114

AKADEMIA OBRONY NARODOWEJ

WYDZIAŁ ZARZĄDZANIA I DOWODZENIA

BEZPIECZEŃSTWO I OCHRONA INFORMACJI W SIECIACH TELEINFORMATYCZNYCH ORGANIZOWANYCH NA POTRZEBY WOJSK LĄDOWYCH

Praca naukowo-badawcza

Biblioteka Główna
Akademii Obrony Narodowej
S/7708
05-007708-003-0

WARSZAWA

75023

AKADEMIA OBRONY NARODOWEJ

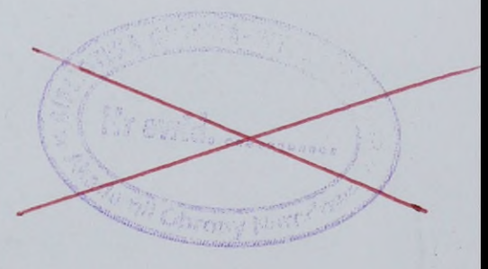
WYDZIAŁ ZARZĄDZANIA I DOWODZENIA

BIBLIOTEKA GŁÓWNA - ARCHIWUM
Nr ewid. 7523
II
Akademii Obrony Narodowej

BEZPIECZEŃSTWO I OCHRONA INFORMACJI W SIECIACH TELEINFORMATYCZNYCH ORGANIZOWANYCH NA POTRZEBY WOJSK LĄDOWYCH

Praca naukowo-badawcza

Kod: II.2.5.4.0. Kryptonim: INFO-01



WARSZAWA **2009**

	1	2	3	
				A

4
Tytuł: BEZPIECZEŃSTWO I OCHRONA INFORMACJI W SIECIACH TELEINFORMATYCZNYCH ORGANIZOWANYCH NA POTRZEBY WOJSK LĄDOWYCH

5	6	7
Rozpoczęto: 22.06.2009 Zakończono: 19.01.2010	Kart:	
8	9	

OPRACOWAŁ:
prof. dr hab. Leopold CIBOROWSKI

RECENZENT:
prof. dr hab. Michał HUZARSKI

Spis treści

Wprowadzenie..... 5

1. Identyfikacja informacji jako zasadniczego przedmiotu poznania..... 9

1.1. Postać rzeczowa oraz funkcje i wartościowanie informacji..... 10

1.1.1. Postać rzeczowa informacji..... 10

1.1.2. Funkcje informacji w działaniach celowych..... 68

1.1.3. Wartościowanie informacji w działaniach celowych..... 99

2. Zagrożenia informacyjne w sieciach teleinformatycznych..... 109

2.1. Zagrożenia informacyjne w relacjach rozpoznawczych..... 110

2.1.1. Dezinformacja jako element zagrożenia – identyfikacja ogólne..... 110

2.1.2. Dezinformacja bezpośrednia (recepcyjna)..... 132

2.1.3. Dezinformacja pośrednia (sensoryczna)..... 134

2.2. Zagrożenia informacyjne w relacjach kierowania..... 136

2.2.1. Penetracja semantyczna (identyfikowanie)..... 138

2.2.2. Destrukcja transmisyjna (semantyki i relacji)..... 175

Zakończenie – podsumowanie wyników badań..... 203

Skorowidz nowej terminologii..... 217

Wykaz rysunków, wykresów i tabel..... 221

Bibliografia..... 225

WPROWADZENIE

W procedurze badawczej, której wyniki przedstawiono w niniejszym sprawozdaniu, przyjęto, że treść znaczeniowa znaku językowego (zestawienia wyrazowego) „bezpieczeństwo i ochrona informacji w sieciach teleinformatycznych" jest antonimem znaku językowego symbolizującego pojęciowo „zagrożenia informacyjne w sieciach teleinformatycznych". Kierując się takim rozumieniem zależności przyjęto, że rozwiązanie problemu, skupionego wokół „bezpieczeństwa i ochrony informacji w sieciach teleinformatycznych, organizowanych na potrzeby wojsk lądowych", będzie bardziej użyteczne, kiedy elementy tego zostaną unaocznione przez pryzmat możliwych zagrożeń. Założono, że znając zagrożenia, każdy konkretny organizator i użytkownik tych sieci będzie bardziej przekonany o potrzebie przestrzegania, stosownych co do tego zasad bezpieczeństwa i ochrony, niż w okolicznościach kiedy te zostaną mu tylko nakazane czy zalecone bez głębszego uzasadnienia potrzeb i wynikających z tego konsekwencji.

Przy rozwiązywaniu tego pojawił się kolejny problem związany z identyfikacją przedmiotu poznania określanego mianem „informacja" i stosownym co do tego językiem opisu. Istniejące na ten temat opracowania merytoryczne i leksykograficzne okazały się wielce zróżnicowane interpretacyjnie. Zaistniała zatem potrzeba, aby w pierwszej kolejności skoncentrować się poznawczo na rozwiązaniu tego problemu, a dopiero w następnej kolejności na jego tytułowej istocie, czyli bezpieczeństwie i ochronie informacji w sieciach teleinformatycznych.

Przyjmując taką koncepcję, całą procedurę poznawczą zdeterminowało dążenie, aby w następstwie rozwiązania problemów, związanych z identyfikacją informacji i zagrożeń informacyjnych, możliwych do występowania w sieciach teleinformatycznych, uzyskać wystarczająco wiarygodne dane do sformułowania zbioru pożądanych wymagań składających się na kształtowanie przestrzeni bezpieczeństwo i ochrony

informacji w sieciach teleinformatycznych, w ogóle, a tym samym i w tego typu sieciach organizowanych na potrzeby wojsk lądowych, których, ze względu na tajemnicę celowo nie wymieniono.

W realizowanych badaniach generalnie kierowano się sparafrazowaną istotą wskazania Mariana Mazura, że dążąc do nazwania czegoś należy w pierwszej kolejności ustalić co różni ludzie określają danym mianem, czyli jakie treści znaczeniowe przypisują do niego i jak się to ma do rzeczywistości. Przyjmując taką koncepcję poznawczą, jakoby automatycznie zaistniała potrzeba skoncentrowania się na badaniach teoretycznych. W następstwie tego podano gruntownej analizie treści zawarte w klasycznej literaturze nawiązującej, w różnych partiach treści, do sytuacji problemowej – począwszy od technicznej i matematycznej, a skończywszy na filozoficznej, co znajduje udokumentowane ślady w przypisach do treści sprawozdania i dołączonej do niego bibliografii. Zebrane w ten sposób treści podawano analizie elementarnej, funkcjonalnej i logicznej, stosując przy tym w szerokim zakresie porównania, analogie, konfrontacje elementów i w szerokim zakresie abstrahowanie izolujące i generalizujące. To stanie, abstrahowanie generalizujące, umożliwiło zebranie wystarczająco reprezentatywnych danych do wnioskowania indukcyjnego, umożliwiającego identyfikowanie szeregu elementu stanowiących reprezentatywne części przedmiotu poznania. Tworząc na tej podstawie modele abstrakcyjne (logiczne, matematyczne i wyobrażeniowe) i w dalszym ciągu bazując na odpowiednio dobranych treściach literaturowych (krajowych i zagranicznych) poszukiwano potwierdzeń faktograficznych, co przy pewnej tolerancji weryfikacyjnej można by nazwać, a nade wszystko ze względu na formę, badaniami dedukcyjnymi. Osiągnięte w ten sposób wyniki badań usystematyzowano sprawozdawczo w dwóch zasadniczych rozdziałach i podsumowaniu.

W rozdziale pierwszym sprawozdania zawarto treści związane z identyfikacją rzeczowej i funkcjonalnej postaci informacji oraz zaprezentowano możliwy sposób jej wartościowania w działaniach celowych. Prowadząc w tym zakresie badania natknięto się na dodatkowy problem związany stricte z językiem opisu. Okazało się, że istniejący w tym zakresie zasób terminologiczny jest zbyt ubogi i do tego jeszcze często niejednoznaczny semantycznie, uniemożliwiający tym samym stosowanie precyzyjnych opisów związanych z przedmiotem poznania. Uwzględniając to i bazując na autorytatywnych opracowaniach leksykograficznych, językoznawczych i podstawach logiki, odnoszących się do klasycznych zasad definiowania, a nade wszystko, na

istocie zidentyfikowanych zjawisk, uzupełniono istniejący zbiór nazw o 31 jednoznacznie zdefiniowanych terminów, wzbogacając w ten sposób pożądany język opisu.

W rozdziale drugi sprawozdania zawarto dociekania poznawcze związane z identyfikacją zagrożeń informacyjnych, możliwych do występowania w sieciach teleinformatycznych. Stosując co do tego wzbogacony język opisu i techniczne uwarunkowania procesów, skoncentrowano się na zagrożeniach informacyjnych możliwych do występowania w relacjach rozpoznawczych i w relacjach kierowania. Problematykę z tym związaną identyfikowano przez pryzmat dezinformacji percepcyjnej i sensorycznej oraz penetracji semantycznej i destrukcji transmisyjnej.

W podsumowaniu wyników badań, stanowiącym zakończenie części merytorycznej sprawozdania, zawarto zbiór przedsięwzięć składających się na kształtowanie pożądanej przestrzeni bezpieczeństwa i ochrony informacji w sieciach teleinformatycznych w ogóle, a tym samym i organizowanych na potrzeby wojsk lądowych, eliminując w ten sposób naruszenie zasad tajemnicy, związanych z ujawnianiem rzeczywiście organizowanych sieci na potrzeby tych wojsk. Zestawiony, co do tego, zbiór wymagań zawiera w sobie elementy funkcjonalne i techniczne, ukierunkowane przeciwko tym elementom zagrożeń, które zostały unaocznione w pierwszej i drugiej części sprawozdania – w pierwszym i drugim rozdziale.

1. IDENTYFIKACJA INFORMACJI JAKO ZASADNICZEGO PRZEDMIOTU POZNANIA

Informacja, elektronika, środowisko informacyjne i środowisko wiedzy to cztery komplementarnie zespolone elementy. Przypuszcza się, że pierwszy z nich – informacja – pojawił się około 40-35 tysięcy lat temu wraz z myśleniem. Naukowcy są zdania, że objawy myślenia ujawniły się równolegle z mową. Język stworzył możliwości do symbolizowania rzeczy znakami językowymi[1]. Wymagał zatem kreatywności i tym samym myślenia abstrakcyjnego. Dowodem tego jest również sztuka. Wielkim przełomem w archeologii okazały się odkrycia, że sztuka, język i myślenie są tym samym. Stało się zatem oczywiste, że odkrycie najwcześniejszych form sztuki pozwala stwierdzić, kiedy człowiek nauczył się myśleć.

Najwcześniejsze ślady sztuki są zaskakująco dojrzałe. Obfitują w szczegóły graficzne oraz misternie wykonane rzeźby (sceny jaskiniowe i figurki). Wszystkie te znaleziska są datowane na około 40-35 tysiące lat, czyli na okres egzystowania homo sapiens. Można przypuszczać, że myślenie i język homo sapiens mogły doprowadzić do eliminacji ze środowiska neandertalczyków[2]. Przyjmując taką tezę można sądzić, że fakt ten jest dowodem wskazującym na siłę umysłu[3] i informacji, stanowiących podstawę świadomego organizowania zbiorowej działalności i wyzwalania w niej efektu synergicznego[4] do zabezpieczania swojej egzystencji w istniejącym oto-

---

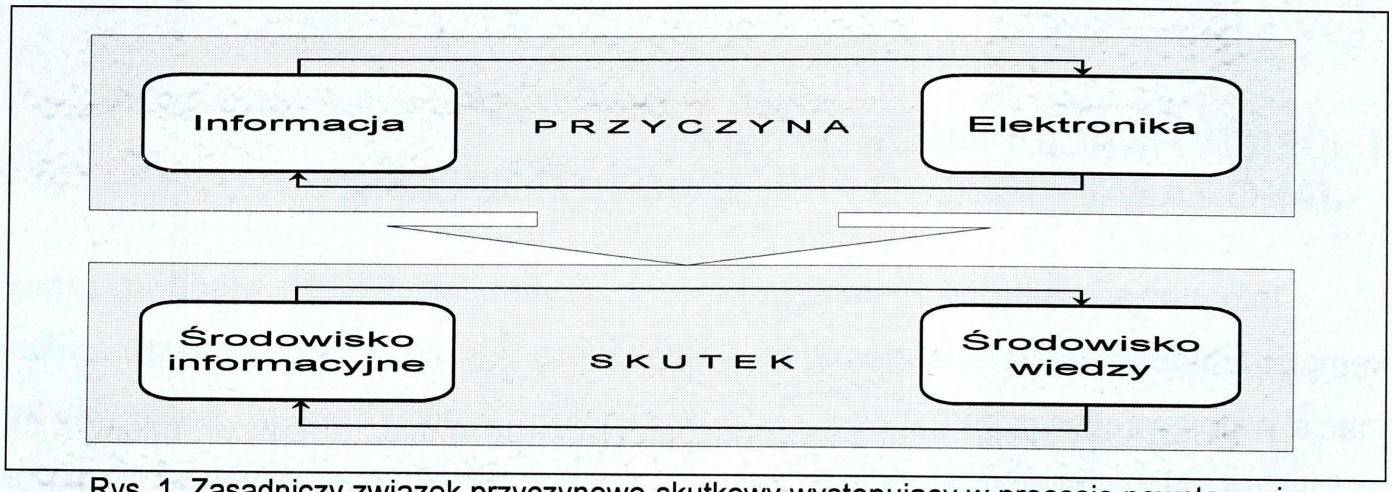
[1] Znak językowy – wszystko co w języku posiada swoje znaczenie (semantykę); najmniejszym znakiem językowym jest morfem [najmniejsza grupa fonemów (najmniejsza jednostka mowy rozróżniana przez użytkowników danego języka), która posiada określone znaczenie i której nie można podzielić na mniejsze jednostki znaczeniowe], a największym – cały tekst; znaki językowe dzielą się na: wzrokowe, słuchowe, dotykowe, węchowe i smakowe (przypis autorski).

[2] Ocenia się, że neandertalczycy żyli 250 – 30 tysięcy lat temu, natomiast homo sapiens pojawił się 230 tysięcy lat temu i egzystuje do dnia dzisiejszego.

[3] Umysł – zespół myślowy funkcji poznawczych mózgu; zdolność myślenia, pojmowania, rozumowania; rozum, intelekt („Słownik języka polskiego", PWN, Warszawa 1981, tom III, s. 601.

[4] Synergia – współdziałanie, kooperacja czynników, skuteczniejsza niż suma ich oddzielnych działań (W. Kopaliński, „Słownik wyrazów obcych i zwrotów obcojęzycznych (wydanie dziewiąte)", WP, Warszawa 1975, s. 939).

czeniu. Elektronika pojawiła się natomiast dość późno – dopiero na przełomie XIX i XX wieku, to znaczy około 40–35 tysiącach lat po informacji. W zespoleniu z nią (z informacją) już bardzo szybko, bo tylko po niespełna 100 latach, wygenerowała nowe warunki bytu społecznego, który można określać mianami *środowiska informacyjnego* i *środowiska wiedzy* (rys. 1).



