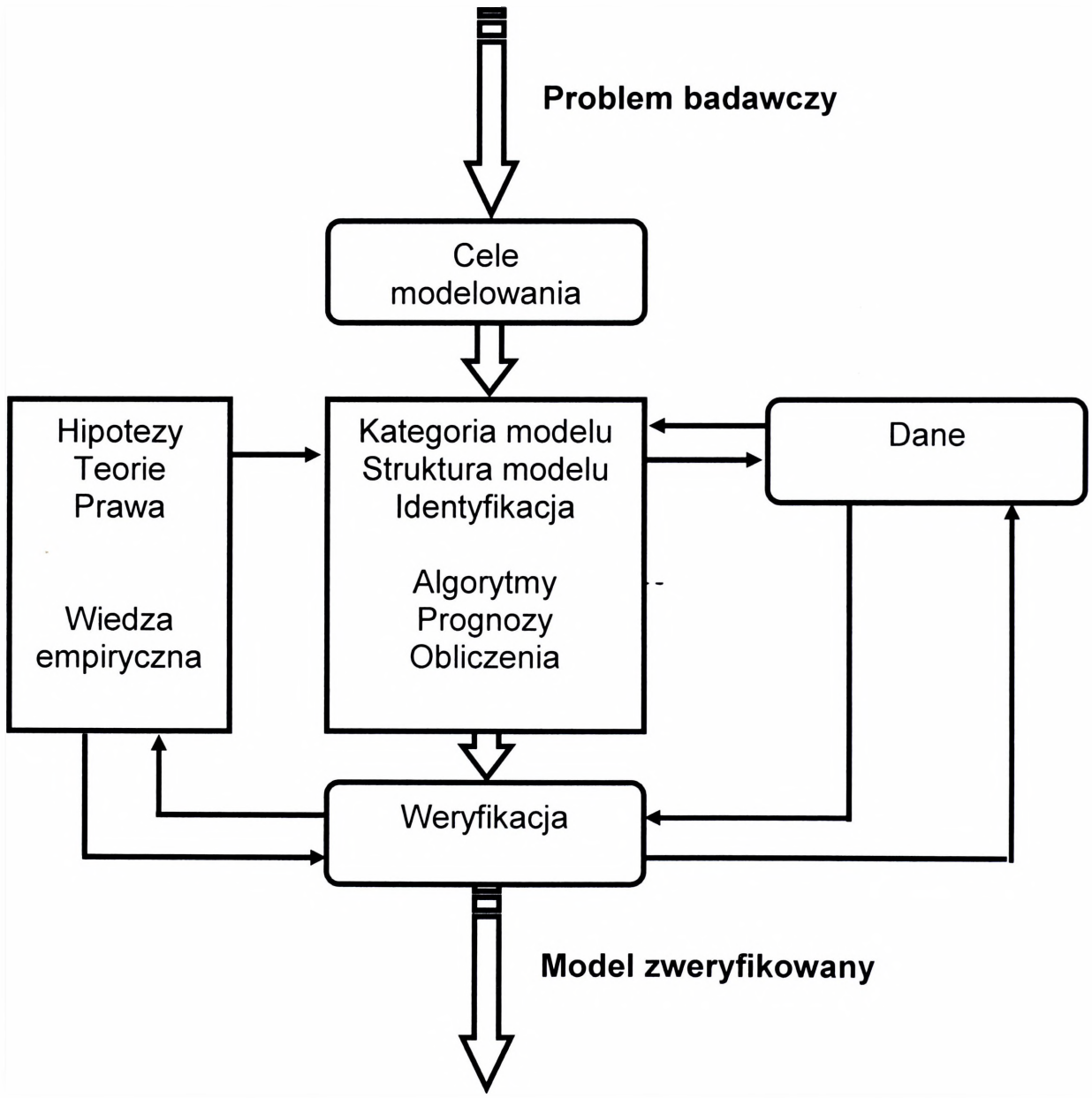
---

[33] T. Söderström, P. Stoica, *Identyfikacja systemów*, Wydawnictwo Naukowe PWN, Warszawa 1997, s. 181÷197.

[34] J. Gutenabum, *Modelowanie matematyczne systemów*, Akademicka Oficyna Wydawnicza EXIT, Warszawa 2003, s. 14.

1.3. Etapy procesu modelowania

Proces modelowania matematycznego dzieli się na kilka zasadniczy etapów do których zaliczamy: sformułowanie celów modelowania, wybór kategorii modelu i określenie jego struktury, identyfikacja, algorytmizacja i weryfikacja obliczeń[35].



Rys. 1.1. Etapy budowy modelu matematycznego
Źródło: J. Gutenabum, *Modelowanie matematyczne systemów*, Akademicka Oficyna Wydawnicza EXIT, Warszawa 2003.

[35] Tamże, s. 20.

Pierwszy etap, pozwalający na sprecyzowanie, dla jakich konkretnych systemów, zjawisk i potrzeb budujemy dany model dzieli je na:

a) modele fenomenologiczne służące opisowi i wyjaśnieniu mechanizmów działania systemu,
b) modele prognostyczne dające przewidywać zachowanie się systemów w przyszłości,
c) modele decyzyjne i optymalizacyjne pozwalające na właściwy dobór oddziaływań oraz wybór najodpowiedniejszych dla działania systemu,
d) modele normatywne mające na celu umożliwienie wyboru struktury i parametrów systemu, spełniającego określone zadania.

Etap drugi, czyli wybór kategorii modelu i budowa jego struktury, jest etapem modelowania właściwego i polega na przetworzeniu interesującego nas fragmentu rzeczywistości na zbiór relacji matematyczno – logicznych.

Jest to najistotniejszy i najtrudniejszy w realizacji etap ze względu na konieczność pogodzenia ze sobą dwóch sprzecznych wymagań tj.: stworzenie modelu łatwego w użytkowaniu i zgodnego z przeznaczeniem z jednoczesnym zachowaniem pełnej jego zgodności z modelowanym systemem (w zakresie będącym w obszarze zainteresowań). Jest to swoista pułapka gdyż zbytnie jego uproszczenie zwykle nie pozwala spełnić warunku drugiego, a wierne odwzorowanie systemu w postaci równań matematycznych uczyni go mało klarownym dla użytkownika. Niezwykle istotnym staje się odnalezienie kompromisu, tzw. „złotego środka", który pozwoli w jak największym stopniu pogodzić oba warunki.

Następnym etapem w procesie konstruowania modelu matematycznego jest identyfikacja modelu. Jest ona niezbędna, ponieważ najczęściej nie znamy większości parametrów modelu i wiedza teoretyczna nie pozwala na takie opracowanie modelu w postaci dającej możliwość wykonania określonych obliczeń. Wyróżnia się tutaj dwie zasadnicze metody identyfikacji: bierną i czynną oraz wykorzystywane rzadziej identyfikacje: jednorazowe i bieżące.

Identyfikacja bierna realizowana jest metodą obserwacji podczas normalnej pracy systemu. Metoda ta obarczona jest wadami związanymi z brakiem możliwości obserwacji działania systemu w warunkach szczególnych, odmiennych od standardowych. Działające systemy, umiejscowione w optymalnych dla ich działania warunkach stacjonarnych nie pozwalają na wyciągnięcie pełnego wachlarza wniosków o ich działaniu.

Dlatego też jako alternatywa realizowana jest droższa i trudniejsza w realizacji *identyfikacja czynna.* Jest ona zaplanowanym i przygotowanym eksperymentem z użyciem badanego systemu. Poza stopniem skomplikowania oraz kosztem, dużym utrudnieniem w jej realizacji jest konieczność ingerencji w działanie badanego systemu. Ta ostatnia przeszkoda, oprócz drugiej w kolejności ekonomicznej, to najczęstszy powód braku możliwości wykonania identyfikacji czynnej.

Nieco rzadziej, zwykle, gdy wymaga tego cel, dla którego model był budowany, stawiane są wymagania by był on poddany *identyfikacji jednorazowej bądź bieżącej.* Najczęściej stosowane są one dla modeli odwzorowujących system podlegający znaczącym zmianom wraz z upływem czasu.

Etapem czwartym omawianego procesu jest algorytmizacja obliczeń w ramach, której rozwiązuje się równania i nierówności oraz zadania optymalizacyjne.

Wśród metod rozwiązywania równań modelowych wyróżniamy rozwiązania analityczne, numeryczne oraz rozwiązania przez symulację.

Rozwiązania analityczne stosujemy w przypadku, gdy jesteśmy w stanie przedstawić rozwiązanie w postaci jawnej, np. $y = u^2$, gdzie u jest zmienną niezależną[36]. W przypadku, gdy nie istnieje możliwość znalezienia na drodze analitycznej postaci jawnej, mamy do czynienia z rozwiązaniami numerycznymi. Istota ich polega na tym, że wartości zmiennych zależnych mogą być określone wyłączne za pomocą procedury numerycznej, czyli określonego algorytmu.

Innym sposobem algorytmizacji obliczeń jest rozwiązanie przez symulację. Modele dostosowane do badań przez symulacje są często wykorzystywane ze względu na uniwersalizm zastosowań. W tym przypadku dane wejściowe (zmienne niezależne) odpowiadają najczęściej wielkościom danych wejściowych systemu rzeczywistego. Istnieje, więc możliwość bezproblemowego porównania danych wyjściowych (zmiennych zależnych) otrzymanych w trakcie symulacji z danymi zebranymi w trakcie obserwacji rzeczywistego działania systemu. Istnieje również w tym przypadku niezwykle łatwa możliwość obserwacji wpływu, jaki wywołuje na wyjściu systemu zmiana danych wejściowych.

Ostatnim etapem tworzenia modelu jest jego weryfikacja. Rozumie się przez nią porównanie wyników modelowania z zachowaniem systemu rzeczywistego,

---

[36] Tamże, s. 26.

z punktu widzenia zgodności z wiedzą teoretyczną oraz badaniami doświadczalnymi[37].

Weryfikacja, która tak naprawdę powinna być wykonywana na wszystkich etapach tworzenia modelu, opiera się na wykorzystaniu dwóch grup kryteriów: kryteriów wewnętrznych i zewnętrznych. Wśród tych pierwszych wyróżniamy określające brak sprzeczności logicznych, *kryteria zgodności formalnej* oraz *zgodność algorytmiczną* stanowiącą potwierdzenie poprawności zastosowanych równań i relacji matematycznych.

Drugą grupę stanowią zgodność heurystyczna i zgodność pragmatyczna.

Zgodność heurystyczna jest związana z poprawnością modelu pod względem jego wartości naukowej i metodologicznej, natomiast *zgodność pragmatyczna* dotyczy bezpośrednio wyników modelowania. Wśród pragmatycznej zgodności modelu matematycznego wyróżniamy między innymi zgodność replikatywną, predyktywną i strukturalną.

Model zgodny replikatywnie oznacza zgodność danych generowanych przez model z danymi uzyskanymi wcześniej z systemu rzeczywistego[38].

W przypadku, gdy następuje zgodność danych otrzymanych w trakcie weryfikacji modelu (jeszcze przed otrzymaniem danych rzeczywistych) z danymi otrzymanymi z systemu rzeczywistego, mówimy o *modelu zgodnym predyktywnie.*

Ostatnim i najbardziej zaawansowanym stopniem zgodności jest *zgodność strukturalna*. Oznacza ona badanie zarówno zgodność danych wyjściowych otrzymanych z modelu z danymi z systemu, jak również zgodności mechanizmów wewnętrznych modelu i systemu.

Nie należy nigdy oczekiwać pełnej identyczności wyjść modelu i systemu. Model wyraża nie wszystkie, lecz jedynie istotne cechy systemu, przy czym to, co jest uznawane za istotne, zależy od celów modelowania.

Należy też powiedzieć o statystycznej weryfikacji modelu. Klasyczny zestaw testów służących weryfikacji statystycznej modelu zawiera następujące testy:

a) istotności parametrów,
b) istotności całego modelu,
c) normalności rozkładu składnika losowego,
d) autokorelacji składników losowych,

---

[37] Tamże, s. 28.

[38] J.M. Szymański, *Życie systemów*, Wydawnictwo Wiedza Powszechna, Warszawa 1991, s. 90÷94.

e) jednorodności wariancji składników losowych.

Stosuje się również testy na liniowość modelu, nieobciążoność modelu, współliniowość zmiennych objaśniających i inne[39].

Ważną kwestią modelowania jest rozwiązywalność równań modelowych.

Wśród metod rozwiązywania równań modelowych można wyróżnić:

- *rozwiązanie analityczne* – w przypadku, gdy jesteśmy w stanie przedstawić rozwiązanie w postaci jawnej np. $y = u^3$, gdzie u jest zmienną niezależną;
- *rozwiązanie numeryczne* – przypadek, gdy nie istnieje praktyczna możliwość znalezienia rozwiązania na drodze analitycznej, a wartości zmiennych zależnych mogą być określone tylko za pomocą odpowiedniego algorytmu (często jest to program komputerowy);
- *rozwiązanie przez symulację* – stosowane gdy zmiennymi niezależnymi modelu są zmienne odpowiadające wielkościom wejściowym systemu rzeczywistego, oraz wyjście jest jednoznaczną funkcją wejścia.

1.4. Dekompozycja modelu

W trakcie budowania modeli często pojawia się problem, czy maksymalnie odwzorować badany system budując wysoce skomplikowany model, czy minimalizować model kosztem niepełnego lub fragmentarycznego odwzorowania rzeczywistości.

Rozstrzygnięcie tego dylematu jest niezwykle istotne dla wyników prowadzonych badań. Zniekształcenie rzeczywistości poprzez zbyt uproszczone jej odwzoro-

---

[39] Ze statystycznego punktu widzenia należy (po oszacowaniu parametrów modelu) wykonać następujące czynności:

- zinterpretować oszacowania parametrów strukturalnych modelu i ocenić ich zgodność z teorią bądź naszą intuicją,
- ocenić wartość współczynnika determinacji R^2. Im jego wartość jest bliższa jedności, tym lepiej. Należy jednak pamiętać, że celem jest ustalenie zależności między zmiennymi objaśniającymi a zmienną objaśnianą i nadanie tej zależności interpretacji, nie zaś dążenie do maksymalizacji wartości współczynnika determinacji R^2,
- przeprowadzić test F. Jeśli wartość Istotność F jest mniejsza od 0,05, to możemy przyjąć, że model został pozytywnie zweryfikowany ze względu na ten test,
- przeprowadzić test istotności każdej zmiennej objaśniającej. Jeśli wartość - p dla każdej zmiennej jest mniejsza od 0,05, to możemy przyjąć, że każda ze zmiennych objaśniających ma wpływ na zmienną objaśnianą,
- upewnić się, czy stosowanie wyżej wymienionych testów statystycznych było uzasadnione, czyli przeprowadzić test normalności rozkładu składnika losowego. Jeśli wartość Statystyka JB jest mniejsza od wartości Istotność JB, to nie mamy podstaw do odrzucenia hipotezy o normalności rozkładu składnika losowego.

wanie może prowadzić w efekcie do błędnych wniosków końcowych prowadzonych badań. Zbyt skomplikowany model może natomiast, z punktu widzenia użyteczności dla prowadzonych badań, być całkowicie nieprzydatny[40].

Jednym z narzędzi pozwalających osiągnąć kompromis pomiędzy złożonością modelu, a jego przydatnością z badawczego punktu widzenia jest ***dekompozycja***.

Dekompozycja pozwala na podział zbudowanego modelu na mniejsze podmodele, wyizolowanie pojedynczych procesów, przebiegów funkcji czy algorytmów. Dekompozycja jest podziałem badanego złożonego modelu na mniejsze modele, w całości wchodzące w skład podstawowego, a wyodrębnione zgodnie z przyjętymi kryteriami czy wskaźnikami. Każdy wyodrębniony model jest nowym modelem realizującym cząstkowe funkcje modelu podstawowego.

W procesie dekompozycji należy jednak pamiętać, aby pomimo podziału systemu na składowe (np. moduły, funkcje) zachować jego hierarchiczność oraz zależności pomiędzy poszczególnymi modułami. Dlatego też koncepcja dekompozycji musi być zgodna z następującymi kryteriami:

- spełnianie warunków modelu pierwotnego (pozostawanie w zgodzie z modelem podstawowym – pierwotnym),
- wskazanie metody rozbioru dekomponowanego modelu,
- zachowanie koordynacji submodeli, tj. zachowanie istniejących zależności i parametrów poszczególnych submodeli[41].

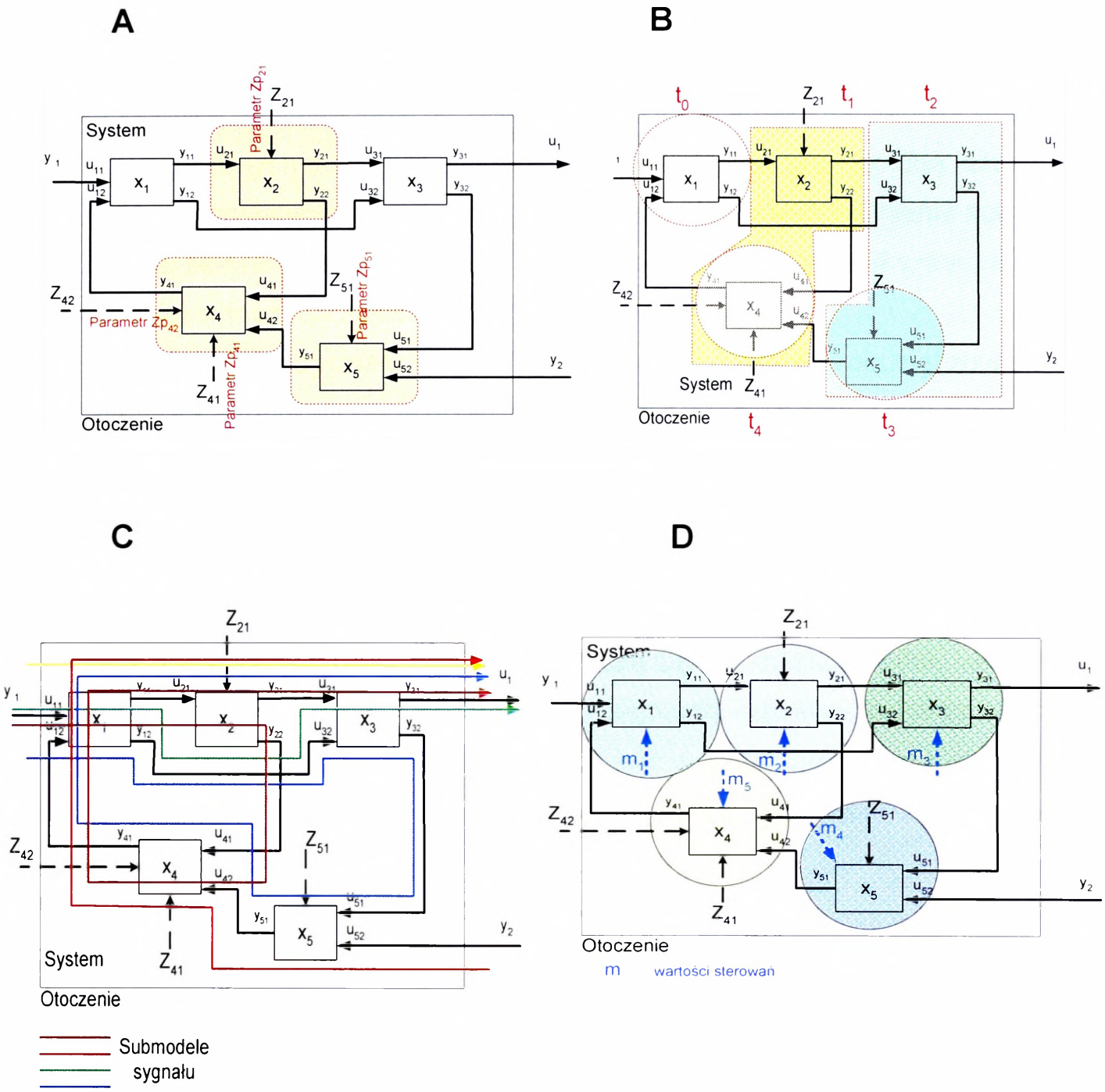
Do zasadniczych rodzajów dekompozycji zaliczamy dekompozycję parametryczną, czasową, sygnału i sterowania – rys. 1.2.

Dekompozycja parametryczna polega na podziale modelu podstawowego zgodnie z oddziałującymi zmiennymi modelu, czyli jego parametrami.

---

[40] J. Gutenabum mówi *o wąskiej ścieżce pomiędzy bagnem komplikacji i przepaściami uproszczenia.*

[41] K. Krakowski, *Symulacje numeryczne w procesie doskonalenia dowództw szczeble taktycznego Wojsk Lądowych SZ RP*, Rozprawa doktorska, Akademia Obrony Narodowej, Warszawa 2006, s. 41.



Rys. 1.2. Przykłady dekompozycji modelu

A. Dekompozycja parametryczna **B. Dekompozycja czasowa**
C. Dekompozycja sygnału systemu **D. Dekompozycja sterowania**

Źródło: Opracowano na podstawie: K. Krakowski, *Symulacje numeryczne w procesie doskonalenia dowództw szczeble taktycznego Wojsk Lądowych SZ RP*, Rozprawa doktorska, Akademia Obrony Narodowej, Warszawa 2006, s.45÷49.

Tak skonstruowana dekompozycja pozwala na badanie danych wyjściowych poszczególnych podmodeli i/lub modelu podstawowego w zależności od wartości oraz ilości zmiennych wejściowych. Kolejnym rodzajem dekompozycji jest ***dekompozycja czasowa.*** Pozwala ona na badanie reakcji badanego modelu na dane wejściowe w określonych przedziałach (chwilach, okresach) czasu. Jej ideą jest taki podział modelu podstawowego, aby umożliwić sekwencyjne wyodrębnienie submodeli, w określonej sekwencji czasowej rozumianej jako umowny przedział czasu, w którym następuje dekompozycja systemu.

Dekompozycja sygnału nie jest zorientowana na fizyczny podział zbudowanego modelu, ale skupia się na przebiegach sygnałów wejściowych. Pozwala na badanie wartości sygnału wejściowego w trakcie przechodzenia przez poszczególne elementy systemu lub wyodrębnione z niego submodele. Dekompozycja sygnału pozwala na badanie przebiegów na przykład sygnałów sterujących, przebiegów procesów technologicznych czy produkcyjnych.

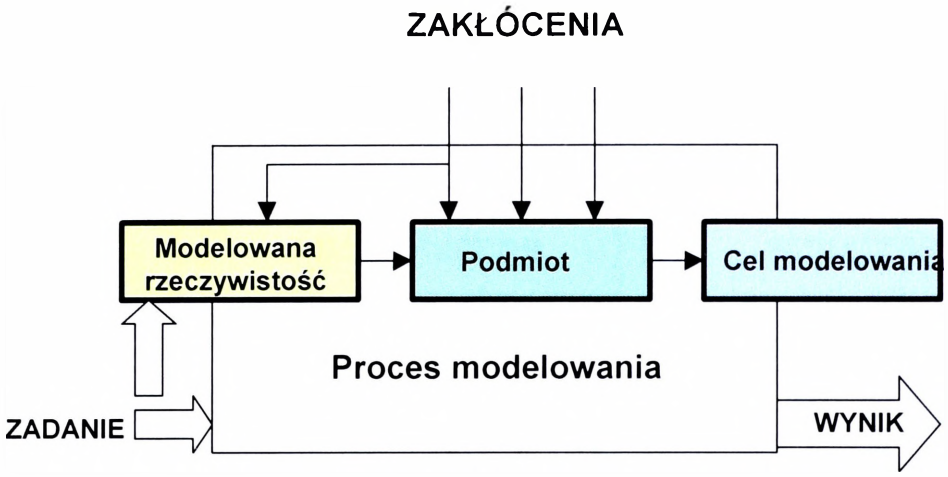
Idea dekompozycji sterowania sprowadza się do podziału modelu według kryterium procedury sterowania i podziału go na segmenty odpowiedzialne za realizację częściowych zadań modelu. Wykorzystywany jest w badaniach na modelach złożonych procesów sterowania. Są to najczęściej modele systemów komputerowych i elektronicznych układów sterowania.

1.5. Struktura modelu

W procesie modelowania zawsze wyróżnia się trzy elementy: przedmiot, podmiot i cel modelowania[42]. Nie bez znaczenia są również zakłócenia mające często znaczący wpływ na wynik końcowy (proces modelowania przedstawia rys. 1.3.).

---

[42] H. Spustek, *Wybrane zagadnienia badań operacyjnych i modelowania liniowego*, Akademia Obrony Narodowej, Warszawa 2002, s. 11.



Rys 1.3. Proces modelowania rzeczywistości
Źródło: H. Spustek, Wybrane zagadnienia badań operacyjnych i modelowania liniowego, AON Warszawa 2002.

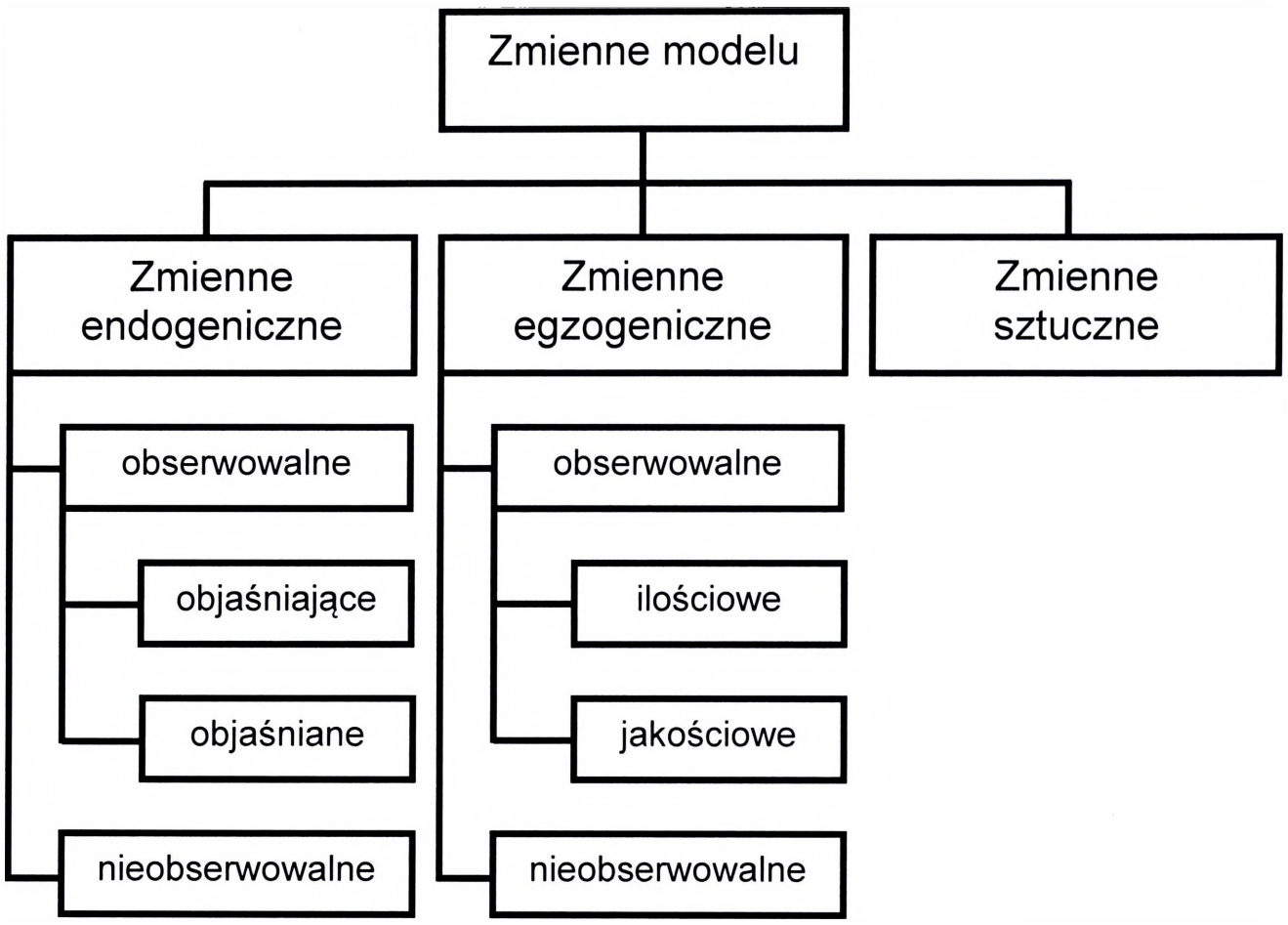
W procesie tym wyróżnia się kilka etapów, od sformułowania założeń modelowych, określenia zmiennych, oszacowania parametrów, określenia ograniczeń, aż po weryfikację modelu.

1.5.1. Zmienne modelu

Istotną rolą w procesie bodowy modelu spełniają ***zmienne modelu***. Dla tych potrzeb wyróżniamy zmienne endogeniczne (zawierające się wewnątrz systemu), egzogeniczne (zawierające się w otoczeniu) oraz zmienne sztuczne (takie, których nie da się zakwalifikować ani do endogenicznych, ani do egzogenicznych).

W zależności od tego, w jaki sposób zmienne oddziałują na system dzielimy je na dodatnie (oddziałujące pozytywnie) i ujemne (oddziałujące na system negatywanie).

Biorąc po uwagę kryterium czasu zmienne dzielimy na: ***zmienne wejściowe***, (ich wartości nie zależą od zachowania modelu systemu), ***zmienne stanu*** (opisujące zmiany wartości cech obiektu w czasie) i ***zmienne wyjściowe*** (opisujące wartości możliwe do zaobserwowania z zewnątrz modelu).



Rys. 1.4. Podstawowy podział zmiennych modelu[43]
Źródło: Opracowanie własne.

W przypadku modeli systemu społecznego zmienne dzielimy na:

- ***zmienne celu*** (zmienne wyjściowe opisujące stan rzeczy pożądany i osiągalny przez działający system),
- ***zmienne diagnozy*** (zmienne stanów systemu w przeszłości i stanów w chwili obecnej, jeżeli system funkcjonuje w teraźniejszości),
- ***zmienne prognostyczne*** (dotyczące skutków zamierzonego działania systemu podlegającego modelowaniu),
- ***zmienne decyzyjne*** (dotyczące wyboru sposobu działania systemu),
- ***zmienne kryterialne*** (zbiór kryteriów oceny – opracowanie otrzymanych wyników – szacowanie wyników)[44].

---

[43] Podział na zmienne endogeniczne i egzogeniczne ma sens głównie w przypadku modeli wielorównaniowych. Zbudowany przez autora rozprawy model jest wielorównaniowy.

[44] J. Zieleniewski, *Organizacja i zarządzanie*, Państwowe Wydawnictwo Naukowe, Warszawa 1981, s. 123÷126.

Zmienne modelowe można podzielić na rodzaje następująco:

A. Zmienne bieżące (bez opóźnienia):

A1: endogeniczne bieżące,

A2: egzogeniczne bieżące.

B. Zmienne opóźnione:

B1: endogeniczne opóźnione,

B2: egzogeniczne opóźnione.

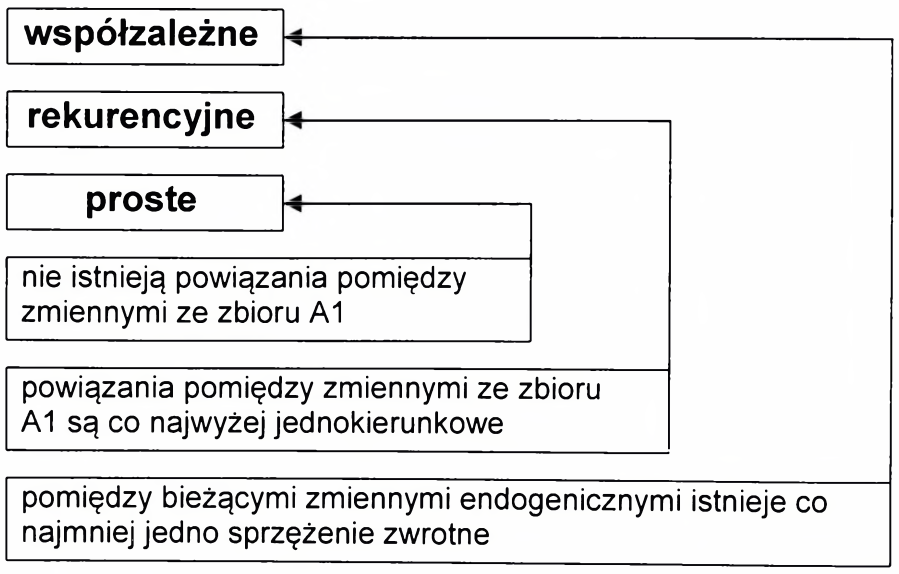
A1 funkcjonuje pod nazwą: *zbiór zmiennych łącznie współzależnych, co oznacza, że do tego zbioru zależą zmienne jednocześnie (łącznie) wyznaczane przez model na dany okres.*

Suma zbiorów: A1, B1 oraz B2 to *zbiór zmiennych z góry ustalonych.*

Zmienne	endogeniczne	egzogeniczne
bieżące	**A1**	**A2**
opóźnione	**B1**	**B2**

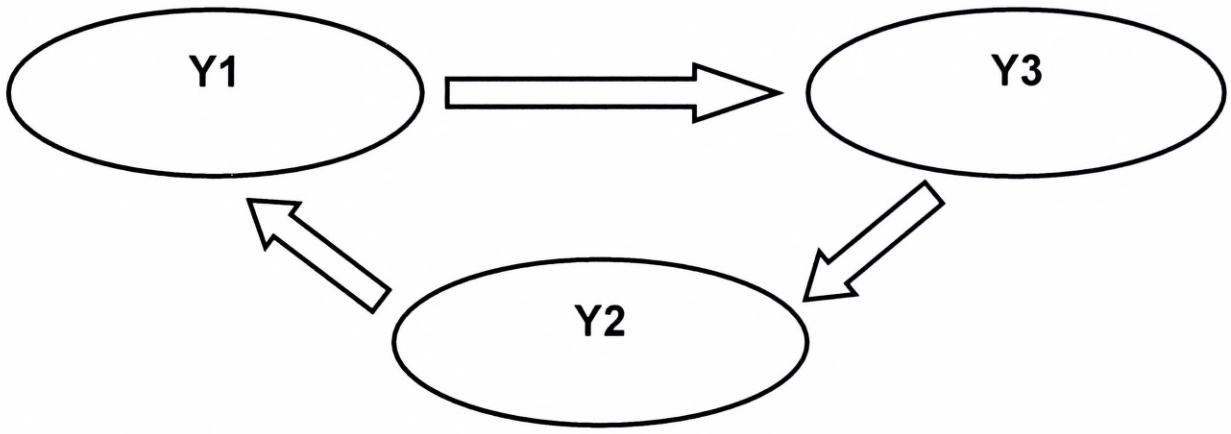
Rys. 1.5. Podział na kategorie zmiennych endogenicznych i egzogenicznych
Źródło: M. Gruszyński, P. Mierzejewski, *Wstęp do ekonometrii w stu oknach,* Wydawnictwo AGH, 1999, s. 33.

Powyższy podział na kategorie zmiennych endogenicznych i egzogenicznych jest istotny jedynie dla modeli o wielu równaniach. Dla modelu o jednym równaniu, w zbiorze A1 występuje tylko jedna zmienna.

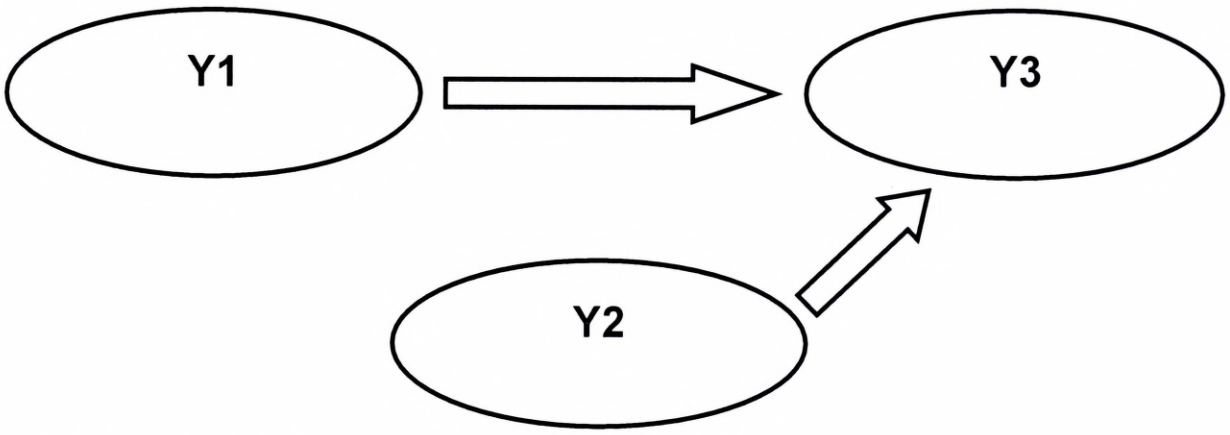


Rys. 1.6. Rodzaje modeli wielorównaniowych
Źródło: M. Gruszyński, P. Mierzejewski, *Wstęp do ekonometrii w stu oknach,* Wydawnictwo AGH, 1999.

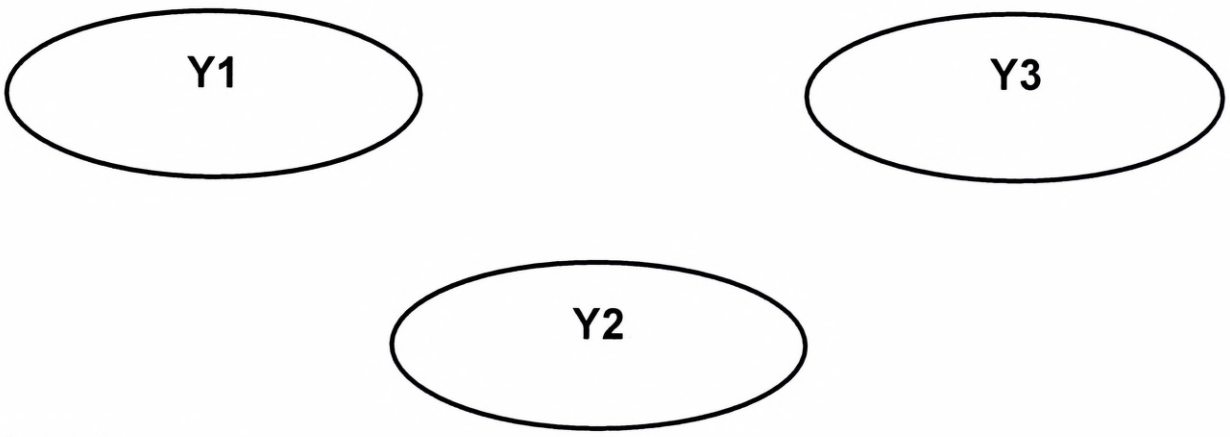
Zależności w modelach wielorównaniowych można przedstawić w postaci graficznej – rys. 1.7.



Model współzależny



Model rekurencyjny



Model prosty

Rys. 1.7. Modele wielorównaniowych w postaci grafu
Źródło: M. Gruszyński, P. Mierzejewski, *Wstęp do ekonometrii w stu oknach,* Wydawnictwo AGH, 1999. s. 34.

Postać strukturalna modelu

$$y_t \mathrm{B} + x_t \Gamma = \xi_t$$

y_t - wektor **G** zmiennych łącznie współzależnych (tj. zmiennych endogenicznych nie opóźnionych),

x_t - wektor **K** zmiennych z góry ustalonych (tj. zmiennych egzogenicznych i opóźnionych zmiennych endogenicznych),

ξ_t - wektor **G** składników losowych poszczególnych równań modelu,

B - macierz kwadratowa stopnia **G**, zawiera współczynniki stojące przy zmiennych łącznie współzależnych,

Γ - macierz **K x G**, współczynników stojących przy zmiennych z góry ustalonych.

Nieznane elementy dwóch powyższych macierzy nazywamy parametrami strukturalnymi modelu. Parametry strukturalne podlegają identyfikacji w toku badań i analiz zebranych danych eksperymentalnych

1.5.2. Parametry modelu

Parametry modelu określają wkład, jaki każda ze zmiennych egzogenicznych wnosi w kształtowanie wartości zmiennej endogenicznej[45].

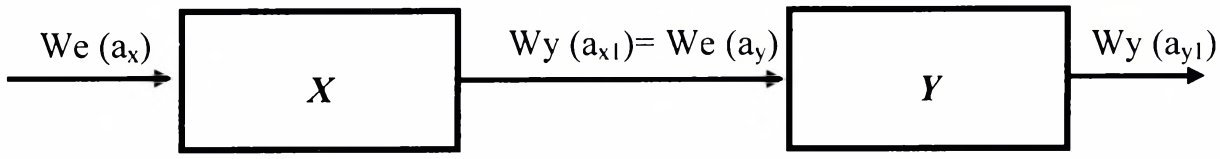
Parametry modelu mogą być w zależności od rodzaju modelu stałe lub zmienne. Parametry stałe występują głownie w modelach deterministycznych, w których możliwe jest określenie wartości sygnału wyjściowego na podstawie sygnału wejściowego. Parametry zmienne (losowe) natomiast występują w modelach stochastycznych, gdzie czynnik losowy nie pozwala na dokonanie dokładnych obliczeń[46].

Parametry modelu mogą przyjmować jedną z postaci: szeregową, równoległą lub zwrotną.

---

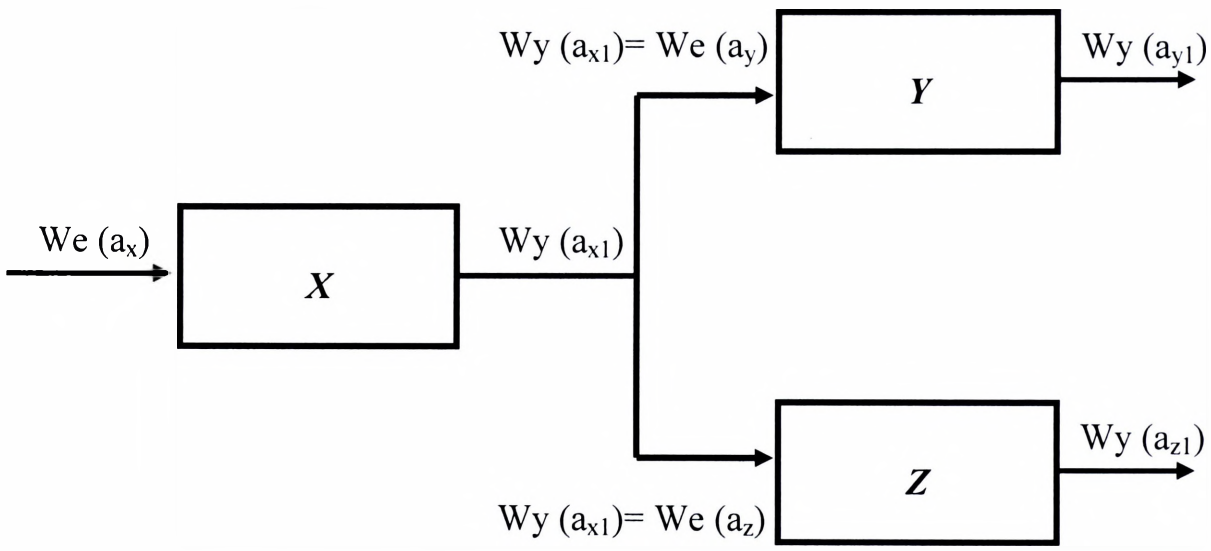
[45] N. Łapińska – Sobczak, *Opisowe modele ekonometryczne*, Wydawnictwo Uniwersytetu Łódzkiego, Łódź 2006, s. 182.

[46] T. Söderström, P. Stoica, *Identyfikacja systemów*, Wydawnictwo Naukowe PWN, Warszawa 1997, s. 183.



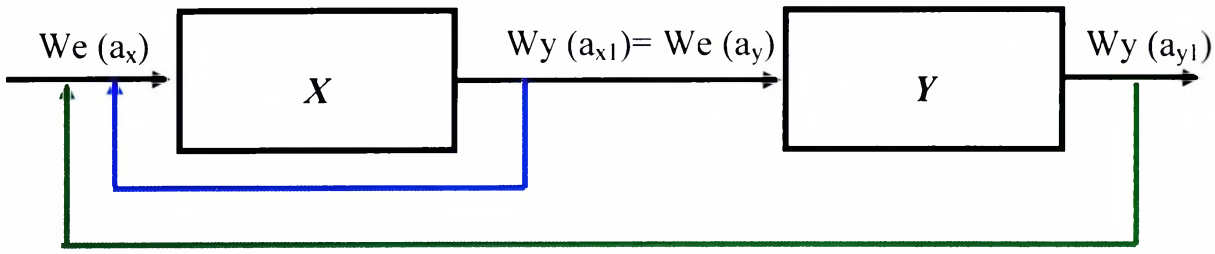
Rys. 1.8. Szeregowa postać parametrów modelu
Źródło: Opracowanie własne.