Rys. 1. Zasadniczy związek przyczynowo-skutkowy występujący w procesie powstawania środowiska informacyjnego i środowiska wiedzy

Źródło: Opracowanie autorskie.

1.1. Postać rzeczowa oraz funkcje i wartościowanie informacji

Chociaż informacja istnieje i funkcjonuje już około 40-35 tysięcy lat, to jednak do chwili obecnej termin ten nie doczekał się jednoznacznej interpretacji pojęciowej, spełniającej warunek: **termin** symbolizuje **pojęcie** (treść znaczeniową wyrazu – jego semantykę) dotyczące **desygnatów** (jednostkowych przedmiotów myślowych), które są przypisane do **terminu**, powodując, że w porozumiewaniu się międzyludzkim **termin** zastępuje **desygnaty** utożsamiające **pojęcie**, które objaśnia **termin**[5].

1.1.1. Postać rzeczowa informacji

O tym, że myślowe wyjaśnianie całościowego ujęcia istotnych cech przedmiotu symbolizowanego terminem **informacja** jest trudne, świadczyć mogą chociażby takie fakty, że Claude Shannon, twórca teorii ilościowej miary informacji i Stafford Beer – autor jednej z pierwszych prac dotyczących zastosowań cybernetyki jako

[5] C.K. Ogden, I.A. Richards, „The Meaning of Meaning: A Study of the Influence of Languaage upon Thought and of the Science of Symbolism", Harcout, Brace & World, New York 1946.

ogólnej teorii sterowania w zarządzaniu systemami ekonomicznymi, w ogóle nie zdefiniowali tego terminu, chociaż często posługiwali się nim w swoich wywodach. Obecnie wielu autorów stara się wypełnić tę lukę semantyczną, jednak do dnia dzisiejszego nie ma co do tego zgodności w formułowanych poglądach. Daje się to dostrzegać zarówno w funkcjonujących normatywach leksykalnych, jak i w literaturze przedmiotu (tab. 1).

Wybrane przykłady pojęciowych interpretacji terminu „informacja" Tabela 1

Lp.	Interpretacja pojęciowa	Źródło
1.	Każdy czynnik zmniejszający stopień niewiedzy (nieokreśloności) o badanym zjawisku, umożliwiający człowiekowi, organizmowi żywemu lub urządzeniu automatycznemu polepszenie znajomości otoczenia i w sprawniejszy sposób przeprowadzenie celowego działania; źródłem informacji są odbierane wiadomości, a miarą informacji jest ilość informacji	„Encyklopedia Powszechna (tom 2)", PWN, Warszawa 1974, s. 281
2.	Wiadomość, wieść, nowina, rzecz zakomunikowana, zawiadomienie, komunikat; pouczenie, powiadomienie, zakomunikowanie o czymś; dane; pokój, okienko, stanowisko, gdzie się udziela informacji (...) – *łac. Informatio*: wyobrażenie, wizerunek	Władysław Kopaliński, „Słownik wyrazów obcych i zwrotów obcojęzycznych (wydanie dziewiąte)", WP, Warszawa 1975, s. 429
3.	Powiadomienie o czymś, zakomunikowanie czegoś; wiadomość, wskazówka, pouczenie (...)	„Słownik języka polskiego tom pierwszy", PWN, Warszawa 1978, s. 788
4.	Pojęcie podstawowe nie w pełni zdefiniowane z uwagi na jego pierwotny, elementarny charakter. Wszystkie dotychczasowe próby definiowania go uważa się powszechnie za niezadowalające, a co najwyżej za ukazujące tylko niektóre aspekty (...)	„Encyklopedia organizacji i zarządzania, PWE, Warszawa 1982, s. 161
5.	W pierwotnym sensie termin ten oznaczał wiadomości ogólne. Wraz z rozwojem cybernetyki i ogólnej teorii systemów termin ten, zachowując swoje pierwotne znaczenie, uległ w wymienionych naukach konkretyzacji i zaczął być używany do określenia wiadomości, wiedzy obserwatora o systemie i otoczeniu, w którym dany system funkcjonuje. Na przykład, w szczególnym przypadku, jeżeli system jest badany za pomocą metody *czarnej skrzynki*, to informacja o jego zachowaniu się jest przedstawiana w postaci zapisu na jego wejściu i wyjściu (...)	„Słownik matematyki i cybernetyki ekonomicznej", PWE, Warszawa 1985, s. 189
6.	Konstrukcja stanu rzeczy, wiadomość; w dyscyplinach naukowych miara niepewności zajścia pewnego zdarzenia (...)	„Nowa encyklopedia powszechna (tom 3)", PWN, Warszawa 1998, s. 53
7.	Przeanalizowana i przetworzona do postaci zrozumiałej dla odbiorcy wiadomość (dana, sygnał), która powiadamia go o sytuacji i ma dla niego wartość w procesie decyzyjnym. Informacja jest pojęciem węższym niż dana, zawiera bowiem tylko te fakty i liczby, które: są przedstawione w formie zrozumiałej dla odbiorcy, dotyczą obszaru zainteresowań odbiorcy, posiadają wartość dla odbiorcy, nie powielają zasobów posiadanej wiedzy (...)	„Leksykon zarządzania", Difin, Warszawa 2004, s. 165
8.	Nazwą treści zaczerpniętej ze świata zewnętrznego, w miarę jak się do niego dostosowujemy i jak dostosowujemy doń swoje zmysły	Norbert Wiener, „Cybernetyka i społeczeństwo", K i W, Warszawa 1960, s. 16
9.	W cybernetyce nazywa się informacją wszelkie działanie fizyczne, któremu towarzyszy działanie psychiczne	Louis Couffignal, „La Cybernetique" Pressem Universitaires, de France, Paris 1963

10. Informacja to zespół nośnika I semantyki, gdzie semantyka jest efektem psychicznym informacji, a nośnik jest zjawiskiem fizycznym skojarzonym z semantyką w celu utworzenia informacji. Przy tłumaczeniu tekstu z jednego języka na inny, informacje zawarte w tekście początkowym pozostają takie same, chociaż zmieniła się ich forma

Louis Couffignal, „Les machines a penser", Les Editions de Minuit, Paris 1964

11. Sygnał (Signal) może, ale nie musi, zawierać lub przenosić wiadomości (Nachricht). Występują tu rozmaite możliwości:

- odbiorca odbiera sygnał „jako sygnał", a nie jako związaną z nim wiadomość (Nachricht),
- odbiorca wprawdzie odbiera wiadomość (Nachricht), ale jej nie rozumie nawet po dłuższym namyśle, np. zakomunikowanie (Mitteilung) fachowej wypowiedzi (Aussage), do której zrozumienia brakuje mu wykształcenia,
- odbiorca wprawdzie rozumie (Nachricht), ale go ona nie interesuje, jest mu obojętna.
- Wiadomość (Nachricht) „znaczy" coś dla odbiorcy, np. informuje go o czymś, a wówczas zawiera dla niego informację (Information).

von Hans-Joachim Flechtner, „Grundbegriffe der Kybernetik", Wissenschaftliche Verlagsgesellschaft M.B.H., Stuttgart 1967, s. 64 i 65

12. Wśród wszystkich możliwych rodzajów wejść (wyjść) wyróżnimy teraz dwa skrajne rodzaje:

(1) *informacyjne,* (2) *rzeczowe.*

Przez „informację" będziemy rozumieli wszelki sygnał, wszelki komunikat, wszelkie zezwolenie, wszelki nakaz i zakaz.

Mówimy, że dane jest informacyjne, zamiast mówić, że każdy jego stan wyróżniony jest informacją. (Uprzedzamy czytelnika, że wyraz „informacja" bywa używany zarówno potocznie, jak i cybernetyce również w innych rozumieniach). Mówimy, że dane jest rzeczowe, zamiast mówić, że żaden jego stan wyróżniony nie jest informacją.

Niekiedy odróżnienie wejścia (wyjścia) rzeczowego od informacyjnego nasuwa w praktyce duże trudności.

Wprowadzenie pojęcia wejścia (ew. wyjścia) informacyjnego umożliwia nam z kolei skonstruowanie trzech doniosłych pojęć:

(1) pojęcia układu informowanego,
(2) pojęcia układu informującego,
(3) pojęcia układu informacyjnego.

Układ informowany – to wszelki i tylko taki układ względnie odosobniony, który posiada choć jedno wejście informacyjne.

Układ informujący – to wszelki i tylko taki układ względnie odosobniony, który posiada choć jedno wyjście informacyjne.

Układ informacyjny – to po prostu układ zarazem informowany i informujący.

Henryk Greniewski, „Elementy cybernetyki sposobem niematematycznym wyłożone" PWN, Warszawa 1959, s. 22 i 23

13. • W języku potocznym wyraz „informacja" używany jest zwykle w ten sposób, że spełnione są trzy warunki poniższe:
  - każda informacja jest wiadomością o czymś,
  - informację uzyskuje tylko człowiek (przez obserwację lub czynność umysłową),
  - informację przekazuje tylko człowiek człowiekowi.

• Natomiast w cybernetyce używa się wyrazu „informacja" w rozumieniu dużo szerszym.

Uogólnienie pojęcia informacji – etap I.

Nie tylko każda wiadomość, lecz również każda decyzja, każdy nakaz, zakaz, zalecenie, sugestia jest informacją.

Uogólnienie pojęcia informacji – etap II.

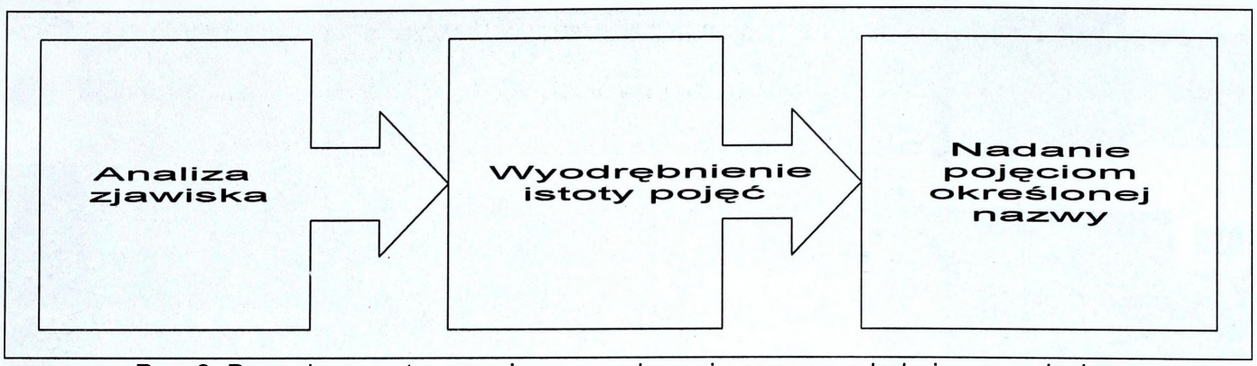
• Przez „informację" będziemy odtąd rozumieli:

Henryk Greniewski, „Sprawy wszystkie i jeszcze inne (o logice i cybernetyce)", KiW, Warszawa 1970, s. 24–25

	– wszelkie uzyskiwanie danych nie tylko przez człowieka, lecz również przez dowolną istotę żywą, organ człowieka lub innej istoty żywej, a także przez maszynę lub jej organ, – wszelkie przekazywanie danych między ludźmi, istotami żywymi i maszynami (ewentualnie organami istot żywych lub maszyn).	
14.	Jest to transformacja jednego komunikatu asocjacji informacyjnej w drugi komunikat tej asocjacji	Marian Mazur „Jakościowa teoria informacji", WNT, Warszawa 1970, s. 70
15	(...)Tak więc, ogólnie biorąc, informacji nie można wyrazić w kategoriach energii (...)	Ludwig von Bertalanffy, „Ogólna teoria systemów (podstawy, rozwój, zastosowania)", PWN, Warszawa 1984, s. 73
16.	(...) W odróżnieniu od zwierzęcia żyjącego w „otoczce" (Umwelt) zdeterminowanej przez jego organizację, człowiek sam tworzy swój świat, nazywany kulturą. Wśród hipotez na temat jego ewolucji wyróżniamy dwa blisko ze sobą powiązane czynniki – język i kształtowanie pojęć. „Język" jako wezwanie lub rozkaz można zaobserwować już w świecie zwierząt; przykładem jest tu śpiew ptaków, ostrzegawczy świst kozicy górskiej itp. Jednak język jako przedstawianie i komunikowanie faktów stanowi monopol człowieka. W szerszym znaczeniu język obejmuje nie tylko mowę oralną, ale również pismo oraz system symboli matematycznych. Są to systemy symboli nie odziedziczonych, lecz systemy symboli dowolnie tworzonych i tradycyjnych. Przede wszystkim wyjaśnia to specyfikę historii człowieka w odróżnieniu od ewolucji biologicznej: jest to tradycja w przeciwieństwie do dziedziczonych mutacji występujących tylko w długim okresie. Po drugie, fizyczną metodę prób i błędów, w dużej mierze charakteryzującą zachowania zwierząt, zastępuje się *eksperymentem myślowym*, czyli eksperymentowaniem przy użyciu symboli pojęciowych. Dlatego staje się możliwa prawdziwa *kierunkowość docelowa*. Kierunkowość docelowa i teologia w sensie metafizycznym, tzn. regulacja zdarzeń w znaczeniu podtrzymywania, produkcji i reprodukcji organicznej całościowości, stanowi ogólne kryterium życia. Z prawdziwej celowości wynika jednak, że działania są prowadzone z pełną świadomością ich celu, ich końcowego wyniku; rzeczywiście istnieje już koncepcja przyszłego celu i ona to wpływa na aktualne działanie. Odnosi się to do prymitywnych działań życia codziennego, a również do najwyższych osiągnięć ludzkiego intelektu w nauce i technice (...).	Ludwig von Bertalanffy, „Ogólna teoria systemów (podstawy, rozwój, zastosowania)", PWN, Warszawa 1984, s. 299 i 300
17.	(...) Istnieje jeszcze jeden ważny, a często pomijany aspekt rzetelności metody uzyskiwania informacji, jest to tzw. rzetelność konsensyjna. Uzyskiwane informacje muszą być na tyle jednoznaczne, żeby każdy odbierający te informacje odbierał je takie same. Przy braku rzetelności konsensyjnej to, jaka informacja zostanie odebrana, zależy od tego kto ją odbiera. Co więcej, niejednoznaczność informacji powoduje, że ta sama osoba może odbierać ją za każdym razem w inny sposób (...)	Ryszard Kietliński, „Aspekty problemu podejmowania decyzji personalnych", art. w Zeszycie Naukowym Uniwersytetu Łódzkiego nr 61, s. 55, UŁ, Łódź 1969

Źródło: Zestawienie autorskie.

W dochodzeniu do pojęciowej interpretacji terminu „informacja" bardzo pomocne zdaje się być wskazanie Mariana Mazura zawarte w książce *Jakościowa teoria informacji.* Autor wypowiada się, że (...) **dążąc do wyjaśnienia czegoś, należy zacząć od analizy zjawisk i dopiero po wyodrębnieniu istotnych pojęć należy nadawać im określone nazwy** (rys. 2).



Rys. 2. Procedura postępowania przy nadawaniu nazw wyodrębnionym pojęciom

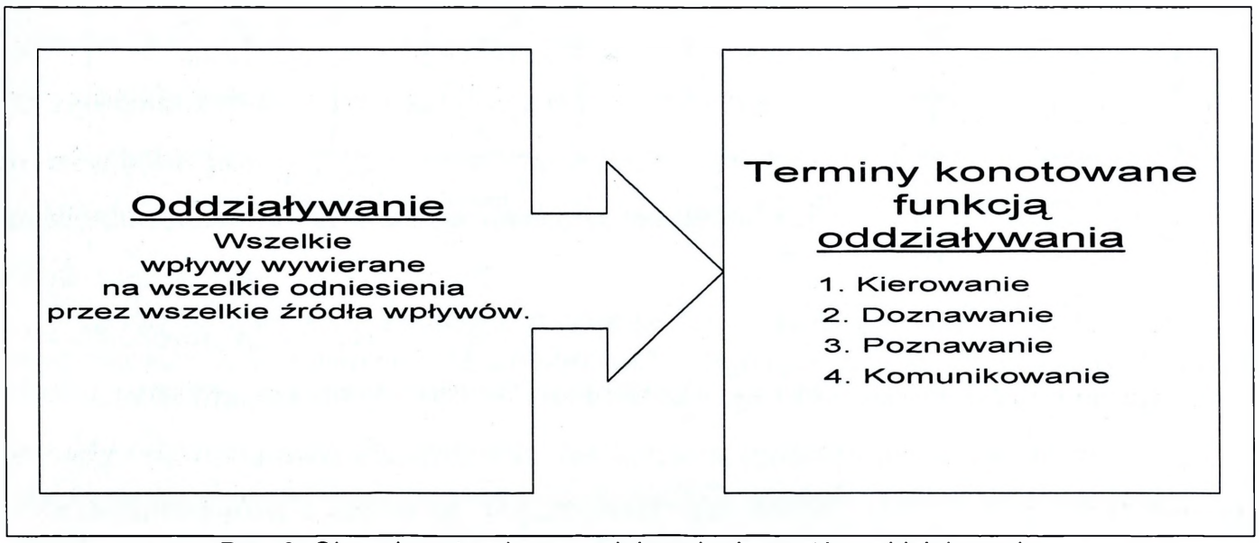
Źródło: Opracowanie autorskie na podstawie: M. Mazur, *Jakościowa teoria informacji*, WNT, Warszawa 1970.

Zastrzega przy tym, że jeżeli jedno z pojęć miałoby objaśniać nazwę **informacja**, to powinno to mieć charakter umowy terminologicznej, podobnie jak się to stało w odniesieniu do terminu **ilość informacji** [6]. Zaznacza jednak, że przedtem należy określić zakres analizowanych zjawisk, czyli ustalić przedmiot badań. Uprzedza też, że narzucająca się tu myśl, aby za przedmiot badań obrać tylko takie zjawiska w których odgrywa rolę informacja, byłaby nielogiczna gdyż postępowanie takie znaczyłoby, że jeszcze przed rozpoczęciem badań przypisuje się wyrazowi **informacja** jakieś znaczenie, chociaż zamierza się je dopiero później określić w umowie terminologicznej, odpowiednio dostosowanej do wyników analizy. Jest zdania, że można uniknąć tej trudności przez objęcie badaniem wszelkich zjawisk. Wskazuje jednak, że praktycznie wystarczy też **ograniczyć się** do takiego dostatecznie dużego ich zakresu, o którym wiadomo, że obejmuje m.in. wszystko to, **co przez rozmaitych ludzi bywa nazywane informacją**. Jako cybernetyk stwierdza, iż nie trudno przy tym spostrzec, że zawsze są to sytuacje, w których chodzi o dążenie do takiego czy innego celu, czyli mówiąc ogólnie, o sterowanie, a wobec tego o do czynienia z problematyką cybernetyczną. Zaznacza, że jako cybernetyk nie interesuje się wszystkimi znaczeniami, w jakich wyraz **informacja** bywa używany, ale sugeruje aby za przedmiot badań obrać tylko te zjawiska, na których polega sterowanie i ujmować je tylko z cybernetycznego punktu widzenia[7].

Marian Mazur, jako cybernetyk, osadził swoje dociekania na temat **informacji** w środowisku **sterowania**, co w jego przypadku jest logiczne i w pełni uzasadnione. Postrzegając natomiast **informację** jako element procedur decyzyjnych, czego potrzeba wynika chociażby z tytułu niniejszego podrozdziału, już tylko z tego względu

[6] M. Mazur, „Jakościowa teoria informacji", WNT, Warszawa 1970, s. 27.
[7] Ibidem.

wydaje się, że dociekania z tym związane należy osadzić w środowisku nieco szerszym, obierając za przedmiot badań nie tylko zjawisko **sterowania**, ale zjawisko **oddziaływania,** którego denotacja[8] uwzględnia znacznie większy zbiór desygnatów[9] niż kryjących się pod nazwą **sterowanie**. **Oddziaływanie** uwzględnia wszelkie wpływy wywierane na wszelkie odniesienia przez wszelkie źródła wpływów. W przestrzeni tej dominujące podprzestrzenie, w których – zgodnie z sugestią Mariana Mazura – można poszukiwać odpowiedzi na zasadnicze pytanie problemowe, dotyczące identyfikacji treści znaczeniowej symbolizowanej terminem **informacja**, zdają się stanowić desygnaty odzwierciedlające myślowe ujęcia istotnych cech przedmiotów, rzeczy i zjawisk przypisywanych semantycznie do terminów: **kierowanie,** doznawanie, **poznawanie** i **komunikowanie**, konotowanych[10] **oddziaływaniem** (rys. 3).



Rys. 3. Obraz konotacyjny zasadniczych elementów oddziaływania

Źródło: Opracowanie autorskie

Terminy te nie wyznaczają przestrzeni związanej tylko i wyłącznie z informacją. Nie obejmują też wszelkich zjawisk. Wyznaczają jednak wystarczająco dużą przestrzeń semantyczną obejmującą treści, które przez rozmaitych ludzi bywają nazywane **informacją**.

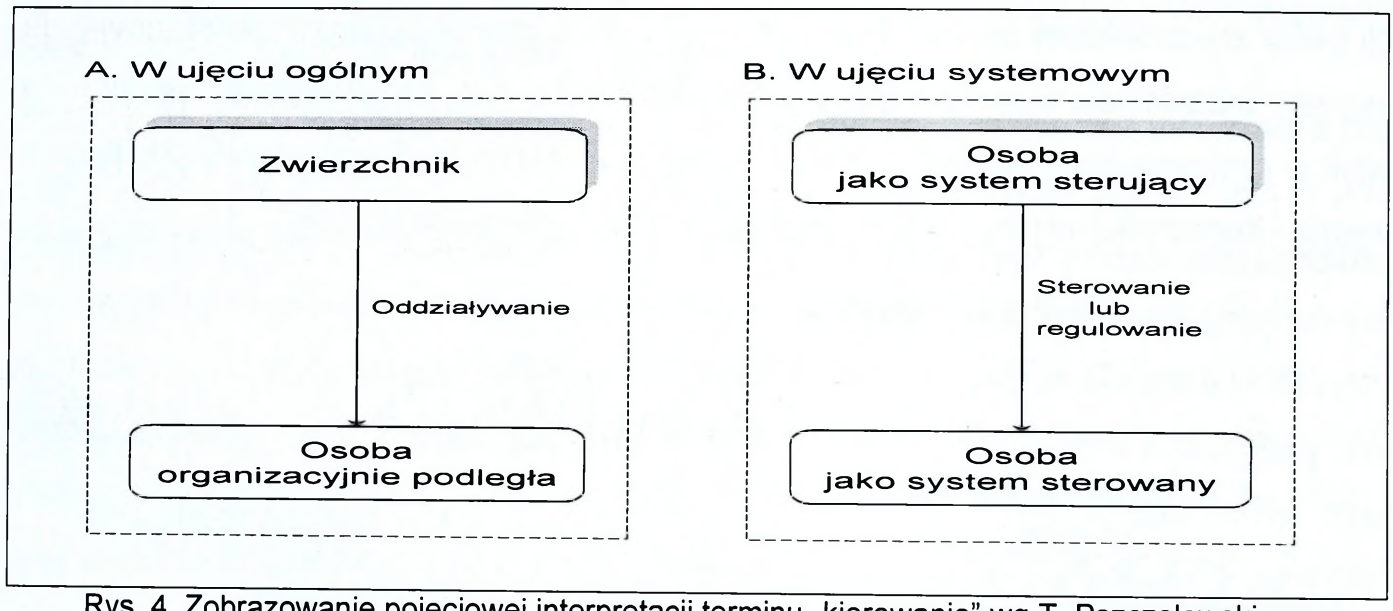
Tadeusz Pszczołowski termin **kierowanie** postrzega pojęciowo jako oddziaływanie zwierzchnika na osobę organizacyjnie mu podporządkowaną, tj. podwładnego, zgodnie z ustaleniami zawartymi w organizacji formalnej albo z wynikającymi

[8] Denotacja – zakres nazwy; zbiór wszelkich desygnatów nazwy (Słownik języka polskiego, PWN, Warszawa 1978, tom I, s. 381).

[9] Desygnat – jednostkowy przedmiot myślowy odpowiadający nazwie (Słownik języka polskiego, PWN,
Warszawa 1978, tom I, s. 387).

[10] Konotacja – cechy współoznaczone łącznie przez daną nazwę; zespół cech, których posiadanie sprawia, że odpowiednie przedmioty należą do tej samej klasy, są desygnatami danej nazwy (Słownik języka polskiego, PWN, Warszawa 1978, tom I, s. 992).

z tego konsekwencjami. Zaznacza przy tym, że kierowanie w ujęciu systemowym można także traktować jako **sterowanie** albo **regulowanie** jednego systemu przez drugi system, gdy pierwszy system jest człowiekiem i drugi system jest człowiekiem[11]. Wynika z tego, że zakres znaczeniowy wyrazu **kierowanie** jest denotacją[12] mieszczącą w swoim wnętrzu semantycznym zakresy znaczeniowe wszelkich terminów symbolizujących zwierzchnie oddziaływania sprawcze, przebiegające w relacjach międzyludzkich (rys. 4).



Rys. 4. Zobrazowanie pojęciowej interpretacji terminu „kierowanie" wg T. Pszczołowskiego

Źródło: Opracowanie autorskie na podstawie: T. Pszczołowski, „Mała encyklopedia prakseologii i teorii organizacji", Zakład Narodowy imienia Ossolińskich, Wrocław – Warszawa – Kraków – Gdańsk 1978, s. 95.

Leszek Pasieczny, Bohdan Gliński, Witold Kieżun, Andrzej K. Koźmiński, Juliusz Kulikowski, Jerzy Kurnal, Stefan Kwiatkowski, Henryk Mreła, Bronisław Ostapczuk i Jerzy Trzcieniecki, jako członkowie Komitetu Redakcyjnego „Encyklopedii organizacji i zarządzania" wyjaśniają[13], że **kierowanie** to termin symbolizujący jedno z podstawowych pojęć organizacyjnych, które najogólniej można rozumieć jako **oddziaływanie** jednego obiektu (kierującego) na inny obiekt (kierowany) zmierzające do tego, aby obiekt kierowany zachowywał się (działał lub funkcjonował) w kierunku osiągnięcia postawionego przed nim celu. Akcentują, że kierowanie jest procesem, w którym można wyróżnić:

- podmiot kierowania (obiekt kierujący),
- przedmiot kierowania (obiekt kierowany),

---

[11] T. Pszczołowski, „Mała encyklopedia prakseologii i teorii organizacji", Zakład Narodowy imienia Ossolińskich, Wrocław – Warszawa – Kraków – Gdańsk 1978 s. 95.

[12] Denotacja – zakres nazwy; zbiór wszystkich desygnatów nazwy („Słownik języka polskiego", PWN, Warszawa 1978, tom I, s. 387).

[13] „Encyklopedia organizacji i zarządzania", PWE, Warszawa 1982, s. 205 i 206.

- stosunek nadrzędności i podporządkowania (podległości)
- cel (lub cele), do których kierowanie zmierza.

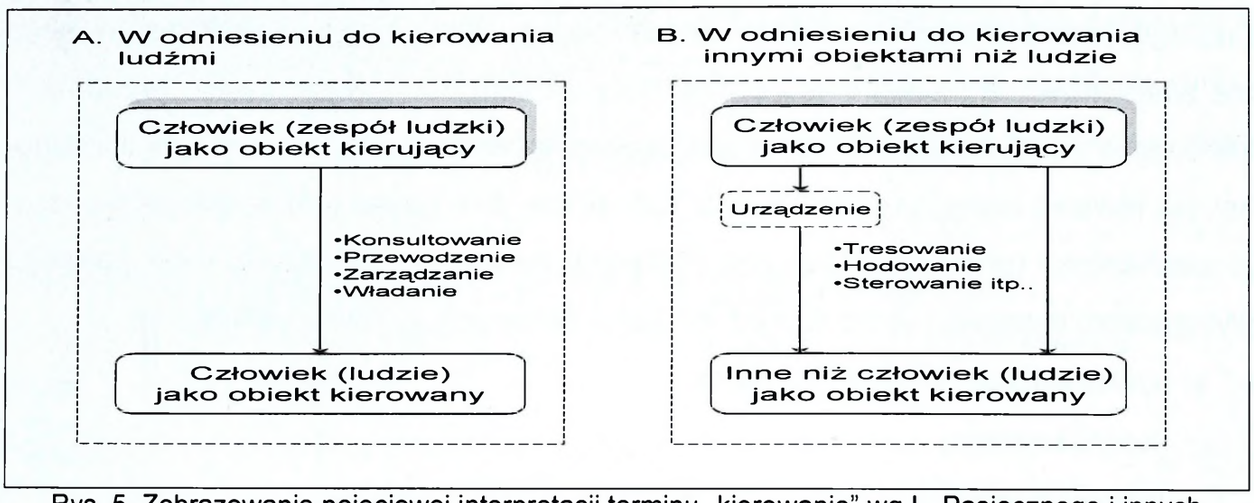
Zaznaczają przy tym, że „podmiot kierowania" może być pojedynczy lub zbiorowy i na ogół jest nim człowiek świadomie kierujący realizacją celów, ale czasem może też zastępować siebie automatycznym urządzeniem. Co się zaś tyczy „przedmiotu kierowania" to wyrażają pogląd, iż najczęściej stanowią go ludzie o różnej liczebności, jak również istoty żywe nie będące ludźmi (np. zwierzęta) oraz rozmaitego rodzaju mechanizmy (pracujące maszyny, pojazdy w ruchu itp.). Dodają do tego, że mogą występować rozmaite, szczegółowe odmiany kierowania różnie określane, np.:

- w odniesieniu do kierowania ludźmi:
  - konsultowanie,
  - przewodzenie,
  - zarządzanie,
  - władanie;
- w odniesieniu do kierowania obiektami nie będącymi ludźmi:
  - tresowanie,
  - hodowanie,
  - sterowanie itp.

Ponadto, na podstawie stwierdzenia, że człowiek czasem może zastępować siebie, w spełnianiu funkcji kierowania, urządzeniem automatycznym przypuszczać można, iż Autorom tego zapisu chodziło o zaakcentowanie, że w każdym układzie kierowania obiektem kierującym jest zawsze człowiek, niezależnie od tego czy generowane przez niego treści kierowania są bezpośrednio przekazywane do obiektu kierowanego, czy też za pośrednictwem urządzenia automatycznego, co może mieć miejsce w odniesieniu do kierowania obiektami nie będącymi ludźmi (rys. 5).