W przypadku szeregowej postaci parametrów modelu zmienna ***X*** oddziałuje na zmienną ***Y***, gdzie wyjście zmiennej ***X*** jest jednocześnie wejściem zmiennej ***Y***.



Rys. 1.9. Równoległa postać parametrów modelu
Źródło: Opracowanie własne.

W przypadku równoległej postaci parametrów modelu zmienna *x* oddziałuje, na co najmniej dwie zmienne ***Y*** i ***Z***, gdzie wyjście zmiennej ***X*** jest jednocześnie wejściem zmiennej ***Y*** i ***Z***.



Rys. 1.10. Zwrotna postać parametrów modelu
Źródło: Opracowanie własne.

W przypadku zwrotnej postaci parametrów modelu wyjście zmiennej ***X*** jest jednocześnie jej wejściem lub wyjście zmiennej ***X*** jest wejściem zmiennej ***Y*** a jej wyjście jest wejściem zmiennej ***X***.

1.5.3. Ograniczenia

Stopień komplikacji matematycznego modelu systemu rzeczywistego uzależniony jest od potrzeb wynikających z zakres prowadzonych badań, właściwego wyznaczenia zmiennych i parametrów modelu a także stopnia zgodności odwzorowania modelu z jego rzeczywistym obrazem (wzorcem) oraz właściwego doboru równań matematycznych opisujących strukturę i zależności między elementami, submodelami[47].

Wysoce skomplikowany model, jak już wspomniano wcześniej może na tyle utrudnić prowadzenie badań, że w skrajnym przypadku ich wykonanie może stać się niemożliwe. Dlatego też zbudowane modele poddawane są uproszczeniom.

Uproszczeń dokonuje się poprzez:

- pomijanie jednego lub więcej elementów, parametrów, zmiennych opisowych modelu;
- zastępowanie zmiennych deterministycznych przez zmienne probabilistyczne;
- uogólnienie wartości zmiennych (jednej lub kilku);

[47] H. Orłowski, J. Hawryluk, *Modelowanie cyfrowe*, Wydawnictwo Naukowo-Techniczne, Warszawa 1971.

– agregowanie elementów w submodele i agregowanie zmiennych opisowych w submodelach[48].

Przy upraszczaniu modelu podstawowego nie można doprowadzić do stanu gdy działania upraszczające zakłócą elementy składowe modelu i relacje między nimi. Najbardziej wyraźną formą uproszczeń jest opisana wcześniej dekompozycja.

1.6. Eksperyment symulacyjny

Symulacja komputerowa polega na badaniu systemu przez eksperymentowanie z jego modelem komputerowym. Obserwując zachowanie modelu w czasie eksperymentu badawczego, wyciągane są wnioski na temat działanie systemu rzeczywistego.

Celem symulacji komputerowych jest zebranie danych o zachowaniu się systemu symulowanego, przy zmiennych warunkach wejściowych, używając komputera oraz odpowiedniego oprogramowania. Potrzeba stosowania symulacji komputerowych zachodzi przede wszystkim wówczas, gdy bezpośrednie badanie zachowania się systemów rzeczywistych jest kosztowne, trudne lub wręcz niewykonalne ze względów pomiarowych. Dzieje się tak między innymi w naukach ekonomicznych i społecznych. Prowadzenie badań symulacyjnych z użyciem komputera wymaga przyjęcia pewnych założeń i metod postępowania zaś tworzenie modelu badanego systemu przebiega wieloetapowo.

Przeprowadzenie eksperymentu symulacyjnego pozwala na określenie „dobroci" wykonanego modelu poprzez porównanie wielkości generowanych przez model z wartościami rzeczywistymi, znanymi z doświadczenia. Eksperymenty symulacyjne przeprowadzane na dobrze skonstruowanym modelu matematycznym, stwarzają możliwość szerokiego przetestowania modelu, co często nie jest możliwe do przeprowadzenia w innej formie.

Zasadniczym problemem, jaki należy rozwiązać podczas planowania eksperymentu symulacyjnego, jest wybór właściwego generatora liczb losowych oraz metody symulacyjnej. Metoda symulacyjna jest rozpatrywana jako imitacja pewnego realnego eksperymentu. Realny eksperyment związany jest z reguły z dużą liczbą przyrodniczych ograniczeń, z kolei metoda symulacyjna również posiada swoją specyfikę.

---

[48] A. Zeliaś, *Teoria prognozy*, Polskie Wydawnictwo Ekonomiczne, Warszawa 1997, s. 334÷339.

Przykładowo, w eksperymentach fizycznych, liczba obiektów biorących udział w eksperymencie rzeczywistym jest przeważnie znacznie większa od tych, które biorą udział w eksperymencie symulacyjnym. Wynika to z faktu ograniczonych możliwości „śledzenia" historii zbyt dużej liczby obiektów.

W metodzie symulacyjnej, ograniczenia przyrodnicze są przeważnie mniej odczuwalne. Spośród metod symulacyjnych najbardziej znane są metody Monte Carlo. Metody te zostały dobrze opisane i wykorzystane z powodzeniem w wielu eksperymentach symulacyjnych[49].

Metodę Monte Carlo (MC) zbudowano w oparciu o proces Markowa oraz generator liczb losowych. Współcześnie mówimy o metodach MC (powstało szereg modyfikacji i rozwinięć metody MC w stosunku do jej pierwotnego algorytmu). Pojawienie się nowych narzędzi do symulowania zjawisk, rozwiązywania różnorodnych zagadnień statystycznych, odsłoniło nowe możliwości maszyn liczących. Metody MC wraz z dynamiką molekularną stanowią dwa filary fizyki numerycznej. Podobnie można powiedzieć o symulacjach zjawisk w innych dziedzinach nauki, w tym, w naukach wojskowych. Doświadczenia symulacyjne w tym zakresie mogą opierać się na dwóch filarach: pierwszy stanowią metody MC a drugi modele teoretyczne, np. modele walki. Dowolne zjawisko przyrodnicze lub społeczne możemy przedstawić w formie opisowej, lub też w postaci sformalizowanej – modelu matematycznego, a następnie aplikacji numerycznej, uwzględniającej techniki obliczeniowe i wiele zmiennych opisujących zachodzące zjawiska, powiązanych równaniami matematycznymi. Nie zawsze udaje się znaleźć rozwiązanie tych równań, wówczas zadawalamy się możliwością określenia zbioru dopuszczalnych rozwiązań. Prawdopodobieństwo wystąpienia każdego rezultatu jest inne. Jeżeli nie możemy dokonać przeglądu wszystkich możliwych rezultatów (ze względu na ich olbrzymią ilość), a szansa na poprawne odgadnięcie wyniku nie wydaje się być wysoka, należy rozważyć możliwość wykorzystania symulacji. Symulacja dostarcza nam informacji na temat zbioru rozwiązań, w celu oszacowania ryzyka związanego z wyborem jednego z nich. Me-

[49] Metoda Monte Carlo (MC) znana od około czterdziestu lat jako dziecko fizyki numerycznej sformułowana została w latach pięćdziesiątych i początku sześćdziesiątych do zastosowania w fizyce do symulacji numerycznych (komputerowych). Jako pierwsi pojęcie to użyli fizycy pracujący w laboratoriach powstałych w Los Alamos w ramach projektu „Manhatann". Olbrzymie zainteresowanie tą metodą wynika z faktu jej użycia w badaniach nad rozszczepianiem ciężkich jąder w reakcjach jądrowych, co między innymi przyczyniło się do budowy pierwszej bomby jądrowej i reaktora jądrowego. Istnieją pewne rozbieżności co do autorstwa metody MC. Jako jej twórców wymienia się między innymi S. Ulama i J. von Neumanna.

toda MC służy do analizy procesów przypadkowych (stochastycznych). Pozwala ona symulować zachowanie się układu zależnego od zespołu parametrów, których wartości podlegają żądanym funkcjom rozkładu prawdopodobieństwa zaistnienia takich a nie innych wyników[50].

Współcześnie, dzięki metodzie MC nie ma konieczności przeprowadzania prób i konstruowania modeli i prototypów po to tylko, aby określić poprawność poczynionych na wstępie założeń. Stworzono zupełnie nową rzeczywistość opisywaną w formie modeli matematycznych wraz z ich wizualizacją.

ALGORYTM METODY MONTE CARLO

Symulacja metodą Monte Carlo obejmuje dwanaście następujących po sobie kroków[51]:

1. Określamy parametr stanowiący podstawowy miernik danego problemu (zjawiska). Przykładem takiego parametru może być zysk, poziom ryzyka.
2. Budujemy model badanego problemu, wykorzystując matematyczne zależności pomiędzy najważniejszymi zmiennymi. Zmienne modelu mogą mieć charakter deterministyczny lub losowy. Zmienne losowe mogą przyjmować wiele wartości, podczas, gdy zmienne deterministyczne mogą przyjmować tylko jedną wartość.
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, wynikająca ze skumulowanego rozkładu prawdopodobieństwa tej zmiennej.
6. Dla każdej zmiennej losowej musi istnieć możliwość wygenerowania liczby losowej.

---

[50] W literaturze bardzo często podawany jest przykład zastosowania metody MC do wyznaczania wartości liczby π. Procedura jej wyznaczenia polegała na rzucaniu igły na odpowiednio przygotowaną (pokrytą siatką współrzędnych) powierzchnię. W przypadku gdy odległości pomiędzy kolejnymi liniami równe były długości igły, to stosunek liczby rzutów, przy których igła przecinała którąkolwiek linię, do liczby wszystkich rzutów dążył do wartości π w miarę wzrostu liczby rzutów. Można też podać przykład zastosowania metody MC, do obliczania pól powierzchni figur płaskich o nieregularnych kształtach. Inny przykład pochodzi od Johna von Neumanna, który już w latach czterdziestych ubiegłego wieku wskazywał na możliwość rozwiązywania tą drogą zagadnień niecałkowalnych w fizyce na drodze numerycznej. Zaproponował wówczas szereg algorytmów sekwencyjnych (ang. step by step).

[51] A. Chyliński, *Metoda Monte Carlo w bankowości*, Wydawnictwo TWIGGER S.A., Warszawa 1999, s. 148÷149.

7. Każdej liczbie losowej musi być przypisana odpowiednia wartość zmiennej losowej.
8. Odpowiednia wartość zmiennej losowej, określona w poprzednim kroku musi, być wykorzystana do wyznaczenia podstawowego miernika danego problemu zgodnie z krokiem
9. Wartość wyznaczona dla podstawowego miernika w kroku 8 musi zostać zapamiętana.
10. Kroki od 6 do 9 muszą być powtarzane wymaganą ilość razy (zazwyczaj od 100 do 1000).
11. Wartości podstawowego miernika, zapamiętane zgodnie z punktem 9, stają się podstawą do określenia jego rozkładu prawdopodobieństwa i skumulowanego rozkładu prawdopodobieństwa.
12. Skumulowany rozkład prawdopodobieństwa utworzony w kroku 11 musi zostać poddany analizie. Podczas analizy wyznaczone są wybrane parametry statystyki opisowej.

Dwanaście kroków widocznych w algorytmie metody MC (rys. 1.11.) może ulec skróceniu do następujących sześciu:

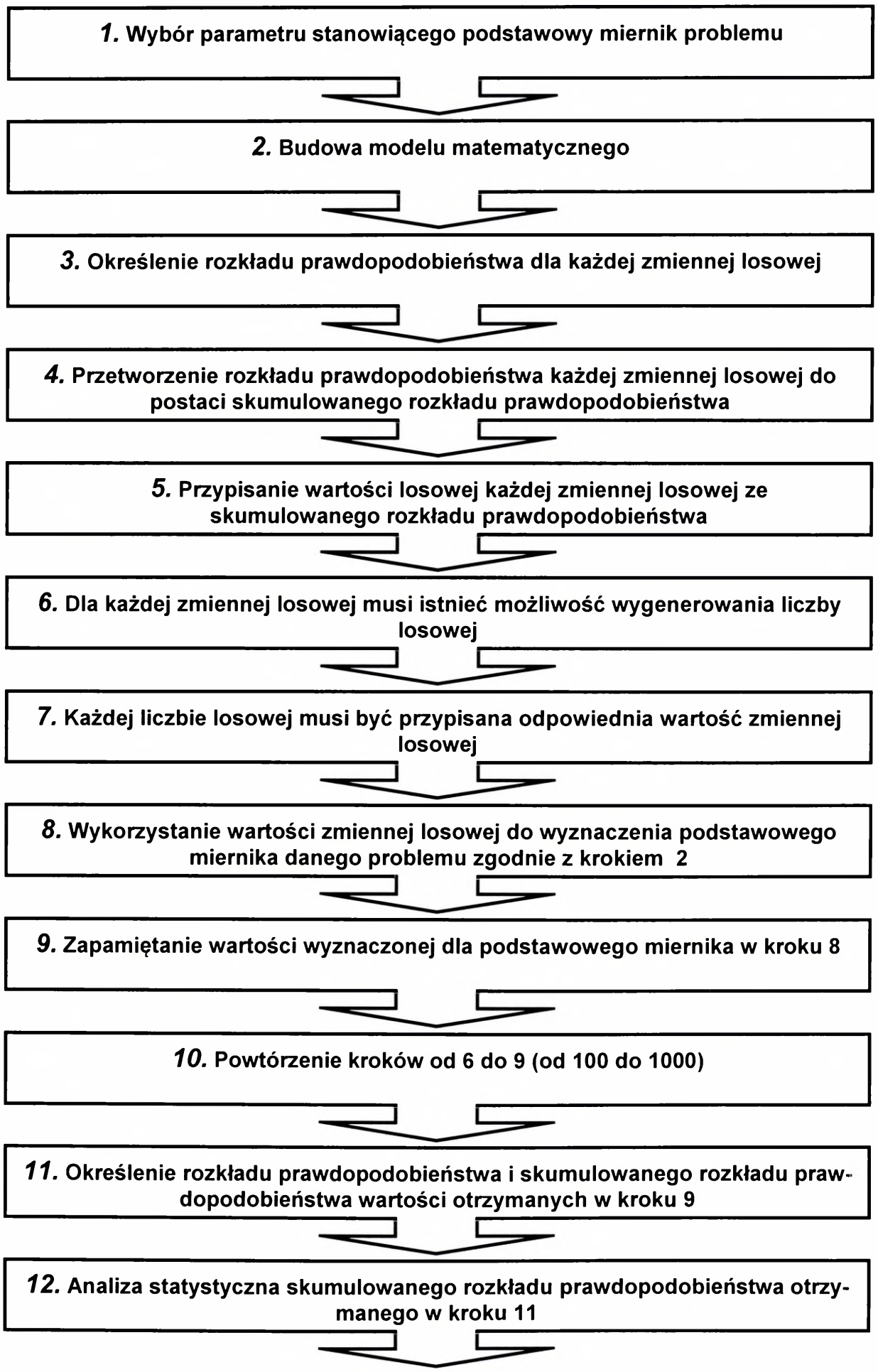
1. Określ punkt początkowy x_0 w przestrzeni fazowej.
2. Wygeneruj nowy stan x'.
3. Oblicz prawdopodobieństwo przejścia $W(x,x')$.
4. Wygeneruj liczbę losową Rε[0,1] (rozkład równomierny).
5. Jeżeli prawdopodobieństwo przejścia W jest mniejsze niż liczba losowa R, to potraktuj ten stary stan jako nowy i wróć do kroku drugiego.
6. W przeciwnym wypadku zaakceptuj nowy stan i wróć do kroku drugiego.[52]

Zarówno w przypadku metody MC opisanej w dwunastu jak i sześciu krokach, aby otrzymać wiarygodny efekt końcowy, należy powtórzyć eksperyment odpowiednią ilość razy.

Metoda MC została zastosowana w części badawczej niniejszej rozprawy. Przeprowadzono eksperyment symulacyjny przy użyciu opracowanego modelu wielorównaniowego, z wykorzystaniem dostępnego oprogramowania komputerowego (patrz rozdział 4.3).

---

[52] D.W. Heermann, *Podstawy symulacji komputerowych w fizyce*, Wydawnictwo Naukowo Techniczne, Warszawa 1997, s. 88.



Rys. 1.11. Dwanaście kroków Metody Monte Carlo

Opracowanie własne na podstawie: Chyliński A., Metoda Monte Carlo w bankowości, Wydawnictwo TWIGGER S.A., Warszawa 1999.

1.7. Wnioski

Celem niniejszego rozdziału było przedstawienie teoretycznych podstaw modelowania matematycznego oraz wykorzystania opracowanego modelu w symulacjach komputerowych.

Treści tego rozdziału pokazują jak zaawansowaną techniką badawczą jest technika modelowania. Jej użycie do badania problematyki bezpieczeństwa informacyjnego we wszystkich sferach, tak cywilnych jak i wojskowych, ma szerokie perspektywy zastosowania.

Dodatkowe korzyści może przynieść wykorzystanie modelu do przeprowadzenia eksperymentów symulacyjnych.

Zastosowanie takiego zestawu badawczego daje podstawy, aby sądzić, że może się on stać skutecznym narzędziem w prognozowaniu naruszeń integralności bezpieczeństwa informacyjnego Sił Zbrojnych RP. Posiadanie takiej wiedzy pozwala na podjęcie działań prewencyjnych oraz zastosowanie metod i środków ochrony adekwatnych do prognozowanych zagrożeń.

Rozdział 2 – Analiza zagrożeń bezpieczeństwa informacyjnego w Siłach Zbrojnych RP

CEL BADAŃ

Celem badań zagadnień poruszanych w niniejszym rozdziale jest: **Klasyfikacja, identyfikacja oraz charakterystyka zagrożeń informacyjnych w Siłach Zbrojnych RP.**

GŁÓWNY PROBLEM BADAWCZY

Stosownie do przyjętego celu badań, problem badawczy sprowadza się do odpowiedzi na pytania: **Jakie są rodzaje zagrożeń bezpieczeństwa informacyjnego w Siłach Zbrojnych RP i jaki jest ich charakter? Jakie zagrożenia są najbardziej prawdopodobne, a jakie najbardziej niebezpieczne?**

HIPOTEZY ROBOCZE

Hipoteza pierwsza

Materiały oraz dokumenty chronione jako informacje niejawne w Siłach Zbrojnych RP narażone są na działania mające na celu naruszenie ich poufności, integralności lub dostępności.

Hipoteza druga

Identyfikacja zagrożeń, określenie ich charakterystyki oraz kategoryzacja pozwala skuteczniej zabezpieczać informacje niejawne w Siłach Zbrojnych RP przed niekorzystnymi na nie oddziaływaniami.

Hipoteza trzecia

Nie można przyjąć jednorodnej procedury oceny zagrożeń informacyjnych dla wszystkich informacji niejawnych w Siłach Zbrojnych RP. Przy analizie należy brać indywidualne cechy oraz uwarunkowania przedmiotu oceny.

2.1. Klasyfikacja informacji niejawnych w Siłach Zbrojnych RP

Aktem prawnym, który stanowi o zasadach ochrony informacji, które wymagają ochrony przed nieuprawnionym ujawnieniem, niezależnie od formy i sposobu ich wyrażenia, jest Ustawa z dnia 22 stycznia 1999 roku o ochronie informacji niejawnych. Zgodnie z nią, informacje stanowiące tajemnicę służbową lub państwową zostały zbiorczo nazwane informacjami niejawnymi. Ustawa w sposób jednoznaczny określa, że ochronie prawnej podlegają zarówno dokumenty jak i materiały. Zróżnicowanie stopnia ich ważności dokonywane jest poprzez nadawanie im odpowiednich klauzul tajności i polega na oznaczeniu ich odpowiednią klauzulą[53].

W celu usystematyzowania pojęć, występujących w rozprawie, związanych z bezpieczeństwem informacyjnym, podano ich znaczenie poniżej.

Materiałem jest dokument lub też chroniony jako informacja niejawna przedmiot bądź dowolna jego część, zwłaszcza urządzenie, wyposażenie lub broń wyprodukowana albo będąca w trakcie produkcji, a także składnik użyty do ich wytworzenia.

Dokumentem jest każda utrwalona informacja niejawna, w szczególności na piśmie, mikrofilmach, negatywach i fotografiach, nośnikach do zapisów informacji w postaci cyfrowej i na taśmach elektromagnetycznych, także w formie mapy, wykresu, rysunku, obrazu, grafiki, fotografii, broszury, książki, kopii, odpisu, wypisu, wyciągu, i tłumaczenia dokumentu, zbędnego lub wadliwego wydruku, odbitki, kliszy, matrycy i dysku optycznego, kalki, taśmy atramentowej, jak również informacja niejawna utrwalona na elektronicznych nośnikach danych.

Nadanie odpowiedniej klauzuli, z czym wiąże się odpowiednie oznaczenie podlegającego ochronie materiału, określa okres ochrony informacji oraz krąg osób mających do niej dostęp. Informacje, którym przyznano odpowiednie klauzule tajności podlegają ochronie zgodnie z przepisami ustawy, co w szczególności oznacza, że:

- mogą być udostępniane wyłącznie osobom uprawnionym do dostępu do informacji określonej klauzuli tajności,
- muszą być wytwarzane, przetwarzane, przekazywane lub przechowywane w warunkach uniemożliwiających ich nieuprawnione ujawnienie, zgodnie z przepisami określającymi wymagania dotyczące kancelarii tajnych, obiegu

[53] Ustawa z dnia 22 stycznia 1999 roku o ochronie informacji niejawnych, art. 19.

i środków fizycznej ochrony informacji niejawnych, odpowiednich dla przyznanej im klauzuli tajności,

- muszą być chronione odpowiednio do przyznanej klauzuli tajności, przy zastosowaniu środków określonych w rozdziale 9 Ustawy z dnia 22 stycznia 1999 roku o ochronie informacji niejawnych (środki ochrony fizycznej informacji niejawnych)[54].

Zgodnie z ustawą, informacje niejawne mogą być klasyfikowane jako informacje stanowiące tajemnicę państwową lub informacje stanowiące tajemnicę służbową. W przypadku zaklasyfikowania informacji jako stanowiącej tajemnicę państwową oznacza się ją klauzulą „tajne" lub „ściśle tajne". Informacje stanowiące tajemnicę służbową oznaczane są natomiast klauzulami „zastrzeżone" i „poufne".

Informacje stanowiące tajemnicę państwową to informacje, których ujawnienie może spowodować istotne zagrożenie dla podstawowych interesów Rzeczypospolitej Polskiej, dotyczących porządku publicznego, obronności, bezpieczeństwa, stosunków międzynarodowych lub gospodarczych państwa[55]. Szczegółowy wykaz rodzajów informacji, które mogą stanowić tajemnicę państwową zawiera załącznik numer 1 do Ustawy z dnia 22 stycznia 1999 roku o ochronie informacji niejawnych. Z zawartego w ustawie zbioru informacji podlegających klasyfikacji jako „ściśle tajne" w Siłach Zbrojnych można wyróżnić:

- informacje dotyczące zagrożeń zewnętrznych bezpieczeństwa państwa o charakterze militarnym, plany i prognozowanie obronne oraz wynikające z nich decyzje i zadania,
- szczegółową strukturę, organizację i funkcjonowanie systemu kierowania państwem oraz dowodzenia Siłami Zbrojnymi w czasie zagrożenia państwa lub wojny,
- lokalizację, wyposażenie, właściwości obronne i organizacja obrony stanowisk kierowania państwem i stanowisk dowodzenia Siłami Zbrojnymi w czasie zagrożenia państwa lub wojny,
- szczegółową organizację, funkcjonowanie systemów łączności kierowania państwem i dowodzenia Siłami Zbrojnymi w czasie wyższych stanów gotowości bojowej i wojny,

---

[54] Ustawa z dnia 22 stycznia 1999 roku o ochronie informacji niejawnych, art. 20.

[55] Tamże, art. 2. ust 1.

- centralny program mobilizacji gospodarki,
- informacje dotyczące planowania, organizacji i funkcjonowania mobilizacyjnego rozwinięcia Sił Zbrojnych,
- szczegółową strukturę Sił Zbrojnych, rodzajów Sił Zbrojnych oraz okręgów wojskowych na czas wojny,
- informacje dotyczące możliwości bojowych Sił Zbrojnych, rodzajów Sił Zbrojnych i okręgów wojskowych oraz potencjalnego przeciwnika na przewidywanych obszarach i kierunkach działań wojennych,
- zadania bojowe Sił Zbrojnych i związków operacyjnych,
- organizację i funkcjonowanie systemu obrony powietrznej i przeciwlotniczej kraju,
- organizację, rozmieszczenie, zadania i możliwości działania systemu rozpoznania i walki radioelektronicznej,
- planowanie i realizacja przedsięwzięć w zakresie operacyjnego maskowania wojsk,
- hasła i kody dostępu do urządzeń przechowujących, przetwarzających i przesyłających informacje oznaczone klauzulą „ściśle tajne",
- szczegółowe wymagania bezpieczeństwa i procedury bezpiecznej eksploatacji systemów i sieci teleinformatycznych służących do wytwarzania, przetwarzania, przekazywania lub przechowywania informacji oznaczonych klauzulą „ściśle tajne"[56].

Do informacji wytwarzanych, przetwarzanych i przechowywanych w jednostkach organizacyjnych Sił Zbrojnych, stanowiących tajemnice państwową, które mogą być oznaczone jako „tajne", możemy zaliczyć:

- dokumenty dotyczące planowania, rozmieszczenie i stanu rezerw państwowych,
- resortowe i wojewódzkie programy mobilizacji gospodarki,
- plany obrony cywilnej państwa oraz plany obrony cywilnej województw,
- szczegółowe założenia finansowe państwa w czasie podwyższonej gotowości obronnej lub wojny,

[56] Ustawa z dnia 22 stycznia 1999 roku o ochronie informacji niejawnych, Załącznik nr 1.

- stan rozwinięcia, ukompletowania i wyposażenie jednostek wojskowych w zakresie nieobjętym postanowieniami Traktatu o konwencjonalnych siłach zbrojnych w Europie (CFE),
- szczegółową strukturę Sił Zbrojnych, rodzajów Sił Zbrojnych oraz okręgów wojskowych,
- plany i prognozy rozwoju organizacyjnego i technicznego Sił Zbrojnych oraz poszczególnych rodzajów wojsk,
- informacje dotyczące przygotowania, budowy, zarządzania oraz funkcjonowania systemów i sieci telekomunikacyjnych, teleinformatycznych i pocztowych służących do przekazywania informacji niejawnych stanowiących tajemnicę państwową, wykorzystywanych dla potrzeb Sił Zbrojnych, służb ochrony państwa lub administracji publicznej w zakresie niezbędnym do zabezpieczenia tych systemów i sieci,
- wojskowe mapy specjalne i fotodokumenty przedstawiające uczytelnione obiekty inżynieryjnej rozbudowy terenu prognozowanych rejonów i kierunków działań wojennych,
- informacje dotyczące przestawienia gospodarki na rzecz obronności w czasie podwyższonej gotowości obronnej państwa lub wojny,
- organizację oraz funkcjonowanie systemu alarmowania wojsk oraz zadania jednostek wojskowych i garnizonów w procesie osiągania wyższych stanów gotowości bojowej,
- organizację oraz funkcjonowanie systemu zaopatrywania Sił Zbrojnych w uzbrojenie, sprzęt wojskowy i amunicję w procesie osiągania wyższych stanów gotowości bojowej,
- szczegółowe wymagania bezpieczeństwa i procedury bezpiecznej eksploatacji systemów i sieci teleinformatycznych służących do wytwarzania, przetwarzania, przekazywania lub przechowywania informacji oznaczonych klauzulą „tajne"[57].

Informacją stanowiącą tajemnice służbową jest informacja niejawna nie będąca tajemnicą państwową, uzyskana w związku z czynnościami służbowymi albo wykonywaniem prac zleconych, której nieuprawnione ujawnienie mogłoby narazić

---

[57] Ustawa z dnia 22 stycznia 1999 roku o ochronie informacji niejawnych, Załącznik nr 1.

na szkodę interes państwa, interes publiczny lub prawnie chroniony interes obywateli albo jednostki organizacyjnej[58] .

Informacjom zakwalifikowanym jako informacje stanowiące tajemnicę służbową nadawane są klauzule:

- „poufne" - w przypadku, gdy ich nieuprawnione ujawnienie powodowałoby szkodę dla interesów państwa, interesu publicznego lub prawnie chronionego interesu obywateli[59],
- „zastrzeżone" - w przypadku, gdy ich nieuprawnione ujawnienie mogłoby spowodować szkodę dla prawnie chronionych interesów obywateli albo jednostki organizacyjnej[60].

Ze względu na specyfikę informacji stanowiących tajemnicę służbową związaną ze zróżnicowaniem obowiązków na poszczególnych stanowiskach ustawodawca nie określił szczegółowego ich wykazu tak jak to zrobił w przypadku informacji stanowiących tajemnicę państwową. Uregulowania takie zawarte są zakresach obowiązków osób funkcyjnych posiadających dostęp do informacji stanowiących tajemnicę służbową.

2.2. Charakterystyka rozważanych zagrożeń dla bezpieczeństwa informacyjnego w Siłach Zbrojnych RP

Klasyfikacja zagrożeń informacyjnych, zarówno w sferze instytucji cywilnych, jak i Sił Zbrojnych RP to problem złożony i niezwykle trudny. Postępujący postęp cywilizacyjny, rozwój nowych technologii i rozwiązań technicznych, rodzą coraz to nowe możliwości, które czynią katalog zagrożeń „żywym" i wciąż ewoluującym. Analizy zagrożeń informacyjnych nie możemy dokonywać w oderwaniu od środowiska, w którym mogą one potencjalnie występować. Wystąpienie zagrożeń, bądź ich brak, uzależniony jest od wielu czynników. W przypadku Sił Zbrojnych, do głównych czynników możemy zaliczyć:

---

[58] Tamże, art. 2 ust. 2.

[59] Tamże, art. 23 ust. 2 pkt l.

[60] Tamże, art. 23 ust. 2 pkt 2.

- zawansowanie techniczne jednostki organizacyjnej (poziom komputeryzacji, dostęp do Internetu oraz sieci resortowych i wewnętrznych, rodzaju użytkowanego sprzętu łączności itp.),
- charakteru oraz specyfiki zadań wykonywanych przez daną jednostkę organizacyjną (jednostka wojskowa, WKU, komórki MON itp.),
- specyfiki wytwarzanych, przetwarzanych i przechowywanych informacji, a co się z tym wiąże nadanych im klauzul tajności,
- dobór użytkowników z uwzględnieniem poziomu ich wyszkolenia, świadomości oraz wiarygodności,
- położenie obiektów i pomieszczeń, w których są wytwarzane, przetwarzane i przechowywane informacje oraz możliwości ich inwigilacji.

Przystępując do charakterystyki zagrożeń dla poszczególnych, indywidualnych jednostek organizacyjnych Sił Zbrojnych, nieodzowne jest posługiwanie się jednoznaczną terminologią, podziałem oraz charakterystyką poszczególnych zagrożeń. Biorąc pod uwagę różne kryteria zagrożenia możemy dzielić, grupować i charakteryzować w dowolny sposób.

Biorąc pod uwagę kryterium pochodzenia i losowości, można wykonać stosowny podział zagrożeń[61]. Pierwszą grupą są zagrożenia losowe wewnętrzne i zewnętrzne. Do zagrożeń losowych wewnętrznych zalicza się:

- niezamierzone błędy operatorów i użytkowników,
- wady sprzętu,
- wady oprogramowania.

Natomiast do zagrożeń losowych zewnętrznych zostały zakwalifikowane:

- zbyt wysoka temperatura lub wilgotność (pożar, zalanie),
- zanieczyszczenia powietrza, kurz, pył,
- zakłócenia w zasilaniu,
- zakłócenia w procesach komunikacji,
- wyładowania atmosferyczne, klęski żywiołowe, itp.

Druga grupą zagrożeń są zagrożenia celowe. Tutaj również dokonano podziału na wewnętrzne i zewnętrzne. Do zagrożeń celowych wewnętrznych zaliczono:

- działania własne pracowników wynikające z chciwości, chęci rewanżu, itp.,

---

[61] A. Barczak, T. Sydoruk, *Bezpieczeństwo systemów informatycznych zarządzania*, Bellona, Warszawa 2003.

- działania użytkowników wykraczające poza ich obowiązki, nadgorliwość itp.,
- szpiegostwo,
- wandalizm, chuligaństwo,
- terroryzm.

Z kolei do zagrożeń celowych zewnętrznych autorzy zaliczyli:

- działania przestępców komputerowych podejmowane z chęci zysku,
- działania przedstawicieli prasy i innych mediów, szukających dostępu do informacji,
- szpiegostwo,
- wandalizm, chuligaństwo,
- terroryzm[62].

Podział ten nie obejmuje przestępstw komputerowych, którym poświęcono, ze względu na rosnącą ich rolę, szczególną uwagę. Do przestępstw komputerowych zaliczono:

- atak siłowy – zgadywanie (łamanie) haseł (ang. Brute force attack),
- podszywanie się lub maskarada (ang. Spoofing),
- podsłuchiwanie (ang. Snifing),
- szukanie dziur, tylne drzwi (ang. Back door),
- blokowanie usług (ang. Denial of Sernice),
- inżynieria społeczna (ang. Social Enginering),
- terroryzm sieciowy,
- przechwyt elektromagnetyczny,
- sabotaż komputerowy,
- wywiad komputerowy,
- szpiegostwo i przestępstwa bankowe,
- piractwo komputerowe,
- kradzież materiałów eksploatacyjnych i zasobów komputerowych[63].

Innym podziałem zagrożeń informacyjnych jest ich podział na dwie grupy: sabotaż i zagrożenia nieumyślne oraz infiltracje czynna i bierną[64].

---

[62] Tamże.

[63] Tamże.

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

Grupę pierwszą stanowią:

- pożary i klęski żywiołowe,
- awarie zasilania energetycznego,
- dezintegracja lub „destrukcja informatyczna" (wirusy komputerowe, bomby logiczne i konie trojańskie itp.),
- fizyczne czynniki destrukcyjne i swoiste oddziaływania ludzi, (ładunki wybuchowe niszczące instalacje komputerowe)[65].

Do grupy drugiej natomiast zaliczono metody infiltracji biernej tj.:

- przechwytywanie elektromagnetyczne,
- dołączenie się do linii transmisji danych w sieciach telekomunikacyjnych lub przechwytywanie sygnałów drogą radiową,
- badanie i kopiowanie zbiorów niezabezpieczonych,
- analiza makulatury lub pozostałości po nośnikach informacji, będąca rezultatem bądź niefrasobliwości w gospodarce makulaturą, bądź zlekceważenia obowiązku demagnetyzacji nośników informacji,
- stosowanie ukrytych nadajników[66].

oraz metody infiltracji czynnej, do których zaliczamy:

- łamanie zabezpieczeń,
- 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)[67].

Kolejnym spojrzeniem na problem podziału i klasyfikacji zagrożeń informacyjnych jest ich podział na[68]:

- nieuprawnione ujawnienie informacji (tzw. „wyciek" lub „przeciek"),
- naruszanie przez władze praw obywatelskich,
- asymetrię w międzynarodowej wymianie informacji,
- działalność grup świadomie manipulujących przekazem informacji,

---

[65] Tamże.

[66] R. Czechowski, P. Sienkiewicz, *Przestępcze oblicza komputerów*, PWN, Warszawa 1993.

[67] Tamże.

[68] P. Bączek, *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Wydawnictwo Adam Marszałek, Toruń 2005.

- niekontrolowany rozwój nowoczesnych technologii bioinformatycznych,
- przestępstwa komputerowe,
- cyberterroryzm,
- walkę informacyjna,
- zagrożenia asymetryczne,
- szpiegostwo[69].

Przy takiej mnogości klasyfikacji zagrożeń koniecznym staje się dokonanie na potrzeby tego opracowania kolejnej, opartej na już dokonanych i uwzględniającej uwarunkowania Sił Zbrojnych. Do zagrożeń występujących w Siłach Zbrojnych możemy zaliczyć:

- nieuprawnione ujawnienie informacji (podsłuch, kradzież, zgubienie, działania psychologiczne i socjotechniczne bądź inna forma utraty informacji),
- zagrożenia z Internetu i przestępstwa komputerowe,
- cyberterroryzm,
- awarie i uszkodzenia sprzętowe,
- emisję ujawniającą.

Określenie pełnego katalogu zagrożeń dla poszczególnych komórek organizacyjnych SZ RP (jednostki wojskowe, instytucje, obiekty itp.) nie jest możliwe bez określenia wielu uwarunkowań jednostkowych. Proponowany podział został wykonany w celu zgeneralizowania zagrożeń i określenia najniebezpieczniejszych i najczęściej występujących. Ich charakterystyka oraz bardziej szczegółowe podziały stanowią treść dalszej części niniejszego rozdziału.

2.2.1. Nieuprawnione ujawnienie informacji

2.2.1.1. Podsłuch

Podsłuch jako sposób i metoda zdobywania informacji nie wymaga ani rekomendowania ani tym bardziej udowadniania jego skuteczności i niesionych zagrożeń. Powszechny wręcz dostęp do urządzeń podsłuchowych, ich coraz bardziej zaawansowane rozwiązania technologiczne niosące za sobą skuteczność z jednoczesną

---

[69] Tamże.

miniaturyzacją, powodują, że podsłuchem jesteśmy zagrożeni w zasadzie zawsze i wszędzie. Montaż urządzeń podsłuchowych, poza podstawowymi informacjami o prawach rządzących rozchodzeniem się fal radiowych, akustyce oraz przepływie prądu, nie wymaga specjalistycznego szkolenia, co czyni potencjalnymi intruzami wszystkich przebywających w naszym otoczeniu. Ze względu na położenie urządzeń w stosunku do podsłuchiwanego środowiska (sala konferencyjna, kancelaria, otwarta przestrzeń itp.) podsłuchy możemy sklasyfikować na podsłuchy zewnętrzne i wewnętrzne. Do podsłuchów wewnętrznych zaliczamy urządzenia (mikrofony, nadajniki itp.) montowane w urządzeniach i infrastrukturze budynku.

Do podstawowych urządzeń wykorzystywanych do podsłuchów zaliczamy nadajniki audio. Skuteczność nadajników oraz możliwości jego wykorzystania uzależnione są w praktyce między innymi od jakości stosowanego odbiornika, mocy wyjściowej nadajnika, miejscowych zakłóceń, warunków atmosferycznych, konstrukcji metalowych w budynki, w którym znajduje się nadajnik.

Najlepsze efekty przekazu emitowanego sygnału można otrzymać w przypadku, gdy osiągnięta zostanie „bezpośrednia widzialność" nadajnika i odbiornika. W praktyce oznacza to brak ciał stałych między nimi. Jest to stan bardzo trudny do osiągnięcia, dlatego musimy brać pod uwagę fakt, że każda przeszkoda, nawet w postaci ściany utrudnia odbiór sygnału. Musimy mieć jednak świadomość, że nawet w zakłóceniach i przy pokonywaniu przeszkód, sygnał z prostych i stosunkowo małych nadajników można transmitować bez problemu sygnał na odległość kilkuset metrów, a nawet kilku kilometrów. Największą ich wadą są ograniczenia czasu pracy związane z koniecznością zapewnienia zasilania w sposób trudny do wykrycia. Najczęściej stosowanymi źródłami zasilania są baterie i akumulatory, które mają ograniczony czas działania. Ponadto nadajniki te ze względu na konieczność ich zainstalowania w pobliżu emitowanego źródła dźwięku narażone są wykrycie.

Inną grupą nadajników są nadajniki do podsłuchu rozmów telefonicznych. Istnieje kilka typów nadajników dających możliwości podsłuchu pełnego przebiegu rozmowy, czyli podsłuchu wszystkich jej uczestników. **Nadajniki podsłuchowe typu wkładkowego** to urządzenia, którymi zastępowane są mikrofony w słuchawkach telefonu. Urządzenie to pozwala na prowadzenie rozmowy w naturalny sposób przez użytkowników aparatu i jednocześnie poprzez nadajnik rozmowa przesyłana jest do odbiornika. Zaletą tego typu nadajników jest brak konieczności zapewnienia zewnętrznego zasilania oraz anteny, gdyż korzystają one z zasilania linii telefonicznej.

Nadajniki podsłuchowe montowane szeregowo lub równolegle na linii telefonicznej to urządzenia, które pozwalają na montaż bez konieczności bezpośredniego dostępu do aparatu telefonicznego.

Poza nadajnikami możliwe jest dodatkowo zainstalowanie urządzeń takich jak rejestratory rozmów i rejestratory wybieranych numerów. Rejestratory są urządzeniami wykorzystującymi najczęściej technologię cyfrowego zapisu dźwięku, dzięki czemu pozwalają na zapis ciągły przez długi okres czasu, a także samoczynne włącznie i wyłączanie tylko w okresie, gdy są w zasięgu dźwięku.

Prostota montażu tego typu urządzeń oraz ograniczenia jego wykrycia powodują, że niosą one ogromne zagrożenia, szczególnie dla niefrasobliwych użytkowników. Dlatego też rozmowy, w których przekazywane są informacje niejawne, należy prowadzić poprzez certyfikowane, zapewniające szyfrowanie sygnału aparaty telefoniczne, spięte w sieć zapewniającymi bezpieczeństwo liniami telefonicznymi.

Możliwością podsłuchu zagrożeni są również użytkownicy telefonów komórkowych. Podsłuchiwanie rozmów prowadzonych przez sieci komórkowe jest jeszcze łatwiejsze niż sieci stacjonarnych. Podsłuch „radiowego" odcinka rozmowy możliwy jest przy użyciu zwykłych urządzeń do wychwytywania sygnałów radiowych i urządzeń nasłuchowych. Specyfika systemów telefonii komórkowej pozwala dodatkowo śledzić położenie naszego telefonu, a co się z tym wiąże i ich użytkowników. Zarówno podsłuch jak i określenie położenia telefonu nie jest możliwe, gdy telefon jest wyłączony. Informacje o tym, że istnieją operatorskie możliwości zdalnego włączenia aparatu są jak do tej pory niepotwierdzone.

Urządzeniami, które odbierają i przetwarzają fale dźwiękowe przenoszone przez drgania powietrza w fale elektryczne są mikrofony. Podstawowymi rodzajami mikrofonów stosowanych do inwigilacji są:

- mikrofony węglowe,
- mikrofony pojemnościowe,
- mikrofony elektrodynamicze,
- mikrofony elektretowe,
- mikrofony indukcyjne,
- mikrofony laserowe i mikrofalowe[70].

[70] Lorak, *Inwigilacja elektroniczna i bezpośrednia*, Wydawnictwo FTA – INSIDER TRADING, 2003.

Mikrofony węglowe to urządzenia działające na tej zasadzie, że rezystancja paczuszki granulek węglowych zmienia się pod wpływem zewnętrznego ciśnienia. Paczuszka taka, jeżeli zostanie umieszczona za membraną wibracyjną i zasilana będzie napięciem prądu stałego, powoduje, że prąd w obwodzie zmieniać się będzie pod wpływem dźwięków uderzających w membranę. Uzyskany w ten sposób efekt modulacji pozwala na przesłanie głosu poprzez obwody elektryczne. Mikrofony tego typu są niezwykle czułe, nie nadają się jednak do daleko posuniętej miniaturyzacji.

Mikrofony pojemnościowe (elektroakustyczne) działają wykorzystując impulsy elektryczne wytworzone przez dźwięki uderzające w membranę, która to używana jest jako jedna z płytek płytowego kondensatora powietrzno – dielektrycznego. Powodowane w ten sposób zmiany kapacytancji (reaktancji pojemnościowej) wytwarzają impulsy elektryczne. Mikrofony tego typu są niezwykle czułe oraz pozwalają odtwarzać dźwięk z niezwykłą wiernością. Ze względu na małą wrażliwość na czynniki zewnętrzne, takie jak np. wibracje, rzadko stosowane do podsłuchu.

Mikrofony elektrodynamiczne przetwarzają falę akustyczna na falę elektryczną za pomocą cewki drucianej w polu stałego magnesu. Ze względu na zalety takie jak małe rozmiary, czułość, odporność na wstrząsy oraz brak konieczności zewnętrznego zasilania są powszechnie stosowane w inwigilacji elektronicznej.

Mikrofony elektretowe należą do grupy nowoczesnych, miniaturowych mikrofonów, których zalety czynią niezwykle przydatnymi podczas inwigilacji. Działanie mikrofonu elektretowego jest podobne jak działanie mikrofonu pojemnościowego, ale jest on znacznie odporniejszy na wstrząsy i drgania ciał stałych. Ze względu na brak możliwości wykorzystania w środowisku, w którym wilgotność powietrza osiąga 90% oraz duże koszty wytwarzania obecnie są rzadko wykorzystywane.

Mikrofony indukcyjne to powszechnie stosowane w przypadku sytuacji, gdy nie występują problemy z ich ukryciem. Stosowane są jako podsłuchy pokojowe, a przykładem ich powszechnego stosowania są słuchawki telefoniczne. Mikrofony te nie są kosztowne i są łatwo osiągalne co dodatkowo wyjaśnia powszechność ich użycia.