Jerzy Kurnal, podejmując problem kierowania wypowiada się, że przez kierowanie rozumie się zwykle takie oddziaływanie na kogoś lub coś, aby powodowało ono czyjeś lub czegoś zachowanie z wolą kierującego. Uzasadnia, że w tym zwięzłym określeniu występują wyraźnie **trzy składniki kierowania**: podmiot kierujący, obiekt kierowany i powiązania miedzy nimi, polegające na takim oddziaływaniu podmiotu kierowania na przedmiot, które wywołuje zachowanie tego ostatniego zgodnie z wolą podmiotu. Podkreśla przy tym, iż z określenia owego wynika również, że **obiektem kierowania** może być istota żywa lub przedmiot martwy, jak również ze-

spół istot żywych lub przedmiotów martwych, podczas gdy **podmiotem kierowania** może być tylko człowiek, gdyż tylko on może posiadać wolę spowodowania zachowania jakiegoś obiektu.[14]

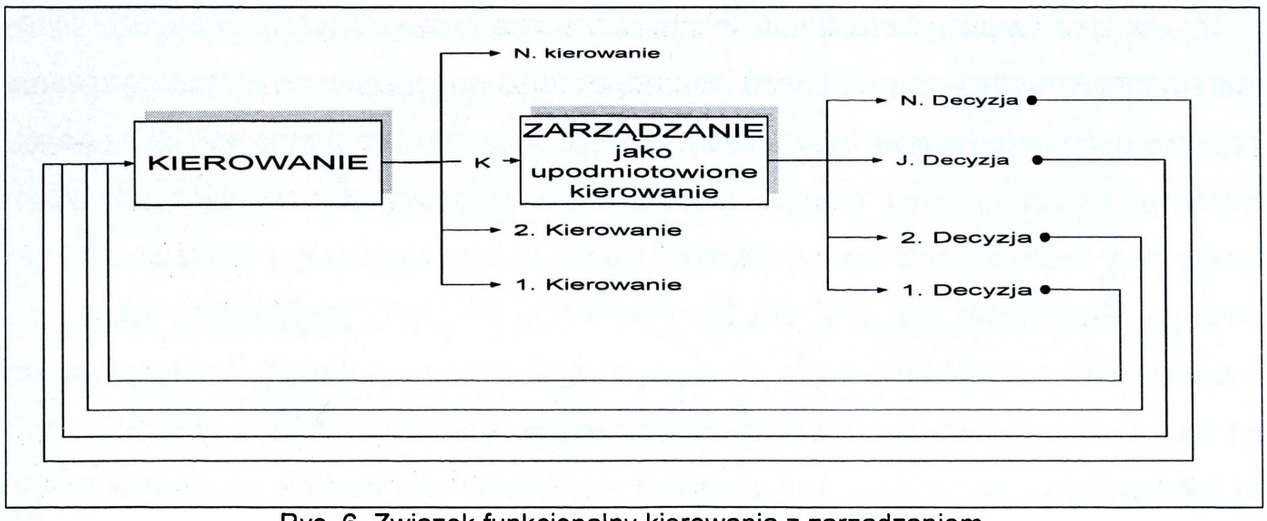


Rys. 5. Zobrazowanie pojęciowej interpretacji terminu „kierowanie" wg L. Pasiecznego i innych

Źródło: Opracowanie autorskie na podstawie: „Encyklopedia organizacji i zarządzania", PWE, Warszawa 1982, s. 205 i 206.

Dalej wypowiada się na temat stosunku wzajemnego dwóch podstawowych pojęć używanych w teorii i praktyce organizacyjnej, które są symbolizowane przez terminy (nazwy): **kierowanie** i **zarządzanie**. Stwierdza, że w tej sprawie i w teorii, i w praktyce istnieje duże pomieszanie pojęć, w związku z czym w literaturze spotkać można wiele i w dodatku zupełnie nieraz przeciwstawnych sobie poglądów. Wyraża przekonanie, że najrozsądniejsze wydaje się przyjęcie tu przekonywającej konwencji, iż **kierowanie jest pojęciem szerszym od zarządzania**.[15] W uzasadnianiu tego przytacza, że rozróżnienie źródeł władzy organizacyjnej oprócz tego, że ułatwia wyjaśnienie istoty pojęcia **kierowanie**, pozwala również na umowne odróżnienie od niego pojęcia **zarządzanie**. Rozwijając tę myśl stwierdza, że w tym stosunkowo szerokim rozumieniu *zarządzanie jest najpowszechniejszą formą sformalizowanego kierowania ludźmi, spotykaną we współczesnej rzeczywistości.*[16] W końcowej części swojego wywodu na ten temat wyraża przekonanie, że różnicę między kierowaniem i zarządzaniem można sprowadzić do stwierdzenia, że *każde zarządzanie jest szczególnym przypadkiem kierowania, ale nie każde kierowanie jest zarządzaniem*[17] (rys. 6).

[14] J. Kurnal, „Zarys teorii organizacji i zarządzania", PWE, Warszawa 1970, s. 358.
[15] Ibidem, s.364.
[16] Ibidem, s.365.
[17] Ibidem, s. 366.

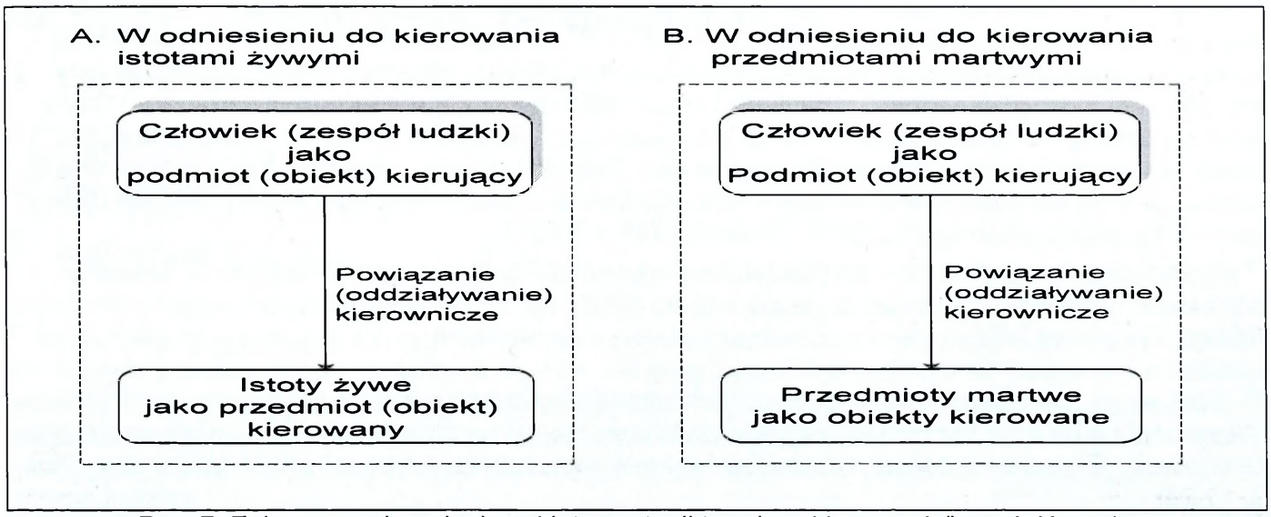


Rys. 6. Związek funkcjonalny kierowania z zarządzaniem

Źródło: Opracowanie autorskie

Z powyższego wynika, iż w interpretacji pojęciowej symbolizowanej przez termin **kierowanie** należy uwzględniać, że (rys. 7):

- strukturę tego zjawiska tworzą trzy następujące składniki:
  - podmiot (obiekt) kierujący,
  - przedmiot (obiekt) kierowania,
  - powiązania istniejące pomiędzy podmiotem (obiektem) kierującym i przedmiotem (obiektem) kierowania;
- podmiotem (obiektem) kierowania może być tylko człowiek, bo tylko on może posiadać wolę spowodowania zachowań jakiegoś obiektu;
- przedmiotem (obiektem) kierowania mogą być:
  - istoty żywe,
  - przedmioty martwe.



Rys. 7. Zobrazowanie pojęciowej interpretacji terminu „kierowanie" wg J. Kurnala

Źródło: Opracowanie autorskie na podstawie: J. Kurnal, „Zarys teorii organizacji i zarządzania", PWE, Warszawa 1970, s. 358–366.

Analizując powyższe treści techniką[18] *porządkowania wstępującego*[19], wyrażone poglądy można interpretować jako odpowiedzi na pytanie: co to jest kierowanie i czym się charakteryzuje? Przy takim założeniu można je też pojmować jako intelektualne przekonania wystarczająco reprezentatywnej grupy autorytetów naukowych, którzy przy nieco zróżnicowanej terminologii ale w istocie sprawy nawiązują do tego samego. Posługując się językiem Henryka Greniewskiego, można powiedzieć, że wszyscy interpretują **kierowanie** jako *układ względnie odosobniony*[20] składający się z trzech komplementarnie zespolonych elementów (obiektów) funkcjonalnych:

1) kierującego – jako generatora wszelkich czynników sprawczych kierowania,
2) kierowanego – jako odbiornika wszelkich generowanych czynników sprawczych,
3) relacyjnego – jako nośnika wszelkich wygenerowanych czynników sprawczych.

W aspekcie poszukiwania tego *co różni ludzie, w ramach **kierowania**, nazywają **informacją***[21] jest istotne jak w literaturze przedmiotu są interpretowane (przedstawiane) **elementy** (obiekty): **kierujący** i **kierowany**. Identyfikując ich treść znaczeniową (semantykę) staje się możliwe ustalenie parametrycznych cech struktury zbiorów stanowiących **czynniki sprawcze kierowania**, czyli tego co kojarzone jest z **informacją**.

Z przytoczonych wcześniej fragmentów literaturowych[22] wynika, że **naczelnym elementem** (obiektem) **kierującym**, stojącym na szczycie każdego układu, jest zawsze **człowiek** określany mianami: zwierzchnika, osoby, zespołu ludzkiego. Jako **elementy** (obiekty) **kierowane** wymieniane są natomiast: osoby, urządzenia, istoty żywe, rośliny i przedmioty martwe. Jako **czynniki sprawcze**, występujące w rela-

---

[18] Technika (w rozumieniu ogólnym) – celowy, racjonalny, oparty na teorii sposób wykonywania prac w jakiejś dziedzinie („Słownik języka polskiego", Warszawa 1981, t. III, s. 486). Technika (w rozumieniu naukowym) – sposób osiągania naukowego celu; naukowy sposób działania (sposób posługiwania się narzędziami naukowymi), gdzie przez narzędzia naukowe rozumie się fizyczny lub pojęciowy aparat (instrument) używany w badaniach naukowych. Techniki użyte przez jakiegoś uczonego są wynikiem jego decyzji (...). Metody to ogólne zasady postępowania badawczego (analiza, synteza itp.). Techniki badawcze odzwierciedlają natomiast sposoby stosowania w tych metodach narzędzi badawczych.(parafraza autorska do: Russell L. Ackoff, „Decyzje optymalne w badaniach stosowanych", PWN, Warszawa 1969, s. 20-21).

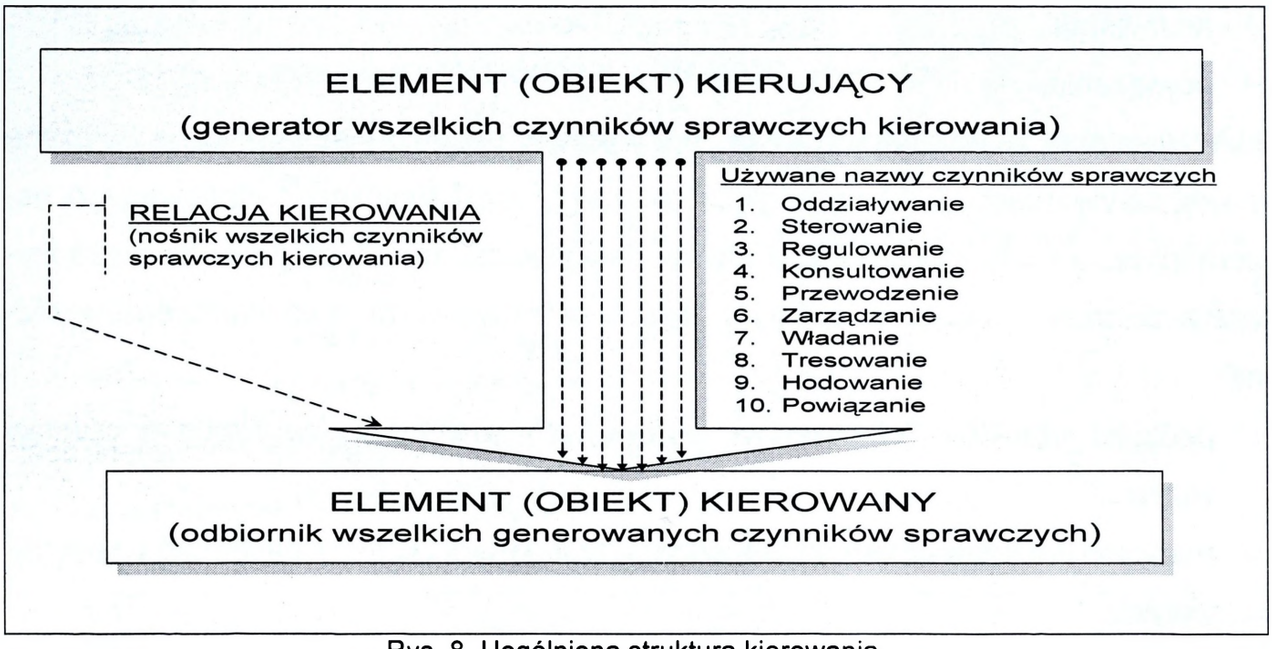
[19] Porządkowanie wstępujące – przekształcanie odpowiedzi na jakieś pytanie dotyczące świata w odpowiedź na pytanie dotyczące czyjegoś umysłu (Adam Morton, „Przewodnik po teorii poznania", Spacja, Warszawa 2002,
s. 305.

[20] Układ względnie odosobniony – przyjmowany subiektywnie, że nie ma on ani jednego wejścia ze Wszechświata i nie ma też żadnego wyjścia do Wszechświata (przypis autorski na podstawie: Henryk Greniewski, „Elementy cybernetyki sposobem niematematycznym wyłożone", PWN, Warszawa 1959, s. 11-23).

[21] Wskazanie Mariana Mazura dotyczące obszaru przedmiotowego, w którym należy poszukiwać odpowiedzi co różni ludzie nazywają „informacją" (M. Mazur, „Jakościowa teoria informacji", WNT, Warszawa 1970, s. 27) – przypis autorski.

[22] Patrz również rys. 12-15.

cjach kierowania są najczęściej wymieniane: oddziaływanie, sterowanie, regulowanie, konsultowanie, przewodzenie, zarządzanie, władanie, tresowanie, hodowanie, powiązanie, które przez różnych ludzi są nazywane **informacjami** (rys. 8).



Rys. 8. Uogólniona struktura kierowania

Źródło: Opracowanie autorskie

Analizując powyższe terminy w aspekcie semantycznym[23] wynika, że nadrzędnym znaczeniowo jest **oddziaływanie**. Zakres pojęciowy[24] tego terminu można zatem uznawać za denotację wszystkich desygnatów[25] przypisywanych do terminów pozostałych (sterowania, regulowania, konsultowania, przewodzenia, zarządzania, władania, tresowania, hodowania, powiązania). Każdy z nich, w jakiejś części, kojarzy się zawsze z przedmiotem myślowym odzwierciedlającym określoną **formę wpływu**, a ta przecież, w najogólniejszej postaci, jest przypisywana do **oddziaływania**. Można zatem interpretować, że treści znaczeniowe:

- sterowania,
- regulowania,
- konsultowania,
- przewodzenia,

[23] Semantyka (semantics) – dyscyplina badająca relacje znaczeniowe występujące pomiędzy znakami językowymi a przedmiotami, do których się one odnoszą. Semantyka zajmuje się badaniem znaczenia słów, czyli interpretacją znaków oraz interpretacją zdań i wyrażeń języka. Semantyka logiczna (nazywana też „teorią modeli") bada języki sztuczne (przedmiotowe) i jest wówczas interpretowana za pomocą metajęzyka. Semantykę nazywa się także „teorią znaczenia" lub „teorią oznaczania" (Quine) – przypis autorski.

[24] Pojęcie – myślowe odzwierciedlenie całościowego ujęcia istotnych cech przedmiotów (rzeczy) czy zjawisk – jest myślowym odzwierciedleniem nazwy (przypis autorski).

[25] Desygnat – przedmiot myślowy odpowiadający wyrazowi; jednostkowy przed myślowy odpowiadający nazwie (Słownik języka polskiego, PWN, Warszawa 1978, tom I, s. 381).

- zarządzania,
- władania,
- tresowania,
- hodowania,
- powiązania,

stanowią sobą, ze względu na **kryterium wpływu**, podzbiory semantyczne związane z **oddziaływaniem**. Dokonując głębszej analizy morfologicznej[26] stosowanego nazewnictwa, a nade wszystko pod kątem słowotwórczym i zasad dobrego porządkowania zbiorów[27], można w ogólnym zbiorze **oddziaływania kierowniczego** wyróżnić:

- podzbiór obiektów (elementów) kierowanych wrażliwych na fizyczne czynniki wpływu,
- podzbiór obiektów (elementów) kierowanych wrażliwych na niefizyczne czynniki wpływu.

Przyjęcie takiego kryterium rozstrzygalności (cechy wyróżnialności) spełnia warunki dobrego porządkowania zbioru, ponieważ:

- suma wyróżnionych podzbiorów ze zbioru obiektów (przedmiotów) kierowanych stanowi zbiór pełny (reguła zupełności):

$$O_K = O_{KF} \cup O_{KNF} = 1^*;$$

- iloczyn wyróżnionych podzbiorów ze zbioru obiektów (przedmiotów) kierowanych stanowi zbiór pusty (reguła rozłączności):

$$O_K = O_{KF} \cap O_{KNF} = 0^*;$$

---

[26] Morfologia (w językoznawstwie) – dziedzina lingwistyki zajmująca się formami odmiennych części mowy (fleksją) oraz słowotwórstwem. W morfologii językoznawczej istnieją dwa główne podejścia – „morfemiczne"
i „leksemiczne". (1) W podejściu „morfemicznym" elementarną jednostką analizy morfologicznej jest abstrakcyjny „morfem", interpretowany jako najmniejsza część wyrazu będąca nośnikiem określonego znaczenia, gdzie „wyraz" jest rozumiany jako „znak prosty", jeśli złożony jest z jednego morfemu, albo jako „znak złożony", jeśli występuje w nim więcej morfemów. (2) W podejściu „leksemicznym" podstawową jednostką analizy, zawierająco w sobie „znak językowy", jest abstrakcyjny „leksem", łączący w sobie funkcję wszystkich cech gramatycznych i postaci dźwiękowych „wyrazu". Terminu „morfem" używa się w odniesieniu do fragmentów „formy wyrazowej". „Morfem", chociaż nie posiada statusu konkretnego „znaku językowego", jest jednak traktowany jako wykładnik „operacji morfologicznej" – jest pomocny w ustalaniu zależności, które występują pomiędzy „leksemami prostymi" i „leksemami złożonymi" (ma to szczególne znaczenie w słowotwórstwie), względnie „leksemami" i realizującymi je „formami wyrazowymi" – to znaczy formami fleksyjnymi i słowotwórczymi (przypis autorski).

[27] Zbiory dobrze uporządkowane – takie gdzie są spełnione warunki: (1) zupełności (suma wyróżnionych podzbiorów stanowi zbiór pełny); (2) rozłączności (iloczyn dowolnej pary wyróżnionych podzbiorów stanowi zbiór pusty); (3) przechodniości (w każdym wyróżnionym podzbiorze musi się znajdować najwcześniejsza cecha wyróżnialności) – przypis autorski.

- każdy z wyróżnionych podzbiorów posiada cechę najwcześniejszą oznaczającą, że jest to podzbiór obiektów (przedmiotów) kierowanych (reguła przechodniości):

$$O_K \Re O_{KF} \wedge O_K \Re O_{KNF} \rightarrow O_K \Re O_{KNF}$$

gdzie:

O_K – zbiór wszystkich obiektów (przedmiotów) kierowanych,

O_{KF} – podzbiór obiektów (przedmiotów) kierowanych wrażliwych na fizyczne czynniki wpływu,

O_{KNF} – podzbiór obiektów (przedmiotów) kierowanych wrażliwych na niefizyczne czynniki wpływu,

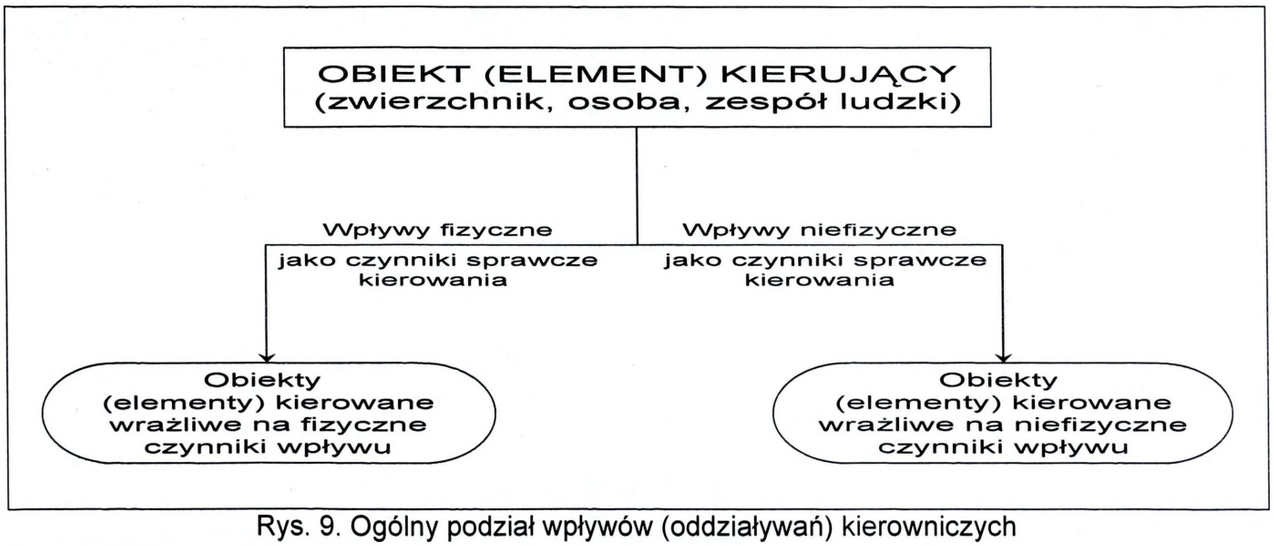
1^* – symbol zbioru pełnego,

0^* – symbol zbioru pustego;

$\Re$ – symbol relacji,

$\wedge$ – znak logiczny oznaczający „i",

co można wyrazić następującym zobrazowaniem graficznym (dendrytem) – rys. 9.



Rys. 9. Ogólny podział wpływów (oddziaływań) kierowniczych

Źródło: Opracowanie autorskie.

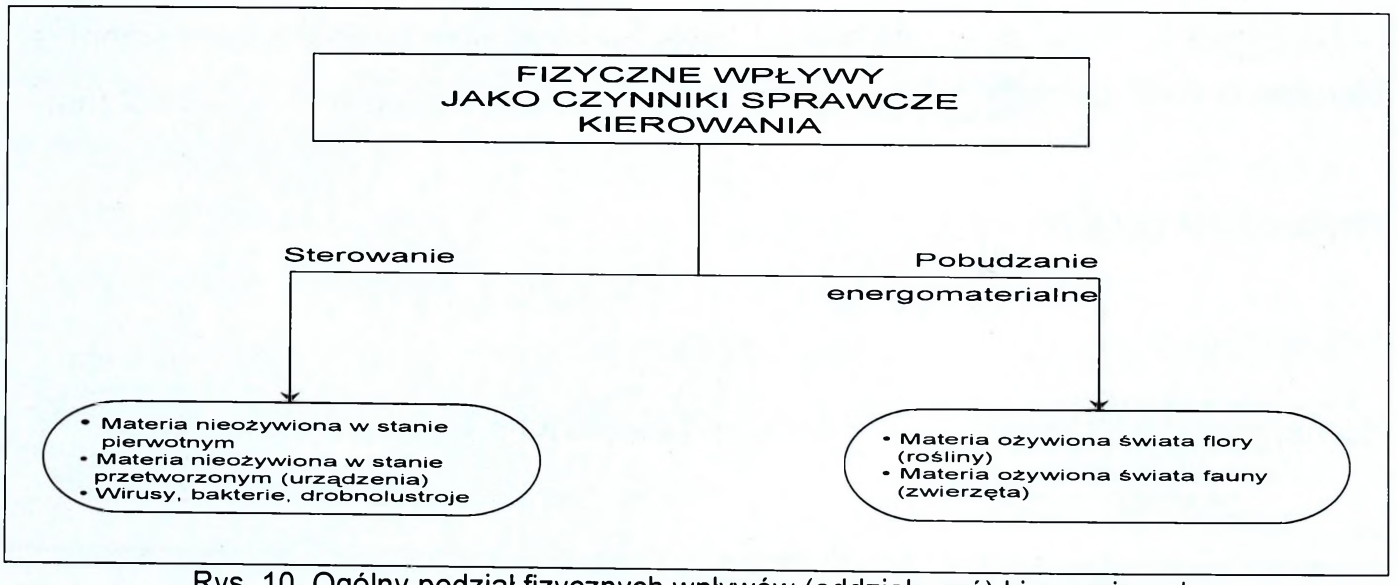
Przyjmując powyższe kryterium kategoryzacji należy mieć na względzie, że kierownicze **wpływy** (oddziaływania) **fizyczne** to nic innego jak oddziaływanie **energomaterialne**[28] obiektu (elementu) kierującego na obiekt (element) kierowany, z takim następstwem sprawczym, że fizyczne czynniki wpływu (oddziaływania), generowane przez obiekt (element) kierujący, wywołują w obiekcie (elemencie) kierowanym zmiany objawiające się:

- bądź to stanem ilościowym energii lub masy (substancji),
- bądź czasowo-przestrzennym przemieszczaniem energii lub masy (substancji).

[28] Termin „energomateria" jest używany jako denotacja zakresu znaczeniowego wyrazów kryjących się pod nazwami: energia i masa (substancja) – przypis autorski.

Innymi słowy, istota sprawcza tej formy oddziaływania (wpływu) kierowniczego sprowadza się do fizycznego wymuszania określonych zmian w przedmiocie (obiekcie) kierowanym, które można przewidywać apriorycznie, z większą dokładnością niż inne. Biorąc to pod uwagę zdaje się być uzasadnione aby tę formę wpływów (oddziaływań) kierowniczych, ze względu na stopień dokładności sprawstwa, określać mianami: **sterowanie** i **pobudzanie energomaterialne**, a do podzbiorów obiektów (elementów) w ten sposób kierowanych zaliczać te, których struktury stanowi (rys. 10):

- w warunkach **sterowania** (charakteryzującego się największym stopniem dokładności sprawczej)[29]:
  - materia nieożywioną w stanie pierwotnym,
  - materia nieożywioną w stanie przetworzonym (wszelkie urządzenia),
  - materia ożywioną nie należącą, ani do istot żywych ani do świata flory (bakterie, wirusy, drobnoustroje);



Rys. 10. Ogólny podział fizycznych wpływów (oddziaływań) kierowniczych
Źródło: Opracowanie autorskie.

- w warunkach **pobudzania energomaterialnego** (charakteryzującego się mniejszym stopniem dokładności sprawczej niż sterowanie)[30]:
  - materia ożywiona świata flory (rośliny),
  - materia ożywiona świata fauny (zwierzęta).

Do zbioru **niefizycznych wpływów** (oddziaływań) kierowniczych, pobudzających do określonych działań obiekty kierowane, można zaliczać **semantykę**[31]

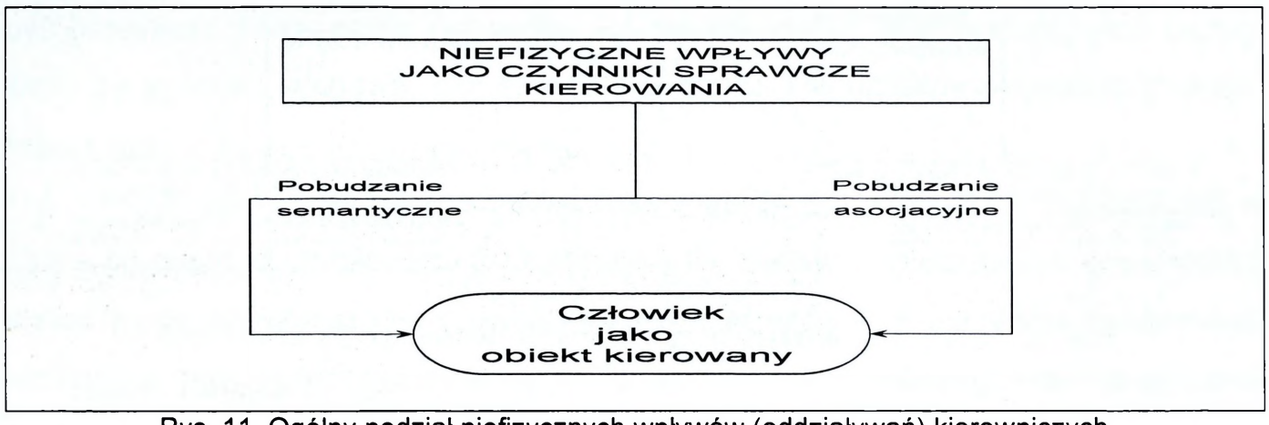
---

[29] Sterować – nadawać okrętowi lub samolotowi kierunek za pomocą steru, sterów; regulować pracę maszyn za pomocą specjalnych urządzeń (S. Skorupka, H. Anderska, Z. Łempicka, „Słownik języka polskiego", PWN, Warszawa 1968, s. 777).