Mikrofony laserowe i mikrofalowe i to urządzenia w skład którego wchodzą nadajnik i odbiornik. W celu podsłuchu kieruje się promień lasera (wiązkę mikrofalową) na szybę okienną z odległości od około 1 metra do 500 metrów. Szyba okienna, pod wpływem toczących się wewnątrz rozmów, drga powodując modulację skierowanej na szybę wiązki. Odbiornik demoduluje odebrany sygnał przekazując go dalej

do urządzeń rejestrujących lub odtwarzających. Mikrofony te posiadają jeszcze wiele wad jednak ich możliwości wróżą im w przyszłości powszechne zastosowanie.

2.2.1.2. Kradzież, zgubienie i inne formy utraty informacji

Praktyka oraz prowadzone badania [71] pokazują, że najsłabszy ogniwem w procesie zabezpieczania informacji są ludzie. Najbardziej niepokojący jest fakt, że najczęściej są to osoby mające określone uprawnienia dostępu. To właśnie te osoby włamują się do systemów, podsłuchują, niszczą dane, wprowadzają wirusy i poprzez zaniedbywanie obowiązków obniżają poziom bezpieczeństwa[72].

Wiele incydentów związanych z bezpieczeństwem informacji ma swoje podłoże w braku świadomości, wiedzy i uwagi użytkowników. Przykładem takich działań jest wykorzystywanie komputerów służbowych do celów prywatnych (w tym instalowanie własnego oprogramowania), przypadkowe usunięcia plików, omijanie lub niestosowanie ochrony antywirusowej oraz wiele innych, które można by mnożyć. Do najpowszechniejszego jednak, należy niewłaściwe stosowanie procedur korzystania z systemu haseł. Użytkownicy ujawniają swoje hasła innym osobom, stosują te same hasła w wielu miejscach, stosują hasła proste i łatwe do odgadnięcia (np. data urodzin, imiona dzieci) oraz zapisują hasła w miejscach ogólnie dostępnych.

Innym, często niezwykle medialnym, przejawem zagrożeń bezpieczeństwa informacyjnego związanym z brakiem odpowiedzialności osób, którym zostały powierzone informacje niejawne, jest wyrzucanie materiałów zaklasyfikowanych wstępnie jako „śmieci". Na wyrzucanych bez wstępnego zniszczenia notatkach i brudnopisach dokumentów, można znaleźć wiele chronionych oficjalnie informacji. Są to zapisane hasła, notatki z niejawnych spotkań, projekty i propozycje niejawnych pism, zapisane, podejmowane istotne decyzje i wiele innych. Do przejawów największej nieodpowiedzialności są przypadki, gdy na miejskich wysypiskach znajdują się pełne zestawy dokumentacji bankowej, danych wrażliwych klientów firm czy poufne dane me-

---

[71] Z raportów **CERT** (Computer Enmergency Response Team Polska), zespołu zajmującego się reagowaniem na zdarzenia naruszające bezpieczeństwo w Internecie, wynika na przykład, że zgłoszonych oszustw komputerowych w 2005 roku było 137. Wzrost w stosunku do roku 2004 wyniósł w tym konkretnym przypadku o prawie 30%. W przypadku zdarzeń związanych z nieuprawnionym gromadzeniem informacji przez użytkowników w analogicznym okresie odnotowano wzrost o prawie 100%.

[72] J. Stokłosa, T. Bilski, T. Pankowski, *Bezpieczeństwo danych w systemach informatycznych*, Wydawnictwo Naukowe PWN, Warszawa - Poznań 2001.

dyczne. Czyny takie, pomimo tego, że podlegają odpowiedzialności karnej, występują i tylko potwierdzają tezę, że ogniwem najsłabszym w systemie zabezpieczeń informacji jest zwykle człowiek.

2.2.1.3. Działania psychologiczne i socjotechniczne

Działania psychologiczne są rodzajem oddziaływań mającym na celu wywołanie u osób poddawanych atakowi określonych emocji, doznań, procesów myślowych oraz działań. Operacje takie posługując się strachem, pożądaniem, logiką, pragnieniami oraz innymi czynnikami mentalnymi mogą być prowadzone w różnym obszarze. Mogą one być skierowane zarówno do całych narodów czy grup ludzi, ale także do pojedynczych jednostek. Uwarunkowaniem w tym przypadku jest tylko wykorzystanie do prowadzenia operacji właściwych środków przekazu. Przy powszechnym dostępie do Internetu, wszechobecnej telewizji oraz prasie, a także wykorzystując inne środki nie jest problemem wprowadzić w przestrzeń informacyjną, informacji będących elementem działań psychologicznych.

W przypadku oddziaływania na szerszym obszarze najczęściej spotkamy się z rozpowszechnianiem informacji, które są kłamstwami, zniekształceniami, mistyfikacjami, oszczerstwami, elementami nękania oraz cenzurowanie informacji[73].

Kłamstwa to działania mające na celu wprowadzenie do świadomości ich odbiorców całkowicie fałszywy obraz rzeczywistości. Przy stosowanych aktualnie formach rejestracji, przetwarzania oraz przesyłania informacji działanie takie nie jest trudne. Wykorzystanie techniki cyfrowej daje nieograniczone możliwości fabrykowania informacji fałszywych oraz fałszowania prawdziwych. Istnieją techniczne możliwości, aby manipulować przekazami telewizyjnymi będącymi relacjami „na żywo".

Zniekształcenia informacji w przeciwieństwie do kłamstw mają pokazać obraz rzeczywistości, ale niepełny. Poprzez właściwy przekaz lub jego montaż można ważne elementy ukryć, uwypuklić nieistotne, przedstawić tylko pewne elementy rzeczywistości lub sugerować interpretację faktów. Często tego typu działania podejmują stacje telewizyjne relacjonujące wydarzenia z miejsc zapalnych takich jak wojny, klęski żywiołowe czy wypadki nadzwyczajne. Powstałe zniekształcenia nie zawsze są

---

[73] Na podstawie: D. Denning, *Wojna informacyjna i bezpieczeństwo informacji*, Wydawnictwo Naukowo - Techniczne, Warszawa 2002.

jednak elementem działań psychologicznych. Część z nich, zwłaszcza, gdy mówimy o przekazach reporterskich, są skutkiem ludzkiego błędu, pośpiechu oraz nierzetelności. Łatwo, bowiem jest wzbudzić ludzkie uczucia pokazując tragedię małych dzieci lub tragedię osób, z którymi się identyfikujemy np. żołnierze uczestniczący w misjach pokojowych i stabilizacyjnych.

Mistyfikacja jest to celowe wprowadzanie w błąd, udawanie kogoś innego, tworzenie pozorów lub aranżowanie fałszywych instytucji, sytuacji[74]. Są one działaniami wprowadzającymi w życie kłamstwa i kreującymi rzeczywistość inną niż jest naprawdę. Właściwie zaplanowana oraz zrealizowana mistyfikacja jest bardzo rzadko odkrywana. W historii mamy przykłady, że dzięki mistyfikacji wygrywano bitwy, które potem stawały się przełomowymi dla losów wojen. Podczas drugiej wojny światowej to właśnie dzięki mistyfikacji polegającej na podrzuceniu Niemcom zwłok ze sfałszowanymi planami inwazji na Sardynię uratowało życie wielu Brytyjskim żołnierzom desantującym się na wybrzeża Sycylii. Mistyfikacje nie są jednak tylko domeną wojskową. Po 1980 roku w wielu krajach pojawiły się piktogramy i kręgi w zbożach. W związku z tym, że w paru przypadkach nie dało się w sposób naukowy potwierdzić ich pochodzenia, stały się one źródłem zainteresowania mediów i nie tylko[75]. To prowokowało, i nadal prowokuje, żądnych rozgłosu ludzi do tworzenia piktogramów, tyle tylko, że za pomocą deski i sznurka.

Oszczerstwa to informacje, które poprzez plotki i kłamstwa dyskredytują, zniesławiają i zmniejszają wiarygodność osoby, wobec której są kierowane. Narażają ją na śmieszność, nienawiść, a w skrajnym przypadku nawet na potępienie. Narzędzie to wykorzystywane jest często przez polityków w czasie kampanii wyborczych. Oszczerstwa mogą przybierać dwie formy tj. potwarzy lub paszkwilu[76]. Potwarz jest słowną forma ich przekazu, paszkwil natomiast to pisemne oświadczenie. Bardziej zaawansowaną formą oszczerstw są teorie spiskowe. O ile oszczerstwa są zwykle kierowane do pojedynczych osób lub grupy ludzi, o tyle teoria spisku to przypisywanie, zwykle decydentom, świadomego wywoływania tragicznych wydarzeń. Medium, które świetnie nadaje się do rozpowszechniania oszczerstw lub przedstawiania teorii

---

[74] http://pl.wikipedia.org/wiki/Mistyfikacja.

[75] http://pl.wikipedia.org/wiki/Mistyfikacja#Przyk.C5.82ady_g.C5.82o.C5.9Bnych_mistyfikacji.

[76] D. Denning, *Wojna informacyjna i bezpieczeństwo informacji*, Wydawnictwo Naukowo - Techniczne, Warszawa 2002.

spiskowych jest Internet. Można w nim zamieścić, co się chce zachowując anonimowość. Zamieszczone informacje, nawet najbardziej nieprawdopodobne i absurdalne obiegną świat i ich zdementowanie wymaga już zdecydowanie większego zaangażowania. Działania takie maja jednak również swoje słabe strony. Zdemaskowanie oszczerstw lub fałszywych teorii spiskowych w złym świetle stawia ich protoplastów, co w przypadku kampanii wyborczych jest pewnym źródłem niepowodzenia.

Nękanie to forma działań psychologicznych skierowana bezpośrednio do oponenta. Celem takiego oddziaływania może być wszystko, od wywierania presji poprzez utrudnianie działań, na pogróżkach kończąc. Nękanie najczęściej przybiera formę przekazywania dużej ilości niechcianych wiadomości. Może to być wysyłanie na adres poczty elektronicznej wielu informacji blokujących normalne jej funkcjonowanie, mogą to być nękające połączenie telefoniczne, listy i każda inna forma komunikacji. Nękanie jest w wielu przypadkach powiązane z działaniami mającymi na celu zniesławienie i podważenie reputacji osoby nękanej. Skomercjalizowaną formą nękanie są informacje reklamowe zwane spamem (ang. *spam* – mielonka). Są to wiadomości reklamowe przesyłane na adresy skrzynek poczty elektronicznej. Te, zwykle niechciane, wiadomości przeszkadzają i utrudniają odebranie poczty, a w skrajnym przypadku uniemożliwiają jej odebranie.

Cenzura to kolejna forma wojny informacyjnej. Cenzurowanie informacji ma na celu ochronę odbiorców przed materiałami będącymi, w ocenie cenzurującego, niewłaściwymi. Działania te mogą być działaniami pozytywnymi i negatywnymi. Negatywnie postrzegana cenzura jest to, na przykład, ograniczanie wolności mediów. Cenzura pozytywna to ograniczanie dostępu do informacji, które ze społecznego, etycznego czy kulturowego punktu widzenia są szkodliwe. Przykładem może być tutaj walka z rozpowszechnianiem pornografii. Niestety instytucja cenzury przy tak daleko zaawansowanym rozwoju technologii staje się coraz mniej skuteczna lub coraz droższa. Internet pozwala na tyle form komunikacji, że powstrzymanie lub pełna kontrola przepływu informacji staje się prawie niemożliwa.

Zagrożenia związane z działaniami psychologicznymi to nie tylko działania mające na celu oddziaływanie na grupy ludzi. Nie mniej groźne dla bezpieczeństwa informacyjnego są przejawy inżynierii społecznej. Są to działania mające na celu skłonienie innych do zrobienia czegoś, czego nie zrobiliby bez oddziaływania. W przypadku użytkowników systemów informacyjnych może to być ujawnienie haseł, udostępnienie informacji niejawnych, ich zmiana czy zniszczenie. Socjologowie zajmują-

cy się tą problematyką wyodrębnili cechy ludzkiej natury na których bazują socjotechnicy podczas prób manipulowania innymi. Są to: władza, symparia, wzajemność, konsekwencja, przyzwolenie społeczne i rzadka okazja.

Władza – ludzie mają tendencję do podporządkowywania się woli osoby, o której sądzą, że ma władzę. Osoba może podporządkować się prośbie, jeżeli wierzy, że rozmówca ma władzę lub jest upoważniony do proszenia o daną przysługę.

Symparia – ludzie mają tendencję do podporządkowywania się, gdy osoba prosząca jest w stanie ukazać się jako sympatyczna, mająca podobne zainteresowania, poglądy i podejście do życia jak ofiara.

Wzajemność – jest to tendencja do podporządkowania się osobie, która daje lub obiecuje dać mam coś w zamian. Prezent może być materialny lub może stanowić radę lub pomoc. Kiedy ktoś zrobił coś dla nas, czujemy potrzebę odwzajemnienia. Ta silna potrzeba ujawnia się nawet wtedy, kiedy nie prosiliśmy o to, co dostaliśmy. Jednym z najbardziej efektywnych sposobów wpływania na ludzi, tak, aby zrobili nam „przysługę" (podporządkowali się prośbie), jest podarowanie im prezentu lub pomoc, która wywołuje poczucie zobligowania.

Konsekwencja – ludzie mają tendencję do podporządkowywania się, jeżeli wcześniej publicznie ogłosili swoje poparcie i zaangażowanie w danej sprawie. Jeżeli raz obiecaliśmy, że coś zrobimy, nie chcemy wyglądać na niegodnych zaufania i postępujemy zgodnie z naszymi wcześniejszymi deklaracjami lub obietnicami.

Przyzwolenie społeczne – ludzie mają tendencję do spełniania próśb, kiedy wydaje się to zgodne z zachowaniem innych. Przykład ze strony innych jest traktowany jako przyzwolenie i potwierdzenie, że dane zachowanie jest prawidłowe i stosowne.

Rzadka okazja – ludzie mają tendencję do podporządkowywania się, kiedy wierzą, że poszukiwany obiekt występuje w ograniczonej ilości i jest pożądany przez innych oraz dostępny tylko przez krótki czas.

Do typowych metod socjotechnicznych zaliczamy: udawanie pracownika lub współpracownika firmy, podszywanie się pod kogoś kto ma władzę, podszywanie się za przedstawiciela personelu pomocniczego (informatycy, sprzątaczki, kurierzy itp.) oraz budowanie zaufania poprzez identyfikację z firmą i chęć pomocy (używanie wewnętrznego żargonu i terminologii, pomoc w obsłudze skomplikowanego sprzętu). Wszystkie te metody opierają się na ludzkich słabościach, niewiedzy, łatwowierności i chęci pomocy. Natomiast ci, którzy uprawiają inżynierię społeczną to mistrzowie

kłamstw ze zdolnościami aktorskimi. Często ich poczynania wiążą się z wcieleniem się w jakąś postać czy osobę.

2.2.1.4. Działania informacyjne w walce zbrojnej

Rola informacji w walce zbrojnej przeszła w ostatnim czasie znaczącą metamorfozę. O tym że, informacja jest swoistą walutą dowodzenia[77] i że bez niej wygrywanie wojen jest niemożliwe wiemy od dawna. Wzrosła natomiast jej rola. Informacja stała się bronią, a nie tylko elementem wspomagającym proces wypracowania decyzji przez dowódcę. „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 czasie kilkunastu dni, podejmować decyzje w ciągu tygodni i realizować je w ciągu miesiąca. W czasie drugiej wojny światowej podstawowym środkiem łączności było radio. Pozwalało na orientowanie się w sytuacji w ciągu godzin, decydowania w ciągu dni i wykonywania decyzji w ciągu tygodnia. Generał Schwarzkopf w czasie wojny z Irakiem obserwował sytuację niemalże w czasie rzeczywistym, orientował się w czasie minut, decydował w czasie godzin wcielał decyzję w czyn tego samego dnia"[78].

To właśnie wojny naszego wieku, a w szczególności wojny prowadzone z udziałem armii Stanów Zjednoczonych w ostatnich dziesięcioleciach, w sposób bardzo dobitny pokazały niezaprzeczalną rolę oddziaływań informacyjnych jako części działań zbrojnych. Dziekan Szkoły Wojny i Strategii Informacyjnej na Narodowym Uniwersytecie Obrony Stanów Zjednoczonych w książce *Information Warfare* napisał: „Na wojnę informacyjną składają się działania, których celem jest ochrona, wykorzystywanie, uszkodzenie, zniszczenie informacji lub zasobów informacji albo też zaprzeczenie informacjom po to, aby osiągnąć znaczne korzyści, jakiś cel lub zwycięstwo nad przeciwnikiem"[79]. Tak złożony proces nie może odbyć się bez zawansowania ogromnych nakładów ludzkich i wykorzystania szerokiego spektrum wysoko technologicznie zawansowanych urządzeń. Współczesne koncepcje walki zbrojnej, opierają się na tworzeniu wielopłaszczyznowej przewagi. Zdobycie jak największej

---

[77] R. Szpyra, *Militarne operacje informacyjne*, Akademia Obrony Narodowej, Warszawa 2003.

[78] R. Szpyra, *Walka informacyjna w przyszłych działaniach sił powietrznych,* Praca badawcza pod kryptonimem „CYBERAWIATOR" Warszawa 2000.

[79] WInn Schwartau, *Information WARFARE*, 2nd ed., Thunders's Mouth Press, 1966.

przewagi oraz dominacji informacyjnej jest celem aktorów odgrywających główne role na współczesnym teatrze działań.

„Nie zrobili tego, ale mogli posłać do Zatoki szczoteczki zamiast kul..." takimi słowami Jim Christy, kierownik programu do spraw badania przestępczości komputerowej i wojny informacyjnej w biurze śledczym Wojsk Lotniczych Stanów Zjednoczonych podsumował działania grupy holenderskich hakerów uważane za początek wojny informacyjnej w ramach konfliktu w Zatoce Perskiej[80]. Na przełomie 1990 i 1991 roku, w trakcie penetracji wojskowych witryn Internetu, zdobyli oni informacje na temat lokalizacji amerykańskich jednostek, uzbrojenia oraz możliwości ogniowych sprzętu będącego na wyposażeniu planowanych do działań oddziałów. Celami ich ataków były również inne, bardziej wyspecjalizowane systemy, takie jak na przykład system zaopatrzenia wojsk. Po zdobyciu wszelkich danych zatarli w rejestrach komputerów wojskowych wszystkie oznaki swojego działania. Zdobyte w ten sposób informacje próbowali później sprzedać Irakowi. Saddam Hussein nie skorzystał jednak z oferty obawiając się prowokacji ze strony tworzącej się przeciw niemu koalicji.

W tym samym czasie Irak przygotowywał się do ekspansji na posiadający ogromne zasoby roponośne, sąsiadujący z nim Kuwejt. Początkiem przygotowań, po kilku wcześniejszych sygnałach dyplomatycznych, była zapoczątkowana w drugiej połowie 1990 roku kampania informacyjna mająca na celu wskazanie na Kuwejt jako źródło powstającego konfliktu. Władze Irackie oskarżały Kuwejt o nieuzasadnione obniżanie cen ropy, przekraczanie limitów wydobycia oraz przywłaszczenie złóż leżących na pograniczu państw. Dodatkowo wskazywano Stany Zjednoczone jako mocarstwo, które działania te wspiera. Przełomowym dla konfliktu stało się zapewnienie, jakiego udzielił ambasador USA w rozmowie z Husseinem, że Stany Zjednoczone nie wesprą żadnej ze stron w konflikcie Iracko – Kuwejckim[81]. W niecałe dwa tygodnie po tym fakcie wojska Husseina, 2 sierpnia 1990 roku, zajęły emirat Kuwejtu i w kilka dni potem ogłosiły, że Kuwejt jako państwo przestaje istnieć. Po tych działaniach Iraku rozpoczęły się międzynarodowe działania mające na celu przywrócenie równowagi w rejonie Zatoki Perskiej. W skład koalicji celem, której miało być wyzwolenie Kuwejtu weszło 28 państw z USA na czele. Rozpoczęła się prawie całkowita

---

[80] Dorothy E. Denning, *Wojna informacyjna i bezpieczeństwo informacji*, Wydawnictwo Naukowo – Techniczne, Warszawa 2002.

[81] R. Willa, *Dezinformacja, propaganda, walka psychologiczna podczas konfliktu w Zatoce Perskiej 1990 – 1991*, http://www.dialogi.umk.pl/dezinformacja - konflikt - zatoka – perska.html.

izolacja Iraku oraz szeroko zakrojona kampania informacyjna mająca na celu z jednej strony obniżenie międzynarodowego znaczenia Iraku, a z drugiej pokazanie decydentom irackim, że skazani są w przypadku konfrontacji zbrojnej na nieuniknioną klęskę. „Była to rzecz jasna forma psychologicznej presji na Husseina, aby ten dawał wygraną i wycofał się z Kuwejtu, bowiem uparte obstawanie przy swoim mogło to tylko spowodować militarną katastrofę Iraku. Ta kampania prasowa miała tez na celu uspokojenie zachodniej opinii publicznej. Chodziło o to, by przeciętny Amerykanin, Anglik czy Francuz z optymizmem patrzył w przyszłość, aby nie bał się nadchodzącego konfliktu. Rzeczywiście działania te odniosły duży sukces. Praktycznie w żadnym kraju nie zrodziła się obawa przed skutkami tej wojny, jej przebiegiem i możliwością przedłużenia się konfliktu"[82].

Niestety ta kampania informacyjna nie przyniosła zamierzonych efektów. W związku z nieugiętą postawą Saddama Husseina w styczniu 1991 roku rozpoczęła się, prowadzona przez wojska koalicyjne, operacja oswobodzenia Kuwejtu pod kryptonimem „Pustynna Burza". Konflikt ten, poza działaniami militarnymi, których nie można w takiej sytuacji uniknąć, odkrył wiele możliwości, jakie niesie za sobą wojna informacyjna. W jego trakcie wystąpiły zamierzone zakłócenia pracy komputerów, wywiad osobowy, wywiad techniczny, wykorzystanie satelit szpiegowskich, podsłuchy i kamery obserwujące, fizyczne niszczenie infrastruktury komunikacyjnej, broń elektroniczna, fałszowanie dokumentów, operacje psychologiczne, manipulowanie przekazami medialnymi, wprowadzanie wirusów komputerowych oraz wiele innych.

O tym, że wojska koalicyjne zdawały sobie sprawę z roli, jaką odgrywa walka informacyjna niech świadczy fakt, że już w 1990 roku do Arabii Saudyjskiej została przeniesiona 4. Grupa Wojny Psychologicznej (ang. 4th Psychological Operations Group – 4th POG). Grupa ta, w której skład wchodziło ok. 900 osób prowadziła szereg działań, które zapewne nie miały decydującego wpływu na losy wojny, ale bezsprzecznie przyczyniły się do przechylenia szali zwycięstwa na stronę wojsk koalicji. Działania 4th POG ukierunkowane były na dostarczenie żołnierzom armii Husseina możliwie największej ilości materiałów propagandowych oraz informacji osłabiających ich morale. Szacuje się, że podczas działań wydrukowano około 50 ulotek[83] na każdego żołnierza armii irackiej. Ich kolportowanie wymagało niezwykłego wysiłku. Były

---

[82] R. Bielecki, *Pustynna Burza*, Wydawnictwo Bellona, Warszawa 1991.

[83] Z. Czarota, *Operacje informacyjne w wojnach nad Zatoką Perską,* http://coniw.wp.mil.pl/modules.php?name=News&file=article&sid=390.

one w tradycyjny sposób zrzucane z samolotów i śmigłowców, wystrzeliwane jako pociski artyleryjskie oraz w wodoodpornej postaci zrzucane na wodę, która wyrzucała je na brzeg. Ulotki przekonywały o bezzasadności oporu, namawiały do poddania oraz deprecjonowały postawę irackich przywódców. Treści przekazywane w kolportowanych ulotkach wspierane były przez emitowane audycje telewizyjne i radiowe. Forma działań na tym obszarze była dwojaka. Po pierwsze koalicjanci emitowali własne audycje, a po drugie zakłócali audycje emitowane przez Irakijczyków i „wchodzili" z własnymi audycjami na ich częstotliwości. Dowódca 4th POG płk Jones uważa, że 144 tysiące irackich jeńców poddało się sprzymierzeńcom bez walki dzięki wojnie psychologicznej[84]. Amerykański Czerwony Krzyż liczbę tę szacuje na 87 tysięcy. Większość z nich ściskała w ręku ulotki lub miała je schowane w ubraniu[85]. Liczba ta uwidacznia, jaką pracę wykonał płk Jones i jego podwładni.

Równolegle z działaniami ofensywnej wojny psychologicznej koalicjanci prowadzili działania mające na celu zniszczenie najważniejszych systemów elektronicznych. W głównej mierze udało się to dzięki zastosowanej broni elektronicznej i fizycznej. Już w pierwszych aktach operacji Pustynna Burza, w trakcie zdobywania przez samoloty wojsk sprzymierzonych przewagi w powietrzu, chmury radiacyjne wystrzeliwane z samolotów obezwładniły iracką obronę przeciwlotniczą. Dla potrzeb walki informacyjnej wykorzystywano również broń konwencjonalną. Jeden z samolotów bojowych typu F – 117 Stealth zniszczył system kabli łączących sztab armii irackiej z wojskami w terenie, kierując precyzyjnie kierowaną bombę wprost na wylot przewodów klimatyzacyjnych irackiej sieci telefonicznej w centrum Bagdadu. W ten sposób irackie wojska szczebla operacyjnego i taktycznego stały się w praktyce skazane na działania samodzielne. Nie miały, bowiem zarówno możliwości komunikowania się ze szczeblem nadrzędnym oraz, a może przede wszystkim, straciły po kolejnych atakach wojsk koalicyjnych możliwość korzystania z informacji zabezpieczanych wcześniej przez systemy radarowe.

Poza brutalnymi atakami w stosunku do systemów informacyjnych stosowane były bardziej wyszukane metody. Jedną z nich było zakażenie irackich systemów komputerowych wirusem, umieszczonym w przesłanych drukarkach. Zainstalowany

---

[84] Tamże.

[85] *Psychological Operations/Warfare*, http://www.geocities.com/Pentagon/1012/psyhist.html.

w chipach drukarek, przesłanych z Francji przez Amman w Jordanii, wirus unieruchomił system Windows w głównych komputerach sztabu wojsk irackich.

W trakcie działań wojska sojusznicze korzystały z wielu rozwiązań i unowocześnień w zbieraniu, przekazywaniu, analizowaniu i wykorzystaniu informacji. Poczynając od siatki wywiadowczej na rozpoznaniu satelitarnym kończąc. Siatki potencjalnych celów opracowane były jeszcze przed wybuchem wojny z wykorzystaniem systemów satelitarnych. Tak sporządzone dane zostały zaimplementowane w głowicach pocisków Tomahawk i porównywane z danymi przekazywanymi przez radary tych pocisków [86]. Wojska koalicyjne korzystały w trakcie poruszania się po pustyni z systemu GPS (ang. Global Position System). Pozwalał on na bezbłędne określenie pozycji własnej dzięki sygnałom emitowanym prze konstelacje 24 satelit. Samoloty wykorzystywały system GPS do dokładnego określania położenia pól naftowych i dodatkowo wykorzystując zainstalowane na ich pokładach kamery wideo i kamery na podczerwień dostarczały danych do stanowisk dowodzenia. Należy tutaj podkreślić ogromną rolę, jaką odegrały w konflikcie bezzałogowe samoloty rozpoznawcze. Wykonały one setki misji i godzin lotów zbierając dane o znaczeniu, którego w czasie działań nie sposób przecenić. Dochodziło również do komicznych wręcz epizodów z ich udziałem, gdyż zdarzało się, że odcięte od informacji i zdezorientowane pododdziały irackie poddawały się, gdy zaobserwowały te maszyny w powietrzu.

Podejmowane przez irackie instytucje próby zrównoważenie działań wojny informacyjnej, w tym głownie wojny psychologicznej, okazały się bezowocne. Sowiecki generał S. Bogdanow, Szef Centrum ds. Studiów Strategicznych i Operacyjnych Sztabu Naczelnego powiedział: „Irak przegrał tę wojnę jeszcze zanim się ona zaczęła. To była wojna wywiadu, broni elektronicznej, dowodzenia i sterowania oraz kontrwywiadu. Żołnierze iraccy byli oślepieni i ogłuszeni... Nowoczesną wojnę można wygrać informatyką i to jest teraz najważniejsze”[87].

Doświadczenia zebrane w czasie wojny w 1991 roku wykorzystywane były również w czasie wojny z Irakiem w roku 2003. Doświadczenia dotyczyły również walki informacyjnej. Ponownie do gry weszła 4 Grupa Wojny Psychologicznej wraz z brytyjskimi elementami wojny psychologicznej. Całokształt działań skupiono na realizacje podstawowych celów:

---

[86] Dorothy E. Denning, *Wojna informacyjna i bezpieczeństwo informacji*, Wydawnictwo Naukowo Techniczne, Warszawa 2002.

[87] Tamże.

- skłonienie maksimum żołnierzy irackich do dezercji,
- pozyskanie poparcia ludności cywilnej Iraku,
- prowadzenie na niespotykaną dotąd skalę wojny propagandowej z dyktaturą Saddama Husseina o pozyskanie opinii publicznej[88].

Zadania te, tak jak i poprzednio, realizowano poprzez kolportowanie ulotek, audycje telewizyjne i radiowe, komunikaty nadawane przez głośniki, w których nawoływano do poddania i przejścia na stronę koalicjantów.

Analizując rolę informacji, jako integralnej części działań zbrojnych nie możemy pominąć działań, które są prowadzone w cyberprzestrzeni, czyli z wykorzystaniem globalnej sieci jaką jest Internet. Za pierwszą wojnę internetową uważa się działania wywołane przez konflikt w Kosowie. Wojna ta prowadzona była równolegle z działaniami na realnym polu walki a użyto w niej całego wachlarza środków. Wykorzystywano sieć internetową do propagandy, komunikowania się, dezinformowania przeciwnika, atakowania za pomocą wirusów, DoS[89], DDoS[90], e – mail bombingu[91], włamywania się na strony internetowe itd.[92]. O zakresie działania zorganizowanych grupy hakerów oraz cyberterrorystów, będących po obu stronach konfliktu niech świadczy fakt, że w trakcie bombardowania Jugosławii zaatakowanych zostało około 100 serwerów NATO, a z drugiej strony oblężenie kilku jugosłowiańskich stron rządo-

---

[88] Z. Czarota, *Operacje informacyjne w wojnach nad Zatoką Perską,* http://coniw.wp.mil.pl/modules.php?name=News&file=article&sid=390.

[89] **DoS**, czyli **Denial of Service** (ang. *odmowa usługi*) - atak na system komputerowy lub usługę sieciową w celu uniemożliwienia działania poprzez zajęcie wszystkich wolnych zasobów. W sieciach komputerowych atak DoS oznacza zwykle zalewanie sieci nadmiarową ilością danych mających na celu wysycenie dostępnego pasma, którym dysponuje atakowany host. Niemożliwe staje się wtedy osiągnięcie go, mimo że usługi pracujące na nim są gotowe do przyjmowania połączeń.

[90] **DDoS** (ang. ***D**istributed **D**enial of **S**ervice*) - atak na system komputerowy lub usługę sieciową w celu uniemożliwienia działania poprzez zajęcie wszystkich wolnych zasobów, przeprowadzany równocześnie z wielu komputerów (np. zombie). Atak DDoS jest odmianą ataku DoS polegającą na jednoczesnym atakowaniu ofiary z wielu miejsc. Służą do tego najczęściej komputery, nad którymi przejęto kontrolę przy użyciu specjalnego oprogramowania (różnego rodzaju tzw. boty i trojany). Na dany sygnał komputery zaczynają jednocześnie atakować system ofiary, zasypując go fałszywymi próbami skorzystania z usług, jakie oferuje. Dla każdego takiego wywołania atakowany komputer musi przydzielić pewne zasoby (pamięć, czas procesora, pasmo sieciowe), co przy bardzo dużej ilości żądań prowadzi do wyczerpania dostępnych zasobów, a w efekcie do przerwy w działaniu lub nawet zawieszenia systemu.

[91] **E-mail bombing** – atak polegający na wysłaniu dużej ilości danych za pośrednictwem usługi *e-mail*, obliczony na wyczerpanie przestrzeni dyskowej ofiary. Przesłanie do pojedynczego użytkownika lub określonej grupy osób znacznej ilości listów o dużych rozmiarach powoduje sparaliżowanie pracy serwera.

[92] A. Bógdał – Brzezińska, M. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie,* Oficyna Wydawnicza ASPRA – JR, Warszawa 2003.

wych, na które w ciągu kilku dni wysłano 500 tysięcy maili spowodowało ich zablokowanie.

Działania w cyberprzestrzeni, tak jak i te na rzeczywistym polu walki, jeżeli mają przynieść wymierny efekt nie mogą być chaotyczne i pozbawione planu. Przykładem, że tak nie jest niech będą działania prowadzone w przestrzeni cybernetycznej w trakcie konfliktu izraelsko – arabskiego. Jedna z działających po stronie Palestyńczyków grup pod nazwą Unity, opracowała czteroczęściowy plan wojny internetowej, polegającej na zniszczeniu izraelskiej infrastruktury internetowej. Pierwsza zaplanowana faza to uderzenie na izraelskie serwery rządowe, druga – atak na cele ekonomiczne np. Bank Izraela, trzecia – uderzenie na głównych dostawców usług internetowych i czwarta będąca kulminacją ataku to skomasowany atak na strony e – commerce[93], mający na celu doprowadzenie do strat finansowych poniesionych w wyniku przerwania operacji finansowych oraz atak na cele zagraniczne (np. w Stanach Zjednoczonych)[94].

Wojny internetowe to, ze względu na możliwości, jakie niosą, niezwykle groźna broń. Nie kończy się ona, bowiem na formach chyba najłagodniejszych, czyli na działaniach psychologiczno – propagandowych. W dobie wszechogarniającej nas sieci i możliwości zdalnego sterowania systemami elektronicznymi i informacyjnymi nabiera ona nowego wymiaru. Brak granic, anonimowość oraz niewielkie koszy w porównaniu z odniesionymi korzyściami to zalety, których wartości nie da się chyba przecenić. Przykładem takiego działania jest siatka Osamy bin Ladena, która po pozornym rozbiciu, przeniosła centrum swoich działań do Internetu. To właśnie w sieci są aktualnie dostępne materiały szkoleniowe, Internet jest medium komunikacyjnym poszczególnych grup czy osób, przez Internet w końcu werbowani są nowi członkowie organizacji i co najgroźniejsze ochotnicy do wykonywania zbrodniczych planów. To właśnie oni stają się coraz trudniej uchwytni i właśnie dzięki obserwacji korespondencji oraz ich kroków w wirtualnym świecie, ich działania są demaskowane najczęściej.

---

[93] **E-commerce** (Handel elektroniczny), to rozmaite procedury wykorzystujące środki i urządzenia elektroniczne (telefon stacjonarny i komórkowy, faks, Internet, telewizję) w celu zawarcia transakcji finansowej. Najbardziej popularną metodą handlu elektronicznego jest handel internetowy, gdzie występują transakcje handlowe pomiędzy sprzedającymi a kupującymi. Najbardziej powszechną formą handlu elektronicznego są sklepy internetowe.

[94] A. Bógdał – Brzezińska, M. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie,* Oficyna Wydawnicza ASPRA – JR, Warszawa 2003.

2.2.2. Zagrożenia związane z Internetem i przestępstwa komputerowe

Dołączanie urządzeń, systemów lub sieci teleinformatycznych do innego urządzenia, systemu lub sieci, które są publicznie dostępne, jest dozwolone jedynie przy zachowaniu środków uniemożliwiających skuteczny atak z zewnątrz. Zastosowane środki ochrony powinny być proporcjonalne do klauzuli tajności informacji niejawnych w nich wytwarzanych, przetwarzanych, przechowywanych i przekazywanych oraz typu chronionego urządzenia, systemu lub sieci[95].

Niemniej jednak, w celu przedstawienia, zagrożeń, na jakie mogą być narażone zasoby informacyjne wykorzystywanych komputerów służbowych, koniecznym staje się przedstawienie tego problemu. W przyszłości może być to bardzo aktualny problem, gdyż zarówno w kraju, jak i w ramach podkomitetu NATO SC 4 ds. INFOSEC *(Information Security)* trwają prace odnośnie wykorzystania tego medium do wymiany informacji (w tym niejawnych).

W momencie, gdy komputer zyskuje podłączenie do sieci, zostaje narażony na wiele zagrożeń, które wynikają z charakteru Internetu jako sieci (brak centralnej kontroli), słabych punktów stosowanych systemów operacyjnych, charakterystyki protokołów i aplikacji sieciowych oraz ogromnej dynamiki rozwoju sieci.

Internet jako sieć komputerowa niesie ze sobą szereg niebezpieczeństw. Wszystkie zagrożenia z jego strony możemy podzielić na następujące klasy:

- uzyskanie dostępu do danych przesyłanych przez sieć lub przechowywanych w komputerach przez osoby niepowołane,
- utrata danych na skutek działań z zewnątrz,
- fałszerstwo danych,
- uniemożliwienie korzystania z usług (zasobów) przez legalnych użytkowników.

Korzystanie z Internetu wiąże się zawsze z narażeniem komputera na niebezpieczeństwo. Przy ściąganiu potrzebnych danych bądź programów możemy (całkowicie nieświadomie) umieścić w swoim systemie podprogramy (wirus, robak, koń trojański, bomba logiczna), które zmieniając kod oryginalnego programu bądź dołączając się do niego wykonują wrogie działania.

---

[95] Rozporządzenie Prezesa RM z dn. 25.02.1999 r. *w sprawie podstawowych wymagań bezpieczeństwa*, DZ.U. Nr 18, poz. 162.

W związku z tym, korzystanie z zasobów sieci Internet, powinno być realizowane tylko i wyłącznie za pośrednictwem wydzielonych stanowisk komputerowych lub sieci lokalnych, niepodłączonych do systemu, w którym przetwarzane są informacje niejawne. Należy mieć również świadomość, że przenoszenie plików z tych stanowisk lub sieci na inne komputery, pomimo kontroli antywirusowej i przestrzegania procedur postępowania, zawsze niesie za sobą trudne do określenia zagrożenia.

2.2.2.1. Ataki na systemy informatyczne

Włamanie się do systemu przez użytkownika nieuprawnionego odbywa się najczęściej przez przechwycenie identyfikatora i hasła użytkownika uprawnionego.
W tym celu stosowanych jest wiele metod. Do zasadniczych należą:

a) zmiana oryginalnego programu, którym użytkownicy rejestrują się w systemie - podstawienie konia trojańskiego,
b) wykorzystanie rezydentnych programów kontrolujących klawiaturę - zapisywanie sekwencji naciskanych klawiszy,
c) podsłuch łącza, którym transmitowane są dane uwierzytelniające:
   - rozgałęźnik na kablu klawiatury i urządzenie rejestrujące transmisję z klawiatury,
   - podsłuch w lokalnej sieci komputerowej,
   - podsłuch w sieci rozległej.
d) atak słownikowy,
e) przeszukiwanie wyczerpującą metodą prób i błędów - atak brutalny,
f) metody fizyczne – obserwacja rąk użytkownika rejestrującego się w systemie,
g) metody inżynierii społecznej - nakłonienie użytkownika do udostępnienia lub zmiany hasła[96].

Atak słownikowy polega na podstawianiu w miejsce hasła ciągów znaków sekwencyjnie pobieranych z pewnego słownika. Obroną przed atakiem słownikowym jest stosowana często w systemach operacyjnych funkcja automatycznego blokowania konta po kilkukrotnym podaniu błędnego hasła. Jednak ta sama funkcja może być wykorzystana przez intruza w celu pozbawienia dostępu uprawnionego użytkownika. Jeżeli plik z hasłami zostanie przejęty przez potencjalnego włamywacza, to atak

[96] J. Stokłosa, T. Bilski, T. Pankowski, *Bezpieczeństwo danych w systemach informatycznych*, Wydawnictwo Naukowe PWN, Warszawa - Poznań 2001.

słownikowy może być przeprowadzony poza systemem, w którym dane hasła są stosowane.

Przeszukiwanie wyczerpujące jest zbliżone do ataku słownikowego. Jednak w tym przypadku w miejsce szukanego hasła podstawia się nie ciągi znaków z ograniczonego zbioru, lecz wszystkie możliwe ciągi. Ze względu na zwykle dużą liczbę kombinacji metoda ta wymaga zastosowania znacznych mocy obliczeniowych.

Ponadto włamania można dokonać wykorzystując programy zmieniające hasła lub je wyłączające, nieobecność użytkownika, haki pielęgnacyjne[97] oraz błędy w systemach operacyjnych i oprogramowaniu użytkowym.

Atak na system informatyczny poprzedzany jest zwykle etapem wstępnym – zbieraniem informacji o atakowanym systemie. Istnieje kilka sposobów zdobywania informacji ułatwiających wykonanie ataku. Najczęściej spotykane to poszukiwanie dokumentów publicznie dostępnych, podstęp szantaż i wymuszenie, a także przeszukiwanie odpadków[98] w siedzibie firm i poza nią[99].

Innym problemem jest możliwość utraty poufności informacji w wyniku analizy danych niestanowiących tajemnicy. To tej sytuacji może dojść, gdy nieuprawniona osoba może, na podstawie danym jawnych wyciągać wnioski, co do danych poufnych (wnioskowanie).

2.2.2.2. Wirusy komputerowe

Do najczęściej występujących zagrożeń związanych z korzystaniem z sieci komputerowych należą programy zakłócające normalne działanie systemów komputerowych, czyli tzw. oprogramowanie złośliwe. Wywoływane zakłócenia mogą polegać na: niszczeniu lub zmianie zawartości plików i dysków, blokowaniu systemu, obciążaniu procesora dodatkową pracą, generowaniu dźwięku, wyświetlaniu nieoczekiwanych tekstów lub obrazów[100], wymazywaniu informacji z twardego dysku, pamię-

---

[97] **Haki pielęgnacyjne** – niejawne instrukcje umożliwiające łatwą obsługę i rozwój oprogramowania.

[98] Często wśród wyrzucanych odpadków i makulatury *znaleźć* można notatki, informacje o klientach, telefonach wewnętrznych, dokumentację techniczną, zapisane nośniki danych.

[99] J. Stokłosa, T. Bilski, T. Pankowski, *Bezpieczeństwo danych w systemach informatycznych*, Wydawnictwo Naukowe PWN, Warszawa - Poznań 2001.

[100] Tamże.

ci BIOS[101], a nawet fizycznego niszczenia sprzętu[102]. Niektóre z tego typu programów są wykorzystywane do ataków na systemy informatyczne. Do tego typu programów zalicza się wirusy, bakterie, robaki, bomby logiczne, konie trojańskie.

Największą liczebnie grupę stanowią **wirusy komputerowe**. Ich liczbę szacuje się na dziesiątki tysięcy i każdego miesiąca ich rośnie. Termin **wirus komputerowy** oznacza program, który potrafi się rozmnażać i dopisywać oraz ukrywać wewnątrz plików zawierających kod wykonywalny (wirusy plików) lub wewnątrz systemowych sektorów na dyskach (wirusy sektorów systemowych). Wirusy plików uaktywniają się w momencie uruchomienia zainfekowanego programu - następuje zarażenie innego pliku z kodem wykonywalnym i/lub wywołanie zakłóceń w działaniu systemu. Wirus dołączony do pliku w komputerze przedostaje się wraz z plikiem na inny komputer (przy przenoszeniu programu na nośniku danych lub w czasie transmisji siecią komputerową). Wirusy sektorów systemowych uaktywniają się przy starcie systemu z zarażonego dysku i zarażają dostępne dyski logiczne.[103]

Bakterie to programy, które nie powodują wprost uszkodzenia plików. Typowa bakteria dzieli się na dwie kopie i uruchamia je w środowisku zasobów danych. Może też tworzyć dwa nowe pliki, z których każdy jest kopią programu wyjściowego. Oba nowe programy będą się następnie mnożyły dalej, tworząc kolejne „potomstwo". Bakterie reprodukują się wykładniczo i zajmują ogromna pamięć procesora, przestrzeni dyskowej i innych zasobów, przez co użytkownik nie może z nich korzystać[104].

Działanie **robaków** jest podobne do bakterii. Jednak w odróżnieniu od bakterii ich polem działania nie jest pojedynczy system, lecz sieć komputerowa. Robak po zagnieżdżeniu się w systemie może zachowywać się jak wirus, bakteria lub koń trojański. W przeciwieństwie do wirusów nie potrzebuje żadnej pomocy użytkowników i rozprzestrzenia się wykorzystując słabe punkty poczty elektronicznej, stron WWW, programów i aplikacji.

---

[101] **BIOS -** (akronim ang. **Basic Input/Output System** - podstawowy system wejścia-wyjścia) to zapisany w pamięci stałej, inny dla każdego typu płyty głównej komputera, zestaw podstawowych procedur pośredniczących pomiędzy systemem operacyjnym a sprzętem. Program konfiguracyjny BIOS-a to BIOS setup.

[102] A. Bógdoł – Brzezińska, M. Gawrycki *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie,* Fundacja Studiów Międzynarodowych, Warszawa 2003.

[103] J. Stokłosa, T. Bilski, T. Pankowski, *Bezpieczeństwo danych w systemach informatycznych*, Wydawnictwo Naukowe PWN, Warszawa - Poznań 2001.

[104] J. Janczak, *Zakłócanie informacyjne*, Warszawa 2001.

Bomba logiczna to rodzaj wirusa komputerowego, który po zainfekowaniu komputera może pozostawać zupełnie nieaktywny, aż do czasu, gdy nastąpi jakieś specyficzne zdarzenie[105]. Eksplozja bomby logicznej, to aktywizacja nowych funkcji elementu logicznego komputera, która prowadzi do zniszczenia lub zdeformowania sprzętu i oprogramowania[106]. Warunkiem aktywacji może być: określona data, zalogowanie się określonego użytkownika, wybrany dzień tygodnia itp.

Terminem **koń trojański** określamy program, który może wykonywać niepożądane działania (usuwać pliki, formatować dysk, przesyłać dane z systemu) bez zgody i często wiedzy użytkownika. Trojany mogą być umieszczone w niemal każdym programie. Najpopularniejszą drogą ich rozpowszechniania jest poczta elektroniczna lub umieszczenie w Internecie. Jest to narzędzie niebezpieczne gdyż pozwala penetrować zasoby informacyjne atakowanego komputera bez zwracania na siebie uwagi. Dzięki koniowi trojańskiemu istnieje na przykład możliwość przechwycenia przez hakerów haseł logowania się do systemu, programów czy aplikacji.

2.2.3. Cyberterroryzm – nowe oblicze terroryzmu

Cyberterroryzm definiowany jest jako politycznie umotywowany atak lub groźba ataku na komputery, sieci lub systemy informacyjne w celu zniszczenia infrastruktury oraz zastraszania lub wymuszenia na rządzie i ludziach daleko idących politycznych i społecznych celów. W szerszym rozumieniu tego słowa, jest to także użycie Internetu do komunikowania się, propagandy i dezinformacji przez organizacje terrorystyczne[107]. Cyberterroryzm jako konwergencja terroryzmu i przestrzeni cybernetycznej zaczyna być postrzegany jako nowa broń masowego rażenia.

Zdecydowana większość ataków na systemy teleinformatyczne prowadzona jest przez hobbystów, nastolatków i ciekawskich sprawdzających swoje zdolności i możliwości. Jednakże zagrożenia płynące z takich zabaw są często trudne do wyobrażenia. Ataki takie mogą przerodzić się w zakłócenia systemów telekomunikacyjnych służb bezpieczeństwa (w tym służba zdrowia, straż, policja itp.), zakłóceń dzia-

---

[105] A. Bógdoł – Brzezińska, M. Gawrycki *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie,* Fundacja Studiów Międzynarodowych, Warszawa 2003.

[106] L. Ciborowski, *Walka informacyjna*, Toruń 1999.

[107] A. Bógdoł – Brzezińska, M. Gawrycki *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie,* Fundacja Studiów Międzynarodowych, Warszawa 2003.

łania zautomatyzowanych linii produkcyjnych (w tym np. zmiana receptur w fabrykach leków), zakłóceń działania powietrznej czy morskiej kontroli ruchu, kradzieży tożsamości, zakłóceń na rynkach finansowych[108] oraz wiele innych.

Pierwsze prace nad analizą zagrożeń związanych z atakami z cyberprzestrzeni przeprowadzono w roku 1996 przez naukowców skupionych wokół RAND Corporation. Przeprowadzono wówczas symulację, której nadano nazwę „The Day After ... in Cyberspace"[109]. W jej trakcie przeprowadzone w cyberprzestrzeni ataki doprowadziły do awarii sieci energetycznych na ogromną skalę, katastrof kolejowych oraz samolotowych, zniszczono systemy informacyjne amerykańskiej armii oraz sparaliżowano systemy bankowe doprowadzając do zachwiania światowego rynku finansowego. Symulacja ta pokazała, że istnieje możliwość sparaliżowania państwa tylko poprzez ataki w cyberprzestrzeni.

Kolejną symulację przeprowadził Komitet Połączonych Sztabów armii amerykańskiej w roku 1997. W ramach gry wojennej pod kryptonimem „Eligible Receiver" ponownie udowodniono, że możliwe jest wyłączenie systemów zasilania miast, wstrzymanie pracy rafinerii ropy naftowej czy przejęcie kontroli nad systemami lotów jedynie tylko poprzez walkę informacyjną oraz cyberataki.

Zagrożenia związane z cyberterroryzmem to grupa zagrożeń rozwijająca się najszybciej. Ze względu na anonimowość, niewielkie potencjalnie koszty ataków oraz ogrom możliwych skutków, są one na pierwszym miejscu zagrożeń globalnych dla bezpieczeństwa, nie tylko informacyjnego.

2.2.4. Awarie i uszkodzenia sprzętowe

Dzięki postępowi w technologii, awaryjność sprzętu komputerowego stale obniża się, wzrasta natomiast trwałość nośników danych. Nie jest jednak możliwe zbudowanie komputerów oraz sieci komputerowych pracujących bezawaryjnie. Ograniczoną trwałość mają wszystkie nośniki danych.

---

[108] www.terorismcentral.com/Newsletters/052602.html#FeatureArticle.

[109] Opis symulacji można odlaneźć w: R. C. Molander, A. S. Riddile, *S. A. Wilson Strategic Information Warfare: A New Face of War*, Santa Monica 1996.

Przyczynami wielu nieprawidłowości działania sprzętu (komputerów, mediów i urządzeń transmisyjnych) są błędy projektowe, wady produkcyjne, błędy instalacji oraz awarie[110].

Błąd projektowy występuje we wszystkich egzemplarzach danego wyrobu. **Wada produkcyjna** występuje w pojedynczym wyrobie lub w pewnej partii. **Błędy instalacji** mogą wynikać z braku doświadczenia, stosowania nieodpowiednich narzędzi i materiałów. **Awarie** są zwykle skutkiem pewnych zjawisk fizycznych, takich jak: nieodpowiednia temperatura, wilgotność, szkodliwe gazy, ładunki elektrostatyczne, pole elektromagnetyczne, nieprawidłowe parametry napięcia zasilającego, drgania i wstrząsy.

Ze względu na konstrukcję i zawieranie elementów mechanicznych, jednym z bardziej zawodnych podzespołów są pamięci dyskowe.

Decydując się na określoną technologię i nośnik przeznaczony do przechowywania danych, zwykle bierze się pod uwagę takie parametry, jak: pojemność, czas dostępu, prędkość transmisji. Ważnym, lecz rzadko uwzględnianym parametrem charakteryzującym pamięci zewnętrzne jest ich trwałość. Od trwałości nośnika, w dużym stopniu, zależy bezpieczeństwo (integralność i dostępność) zapisanych na nim danych. Wszystkie nośniki danych posiadają ograniczoną trwałość, zależną od wielu czynników takich jak technologia produkcji, jakość nośnika, warunki pracy, warunki przechowywania i transportu[111].

Używane aktualnie najpowszechniej magnetyczne i optyczne nośniki danych posiadają krótszą trwałość niż dobrej jakości papier lub celuloidowa taśma filmowa. Odpowiednio wyprodukowany i przechowywany papier nie ulegnie degradacji przez setki lat, natomiast trwałość nośników magnetycznych i optycznych szacuje się zwykle na 10 do 30 lat.

2.2.5. Emisja ujawniająca

Aby skutecznie zabezpieczyć system należy najpierw poznać istotę zagrożeń, na które jest on narażony. Przed opracowaniem poprawnych założeń ochrony elektromagnetycznej należy wiedzieć gdzie szukać źródeł tej emisji. Można spotkać się

---

[110] J. Stokłosa, T. Bilski, T. Pankowski, *Bezpieczeństwo danych w systemach informatycznych*, Wydawnictwo Naukowe PWN, Warszawa - Poznań 2001.

[111] Tamże, s. 23.

z opinią, że niemożliwe jest poprawne zbudowanie zabezpieczeń przed podsłuchem elektromagnetycznym bez pomocy specjalistów oraz drogiego sprzętu pomiarowego. Jednak znajomość przybliżonych odległości, z których taki podsłuch jest możliwy, pozwala na określenie chociażby potrzeb zastosowania ochrony elektromagnetycznej.

Każde urządzenie elektryczne jest źródłem emisji elektromagnetycznej. Wytwarzana przez te urządzania i emitowana dookólnie energia, stanowi źródło promieniowania, niosące część lub całość informacji użytkowej. W literaturze wyszczególniono dwie drogi rozprzestrzeniania się fal elektromagnetycznych z pracujących urządzeń: emisję promieniowaną – radiową (promieniowaną) i emisję przewodzenia[112].

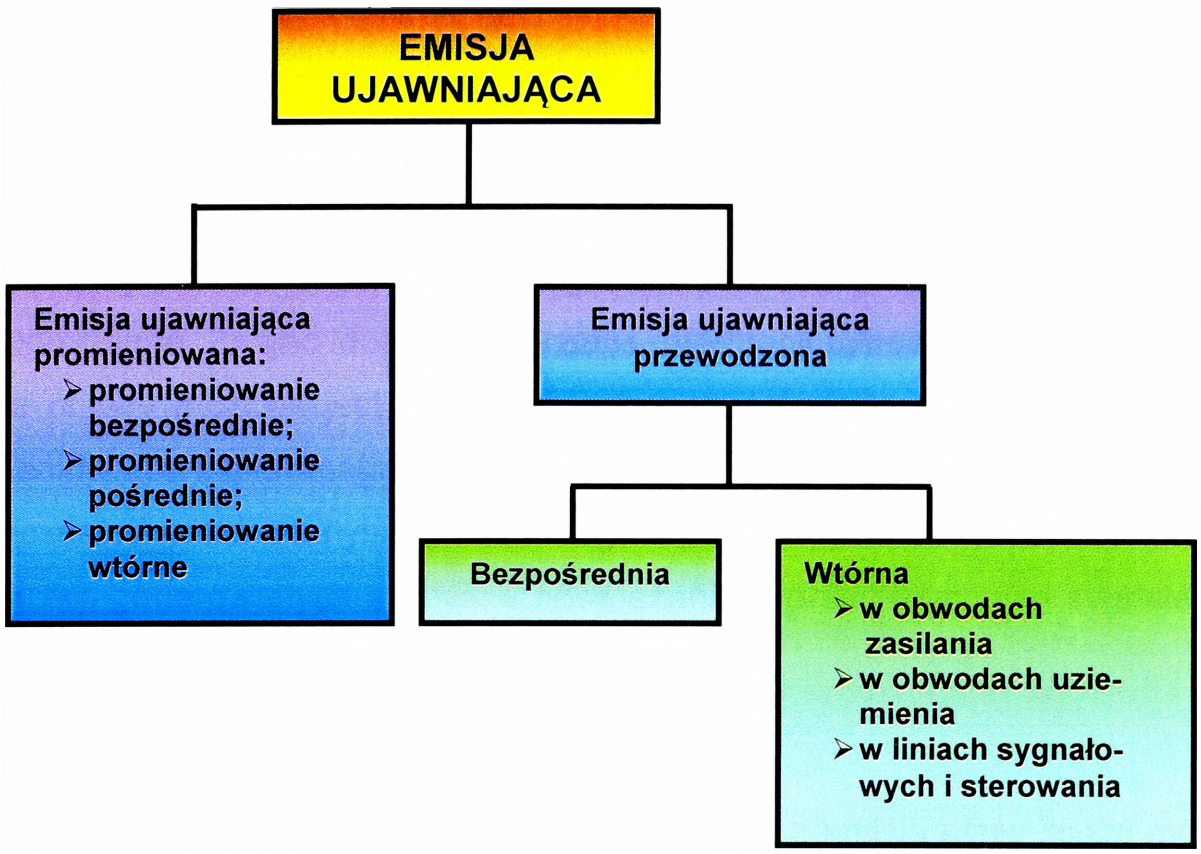
Emisja ujawniająca promieniowana, to emisja sygnałów przez indukowanie pola elektromagnetycznego w przestrzeni otaczającej urządzenia[113]. Można tu wyróżnić promieniowanie bezpośrednie, pośrednie, wtórne. Promieniowanie bezpośrednie jest wynikiem przestrzennej konfiguracji obwodów sygnałowych urządzenia, a promieniowanie pośrednie – niepożądanego oddziaływania na obwody modulacji nadajników. Zjawisko promieniowania wtórnego powstaje w wyniku oddziaływania zewnętrznego silnego pola elektromagnetycznego na nieliniowe elementy urządzenia. W wyniku tego oddziaływania następuje przeniesienie widma sygnału podstawowego (zawierającego informację) w wyższe pasmo częstotliwości. Zjawisko emisji wtórnej występuje w urządzeniach, w których zwykle nie stosuje się wystarczającego ekranowania i filtracji.

Emisja ujawniająca przewodzona, to emisja sygnałów w sieci zasilania, uziemienia oraz w obwodach sygnałowych. Emisję przewodzoną można podzielić na emisję bezpośrednią i wtórną. Przewodzona emisja bezpośrednia jest wynikiem sprzężenia galwanicznego i elektromagnetycznego obwodów sygnałowych z obwodami zasilania i uziemienia. Przewodzona emisja wtórna (podobnie jak promieniowana wtórna) jest wynikiem oddziaływania zewnętrznych sygnałów na nieliniowe układy obwodów zasilania, uziemienia i obwodów sygnałowych urządzeń.

---

[112] **Emisja przewodzenia** – emisja poprzez linie zasilające, sygnałowe, i inne niezamierzone kanały transmisyjne.

[113] Stokłosa J., Bilski T., Pankowski T., *Bezpieczeństwo danych w systemach informatycznych*, PWN Warszawa - Poznań 2001.



Rys. 2.1. Klasyfikacja emisji ujawniającej

Źródło: opracowanie własne na podstawie W. Aloks, C. Karpiński, A. Mencel, *Rola inżynierii kompatybilności elektromagnetycznej w procesie budowy systemów elektronicznych*, Biuletyn WAT, Warszawa 1995.

Wśród działań wykorzystujących zjawisko emisji ujawniającej do przechwycenia poufnych danych wyróżniamy atak bierny i atak aktywny.

Atak bierny to nic innego jak nasłuch fal elektromagnetycznych powstających podczas normalnej pracy systemu, bez ingerencji w jego działanie.

Atak aktywny natomiast to nasłuch radiowy połączony z ingerencją w podsłuchiwany system. Ingerencja taka ma na celu zwiększenie skuteczności podsłuchu i może polegać na zainstalowaniu w podsłuchiwanym systemie oprogramowania wprowadzającego jak największą ilość informacji do emitowanego pola elektromagnetycznego. Działania takie po pierwsze powodują utratę informacji, których utrata bez ingerencji nie była by możliwa, a po drugie zwiększają zasięg emisji ujawniającej.

Monitory kineskopowe

Najbardziej znanym źródłem emisji ujawniającej jest monitor komputerowy z lampą kineskopową. Komputery, bowiem to najczęściej wykorzystywane obecnie urządzenia do przetwarzania oraz archiwizacji danych. Głównymi elementami będącymi źródłem emisji dla monitora CRT to:

- końcowe stopnie tory luminacji,
- doprowadzenia sygnału luminacji do katody kineskopu,
- końcowe stopnie układów odświeżania,
- doprowadzenie sygnałów odświeżania do cewek oraz same cewki.

Rozwiązania techniczne przechwycenia obrazu z odległego monitora zostały już opracowane. Znając ideę przetwarzania informacji cyfrowej na dynamiczne i statyczne obrazy możliwe jest odtworzenie zawartości ekranu monitora na podstawie promieniowania elektromagnetycznego. Aby móc tego dokonać należy posiadać dane o częstotliwości odchylania poziomego i pionowego oraz mieć możliwość synchronizacji generowanych sygnałów odświeżania z przechwyconym sygnałem luminacji.

Wyświetlacze LCD

Powszechna jest opinia, że wszelkie problemy z emisja ujawniającą monitorów CRT możemy zlikwidować poprzez ich zamianę na wyświetlacze oparte o technologię LCD. Niestety nie jest to do końca prawda. Emisja ujawniająca wyświetlacza LCD związana jest ze sposobem sterowania poszczególnych punktów obrazu. W wyświetlaczach LCD sygnały sterujące doprowadzane są do elementów obrazu za pośrednictwem długich, cienkich ścieżek. W połączeniu z dużą impedancją pojedynczego elementu obrazu otrzymujemy sytuację charakteryzującą się dużym prawdopodobieństwem powstania anten liniowych. Dodatkowo w monitorach CRT możemy wyróżnić częstotliwość poziomą (częstotliwość zmiany kolumn), częstotliwość pionową (częstotliwość zmian wiersza) oraz częstotliwość punktową (częstotliwość, z jaką odświeżane są stany poszczególnych elementów obrazowych). Dlatego też technika obrazu z urządzeń wykorzystujących ekran LCD będzie podobna do używanej w przypadku monitorów CRT, a więc ich zastosowanie nie oznacza pełnego zabezpieczenia przez emisja ujawniającą.

Karta graficzna

Kolejnym podzespołem komputera odpowiedzialnym za przetwarzanie obrazów graficznych jest karta graficzna. Szczególnym źródłem emisji ujawniającej w przypadku karty graficznej jest przewód łączący kartę z monitorem. Jest to bardzo niebezpieczne źródło gdyż ze względu na swoje właściwości i rozmiary może się on stać naturalną anteną, która emituje sygnały nawet przy wyłączonym monitorze. Ist-

nieje, zatem niebezpieczeństwo wycieku informacji z urządzeń, w których użycie monitora może być sporadyczne (np. serwer).

Odtworzenie obrazu monitora oraz podsłuch promieniowania związanego z pracą karty graficznej to nie jedyny sposób dostępu do danych. Oprócz metod pasywnych system graficzny może być również inwigilowany w sposób aktywny. Zainstalowane szkodliwe oprogramowanie może przekazywać informacje pozyskane poprzez emisję ujawniającą podzespołów komputera (nie tylko monitora i karty graficznej).

Łącza typu RS – 232

Zastosowanie łączy typu RS – 232 nie kończy się na wykorzystaniu ich w komputerach klasy PC tj.: do łączenia urządzeń peryferyjnych z jednostka centralną. Interfejs ten wykorzystywany jest również do łączenia wszelkiego rodzaju czytników, w tym na przykład czytników kart magnetycznych i klawiatur do wprowadzania kodu PIN w bankomatach. Charakterystyka zastosowanej w standardzie łącza RS – 232 transmisji szeregowej pozwala nawet na odebranie sygnały przy użyciu zwykłego radiomagnetofonu, nagranie go na kasetę i analizowanie w miejscu bezpiecznym dla podsłuchującego.

Możliwość tak łatwego podsłuchu przesyłanych przez łącza RS – 232 danych jest niezwykle niebezpieczne. Należy, zauważyć, że o ile niemożliwe jest przechwycenie wpisywanych haseł i kodów PIN z monitora gdyż najczęściej wyświetlane są gwiazdki, to przez łącze RS – 232 dane te przesyłane są najczęściej w postaci jawnej.

Magistrale danych

Magistrala danych to najprościej mówiąc cyfrowa ścieżka łącząca podzespoły elektroniczne. W systemach komputerowych możemy odnaleźć wiele magistrali łączących elementy na różnych poziomach, łączących podzespoły znajdujące się na płycie głównej komputera, magistrala wejścia wyjścia jak również magistrale wewnątrz bardziej złożonych układów scalonych (magistrala wewnątrz procesora).

Najczęściej magistrala danych zrealizowana jest jako zespół cienkich, długich ścieżek łączących poszczególne układy. Cienkie ścieżki magistral, szczególnie w przypadku zakończenia ich dużą impedancją, mogą tworzyć niezamierzone anteny.

Poziom emisji magistrali danych, zarówno PCI, SCSI jak i wewnętrznych magistrali procesorowych może stanowić dominującą cześć emisji elektromagnetycznej całego systemu. Dodatkowo magistrale mogą być szczególnie podatne na przeprowadzenie ataku aktywnego.

2.3. Wnioski

W wyniku analizy będącej podsumowaniem niniejszego rozdziału, należy w sposób jednoznaczny stwierdzić, że nie można przewidzieć wszystkich zagrożeń bezpieczeństwa informacyjnego, a co się z tym wiąże, ryzyko ich wystąpienia można oszacować i zredukować, ale nie można go całkowicie wyeliminować.

Nieprzewidywalność zagrożeń wiąże się głównie z tym, że w większości przypadków, zagrożenia pochodzą z niezamierzonych działań ludzi mających zbyt mały zasób wiedzy, działających nieostrożnie i nieuważnie oraz którym brakuje wystarczającej praktyki i odpowiednio wysokiej świadomości o potencjalnych zagrożeniach.

Rozdział 3 – Bezpieczeństwo informacyjne w Siłach Zbrojnych RP

CEL BADAŃ

Celem badań zagadnień poruszanych w niniejszym rozdziale jest: **Klasyfikacja oraz charakterystyka podstawowych metod i środków zapewniających bezpieczeństwo informacyjne w Siłach Zbrojnych RP.**

GŁÓWNY PROBLEM BADAWCZY

Stosownie do przyjętego celu badań, problem badawczy sprowadza się do odpowiedzi na pytanie: **Jakimi środkami i metodami zapewniane jest bezpieczeństwo informacyjne w Siłach Zbrojnych RP?**

3.1. Rola bezpieczeństwa informacyjnego w zapewnieniu bezpieczeństwa państwa

Zapewnienie właściwego poziomu bezpieczeństwa informacji będących strategicznym zasobem zarówno w sferze cywilnej jak i wojskowej jest w obecnej rzeczywistości zadaniem niezwykle ważnym i jednocześnie ogromnie trudnym. Jego waga została zauważona w przyjętej w 2007 roku „Strategii bezpieczeństwa narodowego Rzeczypospolitej Polskiej"[114]. Bezpieczeństwo informacyjne i telekomunikacyjne zostało w niej zaliczone, obok bezpieczeństwa zewnętrznego, militarnego, wewnętrznego, obywatelskiego, społecznego, ekonomicznego i ekologicznego jako priorytetowe dla bezpieczeństwa państwa. Czym zatem jest bezpieczeństwo informacyjne skoro odgrywa tak istotna rolę?

Podstawowe rozumienie „bezpieczeństwa informacyjnego" obejmuje ochronę informacji stanowiącej tajemnicę służbową lub państwową[115]. Jest to jednak zbyt wielkie uproszczenie. Taka definicja nie odzwierciedla pełnego spektrum zagadnień mieszczących się w obszarze pojęciowym bezpieczeństwa informacyjnego. Wspo-

---

[114] www.bbn.gov.pl/dokumenty/SBN_RP.pdf.

[115] P. Bączek, *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Wydawnictwo Adam Marszałek, Toruń 2005.

mniana wyżej „Strategia bezpieczeństwa narodowego Rzeczypospolitej Polskiej" definiuje zakresy działań, które mają być swoistym drogowskazem dla organów odpowiedzialnych za zapewnienie bezpieczeństwa informacyjnego i telekomunikacyjnego państwa i wszystkich jego podmiotów. Do zasadniczych działań należy zaliczyć:

- skuteczne zapobieganie próbom destrukcyjnego oddziaływania na infrastrukturę telekomunikacyjną państwa oraz minimalizowanie skutków ewentualnych ataków oraz przywrócenie w krótkim czasie stanu pełnej jej funkcjonalności,
- tworzenie i rozwijanie długofalowych planów ochrony kluczowych systemów teleinformatycznych przed uzyskiwaniem dostępu do danych przez podmioty do tego niepowołane oraz zakłócaniem normalnego ich funkcjonowania, kradzieżami tożsamości i sabotażem,
- przeciwdziałanie przestępczości komputerowej oraz innym wrogim działaniom wymierzonym w infrastrukturę telekomunikacyjna, w tym zapobieganie atakom na jej elementy. Objęcie szczególnym nadzorem informacji przechowywanych i przekazywanych w postaci elektronicznej,
- zapewnienie należytego poziomu bezpieczeństwa, ze szczególnym uwzględnieniem elementów infrastruktury rządowej oraz sektora bankowego,
- zapewnienie dla administracji rządowej, sił zbrojnych i innych kluczowych instytucji państwowych systemu łączności opartego na najnowocześniejszych technologiach telekomunikacyjnych i najnowszych standardach bezpieczeństwa[116].

Podkreślenie roli sił zbrojnych jest tutaj znamienne. Trudno mówić o bezpiecznym państwie bez sprawnych, dobrze zorganizowanych i wyposażonych sił zbrojnych.

Bezpieczeństwo państwa to stan cechujący się brakiem zagrożeń terytorialnych, bezpieczeństwem obywateli oraz sprawnie działającymi władzami. W aspekcie bezpieczeństwa informacyjnego można określić, że sprowadza się do stanu w którym:

- nie są zagrożone strategiczne zasoby informacyjne państwa,
- władze podejmują decyzje dotyczące problematyki wewnętrznej i zewnętrznej w oparciu o prawdziwe, sprawdzone, wiarygodne i aktualne informacje, zaś organizacja ich przepływu nie jest zakłócana,

---

[116] Strategia bezpieczeństwa narodowego Rzeczypospolitej Polskiej, rozdział 3.8, strony 20÷21.

- bezpieczeństwo publicznych sieci teleinformatycznych, prawny system ochrony informacji oraz ochrona danych osobowych obywateli są z mocy prawa gwarantowane przez państwo,
- obywatele mają prawo do prywatności,
- instytucje zbierające informacje o obywatelach, organizacjach i ich działalności nie naruszają prawa,
- zapewniony jest właściwy, w określonym zakresie, dostęp do informacji dla obywateli i ich przedstawicieli.

Wzorując się na polskiej normie[117] można powiedzieć, że bezpieczeństwo informacyjne to takie działania prawne, organizacyjne i techniczne dające gwarancje zapewnienia informacji nienaruszalności jej pięciu podstawowych cech: poufności, integralności, dostępności, rozliczalności, autentyczności i niezawodności[118].

Osiągnięcie tak określonego stanu nie jest jednak procesem łatwym. Dla ułatwienia analizy całości problemu, racjonalnym wydaje się jego dekompozycja na poszczególne, specjalistyczne obszary. Do obszarów tych możemy zaliczyć uregulowania prawne, bezpieczeństwo osobowe (personalne), bezpieczeństwo fizyczne oraz wchodzące w obszar bezpieczeństwa technicznego bezpieczeństwo kryptograficzne, elektromagnetyczne i programowe[119]. Nie jest to katalog ani pełny, ani zamknięty.

W celu budowy modelu bezpieczeństwa informacyjnego Sił Zbrojnych RP, w dalszej części rozdziału scharakteryzowano wyszczególnione wyżej obszary.

---

[117] PN-I-13335-1: 1999 *Technika informatyczna - Wytyczne do zarządzania bezpieczeństwem systemów informatycznych - Pojęcia i modele bezpieczeństwa systemów informatycznych.*

[118] **POUFNOŚĆ**: dostęp do informacji musi być ograniczony jedynie do kręgu użytkowników uprawnionych;
INTEGRALNOŚĆ: informacja musi być zachowana w swej postaci oryginalnej, za wyjątkiem przypadków, gdy jest ona legalnie aktualizowana lub usuwana przez osoby uprawnione,
DOSTĘPNOŚĆ: informacja musi być dostępna dla uprawnionych użytkowników zawsze, kiedy mają taką potrzebę,
ROZLICZALNOŚĆ: dostęp użytkownika do informacji może być przypisany w sposób jednoznaczny tylko temu użytkownikowi,
AUTENTYCZNOŚĆ: tożsamość (pochodzenie) informacji lub podmiotu z nią związanego (np. wysyłającego informację) jest taka jak zadeklarowana,
NIEZAWODNOŚĆ: zachowanie i skutki działania (np. aplikacji bądź urządzeń zawierających informacje podlegające ochronie) są takie jak zamierzone. Bezpieczeństwo zasobów informacyjnych danej instytucji to nie tylko stosowanie

[119] J. Janczak, G. Świdzikowski, *Bezpieczeństwo informacji w wojskowym systemie telekomunikacyjnym*, Akademia Obrony Narodowej, Warszawa 2004, s. 39.

3.2. *Prawne uwarunkowania bezpieczeństwa informacyjnego*

Podstawą wszelkich działań, w tym działań w obszarze ochrony informacji są uwarunkowania i umocowania prawne. Podstawowym dokumentem regulującym te kwestie w polskim porządku prawnym jest *Ustawa z dnia 22 stycznia 1999 roku o ochronie informacji niejawnych*[120]. Jest ona wynikiem prac legislacyjnych mających na celu zapewnienie wymaganego poziomu ochrony informacji niejawnych w kontekście wejścia Polski do Sojuszu Północnoatlantyckiego. Jej opracowanie i wdrożenie było jednym z warunków koniecznych, artykułowanych przez partnerów Sojuszu, do podpisania traktatu akcesyjnego.

Poza Ustawą o ochronie informacji niejawnych regulacje oraz zasady ochrony informacji podczas współpracy między państwami członkowskimi Sojuszu uregulowane są w wielu dokumentach ratyfikowanych przez stronę polską. Kluczowym dokumentem jest *Umowa miedzy stronami Traktatu Północnoatlantyckiego w sprawie ochrony informacji z dnia 6 marca 1997 roku*[121].

Zawarte w Ustawie o ochronie informacji niejawnych unormowania dotyczą wszystkich aspektów istotnych z punktu widzenia ochrony informacji niejawnych. Dotyczą one ogólnych zasad ochrony informacji niejawnych, klauzul tajności, zasad prowadzenia postępowań sprawdzających, dostępu do informacji niejawnych, udostępniania informacji niejawnych, szkolenia w zakresie informacji niejawnych oraz metod zabezpieczenia. Regulacje te, wraz z dokumentami wykonawczymi (rozporządzenia, decyzje itp.) są poruszane w dalszej części pracy w odniesieniu do konkretnych metod i środków zapewniających bezpieczeństwo informacji. Dlatego też ich szczegółowy opis znajduje tam swoje miejsce.

Na podkreślenie natomiast zasługuje fakt, że problematyka ochrony informacji niejawnych znalazła swoje miejsce również w kodeksie karnym[122]. Określone w niniejszym dokumencie konsekwencje przestępstw przeciwko ochronie informacji podkreślają wagę oraz istotę zagadnienia. Najistotniejszymi z punktu widzenia ochrony informacji wydają się być przestępstwa przewidziane w Art. 265 i 266.

---

[120] Ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych, Dz.U. 1999 nr 11 poz. 95.

[121] Umowa między Stronami Traktatu Północnoatlantyckiego o ochronie informacji, sporządzona w Brukseli dnia 6 marca 1997 r., Dz.U. 2000 nr 64 poz. 740

[122] Ustawa z dnia 6 czerwca 1997 r., Kodeks karny (Dz. U. z dnia 2 sierpnia 1997 r.), Rozdział XXXIII - Przestępstwa przeciwko ochronie informacji.

Artykuł 265 §1 przewiduje podstawowy typ przestępstwa tj. ujawnienie lub wykorzystywanie wbrew przepisom tajemnicy państwowej, obciążając go karą pozbawienia wolności od 3 miesięcy do 5 lat. Przepis nie warunkuje sposobu wejścia w posiadanie informacji ani jej ujawnienia. Każda informacja w posiadanie, której wszedł użytkownik, a stanowiąca tajemnicę państwową podlega takiej samej ochronie. Nie ma również znaczenia forma ewentualnego jej ujawnienia. Tak samo traktowany jest przekaz w postaci dokumentu, przekaz ustny czy nośnik elektroniczny z nagranym dokumentem. Istotą rolę dla ustawodawcy ma, kto jest odbiorcą informacji. W przypadku, gdy informacje stanowiące tajemnicę państwową ujawniono osobie działającej w imieniu lub na rzecz podmiotu zagranicznego to zakres przewidywanej kary dla sprawcy zwiększa się w zakresie od 6 miesięcy do 8 lat[123]. Nieco łagodniejsze kary przewidziane są w przypadku nieumyślnego ujawnienia informacji. Osoby, które nieumyślnie ujawniają informacje stanowiące tajemnicę państwową podlegają grzywnie, karze ograniczenia wolności lub karze pozbawienia wolności do roku[124].

Ustawa oprócz ujawnienia przestępstwa przewiduje dodatkowo kary za nieuprawnione wejście w posiadanie informacji oraz jej niszczenie lub znaczące jej zmiany. Dla uzyskujący bez uprawnień informacji nie dla nich przeznaczonej poprzez otwarcie pisma, podłączenie się do przewodu służącego do przekazywania informacji lub przełamywanie ich elektronicznych magnetycznych lub innych zabezpieczeń podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2[125]. Takiej samej karze podlega nieuprawnione zdobywanie informacji przy pomocy przy pomocy urządzeń podsłuchowych wizualnych albo innych specjalnych[126].

Kary przewidziane są również dla przestępstw celowego zniszczenia, uszkodzenia, usunięciu lub zmiany na komputerowym nośniku informacji o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub administracji samorządowej albo gdy działania te uniemożliwiają automatyczne gromadzenie lub przekazywanie tych informacji. Czyny takie podlegają karze pozbawienia wolności od 6 miesięcy do 6 lat[127]. Natomiast, kto nie będąc do tego uprawnionym niszczy, uszkadza usuwa lub zmienia zapis istotnej informacji lub w inny sposób udaremnia lub w znacznym stopniu utrudnia osobie uprawnionej zapoznanie się z nią

---

[123] Tamże, Art. 265. § 2.

[124] Tamże, Art. 265. § 3.

[125] Tamże, Art. 267. § 1.

[126] Tamże, Art. 267. § 2.

[127] Tamże, Art. 269. § 1.

podlega karze grzywnie karze ograniczenia wolności albo pozbawienia wolności do lat 2[128]. W przypadku gdy czyn ten dotyczy zapisu na nośniku komputerowym przewidziana jest kara pozbawienia wolności do 3 lat[129].

Ostatnim niezwykle istotnym zapisem niniejszych przepisów jest regulacja dotycząca wyrządzenia znacznych szkód majątkowych w trakcie celowego niszczenia lub zniekształcania treści informacji. Czyn taki podlega karze pobawienia wolności od 3 miesięcy do 5 lat[130].

Wspomniane regulacje prawne oraz karne nie dają zapewne pełnego obrazu polskiego porządku prawnego w zakresie ochrony informacji. Nie miało ono, bowiem tego na celu. Przedstawione dwa podstawowe dokumenty, czyli Ustawa z dnia 22 stycznia 1999 roku o ochronie informacji niejawnych oraz Ustawa z dnia 6 czerwca 1997 r., Rozdział XXXIII - Przestępstwa przeciwko ochronie informacji, miało na celu przedstawienie podstaw prawnych organizacji ochrony informacji niejawnych oraz konsekwencji popełniania w tym obszarze przestępstw. Kwestie szczegółowe normowane są przez szczegółowe dokumenty wykonawcze. W związku z coraz to nowymi zagrożeniami, oraz ciągłą ewaluacją już rozpoznanych, są one stale aktualizowane i dostosowywane do bieżącej sytuacji.

3.3. Bezpieczeństwo osobowe

Regulacje Ustawy o ochronie informacji niejawnych wymuszają, aby każda osoba mająca dostęp do informacji niejawnych podlegała procedurze weryfikacji. Obowiązujące prawo nie pozawala, bowiem na dostęp do informacji niejawnych tylko z tytułu posiadanego stopnia, piastowania stanowiska czy specjalnych przywilejów. Od tego normatywu ustawodawca przewidział jednak pewne, wyszczególnione w Art. 27 Ustawy, odstępstwa. Na jego mocy, procedurze postępowania sprawdzającego nie są poddawani między innymi: Prezydent RP, Marszałek Sejmu RP, Marszałek Senatu RP, Prezes Rady Ministrów, członków Rady Ministrów oraz Prezesa Sądu Najwyższego.

---

[128] Tamże, Art. 268. § 1.

[129] Tamże, Art. 268. § 2.

[130] Tamże, Art. 268. § 3.

Postępowanie sprawdzające ma na celu ustalenie czy osoba podlegająca sprawdzeniu daje rękojmię[131] zachowania tajemnicy, a w szczególności rozwianie wątpliwości dotyczących:

- możliwego uczestnictwa, współpracy lub popierania przez osobę sprawdzaną działalności szpiegowskiej, terrorystycznej albo innej wymierzonej przeciwko RP,
- ukrywania lub podawania niezgodnych z prawdą informacji mających znaczenie dla ochrony informacji niejawnych, a także występowania związanych z tą osobą okoliczności powodujących ryzyko jej podatności na szantaż lub wywieranie presji,
- przestrzegania przez sprawdzanego porządku konstytucyjnego RP,
- zagrożenia osoby sprawdzanej ze strony obcych służb specjalnych w postaci werbunku lub nawiązania z nią kontaktu, a zwłaszcza obawy o wywieranie w tym celu presji,
- właściwego postępowania z informacjami niejawnymi,
- wyraźnych różnic między poziomem życia, a uzyskiwanymi dochodami,
- informacjami dotyczącymi ewentualnych chorób psychicznych lub innych zakłóceń czynności psychicznych ograniczających sprawność umysłową ograniczających zdolność osoby sprawdzanej do wykonywania obowiązków na danym stanowisku lub prac związanych z dostępem do informacji stanowiących tajemnicę państwową,
- uzależnień od alkoholu lub narkotyków[132].

Postępowanie sprawdzające zakończone jest wydaniem lub odmową wydania poświadczenia bezpieczeństwa uprawniającego do dostępu do informacji niejawnych.

W zależności od stanowiska, o które ubiega się dana osoba prowadzone jest wobec niej jedno z postępowań: postępowanie zwykłe, poszerzone lub specjalne.

Postępowanie zwykłe prowadzone jest wobec osób ubiegających się o stanowiska związane z dostępem do informacji stanowiących tajemnicę służbową (o klauzu-

---

[131] **Rękojmia** oznacza spełnienie ustawowych wymogów dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem m.in. niekaralność za przestępstwa umyślne ścigane z oskarżenia publicznego, brak nałogów lub dolegliwości psychicznych, posiadanie majątku nieprzekraczającego uzyskiwanych dochodów, brak związków z osobami z tzw. grup ryzyka (np. grupy przestępcze).

[132] Ustawa z dnia 22 stycznia 1999 roku o ochronie informacji niejawnych, Art. 35. ust. 1.

lach „zastrzeżone" i „poufne"). Postępowanie takie prowadzone jest przez pełnomocnika ochrony na pisemne polecenie kierownika danej instytucji. Poświadczenie wystawione na podstawie przeprowadzonego zwykłego postępowania sprawdzającego upoważnia do dostępu do informacji niejawnych o klauzuli „zastrzeżone" lub „poufne" przez okres 10 lat.

Poszerzone i specjalne postępowania sprawdzające prowadzone są na wniosek osoby upoważnionej, którą najczęściej jest osoba upoważniona na podstawie przepisów do obsady danego stanowiska, przez Służbę Kontrwywiadu Wojskowego oraz Agencję Bezpieczeństwa Wewnętrznego.

Służba Kontrwywiadu Wojskowego dokonuje sprawdzenia wobec:

- żołnierzy pozostających w czynnej służbie wojskowej i pracowników wojska,
- przedsiębiorców, jednostek naukowych lub badawczo – rozwojowych, a także innych jednostkach organizacyjnych, w zakresie, w jakim realizują one produkcję lub usługi, stanowiące tajemnicę państwową,
- przedsiębiorców zajmujących się obrotem wyrobami, technologiami i licencjami objętymi tajemnicą państwową, jeżeli uczestnikami tego obrotu są SZ RP lub jednostki organizacyjne podległe Ministrowi Obrony Narodowej,
- wojskowych organach ochrony prawa i wojskowych organach porządkowych[133].

W przypadkach innych niż wymienione powyżej, organem właściwym do prowadzenia poszerzonych i specjalnych postępowań sprawdzających, jest Agencja Bezpieczeństwa Wewnętrznego.

Tak samo jak w przypadku postępowania zwykłego, również efektem zakończenia postępowania poszerzonego lub specjalnego jest wydanie lub odmowa wydania poświadczenia bezpieczeństwa. W przypadku odmowy zainteresowanemu przysługuje odwołanie w trybie i na zasadach szczegółowo określonych w Ustawie.

Poświadczenie wystawione na podstawie poszerzonego postępowania sprawdzającego upoważnia do dostępu do informacji stanowiących tajemnicę państwową o klauzuli „tajne" przez okres 7 lat oraz do informacji niejawnych o klauzuli „zastrzeżone" lub „poufne" przez okres 10 lat. Natomiast poświadczenie wystawione na podstawie specjalnego postępowania sprawdzającego dodatkowo upoważnia przez 5 lat do dostępu do informacji niejawnych oznaczonych klauzulą „ściśle tajne".

---

[133] Tamże, Art. 29. pkt 1).

Wydanie poświadczenia bezpieczeństwa nie kończy jednak możliwości weryfikacji osoby, która je otrzymała. W przypadku, gdy w stosunku do takiej osoby zostały ujawnione nowe fakty wskazujące na to, że nie daje ona rękojmi zachowania tajemnicy, służby ochrony państwa lub pełnomocnik ochrony, po poinformowaniu osoby odpowiedzialnej za obsadę stanowiska, przeprowadzają kontrolne postępowanie sprawdzające. Postępowanie kontrolne kończy się wydaniem decyzji o cofnięciu poświadczenia bezpieczeństwa albo informacją skierowaną do osoby odpowiedzialnej za obsadę stanowiska o braku zastrzeżeń, co do rękojmi zachowania tajemnicy przez sprawdzanego.

Nieodzownym elementem bezpieczeństwa osobowego, zwanego także bezpieczeństwem personalnym, jest posiadanie przez osoby upoważnione do dostępu do informacji niejawnych odpowiedniego poziomu wiedzy z tego zakresu. Nie jest możliwym dopuszczenie do prac związanych z dostępem do informacji niejawnych bez przejścia szkolenia z zakresu obowiązujących przepisów, zagrożeń ze strony obcych służb specjalnych i organizacji terrorystycznych, zasad i sposobów ochrony informacji oraz odpowiedzialności karnej, dyscyplinarnej i służbowej za naruszenie przepisów o ochronie informacji.

Poza wspomnianym powyżej obowiązkowym szkoleniu wstępnym, na kierownikach komórek organizacyjnych ciąży obowiązek, poprzez pełnomocników ochrony, prowadzenia ciągłej działalności uświadamiającej, szkoleniowej i edukacyjnej [134] z zakresu ochrony informacji. Poszczególne programy powinny być zróżnicowane i uwzględniające specyfikę stanowisk, posiadaną przez pracowników wiedzę oraz ich zaawansowanie i umiejętności. Zróżnicowanie stanowisk dotyka kolejnej fundamentalnej z punktu widzenia ochrony informacji zasady wiedzy koniecznej (ang. need to know). Należy, bowiem mieć na uwadze, że zazwyczaj najsłabszym ogniwem w systemie ochrony informacji jest człowiek. Nie ma nic groźniejszego niż nielojalny, sfrustrowany i zdecydowany, aby szkodzić pracownik, mający dzięki dostępowi do informacji świetne narzędzie do tego celu działań.

Zapewnienie pełnego bezpieczeństwa osobowego jest wręcz niemożliwe. Trudno, bowiem przewidzieć wszystkie ewentualne zagrożenia mogące płynąć ze strony osób, których wykonywanie obowiązków związane jest z dostępem do informacji nie-

---

[134] J. Janczak, G. Świdzikowski, *Bezpieczeństwo informacji w wojskowym systemie telekomunikacyjnym*, Akademia Obrony Narodowej, Warszawa 2004, s. 44.

jawnych. Można jednak dążyć do osiągnięcia poziomu z akceptowalnym poziomem ryzyka. Aby to osiągnąć należy prowadzić przemyślana politykę opartą na kilku zasadach:

1. Opracowanie procedury pozyskiwania nowych pracowników w oparciu o przygotowane wymagania dotyczące zarówno kwalifikacji jak i predyspozycji psychofizycznych.
2. Prowadzenie stabilnej polityki kadrowej minimalizującej częste zmiany kadrowe na kluczowych stanowiskach oraz stanowiskach wymagających szczególnych kwalifikacji (np. specjalistycznych kursów, dostępu do tajemnicy państwowej o klauzuli „ściśle tajne" itp.).
3. Właściwie dobrany i rzetelnie realizowany program wewnętrznych szkoleń uwzględniających nowe zagrożenia oraz wdrażane technologie.
4. Ciągły nadzór nad personelem, okresowe kontrole wiedzy i egzekwowanie jej wysokiego poziomu, bieżące prowadzenie akcji uświadamiających i edukacyjnych.

3.4. Bezpieczeństwo fizyczne

Fizyczne środki ochrony informacji należą do najpowszechniej stosowanych i obejmują wiele, bardziej lub mniej, zaawansowanych technologicznie metod. Do metod tych zalicza się zarówno zamki i kraty jak i skomplikowane, sprzężone niejednokrotnie z czytnikami linii papilarnych, siatkówki oka, wagami ciała i innymi urządzeniami, komputerowe systemy monitoringu.