[30] Pobudzać – wywołać reakcję czynną, uczuciową, dać impuls do czego (...) [S. Skorupka, H. Anderska,Z. Łempicka, „Słownik języka polskiego", PWN, Warszawa 1968, s. 570].

[31] Semantyka – treść znaczeniowa znaków słownych i znaków wyrazowych (przypis autorski).

i **czynniki sytuacyjne** możliwe do identyfikowania w ramach **percepcji relacyjnej**[32]. Na tego rodzaju wpływy (oddziaływania) kierownicze może być wrażliwy tylko i wyłącznie **człowiek** (homo sapiens) jako istota dostosowana do **myślenia** i **asocjacyjnego kojarzenia**[33] doznań (rys. 11).

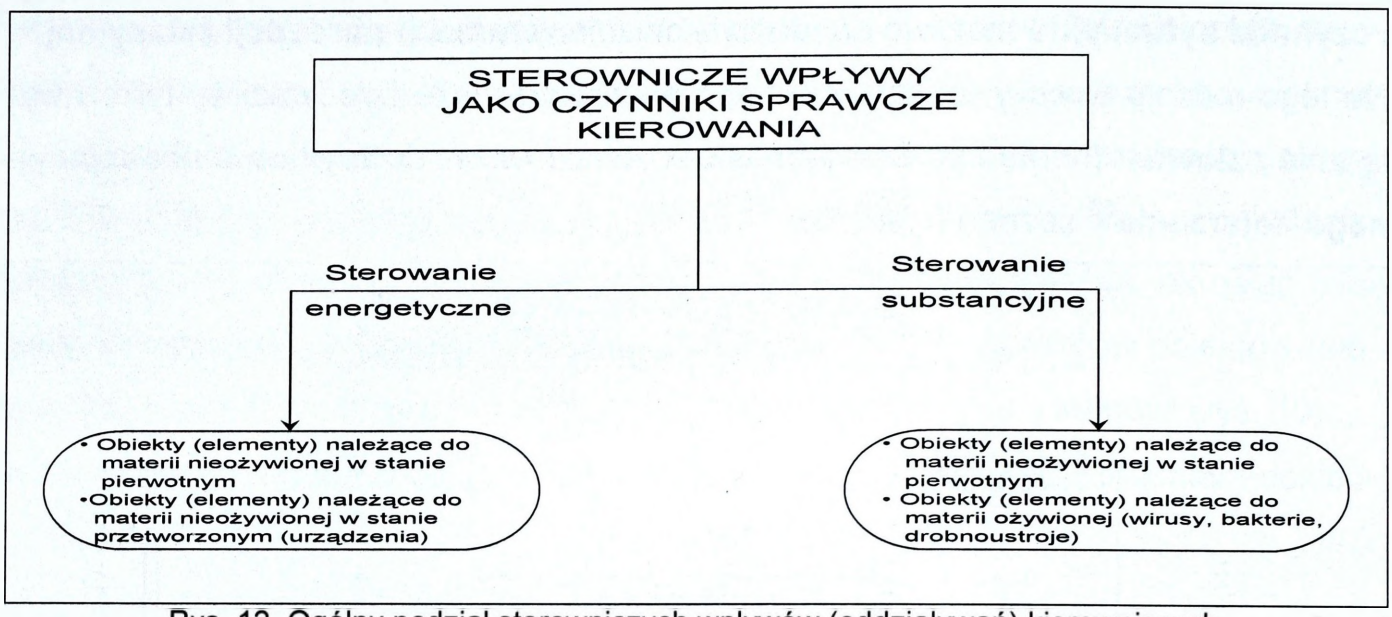


Rys. 11. Ogólny podział niefizycznych wpływów (oddziaływań) kierowniczych
Źródło: Opracowanie autorskie.

Co się zaś tyczy **sterowania**, to w zbiorze tym należy jeszcze uwzględniać, że jedna grupa obiektów jest bardziej wrażliwa na oddziaływania **energetyczne**, druga zaś na **substancyjne**, Dlatego też w ogólnym zbiorze sterowania należy jeszcze dostrzegać (rys. 12):

- sterowanie energetyczne, dostosowane do oddziaływania na:
  - obiekty (elementy) należące do materii nieożywionej znajdującej się w stanie pierwotnym,
  - obiekty (elementy) należące do materii nieożywionej znajdującej się w stanie przetworzonym (wszelkie urządzenia techniczne);
- sterowanie substancyjne, dostosowane do oddziaływania na:
  - obiekty (elementy) należące do materii ożywionej, ale z wyłączeniem istot świata fauny i organizmów świata flory, to znaczy tylko na obiekty (elementy) należące do świata wirusów, bakterii i drobnoustrojów,
  - obiekty (elementy) należące do materii nieożywionej w stanie pierwotnym.

[32] Percepcja relacyjna – użycie zmysłów do stworzenia pewnej więzi między jakąś osobą a konkretnym przedmiotem, która daje tej osobie informacje o tym przedmiocie (A. Morton, „Przewodnik po teorii poznania", Spacja, Warszawa 2002, s. 304.
[33] Asocjacja – łączenie się ze sobą wyobrażeń; związek pomiędzy przedstawieniami polegającymi na tym, że przypomnienie sobie jednej z nich przywołuje na myśl inne; asocjacja pomiędzy wyobrażeniami przedmiotu a jego nazwą (przypis autorski).



Rys. 12. Ogólny podział sterowniczych wpływów (oddziaływań) kierowniczych

Źródło: Opracowanie autorskie.

Sterujące oddziaływanie człowieka na przedmioty (elementy) kierowane nie jest też relacyjnie jednorodne. Może być **bezpośrednie** lub **pośrednie**. Jest to uzależnione od możliwości dostosowywania się efektorów ludzkich[34] do wrażliwości reakcyjnej obiektów (elementów) poddawanych kierowaniu. Posługując się językiem prakseologii można to również nazywać bezpośrednią lub pośrednią więzią przyczynową, rozumianą w ten sposób, że zdarzenie późniejsze jest skutkiem wcześniejszego nacisku, a nacisk wcześniejszy jest przyczyną zdarzenia późniejszego[35]. W ten sposób układ zdarzeń wcześniejszych można nazywać warunkiem wystarczającym zdarzenia późniejszego ze względu na dane prawo następstwa i ze względu na odcinek czasu, który wypełniają wszystkie zdarzenia składowe tego układu. Dlatego też, w aspekcie więzi przyczynowej, **sprawstwo** wynika zawsze ze zdarzeń wcześniejszych pod warunkiem, że te stanowią sobą składniki istotne warunku wystarczającego[36].

W sterowaniu bezpośrednim składniki istotne warunku wystarczającego muszą być spójne z możliwościami fizycznymi ludzkich efektorów. Przykładem takiego sterowania może być kierowanie autem, gdzie człowiek poprzez wykonywanie odpowiednich ruchów rękami, zmienia położenie kierownicy i w ten sposób steruje kierunkiem jazdy. Podobnie rzecz się ma podczas jazdy na rowerze, gdzie cyklista poprzez

---

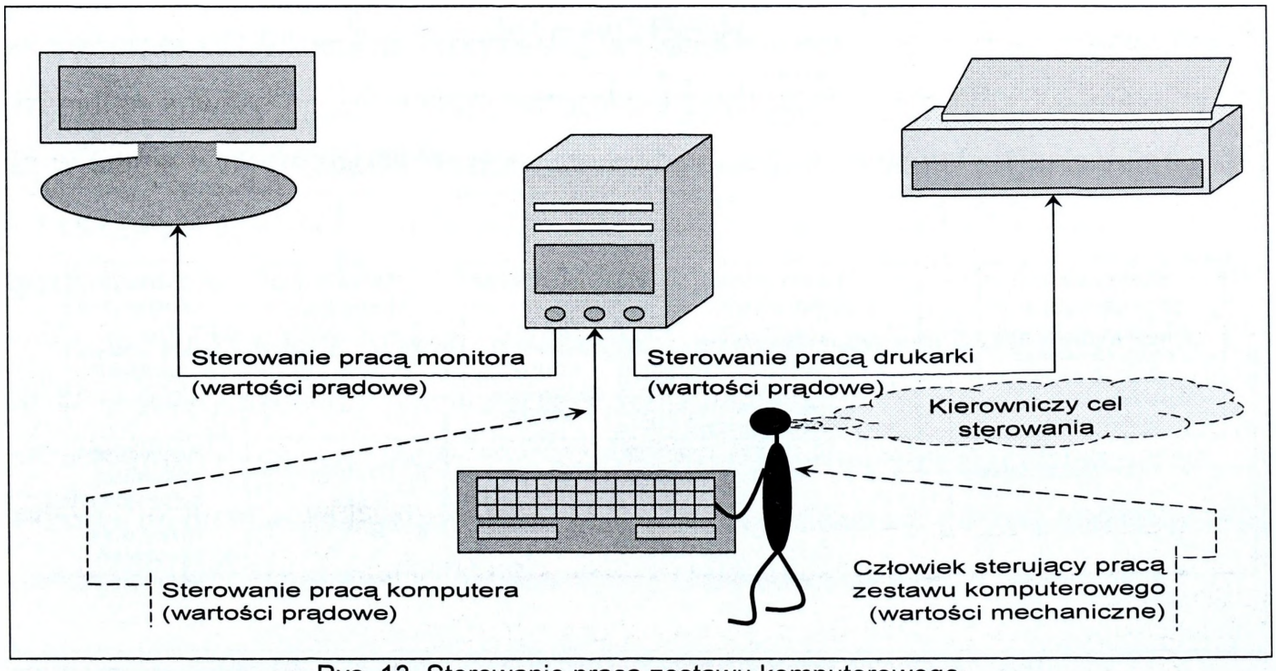
[34] Efektor – narząd wykonawczy w organizmie pobudzany lub hamowany przez impulsy nerwowe (przypis autorski).

[35] T. Kotarbiński, Traktat o dobrej robocie (wdanie siódme)", Ossolineum, Wrocław·Warszawa·Kraków·Gdańsk·
Łódź, 1982, s. 23.

[36] Ibidem, s. 23 i 24.

ruchy swoich kończyn powoduje obracanie się kół swojego pojazdu, a zwroty kierownicy powodują jazdę w pożądanym kierunku. W obydwóch przypadkach czynnikiem sprawczym warunku wystarczającego jest energia ludzkich mięśni przekazywana na odpowiednie elementy pojazdu. Innym przykładem sterowania bezpośredniego może być przemieszczanie przez człowieka elementów materii nieożywionej pod warunkiem, że jej masa wagowa, stanowiąca siłę oporu, nie przekracza jego możliwości fizycznych.

Przykładem pośredniego sterowania, materią nieożywioną znajdującą się w stanie pierwotnym, może być przemieszczanie górotworów za pomocą substancji dynamitu, co jest powszechnie praktykowane w górnictwie. Przykładem pośredniego sterowania materią nieożywioną, ale znajdującą się już w stanie przetworzonym, może być praca człowieka z komputerem. Jak wiadomo zmiany operacyjne w tym urządzeniu są zawsze powodowane wartościami prądowymi, czego ludzkie efektory nie są w stanie wytwarzać. Dlatego też sterowanie jego funkcjonowaniem musi się odbywać pośrednio – poprzez odpowiednio dobrane urządzenia wejściowe, które umożliwiają przetwarzanie funkcji efektorów (dotyku, fali akustycznej wywołanej głosem) na odpowiednie kombinacje prądowe. Wówczas dopiero, po dotarciu odpowiedniego ciągu impulsów elektrycznych do pamięci operacyjnej, zostają uruchamiane stosowne programy, które poprzez procesor realizują określone zadania. Tym samym urządzenia wejściowe (klawiatura, myszka, joystick), postrzegane w relacji „człowiek – komputer", stanowią sobą elementy pośrednie (rys. 13).

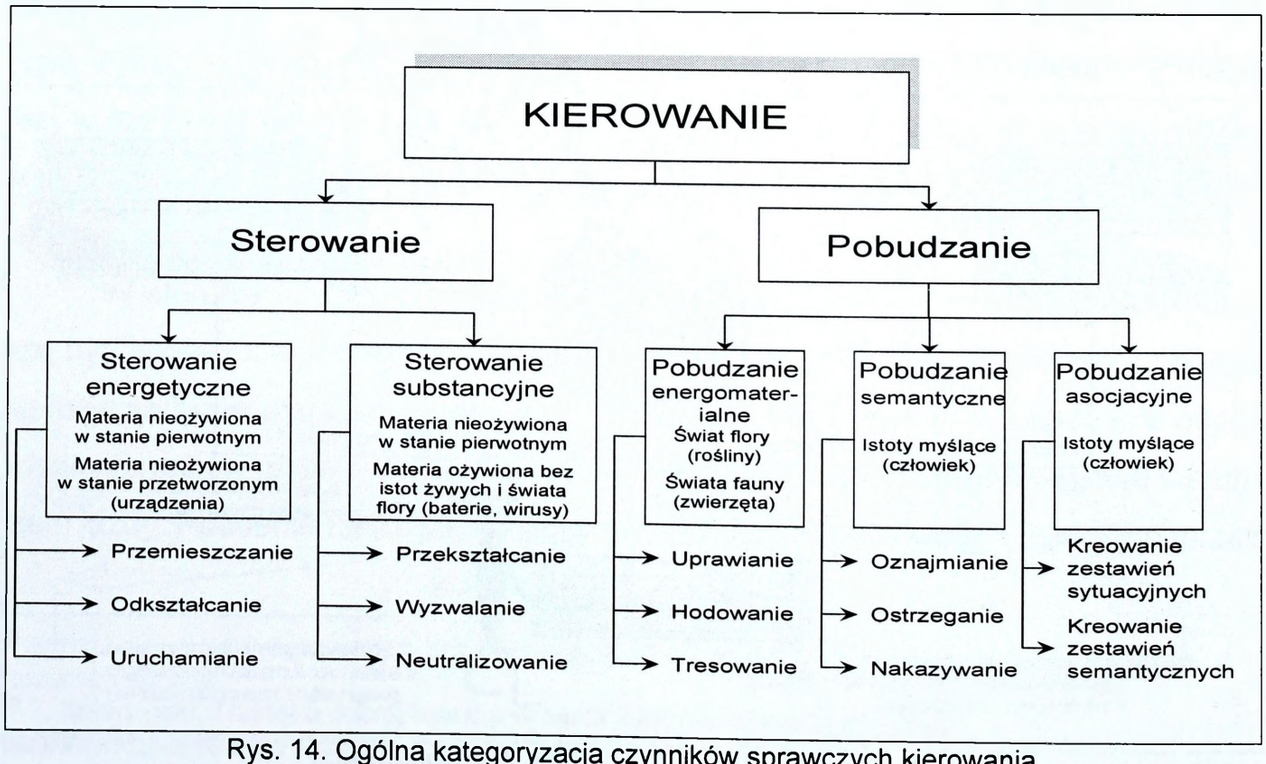


Rys. 13. Sterowanie pracą zestawu komputerowego

Źródło: Opracowanie autorskie

W tym miejscu można już stwierdzić, że wszelkie formy **sterowania** i **pobudzania** stanowią sobą **oddziaływania** kierownicze **wpływające** na zmiany w obiektach poddawanych kierowaniu. Ich siła sprawcza uzewnętrznia się (rys. 14):

- w obszarze sterowania energetycznego:
  - przemieszczaniem,
  - odkształcaniem,
  - uruchamianiem;
- w obszarze sterowania substancyjnego:
  - przekształcaniem,
  - wyzwalaniem,
  - neutralizowaniem;
- w obszarze pobudzania energomaterialnego:
  - uprawianiem,
  - hodowaniem,
  - tresowaniem;
- w obszarze pobudzania semantycznego:
  - oznajmianiem,
  - ostrzeganiem,
  - nakazywaniem;



Rys. 14. Ogólna kategoryzacja czynników sprawczych kierowania

Źródło: Opracowanie autorskie

- w obszarze pobudzania asocjacyjnego:
  - kreowaniem zestawień sytuacyjnych,
  - kreowaniem zestawień semantycznych.