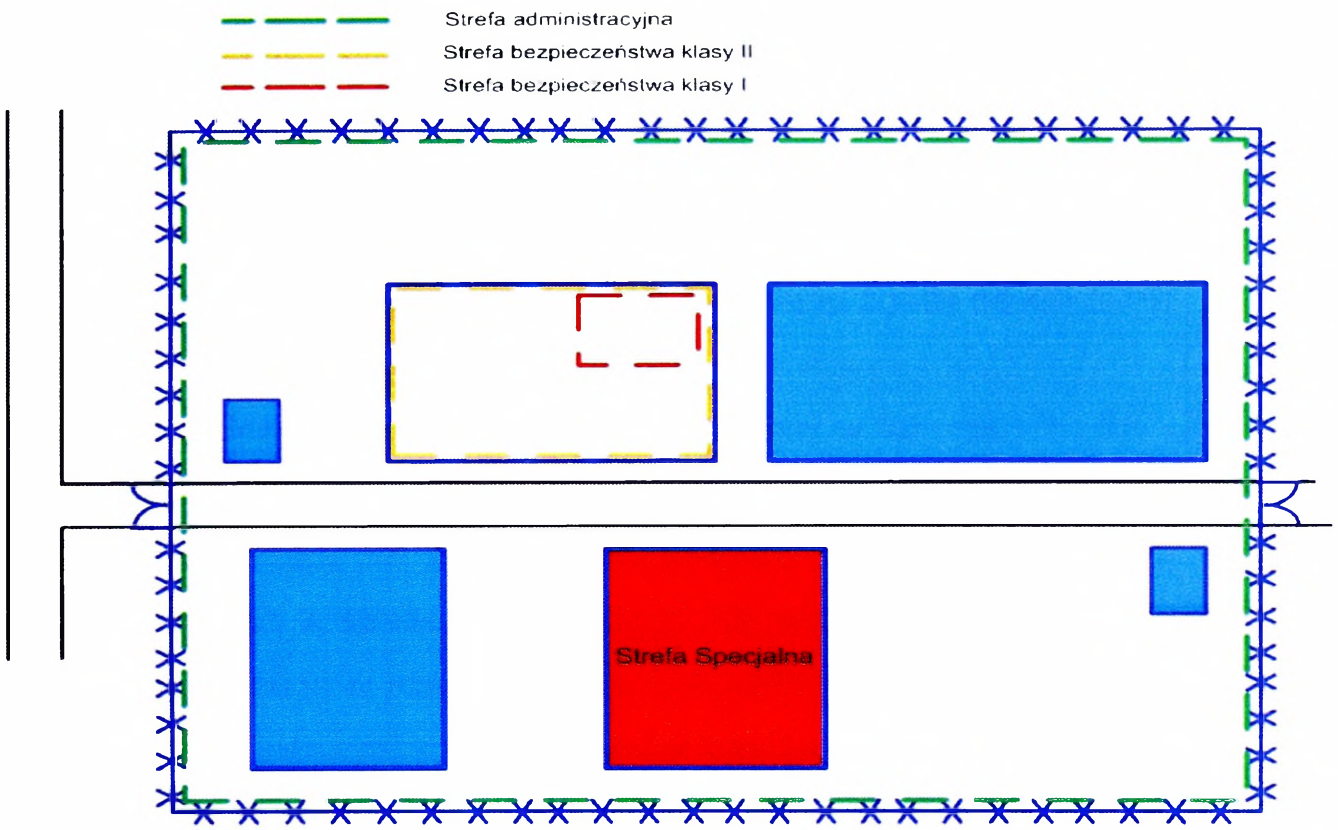
Można, zatem powiedzieć, że pojęcie bezpieczeństwa fizycznego obejmuje bardzo szeroki zestaw działań i środków zapewniających ochronę informacji niejawnych od wytworzenia, aż do zniszczenia lub zarchiwizowania[135].

Ochroną i szczególnym nadzorem należy (zgodnie z obowiązującymi przepisami) objąć w różnym stopniu wydzielone pomieszczenia, budynki w których się one znajdują oraz otaczający teren. Obszar i zakres ochrony uzależniony jest w głównej mierze od ilości oraz klauzul przechowywanych informacji oraz potencjalnych zagrożeń. Do zasadniczych zagrożeń, które powinny być brane pod uwagę

---

[135] P. Bączek, *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Wydawnictwo Adam Marszałek, Toruń 2005.

w trakcie organizacji stref bezpieczeństwa należy zaliczyć możliwość działanie służb specjalnych, zamach terrorystyczny i sabotaż, kradzież i zniszczenie materiałów, nieuprawnione próby wejścia oraz nieuprawniony dostęp przez pracowników do materiałów oznaczonych wyższą klauzulą tajności.



Rys 3.1. Przykład rozmieszczenia stref bezpieczeństwa

Źródło: Opracowanie własne

W celu zminimalizowania lub nawet całkowitego wyeliminowania zagrożeń obiekty podlegające ochronie oraz teren, na którym są one położone dzielony jest na specjalne strefy o różnym poziomie zabezpieczeń (rys. 3.1.). W obiektach lub pomieszczeniach wymagających szczególnej kontroli wejść oraz wyjść oraz kontroli przebywania organizuje się **strefy bezpieczeństwa**. Strefy te w zależności od wymagań dzielone są na I Strefę Bezpieczeństwa, II Strefę Bezpieczeństwa oraz Specjalne Strefy Bezpieczeństwa. Wokół stref bezpieczeństwa należy wydzielić **strefę administracyjną**.

Celem wydzielania **strefy administracyjnej** jest wprowadzanie nadzoru osób oraz pojazdów wchodzących i wjeżdżających do strefy oraz ją opuszczających. Strefa administracyjna może być wydzielona zarówno w budynku lub jego części jak i na

większym, zabezpieczonym terenie. Wydzielenie strefy administracyjnej wiąże się z koniecznością organizacji systemu przepustkowego lub innego systemu dającego możliwość nadania uprawnień do wejścia i przebywania w strefie.

Rodzaj wydzielanej strefy bezpieczeństwa jest uzależniony głównie od potencjalnych możliwości dostępu do informacji niejawnych.

I Strefa Bezpieczeństwa to obszar chroniony w taki sposób, że wejście do niego oznacza możliwość bezpośredniego dostępu do informacji niejawnych. Osoby upoważnione do dostępu do informacji niejawnych, co najmniej o klauzuli informacji przechowywanych w strefie, a nie będący żołnierzami albo pracownikami jednostki organizacyjnej, mogą w niej przebywać wyłącznie pod nadzorem żołnierza lub pracownika pionu ochrony po wcześniejszym uzyskaniu zgody od kierownika danej jednostki organizacyjnej.

II Strefa Bezpieczeństwa to obszar chroniony w taki sposób, że wejście do tej strefy nie oznacza bezpośredniego dostępu do informacji niejawnych. Osoby upoważnione do dostępu do informacji niejawnych, co najmniej o klauzuli informacji przechowywanych w strefie, a nie będący żołnierzami albo pracownikami jednostki organizacyjnej, mogą w niej przebywać bez nadzoru jednak po wcześniejszym uzyskaniu zgody od kierownika danej jednostki organizacyjnej.

W przypadku gdy istnieje konieczność zapewnienia ochrony informacji niejawnych stanowiących tajemnicę państwową, a w szczególności w przypadku prowadzenia rozmów i spotkań organizuje się Specjalne Strefy Bezpieczeństwa. Strefy takie podlegają stałej kontroli oraz wymagają zastosowania urządzeń oraz środków zabezpieczających przed podsłuchem i podglądem. Do Specjalnej Strefy Bezpieczeństwa obowiązuje zakaz wnoszenia przedmiotów i urządzeń bez uprzedniego ich sprawdzenia przez upoważnionego pracownika pionu ochrony.

Dostęp do wydzielonych stref z definicji możliwy jest wyłącznie dla osób posiadających odpowiednie uprawnienia. Kontrola dostępu może być realizowana przez wiele, bardziej lub mniej zawansowanych technologicznie sposobów. Najprostszym jaki można przyjąć, to zorganizowanie systemu przepustowego oraz zorganizowanie systemu ochrony uwzględniającego fizyczne (przez wartownika lub pracownika ochrony) kontrolowanie przepustek u osób wchodzących lub opuszczających daną strefę.

Udoskonalonym sposobem kontroli przepustek jest system oparty o karty magnetyczne i ich czytniki. Wejście do strefy chronionej następuję po uwierzytelnieniu

osoby na podstawie danych zakodowanych na karcie, lub w nowszych wersjach opartych o technikę mikroprocesorową, przez czytniki połączone z systemem wejścia – wyjścia. W przypadku pozytywnej weryfikacji system zezwala na wejście (wyjście) na przykład poprzez otwarcie magnetycznego zamka w drzwiach. Rozwiązania tego typu są jednak obarczone ryzykiem związanym ze zgubieniem, kradzieżą lub podrobieniem karty. Poziom bezpieczeństwa można zwiększyć poprzez na przykład zintegrowanie systemu odczytu karty z identyfikacją na podstawie hasła lub kodu PIN.

Rozwiązania bardziej zaawansowanych systemów kontroli dostępu polegają zwykle na metodach opartych o wiedzę użytkownika lub identyfikatory materialne oraz metody biometryczne. Największą efektywnością wykazuję się systemy stanowiące kompilację kilku sposobów opartych na powyższych metodach.

Do metod opartych na wiedzy użytkownika najczęściej stosowaną jest metoda autoryzacji wejścia poprzez hasło lub kod PIN. Warunkiem skuteczności tej metody jest przestrzeganie kilku, mogących wydawać się banalnymi, zasad. Przede wszystkim hasła i kody PIN należy chronić przed ujawnieniem innym osobom, a zwłaszcza współpracownikom również posiadającym dostęp do strefy. Właściwie zorganizowany system monitoringu pozwala na odtworzenie, wszystkich autoryzowanych hasłami i kodami, wejść i wyjść do i ze strefy. W przypadku korzystania z kodów przypisanych w systemie monitorującym innej osobie, do właściwej identyfikacji koniecznym staje wykonanie dodatkowych sprawdzeń np. zapisów z kamer itp.

Najbardziej zaawansowanymi i dającymi najwyższy poziom bezpieczeństwa są systemy rozpoznające dane biometryczne użytkownika. Cechami które najczęściej stosowane są do uwierzytelniania należą linie papilarne, kształt twarzy lub dłoni, rysunek tęczówki oka lub głos. Wykorzystywane są również takie cechy jak na przykład waga, dzięki kontroli której można uniknąć wejścia osób trzecich wraz z użytkownikami uprawnionymi.

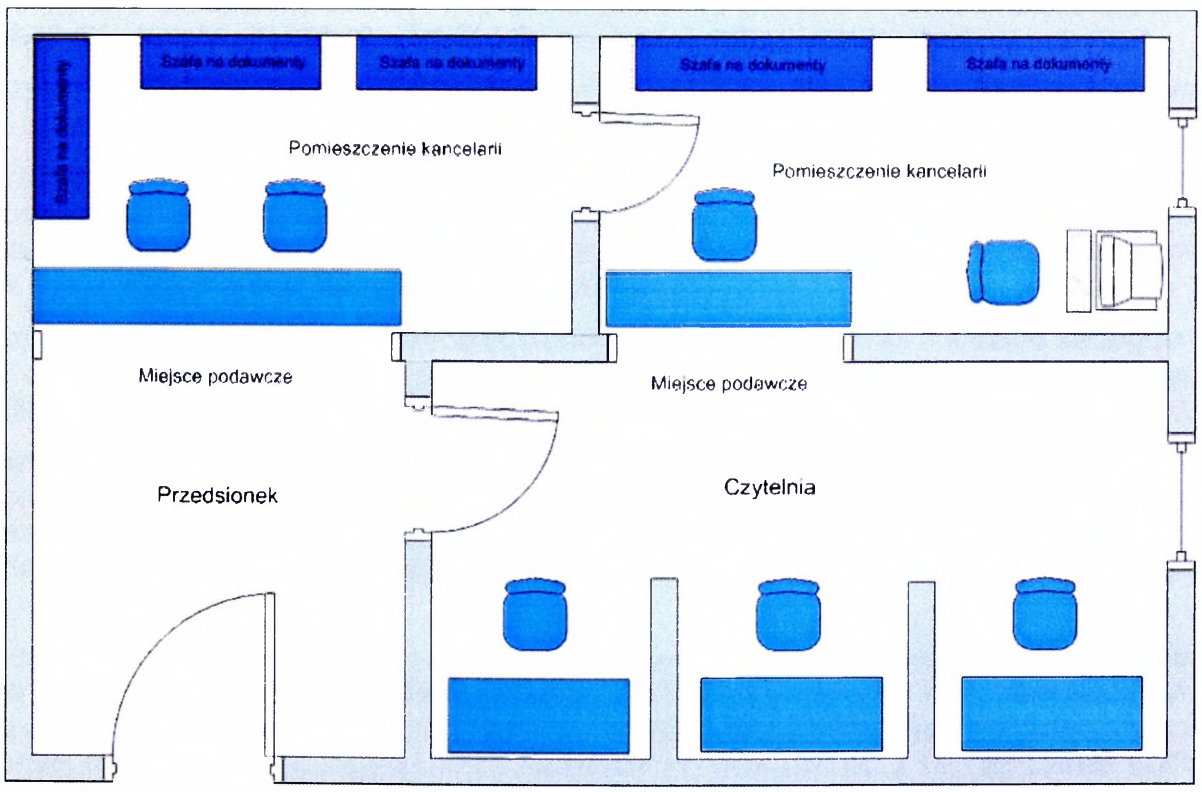
Korzystanie z systemów dostępu opartych na metodzie porównania cech osoby ubiegającej się o autoryzację z cechami indywidualnymi zapisanymi w systemie, rodzi potrzebę zebrania pełnej bazy danych tych drugich. Zebrane, właściwie pomierzone i zweryfikowane cechy indywidualne są w bezpieczny sposób przechowywane w systemie. W procesie autoryzacji są one porównywane z odczytem. W przypadku niektórych cech (jak na przykład waga) procedura porównawcza powinna uwzględniać dopuszczalny poziom niezgodności ze wzorcem. Zakres tolerancji powinien być jednak wielkością zamykającą się maksymalnie w kilku procentach, aby nie utracić

pełnej wiarygodności pomiaru i nie dopuścić do wejścia nieautoryzowanych użytkowników.

3.4.1. Fizyczne zabezpieczenia kancelarii tajnych

W każdej jednostce organizacyjnej, w której są wytwarzane, przetwarzane, przekazywane lub przechowywane dokumenty oznaczone klauzulą „poufne" lub stanowiące tajemnicę państwową organizuje się kancelarię tajną. Jest to wyodrębniona komórka organizacyjna podległa bezpośrednio pełnomocnikowi ochrony i odpowiedzialna za właściwe rejestrowanie, przechowywanie oraz obieg i wydawanie dokumentów osobom do tego uprawnionym.

Kancelarie mogą być organizowane w zależności od zadań oraz typy dokumentacji jako kancelarie tajne-zagraniczne, kancelarie tajne i biblioteki tajne. Ponadto, w przypadku, gdy istnieje konieczność przyjmowania, wytwarzania, przechowywania lub przekazywania w danej jednostce organizacyjnej dokumentów planowania mobilizacyjnego, operacyjnego lub gotowości bojowej organizuje się kancelarię mobilizacyjną. W dalszych rozważaniach pod pojęciem „kancelarii" należy rozumieć wszystkie powyższe komórki.



Rys 3.2. Przykład rozmieszczenia pomieszczeń kancelarii tajnej
Źródło: Opracowanie własne

Ze względu na swoja specyfikę, wymogi w stosunku do organizacji, funkcjonowania i zabezpieczenia pomieszczeń do przyjmowania, wytwarzania, przechowywania lub przekazywania są wysokie i ściśle przez ustawodawcę określone[136].

Zasadnicze wymagania, co do fizycznego zabezpieczenia kancelarii tajnych skupiają się wokół wymagań budowlanych, jakie musi spełniać pomieszczenie, w którym jest ona zlokalizowana, a także wymagań, co do zabezpieczenia drzwi, okien oraz wyposażenia kancelarii.

Kancelarie lokalizuje się w pomieszczeniach spełniających następujące wymagania bezpieczeństwa:

- usytuowanych w budynku, z wyjątkiem poddaszy, o konstrukcji murowanej, betonowej lub innej o podobnych właściwościach (parametrach) konstrukcyjnych, z wejściem co najmniej ze strefy administracyjnej lub w pomieszczeniach oddzielonych od innych pomieszczeń stałymi przegrodami budowlanymi o rozwiązaniach konstrukcyjno-materiałowych zapewniających bezpieczeństwo pożarowe i bezpieczeństwo konstrukcji[137],
- wyposażonych w drzwi wejściowe stalowe lub drewniane o wymaganej konstrukcji zabezpieczone przed włamaniem i wyposażonym w specjalne zamki[138],

---

[136] Ustawa z dnia 22 stycznia 1999 roku o ochronie informacji niejawnych, Rozdział 7 – Kancelarie tajne. Kontrola obiegu dokumentów, Rozdział 9 – Środki ochrony fizycznej informacji niejawnych.

Rozporządzenie Rady Ministrów z dnia 18 października 2005 r. w sprawie organizacji i funkcjonowania kancelarii tajnych.

Zarządzenie Nr 25/ MON Ministra Obrony Narodowej z dnia 17 listopada 2005 r. w sprawie szczególnego sposobu organizacji kancelarii tajnych oraz innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za rejestrowanie, przechowywanie, obieg i udostępnianie materiałów niejawnych, stosowania środków ochrony fizycznej oraz obiegu informacji niejawnych.

Rozporządzenie Ministra Obrony Narodowej z dnia 21 czerwca 2007 roku w sprawie szczegółowych zadań pełnomocników ochrony oraz szczególnych wymagań w zakresie ochrony fizycznej jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych.

[137] Pozbawionych zbędnych otworów, a w przypadku, gdy ściany zewnętrzne lub stropy stanowią granicę strefy bezpieczeństwa, powinny być wykonane z materiałów niepalnych i spełniać wymagania w zakresie klasy odporności pożarowej oraz nośności granicznej odpowiadającej co najmniej konstrukcji murowanej z cegły pełnej klasy 15, o grubości 25 cm lub konstrukcji betonowej o grubości co najmniej 15 cm.

[138] Drzwi wejściowe stalowe lub drewniane pełne o grubości co najmniej 4 cm, obustronnie obite blachą stalową o grubości co najmniej 2 mm, blokowane na 4 krawędziach, zabezpieczone przed wyłamaniem od strony zawiasów, wyposażone w dwa zamki, w tym jeden mechaniczny o skomplikowanym mechanizmie, a drugi szyfrowy, o zmiennym nastawieniu, z tym że zamek szyfrowy powinien być co najmniej trzyzapadkowy, o cichym przesuwie, skali nastawień nie większej niż jedna działka, posiadający co najmniej 100 podziałek na pokrętle, a zmiana kombinacji w zamku szyfrowym powinna być blokowana i uaktywniana kluczem od tyłu skrzynki zamka, zaś drzwi powinny posiadać element samozatrzaskowy uniemożliwiający pozostawienie pomieszczenia otwartego.

– okna zabezpieczone w zależności od wysokości na jakiej się znajdują w stosunku do powierzchni ziemi[139].

Organizacja kancelarii powinna umożliwiać bezkonfliktową pracę personelu kancelarii, przechowywanie dokumentów oraz możliwość ich udostępnienia na miejscu interesantom. Dlatego też oprócz pomieszczeń kancelaryjnych, powinna się ona również składać z czytelni.

Bezpieczeństwo zagwarantowane właściwie dobranymi rozwiązaniami konstrukcyjno – budowlanymi należy wesprzeć elektronicznymi środkami ochrony. Tego rodzaju zabezpieczenia pozwalają na kompleksową ochronę pomieszczeń, a mówiąc bardziej szczegółowo zapewnić natychmiastowe zaalarmowanie w przypadku naruszenia systemu bezpieczeństwa. Do zasadniczych i wykorzystywanych powszechnie rozwiązań w tej dziedzinie zalicza się czujki otwarcia okien i drzwi, czujki zbicia szyb w oknach, czujki ruchu instalowane wewnątrz pomieszczeń, czujki wstrząsowe, przeciwpożarowe, czytniki kontroli dostępu (karty magnetyczne, czytniki biometryczne, zabezpieczenie kodami PIN itp.)[140] oraz system monitoringu telewizyjnego. Ten ostatni powinien pozwalać na kontrolę (wraz z zapisem) wejść do pomieszczeń.

Istotnym elementem systemu monitoringu jest właściwe umieszczenie centrali alarmowej. Powinna się ona znajdować również w strefie bezpieczeństwa, a przynajmniej w strefie administracyjnej, aby nie była narażona na dostęp osób postron-

---

[139] Okna zabezpieczone w sposób uniemożliwiający wgląd do pomieszczeń z zewnątrz z zainstalowanymi w otworach okiennych kratami wykonanymi w ramie z płaskownika stalowego o przekroju nie mniejszym niż 45x6 mm, z prętów stalowych o średnicy co najmniej 20 mm, usytuowanymi pionowo w rozstawie nie większym niż 150 mm, wzmocnionymi płaskownikami stalowymi o przekroju nie mniejszym niż 45x6 mm, usytuowanymi w poziomie, w odstępach nie większych niż 500 mm, z tym że jeżeli ze względów architektoniczno – budowlanych nie ma możliwości zainstalowania kraty, dopuszcza się zamontowanie okna antywłamaniowego, wyposażonego w szyby co najmniej klasy P-6, a rama i szyby powinny posiadać świadectwa kwalifikacyjne. Otwory okienne, których dolna krawędź znajduje się na wysokości powyżej 5 m od poziomu otaczającego terenu, lub górna krawędź więcej niż 3 m od poziomu dachu, wyposaża się w siatkę stalową o grubości drutu nie mniejszej niż 2 mm o oczkach nie większych niż 20x20 mm, folię antywłamaniową lub szyby o podwyższonej odporności na stłuczenie.

[140] Zgodnie z Zarządzeniem Nr 25/ MON Ministra Obrony Narodowej z dnia 17 listopada 2005 r. w sprawie szczególnego sposobu organizacji kancelarii tajnych oraz innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za rejestrowanie, przechowywanie, obieg i udostępnianie materiałów niejawnych, stosowania środków ochrony fizycznej oraz obiegu informacji niejawnych instalowane systemy powinny spełniać parametry określone w Normie Obronnej NO-04-A004 Obiekty Wojskowe. Systemy Alarmowe oraz odpowiadać następującym klasom: SA4 – w przypadku przechowywania dokumentów zawierających informacje niejawne oznaczone klauzulą „Ściśle tajne" oraz SA3 – w przypadku przechowywania dokumentów zawierających informacje niejawne oznaczone klauzulą „Tajne" i „Poufne".

nych. Centrala, a najlepiej centrum monitoringu, powinna umożliwiać monitorowanie wszystkich zainstalowanych systemów począwszy od napadu i włamania na pożarze kończąc. Niebagatelną rolę odgrywa opracowanie zapewniających skuteczność procedur reagowania na zaistniałe incydenty. Powinny one uwzględniać specyfikę ochranianych obiektów i co najważniejsze powinny być znane i stosowane przez nadzorujący personel.

Przechowywanie dokumentów w sposób zapewniający im pełne bezpieczeństwo wymaga, poza przechowywaniem ich w strefach bezpieczeństwa, zastosowania szaf stalowych. W zależności od nadanej klauzuli, dokumenty należy przechowywać w szafach stalowych klasy „A" – dokumenty o klauzuli „zastrzeżone", klasy „B" – dokumenty o klauzuli „tajne" i „poufne" oraz klasy „C" – dokumenty o klauzuli „ściśle tajne".

3.5. Bezpieczeństwo programowe

Bezpieczeństwo programowe zasobów informacji najczęściej sprowadza się do ich ochrony przed złośliwym oprogramowaniem oraz nieuprawnionym dostępem i modyfikacją. Jak pokazują coroczne raporty CERT[141] złośliwe oprogramowanie to jedno z największych zagrożeń, jakie niosą ze sobą niezabezpieczone i nie sprawdzone przez programy antywirusowe informacje. Liczba incydentów naruszenia bezpieczeństwa informacji przez złośliwe programy rośnie z roku na rok[142]. Zapewnienie bezpieczeństwa na tej płaszczyźnie jest równie istotne co trudne. W przypadku ochrony przed wirusami najskuteczniejszą metodą walki jest właściwie prowadzona profilaktyka, czyli działania niedopuszczające by wirusy dostały się do systemu[143].

Rozwój złośliwego oprogramowania oraz programów zabezpieczających zachodzą niemal w zbliżonym tempie. Liczba coraz bardziej wymyślnych i złośliwych

---

[141] CERT Polska (Computer Emergency Response Team Polska) jest zespołem działającym w ramach Naukowej i Akademickiej Sieci Komputerowej, zajmującym się reagowaniem na zdarzenia naruszające bezpieczeństwo w Internecie. CERT Polska działa od 1996 roku, a od 1997 jest członkiem FIRST (Forum of Incidents Response and Security Teams) - największej na świecie organizacji zrzeszającej zespoły reagujące i zespoły bezpieczeństwa z całego świata. Od roku 2000 jest także członkiem inicjatywy zrzeszającej europejskie zespoły reagujące – TERENATF-CSIRT.

[142] Zgodnie z raportami CERT (www. cert.pl) w 2004 roku incydenty związane z działaniem złośliwego oprogramowania obejmowały około 15% wszystkich zarejestrowanych. W roku 2005 liczba ta wzrosła już do ponad 20%.

[143] J. Stokłosa, T. Bilski, T. Pankowski, *Bezpieczeństwo danych w systemach informatycznych*, Wydawnictwo Naukowe PWN, Warszawa - Poznań 2001.

wirusów rośnie. Dlatego też często korzystanie z jednego programu antywirusowego nie wystarcza i generuje się potrzeba równoległego implementowania nawet kilku. Programy te wykorzystują wiele metod wykrywania wirusów w tym:

- poszukiwanie sygnatur (zawartość testowanego pliku jest porównywana ze zbiorem charakterystycznych ciągów bajtów różnych wirusów,
- sprawdzanie integralności (aktualne cechy charakterystyczne takie jak na przykład długość i wartość sumy kontrolnej testowanego pliku są porównywane z wartościami zapamiętanymi w bazie danych gdy plik nie był zainfekowany),
- analiza heurystyczna (badanie zachowania się programów i poszukiwanie prób infekowania systemu[144].

Programy antywirusowe mogą działać w dwóch trybach – trybie rezydentnym lub na żądanie. Programy pracujące w trybie rezydentnym uruchamiają się wraz ze startem systemu i w sposób ciągły i automatyczny testują pliki uruchamianie lub kopiowane na dyski komputerów. W przypadku pracy w trybie „na żądanie" program jest uruchamiany przez użytkownika i dopiero wówczas dokonuje sprawdzenia zapisanych plików oraz pamięci operacyjnej.

Odrębnym zagadnieniem programowej ochrony informacji niejawnych są rozwiązania kontroli dostępu do zabezpieczonych zbiorów, a co za tym idzie rozliczalność zdarzeń i działań mających miejsce w systemie[145]. Zdefiniowanie dla każdego użytkownika zakresu uprawnień (odczyt, modyfikacja, kopiowanie itp.) oraz zbiorów informacji, których nadane uprawnienia dotyczą dają możliwość każdorazowej identyfikacji użytkownika, przydzielenie każdemu użytkownikowi dostępu do ściśle zdefiniowanych zbiorów, monitorowania zdarzeń w systemie, oraz odnotowania prób nieautoryzowanego dostępu, modyfikacji lub zniszczenia zbiorów.

Podstawowymi mechanizmami zabezpieczeń są mechanizmy identyfikacji i uwierzytelniania[146] oraz kontroli dostępu. Wśród metod uwierzytelniania, podobnie jak w systemach ochrony fizycznej, najczęściej stosowane są metody oparte na wie-

---

[144] Tamże.

[145] J. Janczak, G. Świdzikowski, *Bezpieczeństwo informacji w wojskowym systemie telekomunikacyjnym*, Akademia Obrony Narodowej, Warszawa 2004, s. 60.

[146] **Uwierzytelnienie** – sprawdzenie tożsamości użytkownika systemu.

dzy użytkownika, identyfikatory materialne, metody biometryczne lub połączenie ich w dowolnej konfiguracji.

Najbardziej rozpowszechnioną metodą opartą o wiedzę użytkownika jest stosowanie haseł. Praktycznie, metod ta stosowana jest we wszystkich systemach, w których są przetwarzane, przechowywane i przesyłane informacje niejawne, zaś jej stosowanie zalecane jest do zbiorów jawnych. Na to czy stosowane hasła zapewniają odpowiedni poziom bezpieczeństwa w systemie składa się wiele czynników. Do zasadniczych zalicza się długość hasła, złożoność alfabetu, na którym jest ono tworzone, okres ważności, sposób generacji, złożoność hasła oraz metody przechowywania i przesyłania haseł w systemie.

Zwiększanie bezpieczeństwa systemu poprzez wydłużanie haseł tworzonych o coraz bardziej złożone alfabety niesie za sobą również pewne niedogodności, jeżeli nawet nie nowe zagrożenia. Bardziej złożone hasło zwiększa prawdopodobieństwo błędnego wprowadzenia, a co się z tym wiąże zwykle blokadę systemu. Nieodpowiedzialni użytkownicy, aby uniknąć wprowadzania błędnie zapamiętanego hasła zapisują go, niestety najczęściej w miejscach ogólno dostępnych. Skutki ujawnienia hasła można minimalizować poprzez definiowanie okresu jego ważności. Skrajnym i jednocześnie najbezpieczniejszym rozwiązaniem są hasła jednorazowego użytku.

Hasła mogą być tworzone przez użytkownika lub generowane automatycznie. W przypadku rozwiązania pozwalającego użytkownikowi na tworzenie własnych haseł nad ich prawidłowością powinien czuwać administrator systemu. Powinien on uniemożliwić wprowadzanie haseł zbyt prostych, zbyt krótkich, opartych na zbyt ubogim alfabecie oraz cyklicznego wprowadzania takich samych haseł. Przy generatorach automatycznych najistotniejsze jest bezpieczne przechowywanie oraz przesyłanie haseł do użytkowników.

Wykorzystanie identyfikatorów fizycznych oraz metod biometrycznych oparte jest w systemach komputerowych na takich samych zasadach działania jak w przypadku ochrony fizycznej, dlatego też ich ponowne omawianie jest bezprzedmiotowe.

3.6. Bezpieczeństwo kryptograficzne

Kryptografia spełnia taką sama rolę wobec informacji elektronicznych jak zamki w stosunku do informacji drukowanych[147]. Kryptografia pozwala na taką zmianę informacji oryginalnej, by w przypadku jej utraty nie mogła ona być odczytana przez osobę nieuprawnioną. Czynność zmiany informacji w formę niejawną przy pomocy klucza nazywamy szyfrowaniem, natomiast proces odwrotny deszyfrowaniem. Całość procesu natomiast zwana jest systemem kryptograficznym, systemem szyfrowania lub szyfrowaniem.

Istota systemów kryptograficznych to opracowanie procedur doboru oraz dystrybucji kluczy szyfrowania. Szyfry opierają się na dwóch zasadniczych metodach przeobrażenia informacji jawnej w zaszyfrowaną. Są to metody podstawieniowe i przestawieniowe.

Metody przestawieniowe polegają na zmianie za pomocą określonego algorytmu, czyli klucza, pierwotnego porządku znaków za pomocą, którego zapisana jest informacja (litery, cyfry, bity itd.) w inny, maskujący oryginalną treść informacji. Jej odczytanie możliwe jest tylko wówczas, gdy proces ten odwrócimy używając tego samego klucza.

W metodach podstawieniowych istotą szyfrowania jest zmiana znaków za pomocą których zapisana jest informacje na inne ściśle określone w kluczu szyfrowania. Odczyt informacji polega tutaj na wtórnej zamianie znaków zaszyfrowanej informacji na jej oryginalne odpowiedniki.

Znajomość metody szyfrowania nie daje możliwości odczytania zaszyfrowanej informacji. Najistotniejszy jest klucz od poufności którego zależy bezpieczeństwo transmitowanych informacji.

Zastosowanie szyfrowania informacji ma bardzo szerokie spektrum. Obecnie różne metody szyfrowania informacji są wykorzystywane do zabezpieczenia przechowywanych danych, zabezpieczenia rozmów telefonicznych, przesyłanych faksów, poczty elektronicznej, transakcji bankowych (karty płatnicze, transakcje internetowe, karty kredytowe itd.) oraz do tworzenia korporacyjnych oraz firmowych bezpiecznych

---

[147] D. Denning, *Wojna informacyjna i bezpieczeństwo informacji*, Wydawnictwo Naukowo - Techniczne, Warszawa 2002, s. 326.

sieci komputerowych.

Należy tutaj dodać, że poza programowymi możliwościami szyfrowania informacji istnieją także możliwości sprzętowe. Do szyfrowania wykorzystywane są specjalne urządzenia, aplikacje oraz ich części. Wiele aplikacji komputerowych nie będących specjalistycznym oprogramowaniem służącym do zapewnienia bezpieczeństwa danych jest aktualnie uzbrajanych w taką możliwość.

Informacje mogą być szyfrowane na całej drodze przesyłania informacji lub wyłącznie na łączach[148]. W nomenklaturze wojskowych systemów telekomunikacyjnych lub informatycznych sposoby te nazywamy utajnianiem grupowym lub utajnianiem indywidualnym[149].

Utajnianie grupowe stosowane jest zazwyczaj w przypadku, gdy mamy do czynienia z dużym ześrodkowaniem urządzeń końcowych w strefie, w której nie istnieje konieczność utajniania informacji od samego źródła, aż do jej nadawcy. Grupowe urządzenie utajniające instalowane jest przy wyjściu sygnału ze strefy i szyfruje ono wszystkie wychodzące informacje. Deszyfrowanie realizowane jest przez analogiczne urządzenie przy wejściu w strefę bezpieczeństwa urządzeń końcowych - odbiorników.

Utajnianie indywidualne na całej drodze przesyłania informacji stwarza bezpieczny kanał między urządzeniami końcowymi bez względu na ilość urządzeń komutacyjnych lub pośredniczących w przepływie sygnału. Utajnianie indywidualne stosuje się gdy nie ma możliwości zapewnienia poufności i integralności informacji w trakcie jej transmisji wewnątrz strefy bezpieczeństwa, gdy w strefie znajdują się zarówno jawne jak i niejawne urządzenia końcowe oraz gdy istnieją trudności w zorganizowaniu samej strefy.

3.7. Bezpieczeństwo elektromagnetyczne

Jednym ze scharakteryzowanych w rozdziale 2 zagrożeń były zagrożenia związane z niepożądaną emisją sygnałów elektromagnetycznych zwaną emisją ujawniającą.

Skuteczna ochrona przed zjawiskiem emisji ujawniającej nie jest zadaniem ła-

---

[148] Tamże, str. 350.

[149] J. Janczak, G. Świdzikowski, *Bezpieczeństwo informacji w wojskowym systemie telekomunikacyjnym*, Akademia Obrony Narodowej, Warszawa 2004, s.54.

twym. Wymaga zastosowania kombinacji różnych środków technicznych, zabiegów organizacyjnych oraz unormowań prawnych.

Podstawowe działania mające uchronić informacje niejawne przed skutkami emisji ujawniającej polegają na ograniczeniu jej poziomu poprzez tłumienie fali elektromagnetycznej, uziemianie, ekranowanie i filtrowanie oraz odpowiedni dobór parametrów czasowo – częstotliwościowych sygnałów skutecznych.

Praktyczna realizacja ochrony przed nasłuchem elektromagnetycznym wymaga zastosowania jednego, a najlepiej kombinacji kilku, wymienionych poniżej środków:

- kabiny elektromagnetycznej,
- folii elektromagnetycznej, stosowanej w formie tapety,
- lokalizacji w odpowiedniej odległości od miejsc publicznie dostępnych,
- stosowanie bezpiecznego sprzętu, spełniającego określone normy dotyczące emisji ujawniającej (TEMPEST),
- osłony elektromagnetyczne,
- dobór sprzętu i środków ochrony elektromagnetycznej w zależności od środowiska otaczającego sprzęt.

3.7.1. Metody techniczne

Do podstawowych metod obniżenia poziomu emisji ujawniającej zaliczamy ekranowanie pomieszczeń i urządzeń, stosowanie urządzeń o obniżonym konstrukcyjnie poziomie emisji ujawniającej oraz wydzielenie odpowiednich stref ochrony.

Połączenie metod organizacyjnych (strefy ochronne) i metod technicznych pozwala na zapewnienie wymaganego poziomu emisji ujawniającej.

3.7.2. Filtry

Jedną z przyczyn zwiększonego zasięgu emisji ujawniającej jest jej przewodzenie przez sieć energetyczną, miedziane linie sygnałowe oraz inne elementy wychodzące z pomieszczeń, w których umieszczone są pracujące urządzenia telekomunikacyjne. Jednym ze sposobem eliminacji tego zjawiska jest stosowanie filtrów.

Filtry przeciwzakłóceniowe składają się z reguły z odpowiednio połączonych kondensatorów, dławików i rezystorów. Najważniejszym parametrem określającym jego użyteczność jest tłumienność wtrąceniowa. Określa się ją jako stosunek sygnału mierzonego bez filtru do poziomu sygnału w tym samym punkcie obwodu przy zastosowaniu filtracji.

Przy zastosowaniu filtrów należy zwrócić uwagę na czynniki obniżające ich efektywność, czyli sprzężenie pomiędzy wejściem i wyjściem filtru i impedancję pasożytniczą w przewodzie masy.

Aby nie dopuścić do powstania sprzężenia pomiędzy wejściem a wyjściem filtru należy właściwe go zamontować. Przewody wejściowe powinny być możliwie w największym stopniu odseparowane od przewodów wyjściowych.

Filtry dolnoprzepustowe swoje działanie mają zwykle oparte na zwieraniu wysokiej częstotliwości z masą układu za pośrednictwem odpowiedniej pojemności. Filtry te mogą być stosowane w różnych miejscach chronionego systemu. Najczęściej ochronie mogą podlegać:

- napięcia zasilania po stronie uzwojenia pierwotnego transformatora zasilacza,
- napięcie wyjściowe zasilacza,
- przyłączenia przewodów ekranowanych,
- przyłączenia przewodów nieekranowanych,
- linie zegarowe, sygnałowe oraz danych pomiędzy poszczególnymi elementami systemu.

Filtry sieciowe umieszczane są pomiędzy zasilaczem chronionego urządzenia a publiczną siecią energetyczną. Ich zastosowanie pomaga zapobiegać rozprzestrzenianiu się sygnału emisji ujawniającej poprzez sieć elektroenergetyczna. Chronią one także układy elektroniczne systemu przed zakłóceniami przedostającymi się z sieci zasilającej. Najważniejszą rzeczą przy stosowaniu filtrów sieciowych jest ich prawidłowy montaż. Aby móc mówić, że zastosowany filtr jest właściwie zastosowany należy przestrzegać kilku zasad:

- w celu ograniczenia impedancji szeregowej połączenia z masą filtr należy przykręcić bezpośrednio do szyny potencjału odniesienia,
- przewody zasilający i odbiorczy powinny być poprowadzone w przeciwnych kierunkach w celu ograniczenia przesłuchu asymetrycznego pomiędzy równoległymi przewodami,
- w celu ograniczenia efektu anteny ramowej, przewody zasilający i odbiorczy

powinny zostać tak poprowadzone aby maksymalnie przylegały do powierzchni szyny potencjału odniesienia.

Filtry na przyłączeniach przewodów ekranowanych stosujemy w celu eliminacji skutków przesłuchów na złączach i w miejscach innych połączeń. W tym przypadku możemy zastosować trzy rozwiązania:

- uniwersalne łącze filtrujące,
- filtr zintegrowany z linią sygnałową,
- filtr dyskretny.

Filtry na przyłączeniach nieekranowanych stosujemy w celu niedopuszczenia przedostawania się do takich linii sygnałów mogących nieść informacje oraz w celu zabezpieczenia systemu przed zakłóceniami indukowanymi w liniach pod wpływem zewnętrznego pola elektromagnetycznego.

3.7.3. Ekranowanie połączeń, pomieszczeń i budynków

Aby wyeliminować połączenia jako źródła promieniowania elektromagnetycznego należy stosować ekranowanie połączeń. Do ekranowanej obudowy nie powinien wchodzić żaden przewód, który sam nie jest właściwie ekranowany i nie posiada odpowiednich filtrów.

W przypadku ochrony większej ilości urządzeń najbardziej efektywnym rozwiązaniem może okazać się ekranowanie pomieszczeń czy nawet całych budynków. Częściowe ekranowanie budynku można zapewnić już na etapie projektu i budowy. W pewnych zakresach częstotliwości odpowiednia konstrukcja żelbetonowa jest w stanie zmniejszyć poziom promieniowania nawet dziesięciokrotnie. Istotnym elementem ekranującym w konstrukcji budynku są folie aluminiowe stosowane do laminowania pokryć bitumicznych uszczelniających ściany i dachy budynków. Sposób ekranowania oraz materiały do tego użyte zależą od wymaganego stopnia tłumienia. Aby zmniejszyć koszty, celowe jest połączenie mniej efektywnego, a co się z tym wiąże tańszego, ekranowania z innymi środkami ochrony np. z wydzieleniem stref ochronnych obiektów.

Dla szczególnie ważnych elementów sieci najpewniejszym rozwiązaniem jest zastosowanie kabin ekranowanych.

3.7.4. Bezpieczne czcionki

Nie wszystkie obrazy powodują emisję obrazów o takim samym stopniu trudności przechwycenia i odczytania. Dlatego też właściwie zaprojektowana czcionka, niewiele różniąca się wizualnie może w znaczny sposób zwiększyć bezpieczeństwo wyświetlanych na naszym monitorze informacji. Możliwe to jest poprzez jak największą eliminację, szczególnie podatnych na odtwarzanie w wyniku podsłuchu, składowych wysokoczęstotliwościowych obrazu czcionki.

3.7.5. Kanały szyfrowane

Kolejna metodą eliminacji możliwości podsłuchu elektromagnetycznego informacji przesyłanych w liniach transmisyjnych są metody kryptografii. Zastosowanie tej metody generuje jednak potrzebę zastosowania dodatkowych zabezpieczeń zarówno w fazie generowania klucza jak i jego wprowadzania i przetwarzania informacji przez system kryptograficzny.

3.7.6. Sygnały zakłócające

Znając metody wykorzystywane przy podsłuchu elektromagnetycznym można wprowadzać odpowiednie sygnały zakłócające. Ich obecność utrudnia lub nawet uniemożliwia poprawna interpretację informacji zawartych w podsłuchanym sygnale.

3.7.7. Program TEMPEST

TEMPEST jest nazwą powstałego w latach 50 – tych w USA programu ochrony przed niekontrolowaną emisja ujawniającą.

Zarówno normy jak i technologia wytwarzania sprzętu klasy TEMPEST są utajnione. Program TEMPEST nadzoruje Agencja Bezpieczeństwa Narodowego Stanów Zjednoczonych, a produkcja sprzętu, laboratoria pomiarowe oraz pracujący w nich ludzie podlegają okresowej kontroli. Zwykle sprzęt tej klasy jest typowym sprzętem biurowym dostosowanym do spełniania wymagań tej klasy lub opracowywany na indywidualne potrzeby klienta.

Ze względu na ograniczenia użytkownikami sprzętu klasy TEMPEST mogą być wyłącznie instytucje NATO wchodzące w skład sił zbrojnych, komórki dyplomatyczne i wywiadowcze oraz łączność specjalna i instytucje do przetwarzania danych niejawnych.

Zastosowanie sprzętu klasy TEPMEST gwarantuje bezpieczeństwo elektromagnetyczne procesu przetwarzania danych. Można, więc zrezygnować ze stosowania zabezpieczeń fizycznych typu osłony, filtry itp. Jest to dość wygodne i proste rozwiązanie, jednakże jego zastosowanie musi poprzedzić kalkulacja opłacalności oraz należy się liczyć z długą procedura zdobywania zezwolenia na import oraz zastosowanie tego typu sprzętu.

3.8. Wnioski

W celu zorganizowania efektywnego systemu ochrony informacji niejawnych należy przede wszystkim odpowiedzieć na pytania:

1. Jakie kategorie informacji podlegają ochronie w ramach organizowanego systemu?
2. Jakie wymagania stawiane są przed systemem ochrony?
3. Jakie są podstawowe zasady dostępu do chronionych zasobów, czyli kto, do czego i w jakim zakresie powinien mieć dostęp?
4. Kto jest odpowiedzialny za zabezpieczenie aktywów wymagających ochronie?

Zapewnienie bezpieczeństwa informacyjnego ma aktualnie priorytetową pozycję w wielu organizacjach, w tym w jednostkach organizacyjnych Sił Zbrojnych.