Przyjmując, że jednym z **typów** czynności, występujących w nieskończonym zbiorze wszelkich czynności, jest **kierowanie** sprowadzające się do **oddziaływania** obiektu kierującego na obiekt kierowany i rozumiejąc że termin **typ** symbolizuje nadrzędną jednostkę klasyfikacyjną, której przyporządkowuje się pewną serię rzeczy i zjawisk, można też przyjmować, że **sterowanie** i **pobudzanie** stanowią sobą **formy oddziaływania kierowniczego**, a mieszczące się w ich wnętrzu funkcjonalnym zróżnicowane gatunkowo oddziaływania nazywać **rodzajami kierowania**. Oznaczając zatem symbolem „C_k" kierowanie, gdzie „C" oznacza czynność, a przypisany do tego znaku indeks „k" cechę wyróżnialności utożsamiającą ten symbol z **typem** oddziaływania zwanym **kierowanie**, można dalej oznaczać:

- symbolem C_{k1} – **formę** oddziaływania kierowniczego zwaną „sterowaniem",
- symbolem C_{k2} – **formę** oddziaływania kierowniczego zwaną „pobudzaniem",
- symbolem C_{k11} – **rodzaj** oddziaływania kierowniczego zwany „sterowaniem energetycznym",
- symbolem C_{k12} – **rodzaj** oddziaływania kierowniczego zwany „sterowaniem substancyjnym",
- symbolem C_{k21} – **rodzaj** oddziaływania kierowniczego zwany „pobudzaniem energomaterialnym",
- symbolem C_{k22} – **rodzaj** oddziaływania kierowniczego zwany „pobudzaniem semantycznym",
- symbolem C_{k23} – **rodzaj** oddziaływania kierowniczego zwany „pobudzaniem asocjacyjnym";

gdzie:

- indeks znajdujący się na pierwszej pozycji symbolizuje **typ** oddziaływania,
- indeks znajdujący się na drugiej pozycji symbolizuje **formę** oddziaływania,
- indeks znajdujący się na trzecie pozycji symbolizuje **rodzaj** oddziaływania.

Przyjętą co do tego kategoryzację można wyrazić graficznie w postaci następującego dendrytu[37], który spełnia warunki dobrego porządkowania zbiorów (rys. 15):

[37] Dendryt – graficzny obraz struktury [M. Kempisty (redakcja), „Mały słownik cybernetyczny", Wiedza Powszechna, Warszawa 1973, s. 78].

- zupełności, bo:
  - na każdym poziomie podziału suma wyróżnionych podzbiorów stanowi sobą zbiór pełny:

$$C_{k1} \cup C_{k2} = C_k = 1^*$$

gdzie:

$$C_{k1} = C_{k11} \cup C_{k12}$$

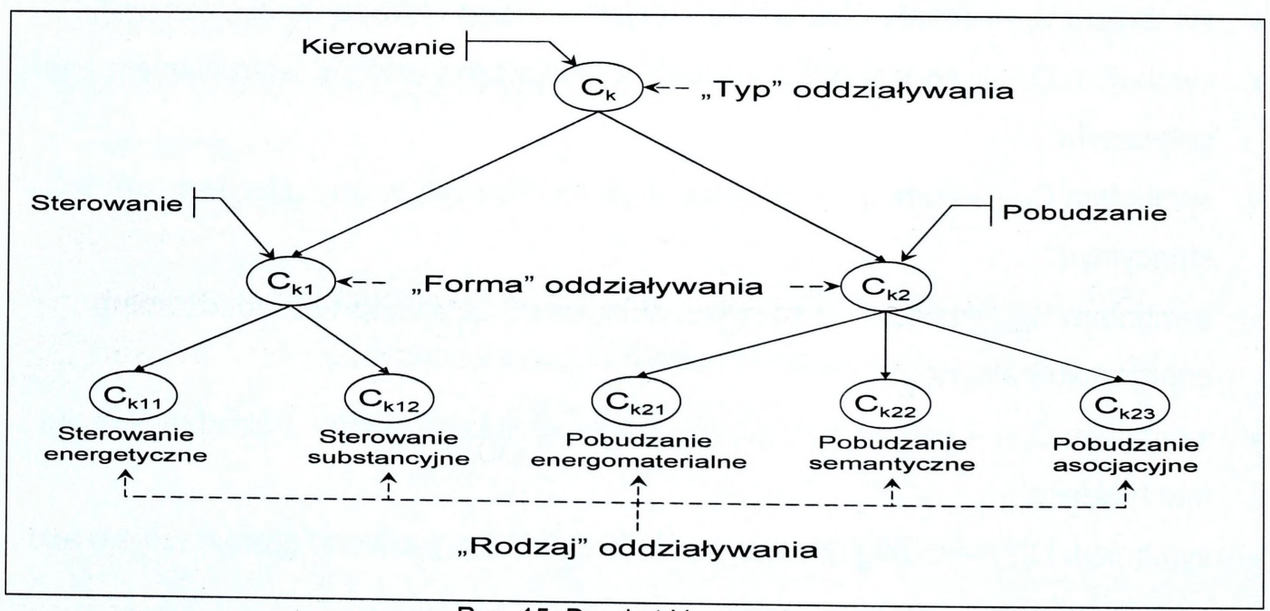
$$C_{k2} = C_{k21} \cup C_{k22} \cup C_{k23};$$

- rozłączności, bo:
  - na każdym poziomie podziału iloczyny dowolnych par wyróżnionych podzbiorów, ze względu na przyjętą cechę wyróżnialności, stanowią zbiory puste:

$$C_{k1} \cap C_{k2} = 0^*;\ C_{k11} \cap C_{k12} = 0^*;\ C_{k11} \cap C_{k21} = 0^*;\ C_{k11} \cap C_{k22} = 0^*;\ C_{k11} \cap C_{k23} = 0^*;$$

$$C_{k12} \cap C_{k21} = 0^*;\ C_{k12} \cap C_{k22} = 0^*;\ C_{k12} \cap C_{k23} = 0^*;\ C_{k21} \cap C_{k22} = 0^*;$$

$$C_{k21} \cap C_{k23} = 0^*;\ C_{k22} \cap C_{k23} = 0^*;$$



Rys. 15. Dendryt kierowania

Źródło: Opracowanie autorskie

- „przechodniości", bo:
  - na każdym poziomie podziału znajduje się cech najwcześniejsza identyfikująca kierowanie:

$$C_k \ \Re \ C_{k1} \wedge C_{k1} \ \Re \ C_{k12} \rightarrow C_k \ \Re \ C_{k12};$$

- „przeciwzwrotności", bo:
  - każdy element wyróżnionego podzbioru, ze względu na zastosowaną cechę wyróżnialności, nie pozostaje w relacji sam do siebie:

$$x \overline{\Re} x;$$

- „spójności", bo:
  - podzbiory wyróżnione ze względu na określona cechę pozostają do siebie w relacji:

$$X = Y \rightarrow X \Re Y \vee Y \Re X.$$

Podsumowując część związaną z poszukiwaniem wyjaśnienia na temat informacji funkcjonującej w przestrzeni kierowania można stwierdzić, że w środowisku tym **informacjami** są najczęściej nazywane różne czynniki sprawcze (fizyczne i niefizyczne) wywierające określone wpływy na obiekty poddawane kierowaniu. Ze względu na dokładność oddziaływania czynniki te są często zaliczane, albo do grupy **informacji sterujących**, albo do grupy **informacji pobudzających**. Analizowana w tym kontekście rozpiętość pojęciowa, przypisywana do tych terminów, zdaje się być nadmiernie rozległa semantycznie i tym samym mało precyzyjna do stosowania w szczegółowych opisach. Wynika z tego, że istnieje potrzeba wprowadzenia do niej stosownych uzupełnień terminologicznych, które wzbogacą i udokładnią język opisu związany z powstawaniem, bytowaniem, funkcjonowaniem i przetwarzaniem informacji.

W przestrzeniach doznawania, poznawania i komunikowania termin **informacja** jest znacznie szerzej stosowany niż w przestrzeni kierowania. Jest powszechnie używany w mediach, w edukacji, w nauce i w życiu codziennym. Na przykład człowiek słuchający radia lub czytający prasę dowiaduje się różnych rzeczy. Rozmawiając z innymi zwykle nazywa to, czego się dowiedział, informacjami. Mówi, że takie czy inne informacje na ten czy inny temat uzyskał z radia lub z prasy. Oznacza to, że zarówno wypowiadane tam słowa jak i zapisane wyrazy, zestawione w zdania i określone grupy zdań, uznał za informacje. Słuchający tego uznał też za informację wypowiedź swojego rozmówcy. Oglądający telewizję zwykle nazywa informacjami swoje doznania wzrokowe (obrazy i sceny sytuacyjne), podobnie jak swoje doznania słuchowe nazywa informacjami odbierający określone efekty dźwiękowe. Podobnie rzecz się ma i z efektami pozostałych doznań zmysłowych (węchowymi, smakowymi i dotykowymi). Informacjami są też nazywane wcześniej nieznane, a w danej chwili dostrzeżone, różnego rodzaju rzeczy, zjawiska i procesy. Przykładem tego może być opisana już w rozdziale pierwszym procedura wykrywania emisji elektronowej, gdzie zaobserwowane przez Juliusza Plücker'a zjawisko było pierwotnie tylko doznaniem

wzrokowym, które komentowano, że „w chwili gdy ciśnienie w szklanej rurze, będącej pod napięciem elektrycznym, zmniejsza się to świecenie przy katodzie wydłuża się". Dopiero po 38 latach wyjaśniono to zjawisko i nadano mu nazwę „promieniowanie katodowe", która semantycznie symbolizuje sobą wszelkie treści fizyczne związane z wymuszania emisji elektronowej w próżni.[38]

Termin **informacja**, z różnymi uzupełnieniami przymiotnikowymi, występuje często w nazewnictwie określonych struktur organizacyjnych. Wyróżnia się informację kolejową, informację autobusową, informację lotniczą, informację turystyczną, informację naukową, informację biblioteczną, a w szerszym ujęciu – nawet służby informacyjne[39]. Mówi się też o informacji drogowej zawartej w znakach przydrożnych[40], o informacji katalogowej[41], o informacji harmonizującej wielopodmiotowe działania kooperacyjne[42] i o informacji jako komitywie językowej (mówionej i pisanej) sprowadzającej się do przekazywania myśli w różnych kontaktach międzyludzkich do czego jest zdolny tylko i wyłącznie człowiek, wyróżniony spośród gatunków stworów żywych Ziemi[43]. Co do tego można przytaczać wiele i innych przykładów. Wydaje się jednak, że i te wystarczą już do przekonania Czytelnika, iż jedną z przyczyn – a być może i główną – jest fakt, że nazwa ta jest używana w rozległej przestrzeni leksemu[44] gdzie nawet tej samej formie gramatycznej przypisuje się zbyt dowolnie różnicowane konotacje[45] pragmatyczne[46] występujące nawet w identycznych ujęciach syntaktycznych[47]. Na przykład tak proste stwierdzenie jak **zła informacja** może być odbierane w różnych kontekstach znaczeniowych. Można go interpretować, że:

---

[38] Rozdział pierwszy – rys. 2 i 3 oraz przypisany do nich tekst.
[39] T. Kotarbiński, „Traktat o dobrej robocie (wdanie siódme)", Ossolineum, Wrocław-▪ Warszawa-▪ Kraków-▪ Gdańsk- ▪ Łódź, 1982, s. 208.
[40] Ibidem.
[41] Ibidem, s. 179.
[42] Ibidem, s. 446-447.
[43] Ibidem, s. 207-208.
[44] Leksem – wyraz rozumiany jako abstrakcyjna jednostka systemu języka słownikowego; składa się na nią znaczenie leksykalne oraz zespół wszystkich funkcji gramatycznych, jakie dany leksem może spełniać, a także zespół form językowych reprezentujących w zdaniach leksem w jego poszczególnych funkcjach – np.: informować, informuję, informujący, informacyjny, informacja itp. należą do form tego samego leksemu (przypis autorski)..
[45] Konotacja – cechy współoznaczone łącznie przez daną nazwę; zespół cech, których posiadanie sprawia, że odpowiednie przedmioty należą do tej samej klasy – są desygnatami danej nazwy („Słownik języka polskiego", PWN, Warszawa 1978, tom I, s. 992).
[46] Pragmatyka – nauka zajmująca się zagadnieniami stosunku, jaki w procesie komunikowania się zachodzi między znakami słownymi a ich interpretatorami; wypowiadającymi słowa lub słuchającymi wypowiedzi („Słownik języka polskiego", PWN, Warszawa 1979, tom II, s. 907).
[47] Syntaktyka – teoria składni logicznej, dział semiotyki badający wzajemne stosunki znaczeniowe między poszczególnymi wyrażeniami języka, tj. jego znakami, w procesie porozumiewania się ludzi („Encyklopedia powszechna", PWN, Warszawa 1976, tom 4, s. 334).

(1) ktoś został powiadomiony o czymś złym dla niego;
(2) ktoś został powiadomiony nie o tym czego oczekiwał;
(3) ktoś został powiadomiony o czymś czego oczekiwał, ale powiadomienie to zawiera istotne dla niego luki;
(4) ktoś ocenił, że informacja, jako określona komórka organizacyjna, źle funkcjonuje;
(5) ktoś ocenił, że procedura informowania jest zła.

Z przytoczonego przykładu wynika, że to samo zestawienie wyrazowe **zła informacja** może mieć pięcioraką konotację, gdzie przedmioty myślowe (desygnaty) przypisywane do tak samo brzmiącego i uporządkowanego zestawienia wyrazowego zostały zinterpretowane diametralnie różnie pod względem znaczeniowym (semantycznym). Odnosząc się natomiast tylko do samego terminu **informacja** wynika też, że i przy takim wyizolowaniu, treść znaczeniowa tego wyrazu nie jest jednoznaczna. W pierwszych trzech przypadkach termin ten został zinterpretowany w rozumieniu **rzeczowym** – został potraktowany jako symbol semantyczny rzeczy nazwanej informacją). W czwartym przypadku termin ten został zinterpretowany w rozumieniu **organizacyjnym** – jako symbol semantyczny tworu organizacyjnego zajmującego się informowaniem. W piątym przypadku termin ten został zinterpretowany w rozumieniu **proceduralnym** – został potraktowany jako symbol semantyczny procedury informowania.