Pomimo nakładów finansowych oraz organizacyjnych, istnieje w tym zakresie wiele braków. Często istnieją braki w planowaniu i organizowaniu działań prewencyjnych i ochronnych. Zdarzają się również braki w zakresie planów przywrócenia systemów informacyjnych do stanu pierwotnego w przypadku potencjalnego ataku.

Działania zaradcze, prowadzone w sposób wycinkowy, wystawiają zasoby informacyjne na zagrożenia związane ze zbyt krótkowzrocznym myśleniem. Do skutecznej ochrony informatycznej potrzebna jest struktura wybiegająca w przyszłość. Umożliwia ona włączenie problematyki bezpieczeństwa do planowanych i permanentnie realizowanych działań.

Rozdział 4 – Modelowanie bezpieczeństwa informacyjnego w Siłach Zbrojnych RP

CEL BADAŃ

Celem badań zagadnień poruszanych w niniejszym rozdziale jest: **Budowa modelu bezpieczeństwa informacyjnego Sił Zbrojnych RP oraz przeprowadzenie eksperymentu symulacyjnego opartego na tym modelu.**

GŁÓWNY PROBLEM BADAWCZY

Stosownie do przyjętego celu badań, problem badawczy sprowadza się do odpowiedzi na pytanie: **Jak powinien być zbudowany model bezpieczeństwa informacyjnego Sił Zbrojnych RP oraz w jaki sposób można przeprowadzić eksperyment symulacyjny przy jego pomocy?**

HIPOTEZY ROBOCZE

Hipoteza pierwsza

Złożoność bezpieczeństwa informacyjnego Sił Zbrojnych RP oraz związanych z nim procesów jest tak duża, że bez przyjęcia uproszczonej formy, przeprowadzenie jego badań jest niezwykle trudne.

Hipoteza druga

Zbudowanie wielorównaniowego modelu bezpieczeństwa informacyjnego Sił Zbrojnych RP pozwoli na przeprowadzenie symulacji komputerowych celem uzyskania odpowiedzi na pytanie o poziom bezpieczeństwa informacyjnego Sił Zbrojnych RP.

4.1. Symulacje komputerowe a budowa modeli fizycznych i opisowych

Symulacja komputerowa nazywana często eksperymentem numerycznym, wymaga opracowanego wcześniej modelu matematycznego modelowanego systemu, zjawiska, obiektu czy też układu. Dobrze opracowany model jest warunkiem koniecznym przeprowadzenia udanych eksperymentów symulacyjnych. Udany eksperyment symulacyjny potwierdza przydatność modelu, co jednocześnie świadczy o jego weryfikowalności. Warunek weryfikowalności jest podstawowym miernikiem „dobroci" opracowanego modelu.

Model matematyczny, odpowiednio dobrany do badań symulacyjnych, jest następstwem procesu tworzenia pewnej formy opisującej w sposób umowny zespół tych cech istotnych rzeczywistości, którą opisał i uprościł model fizyczny. Tworzenie takiej umownej formy zapisu rzeczywistości prowokuje do tego, że wielu ludzi, poświęcających się zagadnieniu tworzenia modeli, wymyśla własne definicje, określające model[150].

Należy tu rozróżnić dwa zasadnicze pojęcia: modelu w ogólności i modelu w sensie matematycznym – modelu opisowego.

W nauce, w zdecydowanej większości przypadków, *model jest rozumiany jako uproszczona reprezentacja rzeczywistości*. Stanowi on pewien substrat rzeczywistości. Ujmuje tylko jej część. Celem tworzenia wszelkich modeli jest dążenie do zrozumienia otaczającej nas rzeczywistości. Stosując modele obserwujemy i sprawdzamy prawa rządzące zjawiskami. Jeżeli prawa te zrozumiemy, to możemy przewidzieć jak dane zjawiska będą przebiegać w przyszłości i w innych warunkach. Do najstarszych sposobów odwzorowania rzeczywistości należą modele *„w skali"*, w których występuje podobieństwo wyłącznie geometryczne. Należą do nich *modele ikonograficzne* (obrazy, mapy, plany) oraz *modele trójwymiarowe* (makiety, miniatury). Wyższy stopień abstrakcji osiągają modele oparte nie na podobieństwie, lecz na *analogii* a więc na odpowiedniej *zgodności wartości wielkości fizycznie różnych*. Są to na przykład modele elektryczne systemów mechanicznych, lub odwrotnie[151].

---

[150] C. Szczepaniak, *Podstawy modelowania systemu człowiek – pojazd – otoczenie*, Wyd. Naukowe PWN, Warszawa 1999, s.11.

[151] J.Gutenbaum, *Modelowanie matematyczne systemów*, OMNITECH PRESS, Warszawa, 1992 r.

Modelem opisowym nazywany jest model w sensie matematycznym będący pojęciem abstrakcyjnym o uproszczonej konstrukcji, odnoszący się do części rzeczywistości, utworzony w określonym celu.

Model matematyczny stanowi równanie bądź układ równań opisujących ilościowo zjawiska obejmowane przez model fizyczny lub w postaci rozwiniętej: model matematyczny to operator, który przekształca dany sygnał wejściowy - $X(t)$ (zmienne wejściowe) w sygnał wyjściowy - $Y(t)$ (zmienne wyjściowe) danego obiektu.[152]

Punktem wyjściowym do budowy modelu opisowego jest model fizyczny. Model fizyczny zachowuje istotne cechy modelowanego systemu rzeczywistego wprowadzając jednocześnie istotne uproszczenia w stosunku do modelowanej rzeczywistości. Celem uproszczeń stosowanych w modelu fizycznym jest uproszczenie przyszłej analizy matematycznej między innymi poprzez pomijanie małych wpływów, co powoduje w efekcie zmniejszenie liczby zmiennych. Najczęściej stosowane przybliżenia w procesie modelowania fizycznego i skutki tych przybliżeń w modelach opisowych pokazuje tabela 1.

Tabela 4.1.

Rodzaje przybliżeń stosowanych w procesie modelowania.

Nr	Rodzaj przybliżenia	Uproszczenie matematyczne
1.	Pomijanie małych wpływów, np. przez intuicję	Zmniejsza liczbę i złożoność równań
2.	Agregacja zmiennych	Zmniejsza liczbę i złożoność równań
3.	Niezależność otoczenia od badanego układu	Zmniejsza liczbę i złożoność równań
4.	Zastępowanie parametrów rozłożonych – skupionymi	Prowadzi do równań różniczkowych zwyczajnych
5.	Zakładanie zależności liniowych	Prowadzi do równań liniowych

[152] J. Osiecki, *Elementy modelowania w dynamice maszyn*, praca zbiorowa, wyd. PAN, Zakład im. Ossolińskich, Wrocław 1974.

Nr	Rodzaj przybliżenia	Uproszczenie matematyczne
6.	Niezależność parametrów od czasu	Prowadzi do równań różniczkowych o stałych współczynnikach
7.	Unikanie nieokreśloności, pomijanie szumów	Usuwa konieczność stochastycznego traktowania problemu

Źródło: Opracowano na podstawie: C. Szczepaniak, Podstawy modelowania systemu człowiek – pojazd – otoczenie, Wyd. Naukowe PWN, Warszawa 1999, s.13.

Przyjmując definicję modelu w postaci rozwiniętej, można zapisać:

$$Y(t) = A_t X(t) \qquad (4.1)$$

gdzie: A_t oznacza pewną operację matematyczną przeprowadzoną na rzeczywistym sygnale wejściowym $X(t)$ obiektu. A_t nazywa się operatorem obiektu[153].

Równanie (4.1) określa zależność pomiędzy sygnałami: wejściowym i wyjściowym. Nadrzędnym celem modelowania jest zapewnienie możliwie małych różnic pomiędzy wartościami rzeczywistymi i modelowymi wspomnianych sygnałów. Ocena tych różnic wykonywana jest w fazie weryfikacji modelu. Przez weryfikację modelu rozumie się *porównanie wyników modelowania z zachowaniem się systemu rzeczywistego, z punktu widzenia zgodności z wiedzą teoretyczną oraz z badaniami doświadczalnymi.*

Etap weryfikacji jest integralnie związany z każdym z poprzednich etapów budowy modelu, a więc powinien być prowadzony we wszystkich fazach tworzenia modelu. Zasadniczym problemem jest tu dobór kryteriów, na podstawie, których będzie można ocenić czy warunki zgodności są spełnione, czy też nie. Wyróżniamy dwie grupy takich kryteriów: kryteria wewnętrzne i kryteria zewnętrzne.

Kryteria wewnętrzne dotyczą wewnętrznych cech modelu. Należą do nich *zgodność formalna*, zapewniająca brak sprzeczności koncepcyjnych, logicznych, matematycznych oraz *zgodność algorytmiczna*, zapewniająca efektywne wykonanie obliczeń czy też symulacji komputerowej z wymaganą dokładnością.

---

[153] Źródło: C. Szczepaniak, *Podstawy modelowania systemu człowiek – pojazd – otoczenie*, Wyd. Naukowe PWN, Warszawa 1999, s.12.

Kryteria zewnętrzne dotyczą celów modelowania i zgodności modelowanych zjawisk z teorią i z danymi doświadczalnymi. Do kryteriów tych należą zgodność heurystyczna i zgodność pragmatyczna.

Zgodność heurystyczna dotyczy walorów naukowych modelu: zgodności interpretacji, weryfikacji hipotez, formułowania nowych zadań badawczych.

Zgodność pragmatyczna dotyczy bezpośrednio wyników modelowania. Weryfikację zgodności pragmatycznej przeprowadza się podając na wejście badanego systemu i na wejście modelu to samo wymuszenie, a następnie porównuje się wielkości uzyskane na wyjściu systemu i modelu. Z powyższego widać, że weryfikacja pragmatyczna nie jest możliwa do przeprowadzenia dla nieistniejących jeszcze systemów.

4.2. Model bezpieczeństwa informacyjnego Sił Zbrojnych RP

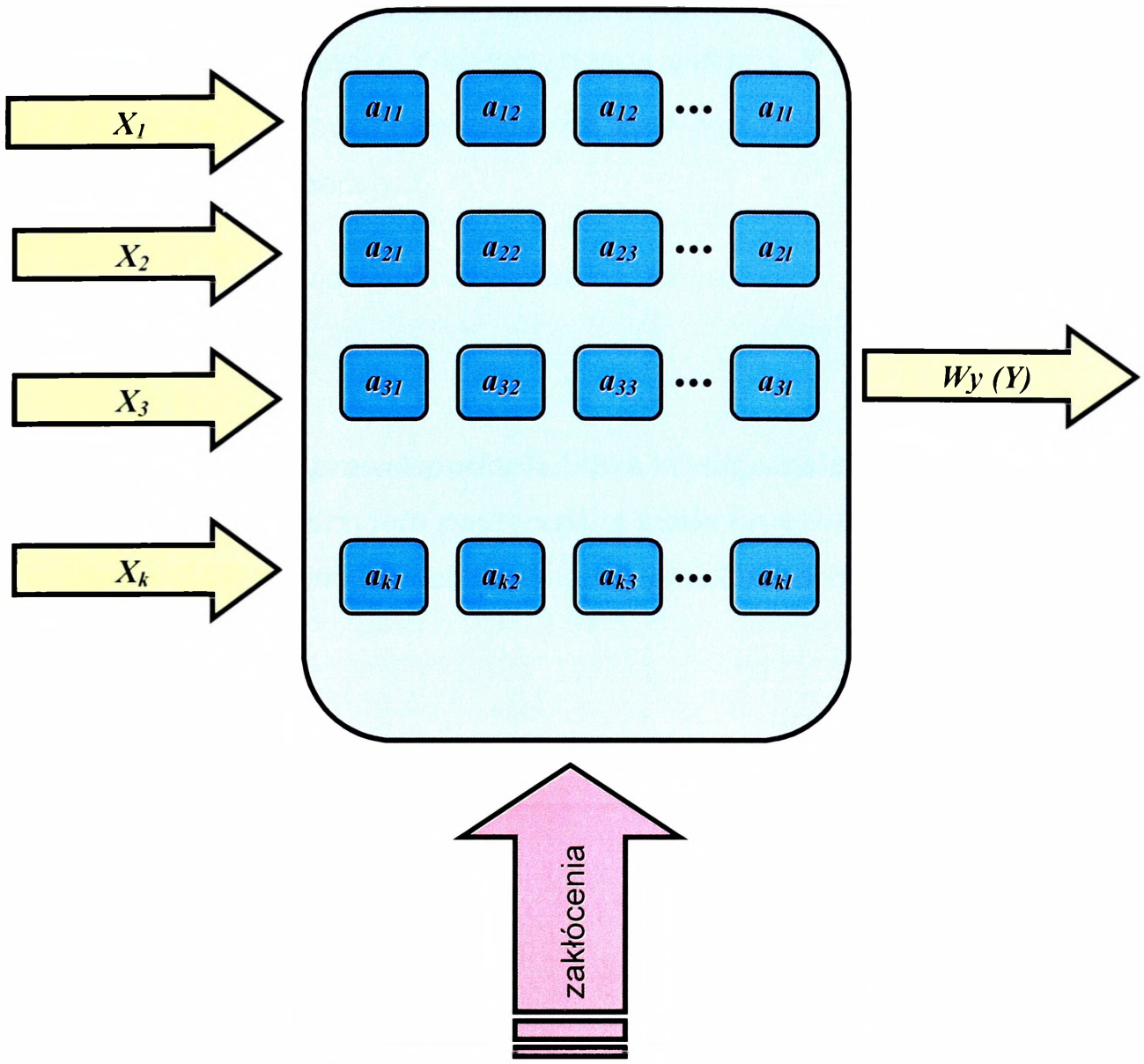
Ocena stopnia zagrożeń mogących oddziaływać na informacje niejawne, będące zasadniczym elementem zapewnienia bezpieczeństwa Siłom Zbrojnym RP, wymaga uwzględnienia szeregu czynników i uwarunkowań. Przystępując do budowy modelu bezpieczeństwa informacyjnego Sił Zbrojnych należy brać pod uwagę, że:

1. Każdy system informacyjny złożony jest z wielu elementów składowych i zapewnienie bezpieczeństwa całości realizowane może być wyłącznie poprzez zapewnienie bezpieczeństwa wszystkim elementom składowym systemu.
2. Zagrożenia oddziałujące na poszczególne elementy systemu są identyfikowalne. Prawdopodobieństwo ich wystąpienia w poszczególnych elementach systemu można w przybliżeniu oszacować.
3. Budowa złożonego modelu bezpieczeństwa informacyjnego, uwzględniającego wielość zagrożeń i elementów, na które one oddziałują implikuje szereg złożonych zależności. Nie jest tak, że jedno zagrożenie oddziałuje na jeden element. Pomiędzy zagrożeniami i elementami systemu zachodzą relacje tego typu, że jedno zagrożenie może oddziaływać na wiele elementów, zaś na jeden element może oddziaływać wiele zagrożeń.

Przy uwzględnieniu powyższego, model bezpieczeństwa informacyjnego Sił Zbrojnych RP został zbudowany z uwzględnieniem następujących założeń:

1. Bezpieczeństwo informacyjne traktowane jest jako jeden obiekt, scalony z szeregu elementów składowych. Elementami tymi są: bezpieczeństwo prawne, bezpieczeństwo osobowe, bezpieczeństwo fizyczne, bezpieczeństwo programowe, bezpieczeństwo kryptograficzne i bezpieczeństwo elektromagnetyczne. Przyjęta koncepcja budowy modelu pozwala na modyfikację powyższego zbioru na potrzeby innych badań.
2. Zbiór zagrożeń podzielony został na zagrożenia: nieuprawnione ujawnienie informacji, zagrożenia z Internetu i przestępstwa komputerowe, cyberterroryzm, awarie i uszkodzenia sprzętowe, emisja ujawniająca. Każda z tych grup podlegała szczegółowym podziałom zawartym w tabeli 4.2.
3. Zagrożenia ***(X_1, X_2, X_3... X_k)*** oddziałując na cały system, oddziałują na wszystkie jego elementy. Skuteczność ochrony przed konkretnym zagrożeniem, dla danego elementu bezpieczeństwa, mierzona jest prawdopodobieństwem zawierającym się w przedziale $0 \leq Y \leq 1$. W wyniku przeprowadzonych badań, specjaliści (eksperci) oszacowali miary prawdopodobieństw. W ankiecie, dla odpowiedzi o prawdopodobieństwo wystąpienia konkretnego zagrożenia, przyjęto skalę: niemożliwe = 1, raczej niemożliwe = 2, trudno powiedzieć = 3, prawdopodobne = 4, bardzo prawdopodobne = 1. Dla potrzeb modelu, wartości te zostały przetransponowane do wartości zawierających się w przedziale **<0, 1>** i tak dla poszczególnych odpowiedzi przyjęto następujące wartości prawdopodobieństwa: *niemożliwe* = ***0***, *raczej niemożliwe* = ***0,25***; *trudno powiedzieć* = ***0,50***, *prawdopodobne* = ***0,75***, *bardzo prawdopodobne* = ***1***. Przyjęta koncepcja modelu pozwala, poprzez swój uniwersalizm, na przyjęcie innej skali prawdopodobieństw.
4. Dla potrzeb modelu i symulacji przyjęto średnią wartość prawdopodobieństwa oddziaływania poszczególnych zagrożeń na składowe bezpieczeństwa informacyjnego sił zbrojnych, obliczoną na podstawie odpowiedzi uzyskanych w toku badań. W przypadku, gdy zagrożenie oddziałuje na daną składową bezpieczeństwa informacyjnego przyjmuje ona obliczoną średnią wartość prawdopodobieństwa. W przypadku, gdy takie oddziaływanie nie występuje, dana składowa bezpieczeństwa informacyjnego, przyjmuje wartość ***0***.

5. Wynikiem oddziaływań określonych zagrożeń na system bezpieczeństwa informacyjnego jest wektor **Y,** którego składowe określają stopień występowania poszczególnych zagrożeń informacyjnych. Na podstawie składowych wektora **Y**, oblicza się jego miarę *Y*, będącą odzwierciedleniem prawdopodobieństwa wystąpienia zagrożenia ze strony wszystkich zagrożeń składowych w procesie oddziaływania na wszystkie elementy składowe systemu bezpieczeństwa Sił Zbrojnych RP. Takie podejście do problemu pozwala na określenie akceptowalnego poziomu wartości *Y* dla rozpatrywanego systemu.
6. Konstrukcja modelu pozwala na opracowanie wspomagających narzędzi komputerowych (np. arkuszy kalkulacyjnych – tak postąpiono w niniejszej rozprawie) wspomagających proces obliczeń oraz symulacji wraz z wizualizacją wyników.
7. W opracowanym modelu założono normalność rozkładu czynnika losowego, co w efekcie pozwala na pominięcie jego wpływu i formalne nieuwzględnienie czynnika losowego w postaci matematycznej modelu – patrz zależność 4.1 oraz 4.2. Założenie o normalności rozkładu czynnika losowego oznacza zerowanie się wartości oczekiwanej czynnika losowego w opracowanym modelu.



Rys. 4.1. Graficzne zobrazowanie modelu bezpieczeństwa informacyjnego Sił Zbrojnych RP

Źródło: Opracowania własne.

Objaśnienia do rys 4.1.

$X_1, X_2, X_3 \ldots X_k$ - składowe wektora sygnału wejściowego – zmienne niezależne przyjmujące wartości „1" lub „0" gdzie:

1 – oznacza zagrożenie oddziałujące;

0 – oznacza zagrożenie które, nie oddziałują.

a_{ij}, *gdzie* $i = 1, 2, 3, \ldots, k$ $j = 1, 2, 3, \ldots, l$.– składowe operatora macierzowego A. Dla poszczególnych zagrożeń, w przypadku ich oddziaływania, przyjmują one uśrednione wartości prawdopodobieństwa, wyszczególnione w tabeli 4.2.

Wektor Y– sygnał wyjściowy będący miarą stopnia bezpieczeństwa informacyjnego SZ RP określonego poprzez prawdopodobieństwa wystąpienia wszystkich składowych zagrożeń: a_{ij} . Wartość *Y* będąca normą wektora ***Y*** zawiera się w przedziale $0 \leq Y \leq 1$, *g*dzie **0** oznacza brak zagrożeń, czyli całkowite bezpieczeństwo informacyjne, a **1** brak bezpieczeństwa.

Zakłócenia – reprezentują wpływ czynnika losowego.

Tabela 4.2.

Uśrednione wartości prawdopodobieństwa wystąpienia zagrożeń. Do obliczenia wartości średniej przyjęto następującą skalę umowną: *niemożliwe =* ***0****, raczej niemożliwe =* ***0,25****; trudno powiedzieć =* ***0,50****, prawdopodobne =* ***0,75****, bardzo prawdopodobne =* ***1***

Lp.	Zagrożenie dla bezpieczeństwa informacji			Ilość odpowiedzi					Uśredniona wartość prawdopodobieństwa
				Niemożliwe	Raczej niemożliwe	Trudno powiedzieć	Prawdopodobne	Bardzo prawdopodobne	
1.	Nieuprawnione ujawnienie informacji								
	1.1	Podsłuch		0	9	32	14	3	**0,55**
	1.2	Kradzież, zgubienie		0	12	7	39	0	**0,62**
	1.3	Zagrożenia socjotechniczne							
		1.3.1	Wykorzystanie władzy	0	4	0	37	17	**0,79**
		1.3.2	Wykorzystanie symparii[154]	0	7	34	6	0	**0,49**

[154] Wyjaśnienie pojęcia ***sympria*** na stronie 63.

Lp.	Zagrożenie dla bezpieczeństwa informacji			Ilość odpowiedzi					Uśredniona wartość prawdopodobieństwa
				Niemożliwe	Raczej niemożliwe	Trudno powiedzieć	Prawdopodobne	Bardzo prawdopodobne	
		1.3.3	Wykorzystanie wzajemności	0	9	33	10	1	**0,51**
		1.3.4	Wykorzystanie konsekwencji	0	10	15	33	0	**0,60**
		1.3.5	Wykorzystanie zasady przyzwolenia społecznego	0	7	18	33	0	**0,61**
		1.3.6	Wykorzystanie okazji	0	9	31	18	0	**0,54**
2.	Zagrożenia z Internetu i przestępstwa komputerowe								
	2.1		Uzyskanie dostępu do danych przesyłanych przez sieć lub przechowywanych w komputerach przez osoby niepowołane	0	1	0	32	25	**0,85**
	2.2		Utrata danych na skutek działań z zewnątrz (Internet)	0	0	9	30	19	**0,79**
	2.3		Fałszerstwo danych	0	11	14	27	0	**0,58**
	2.4		Uniemożliwienie korzystania z usług (zasobów) przez legalnych użytkowników	0	5	7	30	16	**0,75**
	2.5		Zmiana oryginalnego programu, którym użytkownicy rejestrują się w systemie - podstawienie konia trojańskiego	0	2	12	37	7	**0,71**
	2.6		Wykorzystanie rezydentnych programów kontrolujących klawiaturę - zapisywanie sekwencji naciskanych klawiszy	0	8	40	6	4	**0,53**
	2.7		Podsłuch łącza, którym transmitowane są dane uwierzytelniające	1	31	13	12	0	**0,41**
	2.8		Atak słownikowy	0	10	4	41	0	**0,64**
	2.9		Przeszukiwanie wyczerpującą metodą prób i błędów - atak brutalny	2	2	7	47	0	**0,68**
	2.10		Metody fizyczne - patrzenie na ręce użytkownika rejestrującego się w systemie	0	43	4	9	0	**0,35**

Lp.	Zagrożenie dla bezpieczeństwa informacji		Ilość odpowiedzi					Uśredniona wartość prawdopodobieństwa
			Niemożliwe	Raczej niemożliwe	Trudno powiedzieć	Prawdopodobne	Bardzo prawdopodobne	
	2.11	Metody inżynierii społecznej - nakłonienie użytkownika do udostępnienia lub zmiany hasła	0	6	35	17	0	**0,55**
	2.12	Wirusy komputerowe	0	0	5	20	33	**0,87**
3.	Cyberterroryzm		0	0	20	17	21	**0,75**
4.	Awarie i uszkodzenia sprzętowe							
	4.1	Błędy projektowe	5	7	17	19	0	**0,51**
	4.2	Wady produkcyjne	2	9	21	18	0	**0,53**
	4.3	Błędy instalacji	0	8	24	26	0	**0,58**
	4.4	Awarie	0	1	23	34	0	**0,64**
5.	Emisja ujawniająca							
	5.1	Emisja ujawniająca promieniowana	6	12	26	7	0	**0,42**
	5.2	Emisja ujawniająca przewodzona - bezpośrednia	0	21	31	0	0	**0,40**
	5.3	Emisja ujawniająca przewodzona - wtórna	0	35	15	1	0	**0,33**

Źródło: opracowanie własne

Tabela 4.3.

Wpływ poszczególnych kategorii zagrożeń na składowe bezpieczeństwa informacyjnego Sił Zbrojnych RP (podano prawdopodobieństwa wystąpienia poszczególnych zagrożeń w stosunku do wyróżnionych kategorii bezpieczeństwa informacyjnego).

Zagrożenie dla bezpieczeństwa informacji			Składowe bezpieczeństwa informacyjnego Sił Zbrojnych RP					
			Bezpieczeństwo prawne	Bezpieczeństwo osobowe	Bezpieczeństwo fizyczne	Bezpieczeństwo programowe	Bezpieczeństwo kryptograficzne	Bezpieczeństwo elektromagnetyczne
			N_1	N_2	N_3	N_4	N_5	N_6
1. Nieuprawnione ujawnienie informacji								
1.1	Podsłuch		**0,55**	**0**	**0,55**	**0**	**0**	**0**
1.2	Kradzież, zgubienie		**0,62**	**0,62**	**0,62**	**0**	**0**	**0**
1.3	Zagrożenia socjotechniczne							
	1.3.1	Wykorzystanie władzy	**0**	**0,79**	**0,79**	**0**	**0**	**0**
	1.3.2	Wykorzystanie symparii	**0**	**0,49**	**0,49**	**0**	**0**	**0**
	1.3.3	Wykorzystanie wzajemności	**0**	**0,51**	**0,51**	**0**	**0**	**0**
	1.3.4	Wykorzystanie konsekwencji	**0**	**0,60**	**0,60**	**0**	**0**	**0**
	1.3.5	Wykorzystanie zasady przyzwolenia społecznego	**0**	**0,61**	**0,61**	**0**	**0**	**0**
	1.3.6	Wykorzystanie okazji	**0**	**0,54**	**0,54**	**0**	**0**	**0**

Zagrożenie dla bezpieczeństwa informacji		Składowe bezpieczeństwa informacyjnego Sił Zbrojnych RP					
		Bezpieczeństwo prawne	Bezpieczeństwo osobowe	Bezpieczeństwo fizyczne	Bezpieczeństwo programowe	Bezpieczeństwo kryptograficzne	Bezpieczeństwo elektromagnetyczne
		N_1	N_2	N_3	N_4	N_5	N_6
2. Zagrożenia z Internetu i przestępstwa komputerowe							
2.1	Uzyskanie dostępu do danych przesyłanych przez sieć lub przechowywanych w komputerach przez osoby niepowołane	**0,85**	**0,85**	**0,85**	**0,85**	**0,85**	**0**
2.2	Utrata danych na skutek działań z zewnątrz (Internet)	**0,79**	**0**	**0,79**	**0,79**	**0,79**	**0**
2.3	Fałszerstwo danych	**0,58**	**0,58**	**0**	**0,58**	**0,58**	**0**
2.4	Uniemożliwienie korzystania z usług (zasobów) przez legalnych użytkowników	**0,75**	**0,75**	**0**	**0**	**0**	**0**
2.5	Zmiana oryginalnego programu, którym użytkownicy rejestrują się w systemie - podstawienie konia trojańskiego	**0,71**	**0,71**	**0,71**	**0,71**	**0**	**0**
2.6	Wykorzystanie rezydentnych programów kontrolujących klawiaturę - zapisywanie sekwencji naciskanych klawiszy	**0,53**	**0**	**0**	**0,53**	**0**	**0**
2.7	Podsłuch łącza, którym transmitowane są dane uwierzytelniające	**0,41**	**0**	**0,41**	**0**	**0**	**0,41**
2.8	Atak słownikowy	**0,64**	**0,64**	**0**	**0,64**	**0,64**	**0**
2.9	Przeszukiwanie wyczerpującą metodą prób i błędów - atak brutalny	**0,68**	**0**	**0**	**0,68**	**0,68**	**0**
2.10	Metody fizyczne - patrzenie na ręce użytkownika rejestrującego się w systemie	**0,35**	**0,35**	**0**	**0**	**0**	**0**
2.11	Metody inżynierii społecznej - nakłonienie użytkownika do udostępnienia lub zmiany hasła	**0,55**	**0,35**	**0**	**0**	**0**	**0**
2.12	Wirusy komputerowe	**0,87**	**0**	**0**	**0,87**	**0**	**0**
3. Cyberterroryzm		**0,75**	**0**	**0**	**0,75**	**0,75**	**0**

Zagrożenie dla bezpieczeństwa informacji		Składowe bezpieczeństwa informacyjnego Sił Zbrojnych RP					
		Bezpieczeństwo prawne	Bezpieczeństwo osobowe	Bezpieczeństwo fizyczne	Bezpieczeństwo programowe	Bezpieczeństwo kryptograficzne	Bezpieczeństwo elektromagnetyczne
		N_1	N_2	N_3	N_4	N_5	N_6
4. Awarie i uszkodzenia sprzętowe							
4.1	Błędy projektowe	**0,51**	**0,51**	**0**	**0,51**	**0,51**	**0**
4.2	Wady produkcyjne	**0,53**	**0,53**	**0**	**0,51**	**0**	**0**
4.3	Błędy instalacji	**0,58**	**0,58**	**0**	**0**	**0**	**0**
4.4	Awarie	**0,64**	**0**	**0,64**	**0,64**	**0**	**0**
5. Emisja ujawniająca							
5.1	Emisja ujawniająca promieniowana	**0,42**	**0**	**0,42**	**0**	**0**	**0,42**
5.2	Emisja ujawniająca przewodzona - bezpośrednia	**0,40**	**0**	**0,40**	**0**	**0**	**0,40**
5.3	Emisja ujawniająca przewodzona - wtórna	**0,33**	**0**	**0,33**	**0**	**0**	**0,33**

Źródło: opracowanie własne

Model bezpieczeństwa informacyjnego można zapisać w postaci rozwiniętej w sposób następujący:

$$\mathbf{Y} = A\,\mathbf{X} + \xi, \tag{4.2}$$

gdzie $\mathbf{X}$ i $\mathbf{Y}$ są wektorami reprezentującymi sygnały wejściowy i wyjściowy zaś ξ jest wektorem wartości czynnika losowego. Symbolem A oznaczono operator ma-

cierzowy, którego składowe określono na podstawie wyników przeprowadzonych badań (patrz tabela 4.2.). Poszczególne macierze mają postać:

$$\mathbf{Y} = \begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ \dots \\ y_k \end{bmatrix} \qquad A = \begin{bmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1l} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2l} \\ a_{31} & a_{32} & a_{33} & \dots & a_{3l} \\ \dots & \dots & \dots & \dots & \dots \\ a_{k1} & a_{k2} & a_{k3} & \dots & a_{kl} \end{bmatrix} \qquad \mathbf{X} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ \dots \\ x_l \end{bmatrix}. \quad (4.3)$$

Normę wektora $\mathbf{Y}$ przyjęto w postaci: $\|\mathbf{Y}\| = \frac{\sqrt[k]{\sum_{i=1}^{k} y_k}}{k}$. (4.4)

Stosując założenie o normalności czynnika losowego, można przedstawić model (4.2) w postaci poniższego układu równań:

$$\begin{cases} y_1 = a_{11}x_1 + a_{12}x_2 + a_{13}x_3 + \dots + a_{1l}x_l \\ y_2 = a_{21}x_1 + a_{22}x_2 + a_{23}x_3 + \dots + a_{2l}x_l \\ y_3 = a_{31}x_1 + a_{32}x_2 + a_{33}x_3 + \dots + a_{3l}x_l \\ \qquad\qquad \dots\dots\dots\dots\dots \\ y_k = a_{k1}x_1 + a_{k2}x_2 + a_{k3}x_3 + \dots + a_{kl}x_l \end{cases} \quad (4.5)$$

Układ równań (4.5) reprezentuje wielorównaniowy model opisowy bezpieczeństwa informacyjnego RP o zależności prostej. Każde z równań stanowi submodel. Należy zauważyć, że w każdym z submodeli występują jedynie zmienne niezależne x_{ij}. W żadnym z równań nie występuje zależność zmiennej objaśnianej Y od pozostałych zmiennych objaśnianych. Wskazuje to jednoznacznie, że zbudowany model wielorównaniowy nie jest modelem współzależnym ani też rekurencyjnym.

Przykład obliczeniowy

Weźmy pod uwagę następujące rodzaje zagrożeń:

- fałszerstwo danych,

- atak słownikowy,
- wirusy komputerowe,
- podsłuch łączy,

oddziałujące na następujące składowe bezpieczeństwa informacyjnego:

x_1 - bezpieczeństwo programowe,

x_2 - bezpieczeństwo kryptograficzne,

x_3 - bezpieczeństwo elektromagnetyczne.

Operator macierzowy $\mathbf{A}$ redukuje się w tym przypadku do wielkości 4 x 3 i ma następującą postać: $\mathbf{A} = \begin{bmatrix} 0,58 & 0,58 & 0 \\ 0,64 & 0,64 & 0 \\ 0,87 & 0 & 0 \\ 0 & 0 & 0,41 \end{bmatrix}$,

zaś $\mathbf{X} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$ (przy założeniu jednakowego wpływu na każdą z trzech składowych rozpatrywanego bezpieczeństwa).

$$\mathbf{Y} = \begin{bmatrix} 0,58 & 0,58 & 0 \\ 0,64 & 0,64 & 0 \\ 0,87 & 0 & 0 \\ 0 & 0 & 0,41 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0,58 \cdot 1 + 0,58 \cdot 1 + 0 \cdot 1 \\ 0,64 \cdot 1 + 0,64 \cdot 1 + 0 \cdot 1 \\ 0,87 \cdot 1 + 0 \cdot 1 + 0 \cdot 1 \\ 0 \cdot 1 + 0 \cdot 1 + 0,41 \cdot 1 \end{bmatrix} = \begin{bmatrix} 1,16 \\ 1,28 \\ 0,87 \\ 0,41 \end{bmatrix}$$

Norma wektora $\mathbf{Y}$ wynosi: $\|\mathbf{Y}\| = \frac{\sqrt[4]{\sum_{i=1}^{4} y_k}}{4} = \frac{\sqrt[4]{1,16 + 1,28 + 0,87 + 0,41}}{4} = 0,35$.

Interpretacja wyniku:

Prawdopodobieństwa wystąpienia jednoczesnego zagrożenia ze strony: fałszerstwa danych, ataku słownikowego, wirusów komputerowych i podsłuchu łączy (przy założeniu jednakowego wpływu na każdą z trzech składowych rozpatrywanego bezpieczeństwa informacyjnego) wynosi ok. 0,35.

Przeprowadzimy teraz te same obliczenia, z tą różnicą, że wprowadzimy system wag harmonicznych, przydzielając tym samym różny priorytet poszczególnym zmiennym x. Dla zmiennych x_1, x_2, x_3 otrzymujemy następujące wartości wagowe: 0,111; 0,278 oraz 0,611. Wagi zostały obliczone na podstawie wzoru rekurencyjnego:

$$\begin{cases} wh_0 = 0 \\ wh_s = wh_{s-1} + \dfrac{1}{i(i-s+1)} \end{cases} \qquad (4.6)$$

gdzie: i – liczba zmiennych, s – nr zmiennej.

Na podstawie wzoru (4.6) dostajemy:

$$wh_0 = 0\,,$$

$$wh_1 = 0 + \frac{1}{3(3-1+1)} = \frac{1}{9} = 0{,}111$$

$$wh_2 = \frac{1}{9} + \frac{1}{3(3-2+1)} = \frac{1}{9} + \frac{1}{6} = 0{,}278$$

$$wh_3 = 0{,}278 + \frac{1}{3(3-3+1)} = 0{,}278 + \frac{1}{3} = 0{,}611$$

W tym przypadku mamy:

$$\mathbf{X} = \begin{bmatrix} 0,111 \\ 0,278 \\ 0,611 \end{bmatrix},$$

$$\mathbf{Y} = \begin{bmatrix} 0,58 & 0,58 & 0 \\ 0,64 & 0,64 & 0 \\ 0,87 & 0 & 0 \\ 0 & 0 & 0,41 \end{bmatrix} \cdot \begin{bmatrix} 0,111 \\ 0,278 \\ 0,611 \end{bmatrix} = \begin{bmatrix} 0,23 \\ 0,25 \\ 0,09 \\ 0,25 \end{bmatrix}$$

Norma wektora $\mathbf{Y}$ wynosi: $\|\mathbf{Y}\| = \dfrac{\sqrt[4]{\sum_{i=1}^{4} y_k}}{4} = \dfrac{\sqrt[4]{0,23+0,25+0,09+0,25}}{4} = 0,23$.

Interpretacja wyniku:

Prawdopodobieństwa wystąpienia jednoczesnego zagrożenia ze strony: fałszerstwa danych, ataku słownikowego, wirusów komputerowych i podsłuchu łączy, wynosi ok. 0,23 przy założeniu, że poszczególnym zagrożeniom przypisano wagi harmoniczne.

Wydaje się być również interesujący przypadek wykorzystania wag geometrycznych do przeprowadzanych rozważań. Wagi geometryczne (wg_s^i) zdefiniowane są następująco:

$$wq_s^i = \frac{(1-q)q^{i-s}}{(1-q^i)} \qquad (0 < q < 1;\ \ i = 1,2,...,T;\ \ s = 1,2,...,i)\,. \tag{4.7}$$

Wagi te charakteryzują się dużą zmiennością, zależną od parametru q. Dla q bliskiego zera, otrzymuje się wagi dążące szybko do zera zaś dla wartości bliskich jedności otrzymujemy wagi wolno malejące w miarę wzrostu parametru i (pokazują to rys. 4.2.÷4.4.).

W rozważanym przykładzie obliczeniowym, otrzymano następujące wartości wagowe dla poszczególnych zmiennych x_1, x_2, x_3 oraz przykładowych wartości q:

- dla $i = 3$ oraz $q = 0{,}1$

$$wg_1^3 = \frac{0{,}9 * 0{,}1^2}{(1 - 0{,}1^3)} = \frac{0{,}009}{0{,}999} \approx 0{,}01$$

$$wg_2^3 = \frac{0{,}9 * 0{,}1^1}{(1 - 0{,}1^3)} = \frac{0{,}090}{0{,}999} \approx 0{,}09$$

$$wg_3^3 = \frac{0{,}9 * 0{,}1^0}{(1 - 0{,}1^3)} = \frac{0{,}9}{0{,}999} \approx 0{,}90$$

- dla $i = 3$ oraz $q = 0{,}3$

$$wg_1^3 = \frac{0{,}7 * 0{,}3^2}{(1 - 0{,}3^3)} = \frac{0{,}063}{0{,}973} \approx 0{,}06$$

$$wg_2^3 = \frac{0{,}7 * 0{,}3^1}{(1 - 0{,}3^3)} = \frac{0{,}21}{0{,}973} \approx 0{,}22$$

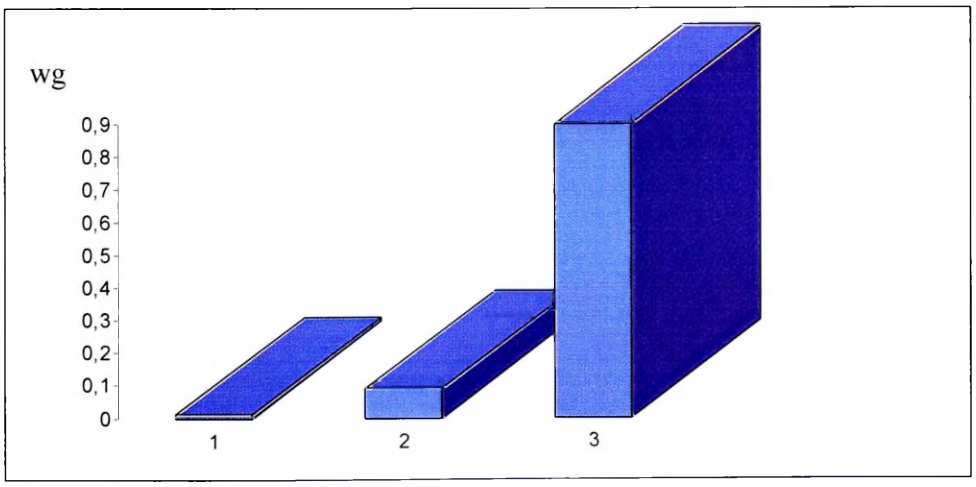
$$wg_3^3 = \frac{0{,}7 * 0{,}3^0}{(1 - 0{,}3^3)} = \frac{0{,}7}{0{,}973} \approx 0{,}72$$

- dla $i = 3$ oraz $q = 0{,}9$

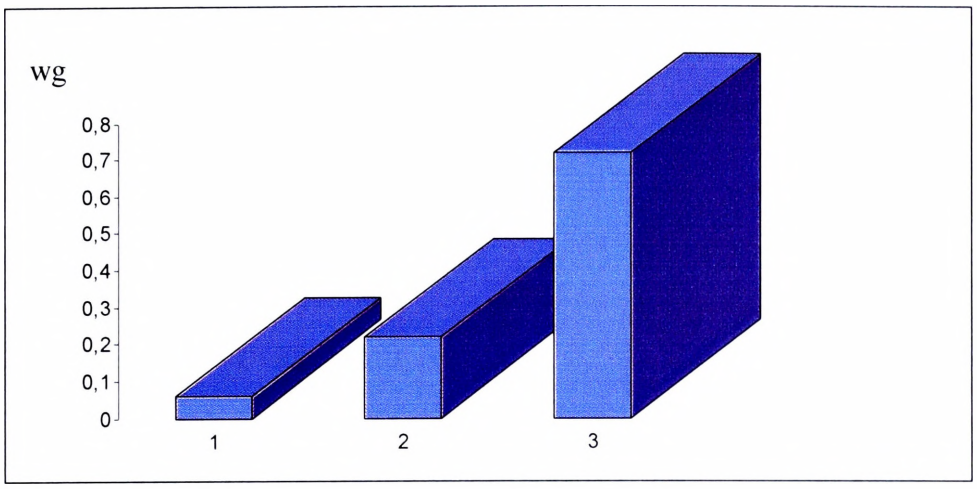
$$wg_1^3 = \frac{0{,}1 * 0{,}9^2}{1 - 0{,}9^3} = \frac{0{,}081}{0{,}271} \approx 0{,}299$$

$$wg_2^3 = \frac{0{,}1 * 0{,}9^1}{1 - 0{,}9^3} = \frac{0{,}09}{0{,}271} \approx 0{,}332$$

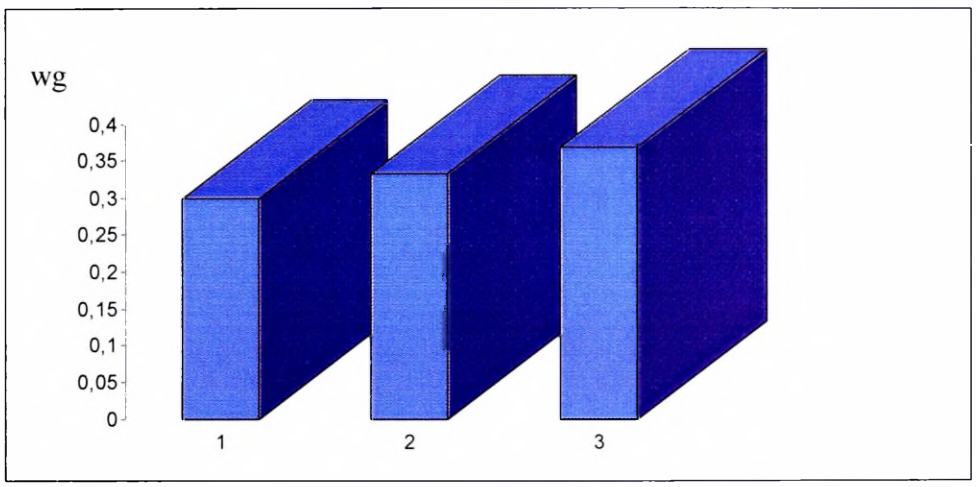
$$wg_3^3 = \frac{0{,}1 * 0{,}9^0}{1 - 0{,}9^3} = \frac{0{,}1}{0{,}271} \approx 0{,}369$$



Rys. 4.2. Wartości wag geometrycznych dla $i = 3$ oraz $q = 0{,}1$.
Źródło: opracowanie własne



Rys. 4.3. Wartości wag geometrycznych dla $i = 3$ oraz $q = 0{,}3$.
Źródło: opracowanie własne



Rys. 4.4. Wartości wag geometrycznych dla $i = 3$ oraz $q = 0{,}9$.
Źródło: opracowanie własne

W przypadku wag geometrycznych, dla $i = 3$ oraz $q = 0{,}1$ mamy:

$$\mathbf{X} = \begin{bmatrix} 0{,}01 \\ 0{,}09 \\ 0{,}90 \end{bmatrix},$$

$$\mathbf{Y} = \begin{bmatrix} 0{,}58 & 0{,}58 & 0 \\ 0{,}64 & 0{,}64 & 0 \\ 0{,}87 & 0 & 0 \\ 0 & 0 & 0{,}41 \end{bmatrix} \cdot \begin{bmatrix} 0{,}01 \\ 0{,}09 \\ 0{,}90 \end{bmatrix} = \begin{bmatrix} 0{,}058 \\ 0{,}064 \\ 0{,}009 \\ 0{,}369 \end{bmatrix}$$

Norma wektora $\mathbf{Y}$ wynosi:

$$\|\mathbf{Y}\| = \frac{\sqrt[4]{\sum_{i=1}^{4} y_k}}{4} = \frac{\sqrt[4]{0{,}058+0{,}064+0{,}009+0{,}369}}{4} = 0{,}21.$$

W przypadku $i = 3$ oraz $q = 0{,}3$:

$$\mathbf{X} = \begin{bmatrix} 0{,}06 \\ 0{,}22 \\ 0{,}72 \end{bmatrix},$$

$$\mathbf{Y} = \begin{bmatrix} 0{,}58 & 0{,}58 & 0 \\ 0{,}64 & 0{,}64 & 0 \\ 0{,}87 & 0 & 0 \\ 0 & 0 & 0{,}41 \end{bmatrix} \cdot \begin{bmatrix} 0{,}06 \\ 0{,}22 \\ 0{,}72 \end{bmatrix} = \begin{bmatrix} 0{,}162 \\ 0{,}179 \\ 0{,}052 \\ 0{,}295 \end{bmatrix}$$

Norma wektora $\mathbf{Y}$ wynosi:

$$\|\mathbf{Y}\| = \frac{\sqrt[4]{\sum_{i=1}^{4} y_k}}{4} = \frac{\sqrt[4]{0{,}162+0{,}179+0{,}052+0{,}295}}{4} = 0{,}23.$$

Zaś w przypadku $i = 3$ oraz $q = 0{,}9$:

$$\mathbf{X} = \begin{bmatrix} 0{,}299 \\ 0{,}332 \\ 0{,}369 \end{bmatrix},$$

$$\mathbf{Y} = \begin{bmatrix} 0{,}58 & 0{,}58 & 0 \\ 0{,}64 & 0{,}64 & 0 \\ 0{,}87 & 0 & 0 \\ 0 & 0 & 0{,}41 \end{bmatrix} \cdot \begin{bmatrix} 0{,}299 \\ 0{,}332 \\ 0{,}369 \end{bmatrix} = \begin{bmatrix} 0{,}366 \\ 0{,}404 \\ 0{,}260 \\ 0{,}151 \end{bmatrix}$$

Norma wektora $\mathbf{Y}$ wynosi:

$$\|\mathbf{Y}\| = \frac{\sqrt[4]{\sum_{i=1}^{4} y_k}}{4} = \frac{\sqrt[4]{0{,}366+0{,}404+0{,}260+0{,}151}}{4} = 0{,}26 .$$

Interpretacja wyniku:

Prawdopodobieństwa wystąpienia jednoczesnego zagrożenia ze strony: fałszerstwa danych, ataku słownikowego, wirusów komputerowych i podsłuchu łączy zawiera się w przedziale (0,21 0,26), przy założeniu, że poszczególnym zagrożeniom przypisano wagi geometryczne. Wartość średnia prawdopodobieństwa wynosi: 0,235 co daje wynik różniący się od uzyskanego w przypadku stosowania wag harmonicznych, o ok. 2%. Przeprowadzona analiza wskazuje na zasadność stosowania wag harmonicznych do rozważanych zagadnień oceny prawdopodobieństwa występowania poszczególnych rodzajów zagrożeń bezpieczeństwa informacyjnego Sił Zbrojnych RP.

4.3. Wykorzystanie arkusza kalkulacyjnego Microsoft Excel do oceny prawdopodobieństwa wystąpienia zagrożeń dla bezpieczeństwa informacyjnego Sił Zbrojnych RP

Opracowany arkusz kalkulacyjny uwzględnia wszystkie wcześniejsze założenia budowy modelu oraz algorytmu obliczeniowego. Od użytkownika wymaga się jedynie określenia, które z przyjętych zagrożeń będą oddziaływać, a które nie. Wyboru tego dokonuje się poprze przypisanie odpowiednim komórkom arkusza, zgodnie z przyjętymi założeniami, wartości ***1*** lub ***0***. Przykładowe arkusze wraz z obliczeniami przedstawiają tabele 4.4 i 4.5. Tabela 4.6. obrazuje obliczenia przy założeniu jednakowego wpływu na każdą ze składowych rozpatrywanego bezpieczeństwa, natomiast tabela 4.7. po wprowadzeniu systemu wag harmonicznych.

Wykorzystanie do obliczeń arkusza kalkulacyjnego MS Excel było uzasadnione zarówno dużą popularnością tego narzędzia jak również dużą jego mocą obliczeniową. Ponadto możliwe jest wykorzystanie zaprojektowanego arkusza kalkulacyjnego

jako serwera automatyzacji. Wówczas napisanie prostego programu – klienta w dowolnym języku wysokiego poziomu, umożliwia łatwe przeprowadzenie eksperymentów symulacyjnych bez konieczności bezpośredniej ingerencji w zaprojektowany arkusz kalkulacyjny. W ramach rozprawy wykonano jedynie projekt arkusza kalkulacyjnego z wbudowanym makropoleceniem. Umożliwiło to sprawne przeprowadzenie eksperymentu bez konieczności tworzenia dodatkowej aplikacji komputerowej.

Tabela 4.4.

Arkusz kalkulacyjny do obliczeń normy wektora $\|Y\|$ przy założeniu jednakowego wpływu na każdą ze składowych rozpatrywanego bezpieczeństwa (Przykład)

Zagrożenia dla bezpieczeństwa informacyjnego Sił Zbrojnych RP			**Składowe bezpieczeństwa informacyjnego Sił Zbrojnych RP**					
			Bezpieczeństwo prawne	Bezpieczeństwo osobowe	Bezpieczeństwo fizyczne	Bezpieczeństwo programowe	Bezpieczeństwo kryptograficzne	Bezpieczeństwo elektromagnetyczne
			a					
Podsłuch	$X_1=$	1	**0,55**	**0**	**0,55**	**0**	**0**	**0**
Kradzież, zgubienie	$X_2=$	1	**0,62**	**0,62**	**0,62**	**0**	**0**	**0**
Wykorzystanie władzy	$X_3=$	1	**0**	**0,79**	**0,79**	**0**	**0**	**0**
Wykorzystanie symparii	$X_4=$	1	**0**	**0,49**	**0,49**	**0**	**0**	**0**
Utrata danych na skutek działań z zewnątrz (Internet)	$X_5=$	1	**0,79**	**0**	**0,79**	**0,79**	**0,79**	**0**
Fałszerstwo danych	$X_6=$	1	**0,58**	**0,58**	**0**	**0,58**	**0,58**	**0**

$$Y = \begin{pmatrix} 1{,}1 \\ 1{,}9 \\ 1{,}6 \\ 1 \\ 3{,}2 \\ 2{,}3 \end{pmatrix} \qquad \|Y\| = 0{,}25$$

Tabela 4.5.

Arkusz kalkulacyjny do obliczeń normy wektora $\|Y\|$ po wprowadzeniu systemu wag harmonicznych (Przykład)

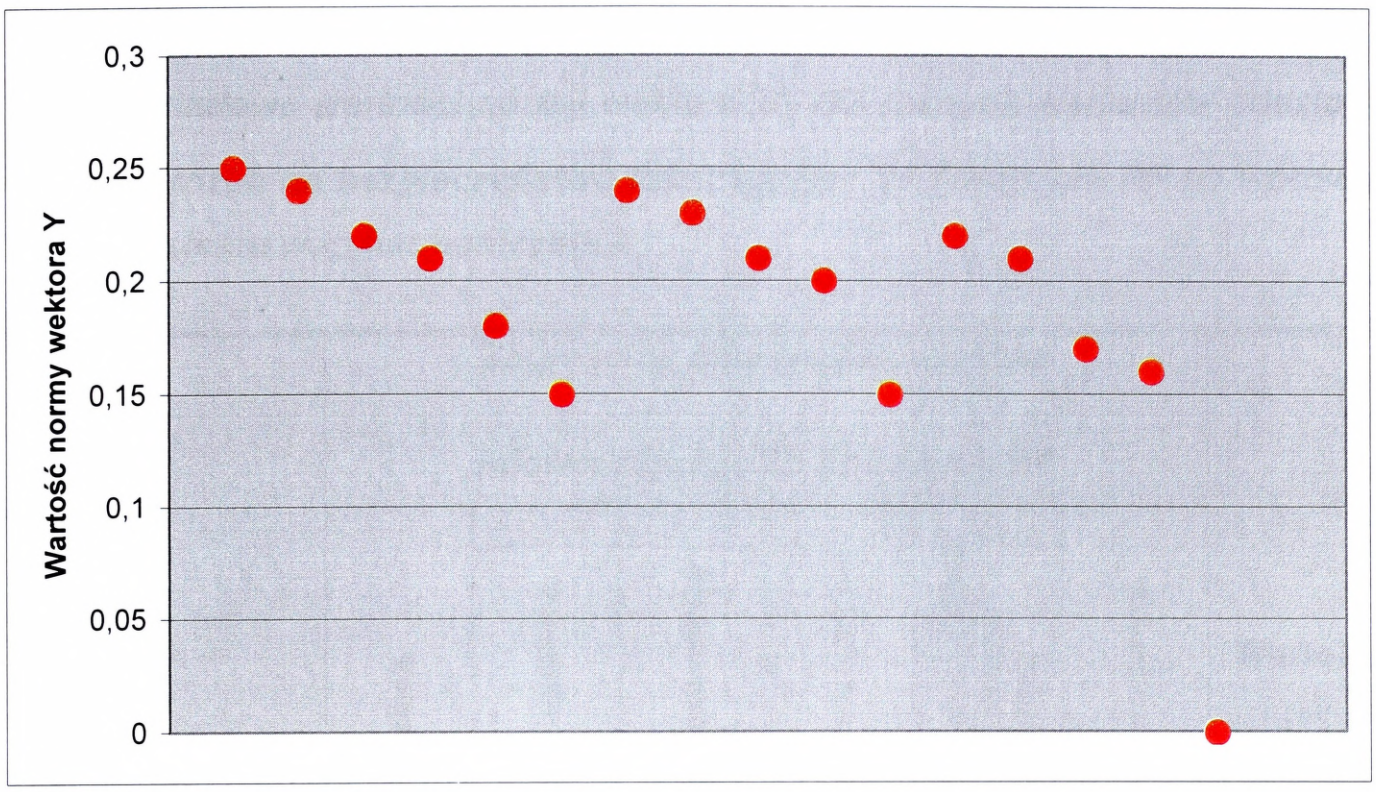
Zagrożenia dla bezpieczeństwa informacyjnego Sił Zbrojnych RP			**wartość wagowa**	**Składowe bezpieczeństwa informacyjnego Sił Zbrojnych RP**					
				Bezpieczeństwo prawne	Bezpieczeństwo osobowe	Bezpieczeństwo fizyczne	Bezpieczeństwo programowe	Bezpieczeństwo kryptograficzne	Bezpieczeństwo elektromagnetyczne
				a					
Podsłuch	$X_1=$	1	**0,028**	**0,55**	**0**	**0,55**	**0**	**0**	**0**
Kradzież, zgubienie	$X_2=$	1	**0,061**	**0,62**	**0,62**	**0,62**	**0**	**0**	**0**
Wykorzystanie władzy	$X_3=$	1	**0,103**	**0**	**0,79**	**0,79**	**0**	**0**	**0**
Wykorzystanie symparii	$X_4=$	1	**0,158**	**0**	**0,49**	**0,49**	**0**	**0**	**0**
Utrata danych na skutek działań z zewnątrz (Internet)	$X_5=$	1	**0,242**	**0,79**	**0**	**0,79**	**0,79**	**0,79**	**0**
Fałszerstwo danych	$X_6=$	1	**0,408**	**0,58**	**0,58**	**0**	**0,58**	**0,58**	**0**

$$Y = \begin{pmatrix} 0{,}0718 \\ 0{,}1188 \\ 0{,}1295 \\ 0{,}0803 \\ 0{,}4191 \\ 0{,}2836 \end{pmatrix} \qquad \|Y\| = 0{,}17$$

Tabela 4.6.

Przykładowe wartości normy wektora $\|Y\|$ dla różnych wariantów oddziaływania zagrożeń na bezpieczeństwo informacyjne Sił Zbrojnych RP przy założeniu jednakowego wpływu na każdą ze składowych rozpatrywanego bezpieczeństwa

	Zagrożenia dala bezpieczeństwa informacyjnego Sił Zbrojnych RP						Wartość $\|Y\|$
	Podsłuch	Kradzież, zgubienie	Wykorzystanie władzy	Wykorzystanie sympatii	Utrata danych na skutek działań z zewnątrz (Internet)	Fałszerstwo danych	
Oddziaływanie zagrożeń na bezpieczeństwo informacyjnej Sił Zbrojnych RP	1	1	1	1	1	1	**0,25**
	1	1	1	1	1	0	**0,24**
	1	1	1	1	0	0	**0,22**
	1	1	1	0	0	0	**0,21**
	1	1	0	0	0	0	**0,18**
	1	0	0	0	0	0	**0,15**
	0	1	1	1	1	1	**0,24**
	0	1	1	1	1	0	**0,23**
	0	1	1	1	0	0	**0,21**
	0	1	1	0	0	0	**0,20**
	0	1	0	0	0	0	**0,15**
	0	0	1	1	1	1	**0,22**
	0	0	1	1	1	0	**0,21**
	0	0	1	1	0	0	**0,17**
	0	0	1	0	0	0	**0,16**
	0	0	0	0	0	0	**0**



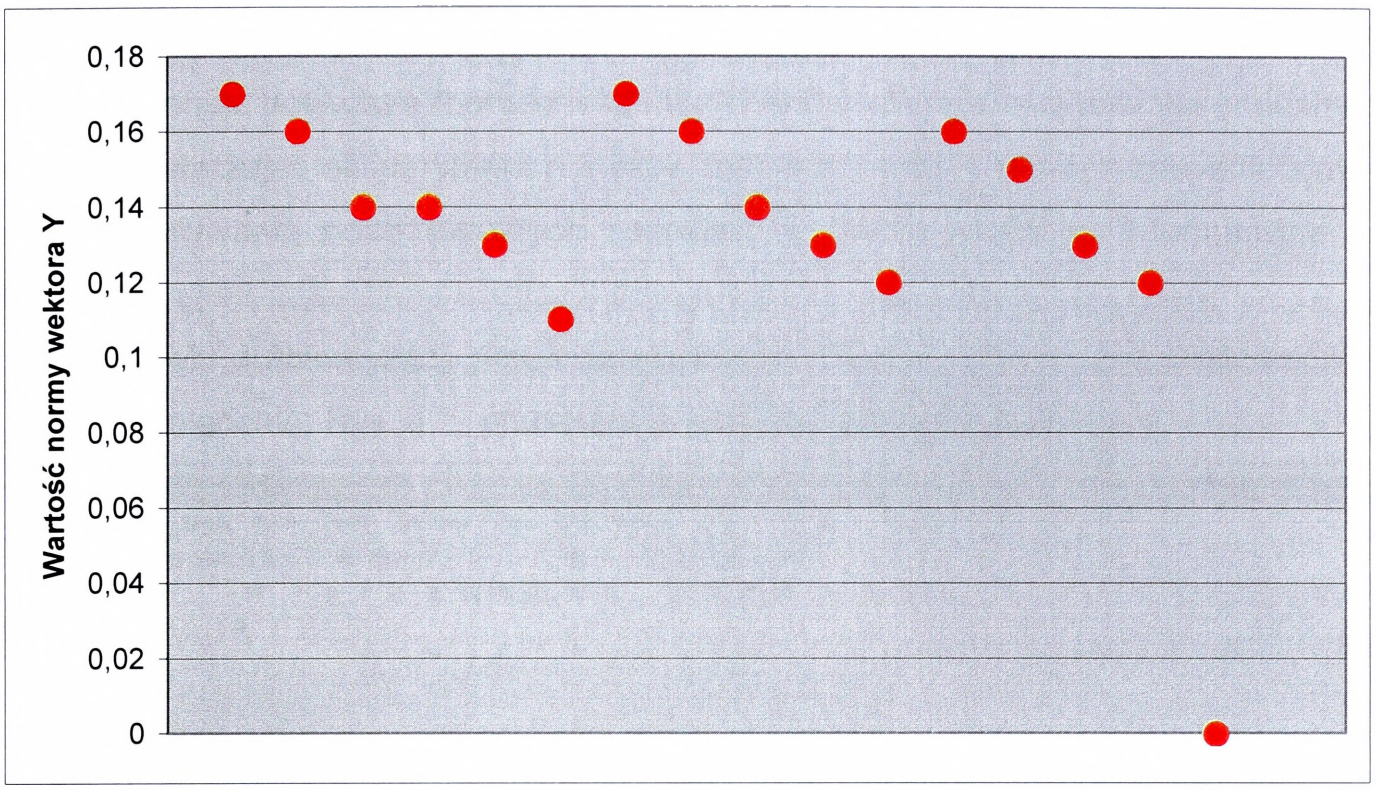
Rys. 4.5. ***Rozkład wartości normy wektora $\|Y\|$ dla różnych wariantów oddziaływania zagrożeń na bezpieczeństwo informacyjne Sił Zbrojnych RP przy założeniu jednakowego wpływu na każdą ze składowych rozpatrywanego bezpieczeństwa***

Źródło: Opracowanie własne.

Tabela 4.7.

Przykładowe wartości normy wektora $\|Y\|$ dla różnych wariantów oddziaływania zagrożeń na bezpieczeństwo informacyjne Sił Zbrojnych RP po wprowadzeniu systemu wag harmonicznych

	Zagrożenia dala bezpieczeństwa informacyjnego Sił Zbrojnych RP						Wartość $\|Y\|$
	Podsłuch	Kradzież, zgubienie	Wykorzystanie władzy	Wykorzystanie symparii	Utrata danych na skutek działań z zewnątrz (Internet)	Fałszerstwo danych	
Oddziaływanie zagrożeń na bezpieczeństwo informacyjne Sił Zbrojnych RP	1	1	1	1	1	1	**0,17**
	1	1	1	1	1	0	**0,16**
	1	1	1	1	0	0	**0,14**
	1	1	1	0	0	0	**0,14**
	1	1	0	0	0	0	**0,13**
	1	0	0	0	0	0	**0,11**
	0	1	1	1	1	1	**0,17**
	0	1	1	1	1	0	**0,16**
	0	1	1	1	0	0	**0,14**
	0	1	1	0	0	0	**0,13**
	0	1	0	0	0	0	**0,12**
	0	0	1	1	1	1	**0,16**
	0	0	1	1	1	0	**0,15**
	0	0	1	1	0	0	**0,13**
	0	0	1	0	0	0	**0,12**
	0	0	0	0	0	0	**0**



Rys. 4.6. ***Rozkład wartości normy wektora $\|Y\|$ dla różnych wariantów oddziaływania zagrożeń na bezpieczeństwo informacyjne Sił Zbrojnych RP przy założeniu jednakowego wpływu na każdą ze składowych rozpatrywanego bezpieczeństwa***

Źródło: Opracowanie własne.

Eksperyment symulacyjny wykonany przy pomocy arkusza MS Excel

W przeprowadzonym eksperymencie symulacyjnym zastosowano metodę Monte Carlo (patrz opis w rozdziale 1.6.), którą zaimplementowano do arkusza kalkulacyjnego MS Excel, wykorzystując dostępne funkcje analityczne.

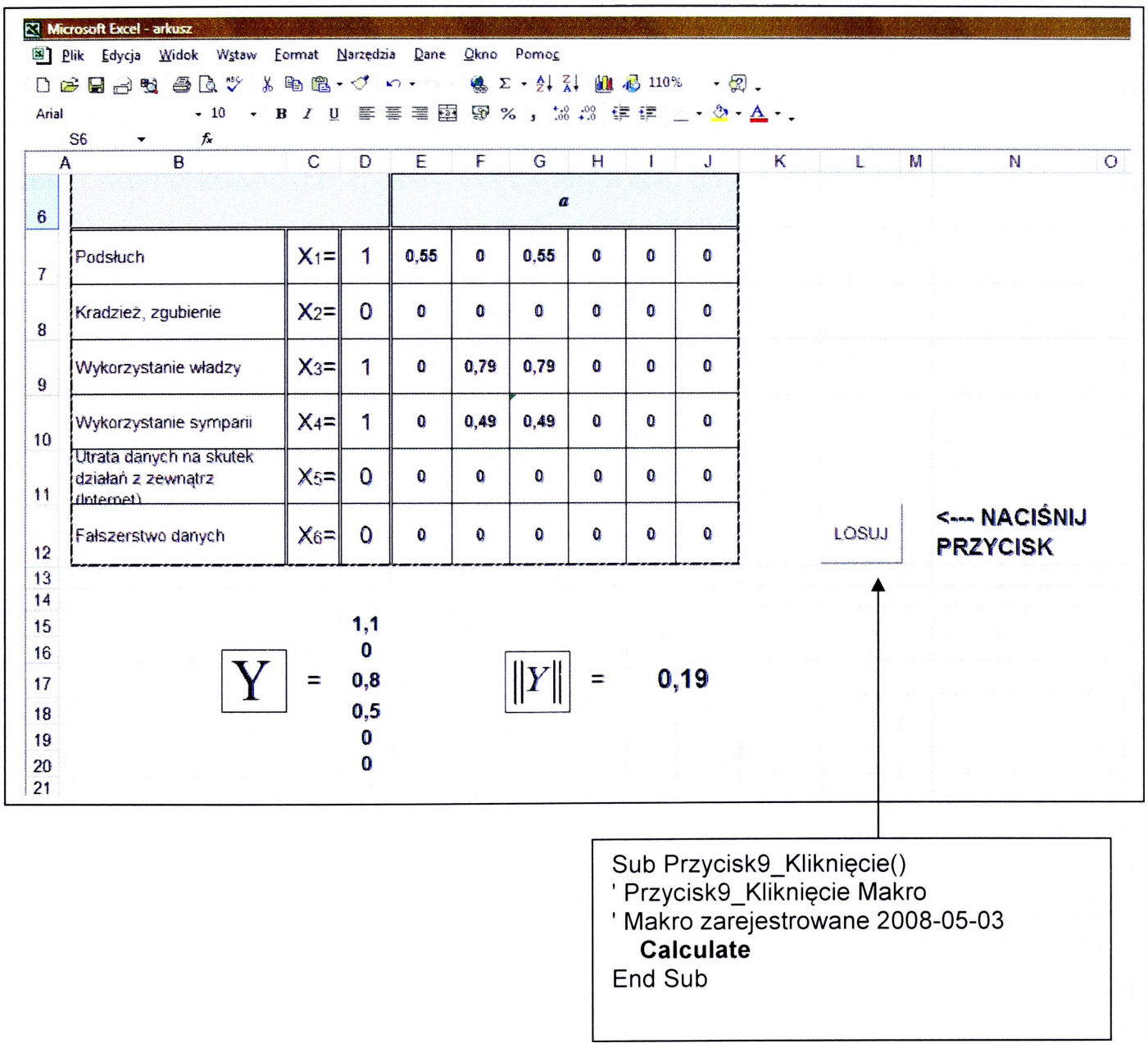
W arkuszu kalkulacyjnym MS Excel występuje funkcja bezargumentowa LOS(), zwracająca liczbę losową z przedziału (0,1) po każdorazowym przeliczeniu arkusza kalkulacyjnego[155]. Wartości zwracane przez funkcję LOS() mają jednostajny rozkład prawdopodobieństwa ich wystąpienia, co oznacza, że szansa wystąpienia każdej liczby należącej do przedziału (0,1) jest jednakowa. Jest to uzasadnione poprzez stałą i różną od zera wartość funkcji gęstości prawdopodobieństwa.

[155] Przeliczenie arkusza kalkulacyjnego można wywołać każdorazowo po naciśnięciu klawisza funkcyjnego F9 lub uruchomieniu stosownego makropolecenia.

W zaprojektowanym eksperymencie symulacyjnym wykorzystano funkcję LOS() do losowego generowania jednej z dwóch wartości: 0 lub 1, co można osiągnąć poprzez formułę: **=JEŻELI(ZAOKR.W.DÓŁ(1-LOS();0,5)=0,5;1;0)**.

Wpisując powyższą formułę w komórki odpowiadające rozważanym zmiennym x_i oraz powtarzając eksperyment n – razy, możliwym staje się prognozowanie zjawiska oddziaływania poszczególnych zagrożeń na bezpieczeństwo informacyjne sił zbrojnych.

W celu automatyzacji przeprowadzanych obliczeń, można użyć odpowiedniego makropolecenia. Rys. 4.7. przedstawia przykład takiego rozwiązania.



Rys. 4.7. Zrzut ekranowy arkusza kalkulacyjnego z zaimplementowanym makropoleceniem ułatwiającym przeprowadzenie eksperymentów symulacyjnych.

Źródło: Opracowanie własne.

4.4. Wnioski

Złożoność problematyki bezpieczeństwa informacyjnego Sił Zbrojnych RP wymaga zastosowania do jego badań zaawansowanych metod i technik badawczych. Opierając się na badaniach ankietowych uzyskano wartości składowych bezpieczeństwa informacyjnego Sił Zbrojnych RP. Wartości te tworzą zbiór elementów operatora macierzowego **A** zaproponowanego modelu opisowego.

W trakcie badań stwierdzono, że najlepszym modelem bezpieczeństwa informacyjnego Sił Zbrojnych będzie wielorównaniowy, opisowy, model analityczny. Opracowany model nie pozwala na odwzorowanie całego spektrum zagadnień związanych z problematyką bezpieczeństwa informacyjnego, jednakże jego budowa pozwala na przeprowadzenie symulacji komputerowych. Symulacje nie wymagają tworzenia skomplikowanych aplikacji komputerowych, gdyż oczekiwane wyniki osiągnięto już przy wykorzystanie arkusza kalkulacyjnego MS Excel.

Stan, jaki osiągnięto na koniec badań realizowanych w ramach dysertacji, pozwala na dalsze ich prowadzenie oraz udoskonalanie zarówno zaproponowanego modelu jak i narzędzi symulacyjnych.

ZAKOŃCZENIE

Celem dysertacji było określenie możliwości zastosowania metod symulacji komputerowych w modelowaniu bezpieczeństwa informacyjnego w siłach zbrojnych.

Przeprowadzone badania pozwoliły na rozwiązanie problemu badawczego w pełnym zakresie biorąc po uwagę przyjęte ograniczenia. Procedura badawcza pozwoliła na potwierdzenie hipotez roboczych i osiągnięcie celu dysertacji.

Badania były oparte na szerokim spektrum materiałów teoretycznych. Wykorzystano dostępne materiały z zakresu metodologii badań naukowych, identyfikacji zagrożeń informacyjnych, teorii modelowania i symulacji, a także akty prawne ogólno dostępne i unormowania resortu obrony narodowej.

Przedstawione w dysertacji wyniki otrzymano na podstawie przeprowadzonych badań empirycznych, w tym modelowania bezpieczeństwa informacyjnego Sił Zbrojnych RP oraz na podstawie zrealizowanych badań ankietowych. Badania empiryczne poprzedzone były wstępnymi badaniami teoretycznymi, które pozwoliły na ustalenie teoretycznych podstaw problemu badawczego.

Przeprowadzone badania teoretyczne i empiryczne modelowania bezpieczeństwa informacyjnego Sił Zbrojnych RP, pozwalają na sformułowanie następujących wniosków:

1) Bezpieczeństwo informacyjne Sił Zbrojnych zależy od wielu złożonych czynników. Ich identyfikacja oraz określenie możliwych zagrożeń i skutków wystąpienia pozwoli na zorganizowanie właściwego systemu zabezpieczeń.
2) Najważniejszym elementem w zapewnieniu bezpieczeństwa informacyjnego jest właściwy dobór personelu posiadającego właściwy poziom wiedzy oraz świadomoś możliwych zagrożeń. Należy prowadzić cykliczne szkolenia personelu, w celu podniesienia poziomu świadomości zagrożeń oraz rozpowszechniania wiedzy o metodach ataków i ochrony przed nimi.
3) Incydenty naruszeń bezpieczeństwa informacyjnego są coraz rozleglejsze i coraz trudniej ustalić źródło ataku, a faktyczne szkody ujawniają się dopiero po pewnym czasie.
4) Modelowanie jest zaawansowaną techniką badawczą, mającą perspektywy zastosowania w analizie problematyki bezpieczeństwa informacyjnego zarówno w sferze wojskowej jak i cywilnej.

5) Zbudowany w ramach dysertacji model bezpieczeństwa informacyjnego Sił Zbrojnych RP pozwala na szacowanie ryzyka wystąpienia zespołu zagrożeń.
6) Do skutecznego prognozowania skutków wystąpienia zagrożeń informacyjnych mogą być wykorzystywane metody symulacyjne, w tym metody symulacji komputerowych.
7) Zastosowanie eksperymentów symulacyjnych w bieżącym prognozowaniu naruszenia integralności bezpieczeństwa informacyjnego Sił Zbrojnych RP pozwoli na właściwy dobór metod i środków ochrony.
8) Prowadzanie eksperymentów symulacyjnych nie wymaga specjalistycznych, a co się z tym wiąże, kosztownych aplikacji komputerowych. Możliwości takie dają powszechnie dostępne aplikacje.
9) Zaproponowany wielorównaniowy, opisowy, model analityczny dobrze odzwierciedla sytuacje rzeczywiste przy przyjętych ograniczeniach badawczych. Model ten nie pretenduje do miana „modelu wyjaśniającego" całe spektrum zagadnień związanych z problematyką bezpieczeństwa informacyjnego. Przeprowadzone badania wykazały celowość budowy modelu oraz wskazują na potrzebę tego typu rozważań teoretycznych.
10) Poruszona w dysertacji problematyka nie została wyczerpana. Zasadnym wydaje się prowadzenie dalszych, szczegółowych badań w tym zakresie. Szczególne możliwości istnieją w obszarze uniwersalizacji modelu bezpieczeństwa oraz tworzenia koncepcji wykorzystania techniki komputerowej w prowadzeniu eksperymentów symulacyjnych. Prawdopodobnie autor niniejszej rozprawy będzie kontynuował prace w tym kierunku, co wynika z jego zainteresowań naukowych.

Można powiedzieć, że cechą obecnego stulecia jest przewartościowanie zagrożeń oraz zmiana znaczenia poszczególnych komponentów Sił Zbrojnych. Prowadzenie działań skoncentrowanych na oddziaływania w sferze informacyjnej oraz powszechne stosowanie wysoce zawansowanych technologii informacyjnych rodzi ogromne możliwości, odpłacając się w zamian nowymi rodzajami zagrożeń. To nie wielkie armie stanowią obecnie główne źródło zagrożeń, lecz organizacje o bliżej nieokreślonej strukturze. Powszechność dostępu do Internetu daje tym organizacjom możliwości zarówno szybkiej i anonimowej komunikacji jak i wkłada do ręki broń, jakiej do tej pory nie znano. Możliwości zdalnych ataków na zasoby informacyjne Sił

Zbrojnych i organizacji cywilnych oraz techniczne zdolności oddziaływania na systemy sterowania elementami infrastruktury krytycznej każdego państwa okazuje nową jakość zagrożeń.

Dlatego też tak istotne są działania wyprzedzające, prognozowanie potencjalnych ataków oraz tworzenie systemów zabezpieczeń. Nieocenionym elementem takich działań mogą stać się narzędzia oparte na technikach modelowania i symulacji komputerowych.

W przedstawionej dysertacji podjęto próbę zbudowania narzędzia, pozwalającego na wstępne, szacunkowe określenie wielkości potencjalnego zagrożenia. Zaproponowana postać modelu oraz przeprowadzone badania pozwalają stwierdzić, że cel ten został osiągnięty.

BIBLIOGRAFIA

1. Aloks W., Karpiński C., Mencel A., *Rola inżynierii kompatybilności elektromagnetycznej w procesie budowy systemów elektronicznych*, Biuletyn WAT, Warszawa 1995.
2. Barczak A., Sydoruk T., *Bezpieczeństwo systemów informatycznych zarządzania*, Bellona, Warszawa 2003.
3. Bączek P., *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Wydawnictwo Adam Marszałek, Toruń 2005.
4. Białnicki – Birula. I., Białnicka – Birula I., *Modelowanie rzeczywistości*, Wydawnictwo Naukowo – Techniczne, Warszawa 2007.
5. Bielecki R., *Pustynna Burza*, Wydawnictwo Bellona, Warszawa 1991.
6. Bógdoł – Brzezińska A., Gawrycki M., *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Fundacja Studiów Międzynarodowych, Warszawa 2003.
7. Ciborowski L., *Walka informacyjna*, Toruń 1999.
8. Cieślarczyk M., *Metody, techniki i narzędzia badawcze oraz elementy statystyki stosowane w pracach magisterskich i doktorskich*, Akademia Obrony Narodowej, Warszawa 2006.
9. Chyliński A., *Metoda Monte Carlo w bankowości*, Wydawnictwo TWIGGER S.A., Warszawa 1999.
10. Czarota Z., *Operacje informacyjne w wojnach nad Zatoką Perską*, http://coniw.wp.mil.pl/modules.php?name=News&file=article&sid=390.
11. Czechowski R., Sienkiewicz P., *Przestępcze oblicza komputerów*, PWN, Warszawa 1993.
12. Denning D., *Wojna informacyjna i bezpieczeństwo informacji*, Wydawnictwo Naukowo - Techniczne, Warszawa 2002.
13. Gawliczek P., Pawłowski J., *Zagrożenia asymetryczne*, Akademia Obrony Narodowej, Warszawa 2003.
14. Gert B., *Hacker Can Shut Down the Power Grid*, Military Admits, Washington Times 16 kwietnia 1998 r.
15. Goban-Klas T., Sienkiewicz P., *Społeczeństwo informacyjne: Szanse, zagrożenia, wyzwania*, Wydawnictwo Fundacji Postępu Telekomunikacji, Kraków 1999.
16. Gruszyński M., *Mierzejewski P., Wstęp do ekonometrii w stu oknach*, *Wydawnictwo AGH, 1999.*
17. Gutenabum J., *Modelowanie matematyczne systemów*, Akademicka Oficyna Wydawnicza EXIT, Warszawa 2003.
18. Hajduk E., *Hipoteza w badaniach pedagogicznych*, wyd. WSP, Zielona Góra 1996.
19. Heermann D.W., *Podstawy symulacji komputerowych w fizyce*, WNT, Warszawa 1997.

20. Janczak J., *Zakłócanie informacyjne*, Akademia Obrony Narodowej, Warszawa 2001.
21. Janczak J., Świdzikowski G., *Bezpieczeństwo informacji w wojskowym systemie telekomunikacyjnym*, Akademia Obrony Narodowej, Warszawa 2004.
22. Jemioło T., *Modelowanie zagrożeń dla bezpieczeństwa informacyjnego państwa: teoria walki informacyjnej*, Akademia Obrony Narodowej, Warszawa 2004.
23. Kinasiewicz M., *Modelowanie procesów walki informacyjnej: model „Cyberwar", Akademia Obrony Narodowej*, Warszawa 2006.
24. Kopaliński W., *Słownik wyrazów obcych i zwrotów obcojęzycznych*, wydanie XVII rozszerzone, Wydawnictwo Wiedza Powszechna, Warszawa 1989.
25. Krakowski K., *Symulacje numeryczne w procesie doskonalenia dowództw szczeble taktycznego Wojsk Lądowych SZ RP*, Rozprawa doktorska, Akademia Obrony Narodowej, Warszawa 2006.
26. Lorak, *Inwigilacja elektroniczna i bezpośrednia*, Wydawnictwo FTA – INSIDER TRADING, 2003.
27. Łapińska – Sobczak N., *Opisowe modele ekonometryczne*, Wydawnictwo Uniwersytetu Łódzkiego, Łódź 2006.
28. Łobocki M., *Wprowadzenie do metodologii badań pedagogicznych*, wyd. Impuls. Kraków 2007.
29. Majewski T., *Miejsce celów, problemów i hipotez w procesie badań naukowych*, Akademia Obrony Narodowej, Warszawa 2006.
30. Majewski T., *Ankieta i wywiad w badaniach wojskowych*, Akademia Obrony Narodowej, Warszawa 2002.
31. Molander R. C., Riddile A. S., Wilson S. A., *Strategic Information Warfare: A New Face of War*, Santa Monica 1996.
32. Nowak S., *Metodologia badań społecznych*, Warszawa 1985.
33. Orłowski H., Hawryluk J., *Modelowanie cyfrowe*, Wydawnictwo Naukowo-Techniczne, Warszawa 1971.
34. Osiecki J., *Elementy modelowania w dynamice maszyn*, praca zbiorowa, wyd. PAN, Zakład im. Ossolińskich, Wrocław 1974.
35. Pilch T., *Zasady badań pedagogicznych*, (wyd. II), wyd. WA „Żak", Warszawa 1998.
36. *Rozporządzenie Prezesa RM z dn. 25.02.1999 r. w sprawie podstawowych wymagań bezpieczeństwa, DZ.U. Nr 18, poz. 162.*
37. Spustek H., *Wybrane zagadnienia badań operacyjnych i modelowania liniowego*, Akademia Obrony Narodowej, Warszawa 2002.
38. Spustek H., Żach A., *Zjawiska emisji elektromagnetycznej a bezpieczeństwo informacyjne,* Akademia Obrony Narodowej, Warszawa 2007.
39. Spustek H., Żach A., *Modelowanie zagrożeń informacyjnych*, Materiały XII konferencji z cyklu Komputerowe Systemy Wielodeostępowe KSW' 2006, Bydgoszcz – Ciechocinek 2006.

40. Stokłosa J., Bilski T., Pankowski T., *Bezpieczeństwo danych w systemach informatycznych*, Wydawnictwo Naukowe PWN, Warszawa - Poznań 2001.
41. Söderström T., Stoica P., *Identyfikacja systemów*, Wydawnictwo Naukowe PWN, Warszawa 1997.
42. *Strategia bezpieczeństwa narodowego Rzeczypospolitej Polskiej, www.bbn.gov.pl/dokumenty/SBN_RP.pdf.*
43. Szczepaniak C., *Podstawy modelowania systemu człowiek – pojazd – otoczenie*, Wyd. Naukowe PWN, Warszawa 1999.
44. Szpyra R., *Militarne operacje informacyjne*, Akademia Obrony Narodowej, Warszawa 2003.
45. Szpyra R., *Walka informacyjna w przyszłych działaniach sił powietrznych, Praca badawcza pod kryptonimem „CYBERAWIATOR"* , Warszawa 2000.
46. Szymański J.M., Życie systemów, *Wydawnictwo Wiedza Powszechna,* Warszawa 1991.
47. Söderström T., Stoica P., *Identyfikacja systemów,* Wydawnictwo Naukowe PWN, Warszawa 1997.
48. Willa R., *Dezinformacja, propaganda, walka psychologiczna podczas konfliktu w Zatoce Perskiej 1990 – 1991*, http://www.dialogi.umk.pl/dezinformacja - konflikt - zatoka – perska.html.
49. *Umowa między Stronami Traktatu Północnoatlantyckiego o ochronie informacji, sporządzona w Brukseli dnia 6 marca 1997 r., Dz.U. 2000 nr 64 poz. 740.*
50. *Ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych, Dz.U. 1999 nr 11 poz. 95.*
51. *Ustawa z dnia 6 czerwca 1997 r., Kodeks karny (Dz. U. z dnia 2 sierpnia 1997 r.), Rozdział XXXIII - Przestępstwa przeciwko ochronie informacji.*
52. *Ustawa z dnia 22 stycznia 1999 roku o ochronie informacji niejawnych.*
53. Zaczyński W., *Praca badawcza nauczyciela*, Warszawa 1997.
54. Zeliaś A., *Teoria prognozy*, Polskie Wydawnictwo Ekonomiczne, Warszawa 1997.
55. Zieleniewski J., *Organizacja i zarządzanie*, Państwowe Wydawnictwo Naukowe, Warszawa 1981.
56. Żach A., *Scenariusze zagrożenia informacyjnego państwa*, Akademia Obrony Narodowej, Warszawa 2003.
57. http://pl.wikipedia.org/wiki/Mistyfikacja.
58. http://pl.wikipedia.org/wiki/Mistyfikacja#Przyk.C5.82ady_g.C5.82o.C5.9Bnych_mistyfikacji.
59. *PN-I-13335-1: 1999 Technika informatyczna - Wytyczne do zarządzania bezpieczeństwem systemów informatycznych - Pojęcia i modele bezpieczeństwa systemów informatycznych.*

ZAŁĄCZNIKI

Załącznik 1

Zestawienie wyników badań ankietowych

W przedstawionych poniżej wynikach badań liczba respondentów była różna ze względu na unikanie przez badanych odpowiedzi na poszczególne pytania.

Brak odpowiedzi w metryczkach (8 na 58 respondentów) nie pozwoliła na wykonanie pełnej analizy badanej grupy.

1. Opinia respondentów na temat prawdopodobieństwa wystąpienia nieuprawnionego ujawnienia informacji

1.1. Podsłuch

Tabela 1

Prawdopodobieństwa wystąpienia	Ilość respondentów	Procent
Niemożliwe	0	0
Raczej niemożliwe	9	16
Trudno powiedzieć	32	55
Prawdopodobne	14	24
Bardzo prawdopodobne	3	5
Razem	**58**	**100**

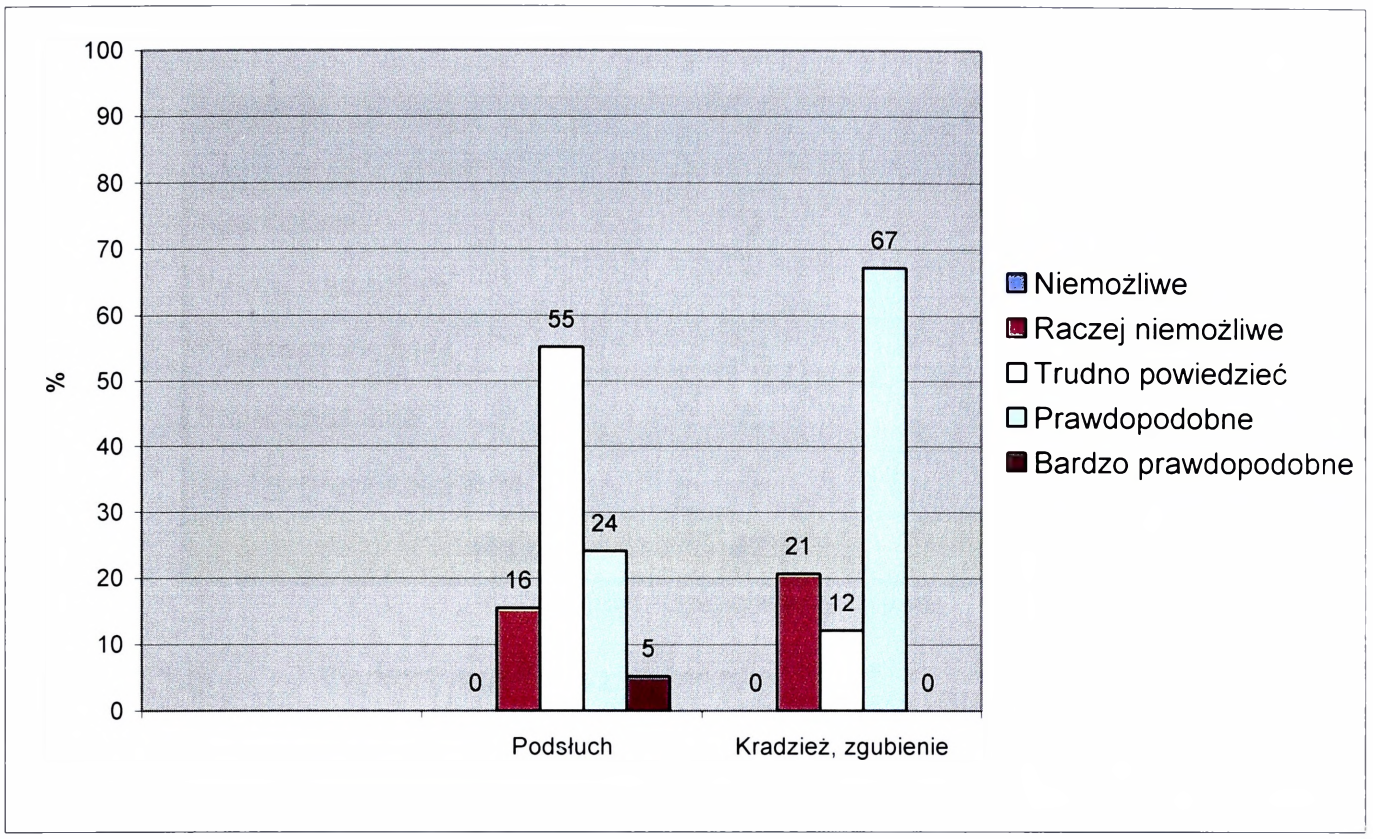
Źródło: Opracowanie własne.

1.2. Kradzież, zgubienie

Tabela 2

Prawdopodobieństwa wystąpienia	Ilość respondentów	Procent
Niemożliwe	0	0
Raczej niemożliwe	12	21
Trudno powiedzieć	7	12
Prawdopodobne	39	67
Bardzo prawdopodobne	9	0
Razem	**58**	**100**

Źródło: Opracowanie własne.



Wykres 1. *Procentowe zestawienie opinii respondentów na temat prawdopodobieństwa wystąpienia nieuprawnionego ujawnienia informacji*
Źródło: Opracowanie własne.

1.3. Zagrożenia socjotechniczne

1.1.3. Wykorzystanie władzy

Tabela 3

Prawdopodobieństwa wystąpienia	Ilość respondentów	Procent
Niemożliwe	0	0
Raczej niemożliwe	4	7
Trudno powiedzieć	0	0
Prawdopodobne	37	64
Bardzo prawdopodobne	17	29
Razem	**58**	**100**

Źródło: Opracowanie własne.

1.1.4. Wykorzystanie symparii

Tabela 4

Prawdopodobieństwa wystąpienia	Ilość respondentów	Procent
Niemożliwe	0	0
Raczej niemożliwe	7	15
Trudno powiedzieć	34	72
Prawdopodobne	6	13
Bardzo prawdopodobne	0	0
Razem	**47**	**100**

Źródło: Opracowanie własne.

1.1.5. Wykorzystanie wzajemności

Tabela 5

Prawdopodobieństwa wystąpienia	Ilość respondentów	Procent
Niemożliwe	0	0
Raczej niemożliwe	9	17
Trudno powiedzieć	33	62
Prawdopodobne	10	19
Bardzo prawdopodobne	1	2
Razem	**53**	**100**

Źródło: Opracowanie własne.

1.1.6. Wykorzystanie konsekwencji

Tabela 6

Prawdopodobieństwa wystąpienia	Ilość respondentów	Procent
Niemożliwe	0	0
Raczej niemożliwe	10	17
Trudno powiedzieć	15	26
Prawdopodobne	33	57
Bardzo prawdopodobne	0	0
Razem	**58**	**100**

Źródło: Opracowanie własne.

1.1.7. Wykorzystanie zasady przyzwolenia społecznego

Tabela 7

Prawdopodobieństwa wystąpienia	Ilość respondentów	Procent
Niemożliwe	0	0
Raczej niemożliwe	7	12
Trudno powiedzieć	18	31
Prawdopodobne	33	57
Bardzo prawdopodobne	0	0
Razem	**58**	**100**

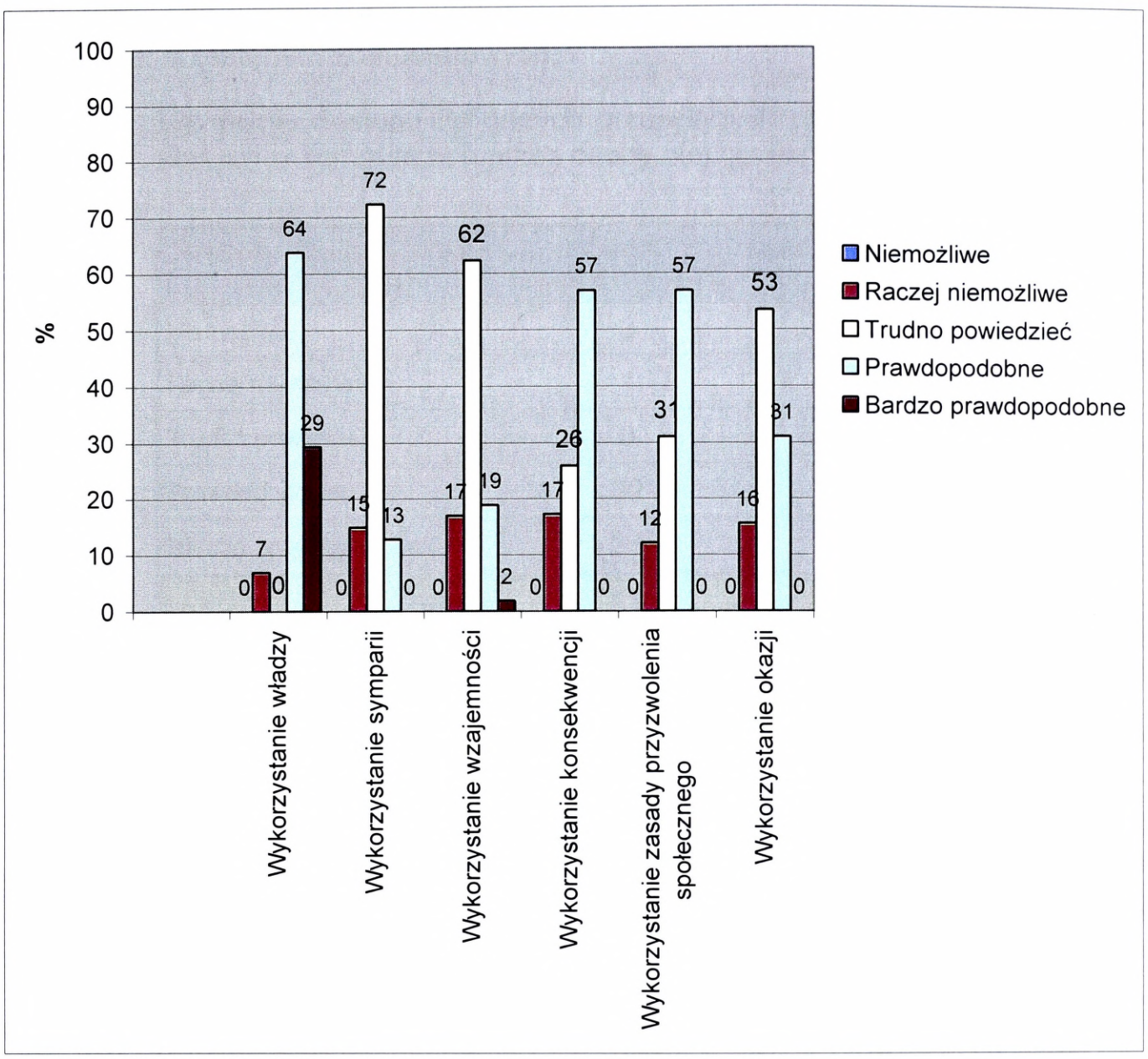
Źródło: Opracowanie własne.

1.1.8. Wykorzystanie okazji

Tabela 8

Prawdopodobieństwa wystąpienia	Ilość respondentów	Procent
Niemożliwe	0	0
Raczej niemożliwe	9	16
Trudno powiedzieć	31	53
Prawdopodobne	18	31
Bardzo prawdopodobne	0	0
Razem	**58**	**0**

Źródło: Opracowanie własne.



Wykres 2. *Procentowe zestawienie opinii respondentów na temat prawdopodobieństwa wystąpienia zagrożeń socjotechnicznych*
Źródło: Opracowanie własne

2. Opinia respondentów na temat prawdopodobieństwa wystąpienia zagrożeń z Internetu i przestępstw komputerowych

2.1. Uzyskanie dostępu do danych przesyłanych przez sieć lub przechowywanych w komputerach przez osoby niepowołane

Tabela 9

Prawdopodobieństwa wystąpienia	Ilość respondentów	Procent
Niemożliwe	0	0
Raczej niemożliwe	1	2
Trudno powiedzieć	0	0
Prawdopodobne	32	55
Bardzo prawdopodobne	25	43
Razem	**58**	**100**

Źródło: Opracowanie własne.

2.2. Utrata danych na skutek działań z zewnątrz (Internet)

Tabela 10

Prawdopodobieństwa wystąpienia	Ilość Respondentów	Procent
Niemożliwe	0	0
Raczej niemożliwe	0	0
Trudno powiedzieć	9	16
Prawdopodobne	30	52
Bardzo prawdopodobne	19	33
Razem	**58**	**100**

Źródło: Opracowanie własne.

2.3. Fałszerstwo danych

Tabela 11

Prawdopodobieństwa wystąpienia	Ilość Respondentów	Procent
Niemożliwe	0	0
Raczej niemożliwe	11	21
Trudno powiedzieć	14	27
Prawdopodobne	27	52
Bardzo prawdopodobne	0	0
Razem	**52**	**100**

Źródło: Opracowanie własne.

2.4. Uniemożliwienie korzystania z usług (zasobów) przez legalnych użytkowników

Tabela 12

Prawdopodobieństwa wystąpienia	Ilość Respondentów	Procent
Niemożliwe	0	0
Raczej niemożliwe	5	9
Trudno powiedzieć	7	12
Prawdopodobne	30	52
Bardzo prawdopodobne	16	28
Razem	**58**	**100**

Źródło: Opracowanie własne.

2.5. Zmiana oryginalnego programu, którym użytkownicy rejestrują się w systemie - podstawienie konia trojańskiego

Tabela 13

Prawdopodobieństwa wystąpienia	Ilość Respondentów	Procent
Niemożliwe	0	0
Raczej niemożliwe	2	3
Trudno powiedzieć	12	21
Prawdopodobne	37	64
Bardzo prawdopodobne	7	12
Razem	**58**	**100**

Źródło: Opracowanie własne.

2.6. Wykorzystanie rezydentnych programów kontrolujących klawiaturę - zapisywanie sekwencji naciskanych klawiszy

Tabela 14

Prawdopodobieństwa wystąpienia	Ilość Respondentów	Procent
Niemożliwe	0	0
Raczej niemożliwe	8	14
Trudno powiedzieć	40	69
Prawdopodobne	6	10
Bardzo prawdopodobne	4	7
Razem	**58**	**100**

Źródło: Opracowanie własne.

2.7. Podsłuch łącza, którym transmitowane są dane uwierzytelniające

Tabela 15

Prawdopodobieństwa wystąpienia	Ilość Respondentów	Procent
Niemożliwe	1	2
Raczej niemożliwe	31	54
Trudno powiedzieć	13	23
Prawdopodobne	12	21
Bardzo prawdopodobne	0	0
Razem	**57**	**100**

Źródło: Opracowanie własne.

2.8. Atak słownikowy

Tabela 16

Prawdopodobieństwa wystąpienia	Ilość Respondentów	Procent
Niemożliwe	0	0
Raczej niemożliwe	10	18
Trudno powiedzieć	4	7
Prawdopodobne	41	75
Bardzo prawdopodobne	0	0
Razem	**55**	**100**

Źródło: Opracowanie własne.

2.9. Przeszukiwanie wyczerpującą metodą prób i błędów - atak brutalny

Tabela 17

Prawdopodobieństwa wystąpienia	Ilość Respondentów	Procent
Niemożliwe	2	3
Raczej niemożliwe	2	3
Trudno powiedzieć	7	12
Prawdopodobne	47	81
Bardzo prawdopodobne	0	0
Razem	**58**	**100**

Źródło: Opracowanie własne.

2.10. Metody fizyczne - patrzenie na ręce użytkownika rejestrującego się w systemie

Tabela 18

Prawdopodobieństwa wystąpienia	Ilość Respondentów	Procent
Niemożliwe	0	0
Raczej niemożliwe	43	77
Trudno powiedzieć	4	7
Prawdopodobne	9	16
Bardzo prawdopodobne	0	0
Razem	**56**	**100**

Źródło: Opracowanie własne.

2.11. Metody inżynierii społecznej - nakłonienie użytkownika do udostępnienia lub zmiany hasła

Tabela 19

Prawdopodobieństwa wystąpienia	Ilość respondentów	Procent
Niemożliwe	0	0
Raczej niemożliwe	6	10
Trudno powiedzieć	35	60
Prawdopodobne	17	29
Bardzo prawdopodobne	0	0
Razem	**58**	**100**

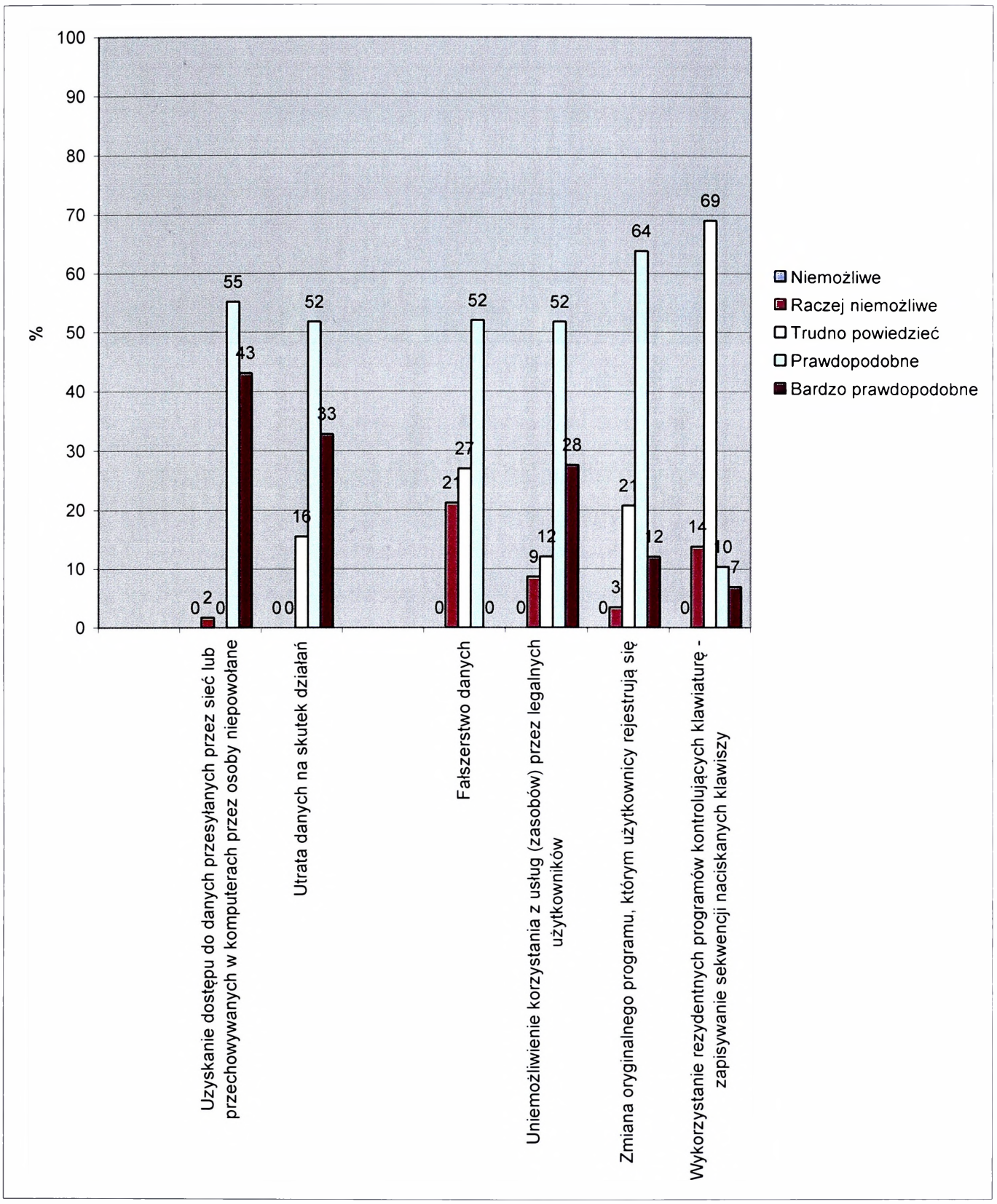
Źródło: Opracowanie własne.

2.12. Wirusy komputerowe

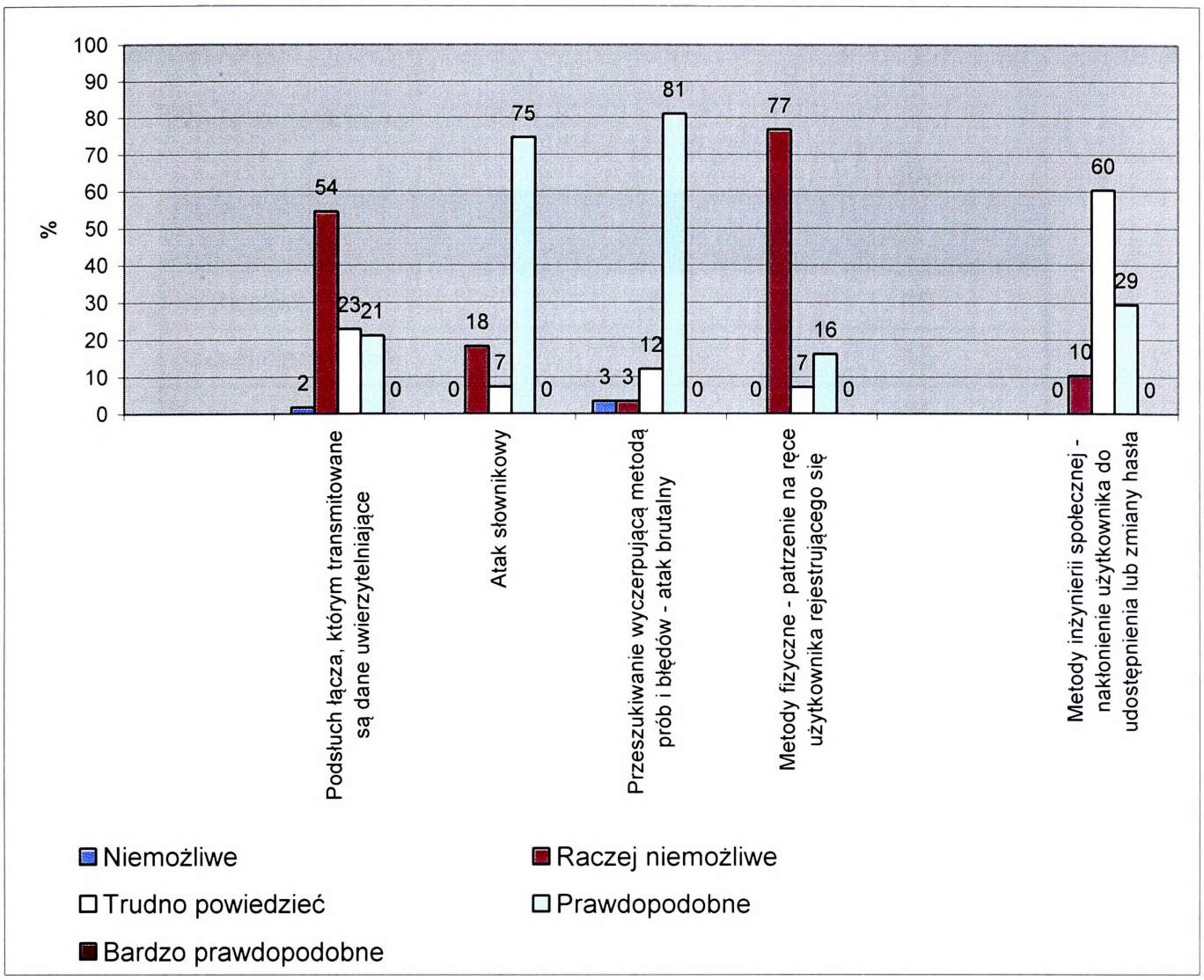
Tabela 20

Prawdopodobieństwa wystąpienia	Ilość respondentów	Procent
Niemożliwe	0	0
Raczej niemożliwe	0	0
Trudno powiedzieć	5	9
Prawdopodobne	20	34
Bardzo prawdopodobne	33	57
Razem	**58**	**100**

Źródło: Opracowanie własne.



Wykres 3. *Procentowe zestawienie opinii respondentów na temat prawdopodobieństwa wystąpienia zagrożeń z Internetu i przestępstw komputerowych*
Źródło: Opracowanie własne



Wykres 4. *Procentowe zestawienie opinii respondentów na temat prawdopodobieństwa wystąpienia zagrożeń z Internetu i przestępstw komputerowych*
Źródło: Opracowanie własne

3. Opinia respondentów na temat prawdopodobieństwa wystąpienia zagrożeń związanych z cyberterroryzmem

Tabela 21

Prawdopodobieństwa wystąpienia	Ilość respondentów	Procent
Niemożliwe	0	0
Raczej niemożliwe	0	0
Trudno powiedzieć	20	34
Prawdopodobne	17	29
Bardzo prawdopodobne	21	36
Razem	**58**	**100**

Źródło: Opracowanie własne.

4. Opinia respondentów na temat prawdopodobieństwa wystąpienia awarii i uszkodzeń sprzętowych

5.1. Błędy projektowe

Tabela 22

Prawdopodobieństwa wystąpienia	Ilość respondentów	Procent
Niemożliwe	5	10
Raczej niemożliwe	7	15
Trudno powiedzieć	17	35
Prawdopodobne	19	40
Bardzo prawdopodobne	0	0
Razem	**48**	**100**

Źródło: Opracowanie własne.

5.2. Wady produkcyjne

Tabela 23

Prawdopodobieństwa wystąpienia	Ilość respondentów	Procent
Niemożliwe	2	4
Raczej niemożliwe	9	18
Trudno powiedzieć	21	42
Prawdopodobne	18	36
Bardzo prawdopodobne	0	0
Razem	**50**	**100**

Źródło: Opracowanie własne.

5.3. Błędy instalacji

Tabela 24

Prawdopodobieństwa wystąpienia	Ilość respondentów	Procent
Niemożliwe	0	0
Raczej niemożliwe	8	14
Trudno powiedzieć	24	41
Prawdopodobne	26	45
Bardzo prawdopodobne	0	0
Razem	**58**	**100**

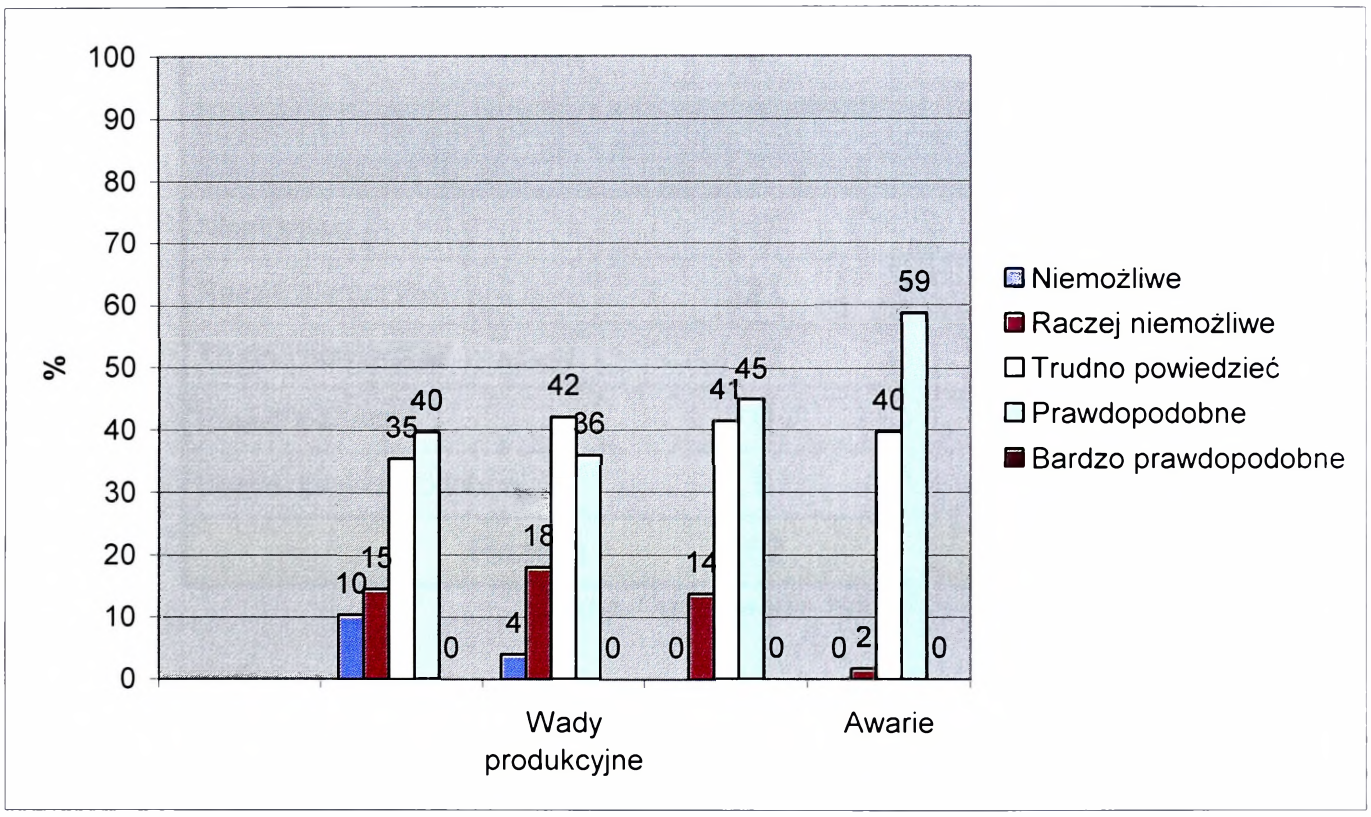
Źródło: Opracowanie własne.

5.4. Awarie

Tabela 25

Prawdopodobieństwa wystąpienia	Ilość respondentów	Procent
Niemożliwe	0	0
Raczej niemożliwe	1	2
Trudno powiedzieć	23	40
Prawdopodobne	34	59
Bardzo prawdopodobne	0	0
Razem	**58**	**100**

Źródło: Opracowanie własne.



Wykres 5. *Procentowe zestawienie opinii respondentów na temat prawdopodobieństwa wystąpienia awarii i uszkodzeń sprzętowych*
Źródło: Opracowanie własne

5. Opinia respondentów na temat prawdopodobieństwa wystąpienia zagrożeń związanych z występowaniem emisji ujawniającej

5.1. Emisja ujawniająca promieniowana

Tabela 26

Prawdopodobieństwa wystąpienia	Ilość respondentów	Procent
Niemożliwe	6	12
Raczej niemożliwe	12	24
Trudno powiedzieć	26	51
Prawdopodobne	7	14
Bardzo prawdopodobne	0	0
Razem	**51**	**100**

Źródło: Opracowanie własne.

5.2. Emisja ujawniająca przewodzona - bezpośrednia

Tabela 27

Prawdopodobieństwa wystąpienia	Ilość respondentów	Procent
Niemożliwe	0	0
Raczej niemożliwe	21	0
Trudno powiedzieć	31	40
Prawdopodobne	0	60
Bardzo prawdopodobne	0	0
Razem	**52**	**100**

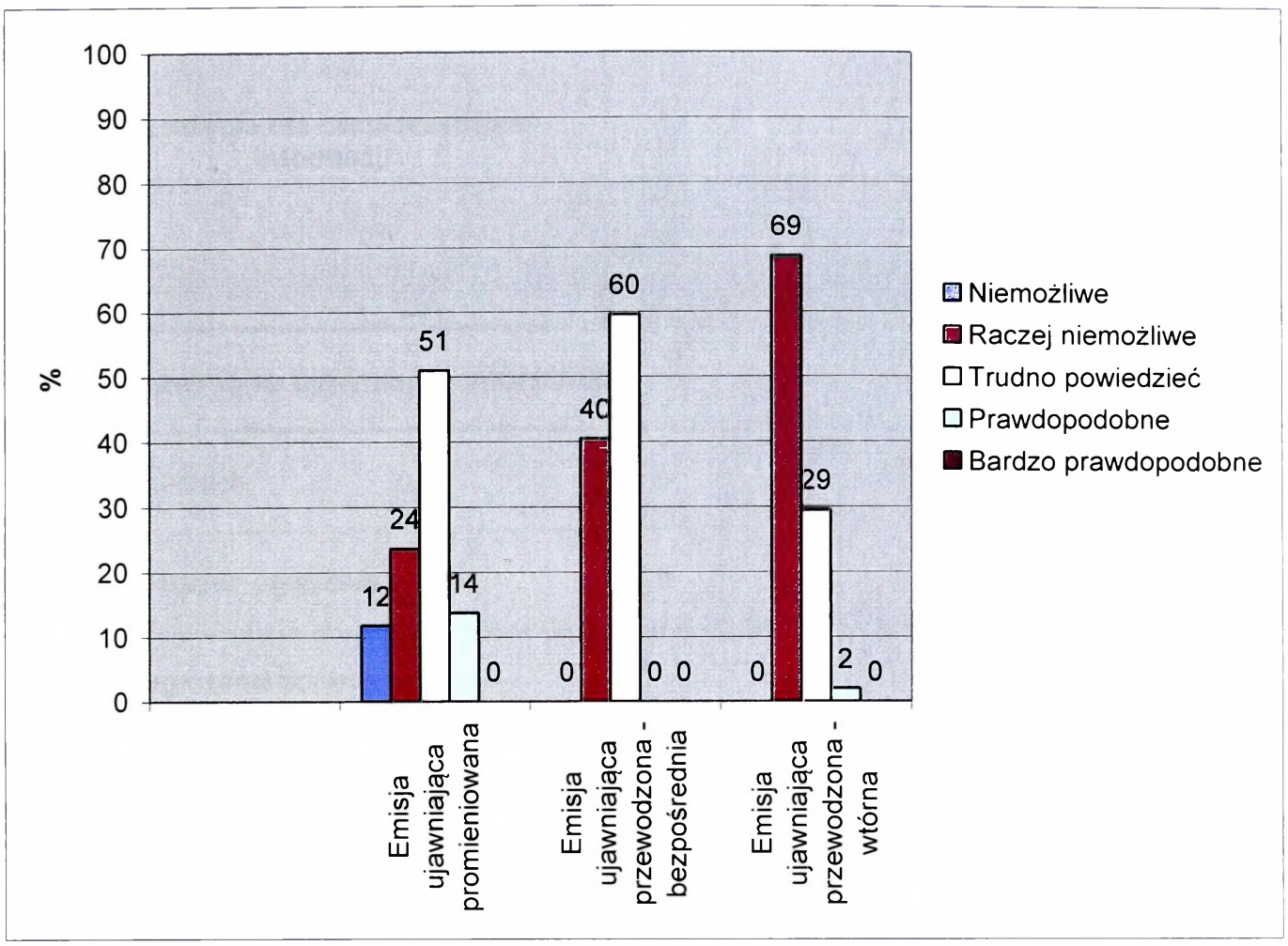
Źródło: Opracowanie własne.

5.3. Emisja ujawniająca przewodzona - wtórna

Tabela 28

Prawdopodobieństwa wystąpienia	Ilość respondentów	Procent
Niemożliwe	0	0
Raczej niemożliwe	35	69
Trudno powiedzieć	15	29
Prawdopodobne	1	2
Bardzo prawdopodobne	0	0
Razem	**51**	**100**

Źródło: Opracowanie własne.



Wykres 6. *Procentowe zestawienie opinii respondentów na temat prawdopodobieństwa wystąpienia zagrożeń związanych z występowaniem emisji ujawniającej*
Źródło: Opracowanie własne

Zbiorcze zestawienie odpowiedzi respondentów

Tabela 29

Lp.	Zagrożenie dla bezpieczeństwa informacji		Prawdopodobieństwo wystąpienia Zagrożenia					Razem
			Niemożliwe	Raczej niemożliwe	Trudno powiedzieć	Prawdopodobne	Bardzo prawdopodobne	
1.	Nieuprawnione ujawnienie informacji							
	1.1	Podsłuch	0	9	32	14	3	**58**
	1.2	Kradzież, zgubienie	0	12	7	39	0	**58**
	1.3	Zagrożenia socjotechniczne						
		1.3.1 Wykorzystanie władzy	0	4	0	37	17	**58**
		1.3.2 Wykorzystanie symparii	0	7	34	6	0	**47**
		1.3.3 Wykorzystanie wzajemności	0	9	33	10	1	**53**
		1.3.4 Wykorzystanie konsekwencji	0	10	15	33	0	**58**
		1.3.5 Wykorzystanie zasady przyzwolenia społecznego	0	7	18	33	0	**58**
		1.3.6 Wykorzystanie okazji	0	9	31	18	0	**58**
2.	Zagrożenia z Internetu i przestępstwa komputerowe							
	2.1	Uzyskanie dostępu do danych przesyłanych przez sieć lub przechowywanych w komputerach przez osoby niepowołane	0	1	0	32	25	**58**
	2.2	Utrata danych na skutek działań z zewnątrz (Internet)	0	0	9	30	19	**58**
	2.3	Fałszerstwo danych	0	11	14	27	0	**52**

Lp.		Zagrożenie dla bezpieczeństwa informacji	Prawdopodobieństwo wystąpienia Zagrożenia					Razem
			Niemożliwe	Raczej niemożliwe	Trudno powiedzieć	Prawdopodobne	Bardzo prawdopodobne	
	2.4	Uniemożliwienie korzystania z usług (zasobów) przez legalnych użytkowników	0	5	7	30	16	**58**
	2.5	Zmiana oryginalnego programu, którym użytkownicy rejestrują się w systemie - podstawienie konia trojańskiego	0	2	12	37	7	**58**
	2.6	Wykorzystanie rezydentnych programów kontrolujących klawiaturę - zapisywanie sekwencji naciskanych klawiszy	0	8	40	6	4	**58**
	2.7	Podsłuch łącza, którym transmitowane są dane uwierzytelniające	1	31	13	12	0	**57**
	2.8	Atak słownikowy	0	10	4	41	0	**55**
	2.9	Przeszukiwanie wyczerpującą metodą prób i błędów - atak brutalny	2	2	7	47	0	**58**
	2.10	Metody fizyczne - patrzenie na ręce użytkownika rejestrującego się w systemie	0	43	4	9	0	**56**
	2.11	Metody inżynierii społecznej - nakłonienie użytkownika do udostępnienia lub zmiany hasła	0	6	35	17	0	**58**
	2.12	Wirusy komputerowe	0	0	5	20	33	**58**
3.		Cyberterroryzm	0	0	20	17	21	**58**
4.		Awarie i uszkodzenia sprzętowe						
	4.1	Błędy projektowe	5	7	17	19	0	**48**
	4.2	Wady produkcyjne	2	9	21	18	0	**50**
	4.3	Błędy instalacji	0	8	24	26	0	**58**
	4.4	Awarie	0	1	23	34	0	**58**

Lp.		Zagrożenie dla bezpieczeństwa informacji	Prawdopodobieństwo wystąpienia Zagrożenia					Razem
			Niemożliwe	Raczej niemożliwe	Trudno powiedzieć	Prawdopodobne	Bardzo prawdopodobne	
5.	Emisja ujawniająca							
	5.1	Emisja ujawniająca promieniowana	6	12	26	7	0	**51**
	5.2	Emisja ujawniająca przewodzona – bezpośrednia	0	21	31	0	0	**52**
	5.3	Emisja ujawniająca przewodzona – wtórna	0	35	15	1	0	**51**

Źródło: Opracowanie własne.

Załącznik 2

AKADEMIA OBRONY NARODOWEJ
WYDZIAŁ WOJSK LĄDOWYCH

KWESTIONARIUSZ ANKIETY

Celem przeprowadzanej ankiety jest poznanie opinii ankietowanych ekspertów na temat prawdopodobieństwa wystąpienia wyszczególnionych w ankiecie zagrożeń dla bezpieczeństwa informacyjnego Sił Zbrojnych.

Wyniki badań uzyskane tą drogą wzbogacą wiedzę z zakresu rozpatrywanych zagadnień i stanowić będą podstawę do opracowania założeń do eksperymentów symulacyjnych w obszarze badań bezpieczeństwa informacyjnego Sił Zbrojnych. Poniższa ankieta stanowi ważną część badań empirycznych wykonywanych w ramach opracowywanej rozprawy doktorskiej na temat: „SYMULACJE KOMPUTEROWE W MODELOWANIU BEZPIECZEŃSTWA INFORMACYJNEGO W SIŁACH ZBROJNYCH", pod kierownictwem płk. dr. hab. Henryka SPUSTKA.

Ankieta jest anonimowa, a wyniki jej badań będą wykorzystywane wyłącznie do celów naukowych i prezentowane wyłącznie w sposób zbiorczy.

Jeżeli wyraża Pani/Pan zgodę na umieszczenie własnych danych w opracowaniach wyników badań ***proszę o podanie danych kontaktowych w metryczce załączonej na początku kwestionariusza ankiety .***

Serdecznie dziękuję za współpracę

kpt. mgr inż. Adam ŻACH

WARSZAWA
2008

METRYCZKA

1. Jak długo zajmuje się Pani/Pan zawodowo problematyką bezpieczeństwa informacji niejawnych?

    a) Do 3 lat;
    b) 4-6 lat;
    c) 7-10 lat;
    d) 10-15 lat;
    e) 16 lat i więcej.

2. Jak długo pracuje Pani/Pan na obecnym stanowisku?

    a) Do 1 roku;
    b) 2-3 lata;
    c) 4-6 lat;
    d) 7 i więcej.

3. Jaki rodzaj pracy wykonuje Pani/Pan w ramach obowiązków na zajmowanych stanowisku?

    a) Funkcje kierownicze;
    b) Zadania analityczne;
    c) Zadania operacyjne;
    d) Zadania kontrolne;
    e) Inne (jakie?) .....

4. Jaki jest Pani/ Pana korpus osobowy?

    a) Korpus oficerów zawodowych;
    b) Korpus podoficerów zawodowych;
    c) Funkcjonariusz;
    d) Inny (jaki?) .....

5. Jakie ma Pani/Pan wykształcenie?

    a) Średnie;
    b) Policealne;
    c) Wyższe I stopnia;
    d) Wyższe II stopnia;
    e) Wyższe III stopnia.

6. W jakiej instytucji obecnie Pani/Pan pracuje?

(proszę podać, jeżeli jest to możliwe, nazwę instytucji)

.....

7. Jakie zajmuje Pani/Pan stanowisko służbowe:

(proszę podać, jeżeli jest to możliwe, nazwę stanowiska)

.....

8. Dane kontaktowe:

    a) Imię i Nazwisko – .....
    b) Telefon – .....

c) E – mail – .....

9. Oświadczenie

Wyrażam zgodę na:

a) **Wyłącznie** anonimowe wykorzystywanie reprezentowanych w ankiecie ocen i poglądów i prezentowanie ich wyłącznie w sposób zbiorczy.

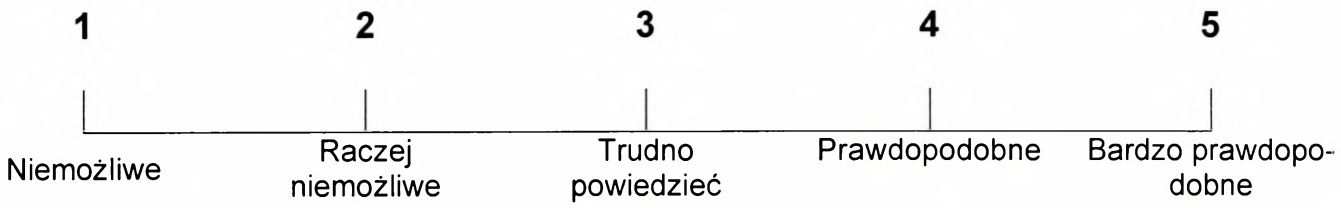
b) **Zgodę** na umieszczenie reprezentowanych w ankiecie ocen i podglądów wraz z podaniem moich danych jako źródło ich pochodzenia.

ANKIETA

Proszę o określenie, zgodnie z własną oceną, prawdopodobieństwa wystąpienia wyszczególnionych w tabeli zagrożeń biorąc pod uwagę zarówno zagrożenia dla pojedynczych komputerów czy wręcz dokumentów jak i całych systemów informacyjnych.

W związku z ogromem materiałów na temat zagrożeń dla bezpieczeństwa informacji, w tabeli mogły nie znaleźć się zagrożenia, które uważa Pani/Pan za istotne. W takim przypadku proszę wpisać je z wolne wiersze pozostawione do tego celu.

Prawdopodobieństwo proszę określić zgodnie z poniższą 5 – stopniową skalą.



Lp.	Zagrożenie dla bezpieczeństwa informacji			Prawdopodobieństwo wystąpienia zagrożenia	Uwagi
1.	Nieuprawnione ujawnienie informacji				
	1.1	Podsłuch			
	1.2	Kradzież, zgubienie			
	1.3	Zagrożenia socjotechniczne*			
		1.3.1	Wykorzystanie władzy		
		1.3.2	Wykorzystanie symparii		
		1.3.3	Wykorzystanie wzajemności		
		1.3.4	Wykorzystanie konsekwencji		
		1.3.5	Wykorzystanie zasady przyzwolenia społecznego		
		1.3.6	Wykorzystanie okazji		

Lp.	Zagrożenie dla bezpieczeństwa informacji		Prawdopodobieństwo wystąpienia zagrożenia	Uwagi
2.	Zagrożenia z Internetu i przestępstwa komputerowe			
	2.1	Uzyskanie dostępu do danych przesyłanych przez sieć lub przechowywanych w komputerach przez osoby niepowołane		
	2.2	Utrata danych na skutek działań z zewnątrz (Internet)		
	2.3	Fałszerstwo danych		
	2.4	Uniemożliwienie korzystania z usług (zasobów) przez legalnych użytkowników		
	2.5	Zmiana oryginalnego programu, którym użytkownicy rejestrują się w systemie - podstawienie konia trojańskiego		
	2.6	Wykorzystanie rezydentnych programów kontrolujących klawiaturę - zapisywanie sekwencji naciskanych klawiszy		
	2.7	Podsłuch łącza, którym transmitowane są dane uwierzytelniające		
	2.8	Atak słownikowy		
	2.9	Przeszukiwanie wyczerpującą metodą prób i błędów - atak brutalny		
	2.10	Metody fizyczne - patrzenie na ręce użytkownika rejestrującego się w systemie		
	2.11	Metody inżynierii społecznej - nakłonienie użytkownika do udostępnienia lub zmiany hasła		
	2.12	Wirusy komputerowe		
3.	Cyberterroryzm			
4.	Awarie i uszkodzenia sprzętowe			
	4.1	Błędy projektowe		
	4.2	Wady produkcyjne		
	4.3	Błędy instalacji		

Lp.	Zagrożenie dla bezpieczeństwa informacji		Prawdopodobieństwo wystąpienia zagrożenia	Uwagi
	4.4	Awarie		
5.	Emisja ujawniająca			
	5.1	Emisja ujawniająca promieniowana		
	5.2	Emisja ujawniająca przewodzona - bezpośrednia		
	5.3	Emisja ujawniająca przewodzona - wtórna		

*)ZAGROŻENIA SOCJOTECHNICZNE

Cechy, na jakich bazują socjotechnicy podczas swoich prób manipulowania innymi.

Władza – ludzie mają tendencję do podporządkowywania się woli osoby, o której sądzą, że ma władzę. Osoba może podporządkować się prośbie, jeżeli wierzy, że rozmówca ma władzę lub jest upoważniony do proszenia o daną przysługę.

Symparia – ludzie mają tendencję do podporządkowywania się, gdy osoba prosząca jest w stanie ukazać się jako sympatyczna, mająca podobne zainteresowania, poglądy i podejście do życia jak ofiara.

Wzajemność – jest to tendencja do podporządkowania się osobie, która daje lub obiecuje dać mam coś w zamian. Prezent może być materialny lub może stanowić radę lub pomoc. Kiedy ktoś zrobił coś dla nas, czujemy potrzebę odwzajemnienia. Ta silna potrzeba ujawnia się nawet wtedy, kiedy nie prosiliśmy o to, co dostaliśmy. Jednym z najbardziej efektywnych sposobów wpływania na ludzi, tak, aby zrobili nam „przysługę" (podporządkowali się prośbie), jest podarowanie im prezentu lub pomoc, która wywołuje poczucie zobligowania.

Konsekwencja – ludzie mają tendencję do podporządkowywania się, jeżeli wcześniej publicznie ogłosili swoje poparcie i zaangażowanie w danej sprawie. Jeżeli raz obiecaliśmy, że coś zrobimy, nie chcemy wyglądać na niegodnych zaufania i postępujemy zgodnie z naszymi wcześniejszymi deklaracjami lub obietnicami.

Przyzwolenie społeczne – ludzie mają tendencję do spełniania próśb, kiedy wydaje się to zgodne z zachowaniem innych. Przykład ze strony innych jest traktowany jako przyzwolenie i potwierdzenie, że dane zachowanie jest prawidłowe i stosowne.

Rzadka okazja – ludzie mają tendencję do podporządkowywania się, kiedy wierzą, że poszukiwany obiekt występuje w ograniczonej ilości i jest pożądany przez innych oraz dostępny tylko przez krótki czas