Podobne przykłady można mnożyć, co z pewnością znużyłoby Czytelnika. Taki sam efekt mogłoby spowodować dążenie do wypełniania przestrzeni tego leksemu możliwymi formami językowymi. Dlatego też wydaje się być celowe aby związaną z tym problematykę wyjaśniającą ograniczyć do kanonicznych postaci leksemu, czyli do lemm[48] występujących w częściach mowy odnoszących się tylko do:

- **czasownika** występującego w formie bezokolicznikowej (informować),
- **rzeczownika** występującego w mianowniku liczby pojedynczej (informacja),
- **przymiotnika** występującego w mianowniku liczby pojedynczej rodzaju męskiego w stopniu równym (informacyjny).

[48] Lemma – kanoniczna (podstawowa) forma leksemu; lemmy mają szczególnie ważne znaczenie w językach o złożonej procedurze odmiany. W języku polskim lemmami są: czasownik występujący w formie bezokolicznikowej, rzeczownik występujący w mianowniku liczby pojedynczej, przymiotnik występujący w mianowniku liczby pojedynczej rodzaju męskiego stopnia równego, przysłówek stopnia równego oraz liczebnik i zaimek.

Tadeusz Kotarbiński w swoim wywodzie na temat roli spełnianej przez informację w kooperacjach pozytywnych wyraził się, że języki etniczne kształtowały się bynajmniej nie według odgórnego planu, lecz w drodze kooperacji żywiołowej[49]. Można przypuszczać, że w podobny sposób powstało łacińskie słowo **informatio**[50] symbolizujące **wyobrażenie**, czyli wywołany w świadomości człowieka jakiś obraz przedmiotu lub sytuacji, który w danej chwili nie oddziałuje na jego narządy zmysłowe, a opiera się tylko na uprzednio poczynionych spostrzeżeniach i fantazji ludzkiej[51]. Na tej podstawie można przyjmować, że **informacja** jest tylko **semantyką** każdej nazwy, czyli treścią znaczeniową znaków językowych, które w różnych ujęciach syntaktycznych spełniają funkcję czynników sprawczych w stosunku do ludzkich wyobrażeń. Powodują asocjacje treści znaczeniowych z wcześniej poznanymi i zapamiętanymi stanami rzeczy, które przy ich użyciu były opisywane. Tadeusz Kotarbiński, jak już wcześniej akcentowano, procedurę tę nazywa **komitywą językową**[52] sprowadzającą się do komunikowania **treści myślowych** za pośrednictwem mowy mówionej lub pisanej, czyli narzędzia komunikacyjnego zwanego językiem etnicznym. Wynika z tego jednoznaczna sugestia, aby wyjaśnienia pojęciowego terminu **informacja** poszukiwać w sferze funkcji językowych.

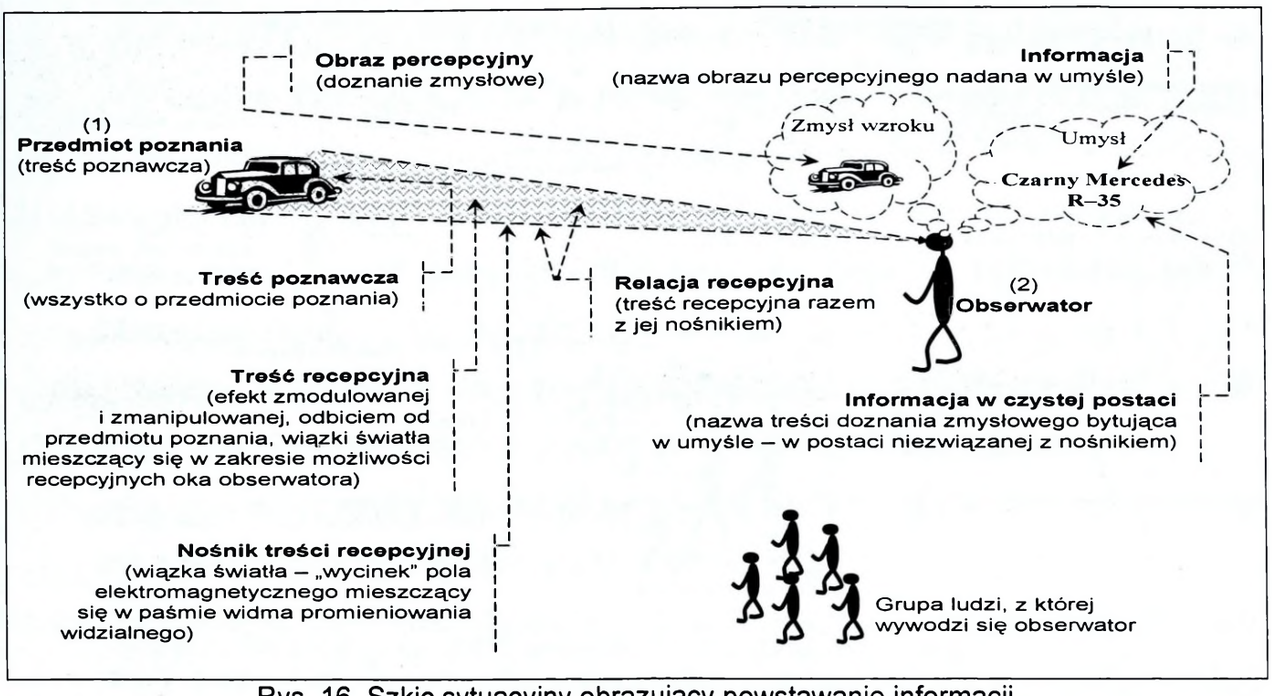
Czym zatem jest język?, Jak powstaje i jakie spełnia funkcje? Na te pytania odpowiadało i odpowiada wielu naukowców. Przeprowadzono i prowadzi się nadal wiele badań. Powstało wiele prac naukowych, promocyjnych i publikacji. Problematyce językoznawstwa są poświęcane specjalne studia. Niemniej jednak w wyjaśnianiu przedmiotowej sprawy zdają się być przydatne niektóre wskazania, jak chociażby amerykańskiego profesora językoznawstwa, kierownika Katedry Lingwistyki i Filozofii z Massachusetts Institute of Technology, Noamy Avrama Chomskyego, zawarte w jego książce „Syntactic Structures" (Struktury syntaktyczne)[53]. Wymieniony autor wyraził się, że *język jest nieskończonym zbiorem zdań, generowanych za pomocą skończonej liczby reguł i słów*[54]. Z tego okresu pochodzi też jego słynne zdanie: *Colorless green ideas sleep furiously* (bezbarwne zielone idee wściekle śpią), które jest

---

[49] T. Kotarbiński, „Traktat o dobrej robocie (wdanie siódme)", Ossolineum, Wrocław▪ Warszawa▪ Kraków▪ Gdańsk▪ ▪ Łódź, 1982, s. 209.
[50] W. Kopaliński, „Słownik wyrazów obcych i zwrotów obcych", WP, Warszawa 1975, s. 429.
[51] „Słownik języka polskiego", PWN, Warszawa 1981, tom III, s. 826.
[52] T. Kotarbiński, „Traktat o dobrej robocie (wydanie siódme)", Ossolineum, Wrocław▪ Warszawa▪ Kraków▪ Gdańsk▪ ▪ Łódź, 1982, s. 207-208.
[53] N.A. Chomsky, „Syntactic Structures", The Hague/Paris, Mouton 1957.
[54] Ibidem, s. 15.

poprawne gramatycznie, ale bezsensowne. W ten sposób autor chciał wykazać, że składnia nie tworzy podstawowej struktury języka. Wskazał, że zasadniczą strukturę tworzą **słowa** (wyrazy), które jako nazwy o określonych desygnatach, mają konkretne znaczenia i mogą być używane w różnych kontekstach pragmatycznych, a w tym i zupełnie bezsensownych. Tym samym uzasadnia to stwierdzenie, że język jest nieskończonym zbiorem zdań.

Rozpocznijmy zatem nasz wywód od procedury powstawania nazw. Wyobraźmy sobie następującą sytuację (rys. 16):



Rys. 16. Szkic sytuacyjny obrazujący powstawanie informacji

Źródło: Opracowanie autorskie

(1) Jakaś grupa ludzi nigdy nie widziała żadnego samochodu i nigdy nie słyszała, że takie w ogóle istnieją.

(2) Pewnego razu jeden z członków tej grupy wyszedł i zobaczył samochód, nie wiedząc absolutnie co to jest.

(3) Zaciekawiony tym obiektem dokładnie go obejrzał, sporządził jego dokładny szkic, zapoznał się z jego przeznaczeniem i spełnianymi funkcjami.

(4) Odchodząc z miejsca zdarzenia postanowił nazwać ten obiekt „czarny Mercedes R-35".

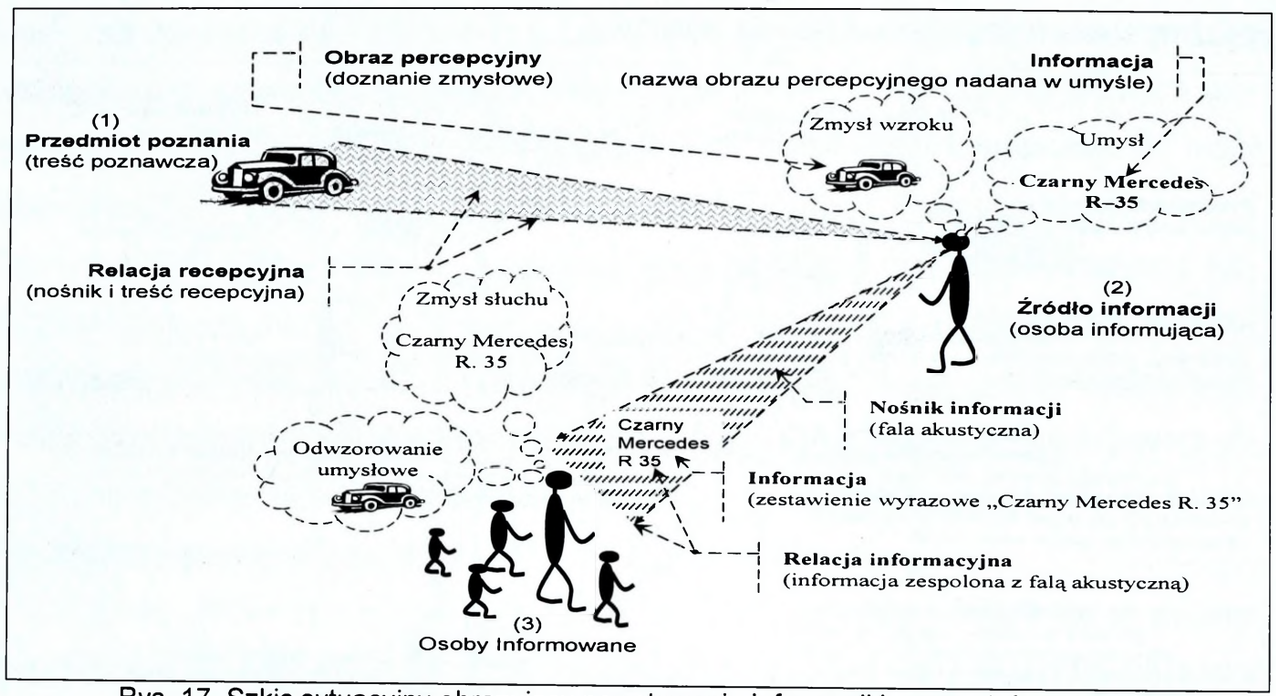
(5) Po powrocie do grupy dokładnie opowiedział, za pomocą znanych grupie słów (terminów) i reguł stosowanego przez nich języka, co go spotkało (rys. 25):

- brakujące do opisu terminy uzupełnił prezentacją sporządzonego szkicu obiektu,

– objaśnił im zasady funkcjonowania i przeznaczenie obiektu.

(6) Na koniec oznajmił, że zaobserwowany i zidentyfikowany obiekt nazwał „czarny Mercedes R-35", czyli poinformował członków grupy jaki przedmiot myślowy (jaka treść informacyjna) kryje się pod tą nazwą – pod tym zestawieniem wyrazowym.

W aspekcie sprawczości, wyjaśniającej związki przyczynowo-skutkowe poprzez pryzmat warunku wystarczającego i czynników istotnych tego warunku, opisane wyżej zdarzenia (rys. 16 i 17) można interpretować:



Rys. 17. Szkic sytuacyjny obrazujący powstawanie informacji i proces informowania

Źródło: Opracowanie autorskie

(1) obserwator nadał nazwę zaobserwowanemu obiektowi, bo (dot. rys. 16):

– jako homo sapiens posiada umysł[55], który jest dostosowany do nadawania określonych nazw, w mowie wewnętrznej, różnym doznaniom zmysłowym (wzrokowym, słuchowym, smakowym, węchowym, dotykowym);

ale i dla tego, że zaistniały przy tym czynniki istotne i wystarczające do spełnienia tego warunku, które objawiły się wcześniej przez pryzmat następujących zdarzeń fizycznych:

– w zasięgu horyzontu optycznego[56] obserwatora pojawił się obiekt fizyczny jako **przedmiot poznania** o określonej **treści poznawczej**,

[55] Termin „umysł" został użyty w znaczeniu, że jest to zespół myślowy funkcji poznawczych mózgu (przypis autorski).

[56] Wzór empiryczny wyznaczający horyzont optyczny:

$$H_{optyczny} = 3{,}57\left(\sqrt[2]{h_{obiektu}} + \sqrt[2]{h_{obserwatora}}\right),$$

gdzie:

- wiązka światła odbita od **przedmiotu poznania** została odpowiednio zmodulowana i zmanipulowana[57] jego kształtami i kolorami, co w postaci konkretnej **treści recepcyjnej** zostało odzwierciedlone na siatkówce oka obserwatora, tworząc na niej subiektywny obraz obiektu[58],
- obiekt odzwierciedlony na siatkówce oka obserwatora zostało **percypowany** do podkorowego zmysłu wzroku i w ten sposób spowodował jego **widzenie**, czyli tak zwany **obraz percepcyjny**[59],
- fizyczne **widzenie** obiektu (obraz percepcyjny) spowodowało **asocjację**, która doprowadziła do nadania temu **widzeniu** (temu obrazowi percepcyjnemu) nazwy **czarny Mercedes R 35**, w mowie wewnętrznej obserwatora (w umyśle obserwatora);

(2) obserwator stał się **źródłem informacji** bo (dot. rys. 17):

- poinformował innych jaki **przedmiot myślowy** kryje się pod nazwą **czarny Mercedes R-35**;

ale i dlatego, że zaistniały przy tym czynniki istotne i wystarczające do spełnienia tego warunku, które objawiły się przez pryzmat następujących zdarzeń:

- jako pierwszy z grupy zidentyfikował **przedmiot poznania** i **treściom poznania** nadał nazwę **czarny Mercedes R-35**,
- znalazł się w bezpośredniej bliskości innych, i w ten sposób za pocą stosowanego przez nich języka etnicznego oraz sporządzonych wcześniej szkiców i wykonanych zdjęć poznanego przedmiotu stworzył, pomiędzy sobą i grupą, głosowe i wzrokowe **relacje percepcyjne**, które spowodowały, że wytworzone tą drogą **obrazy percepcyjne**, jako denotacje wyobrażeniowe zostały przypisane do terminu **czarny mercedes R-35**.

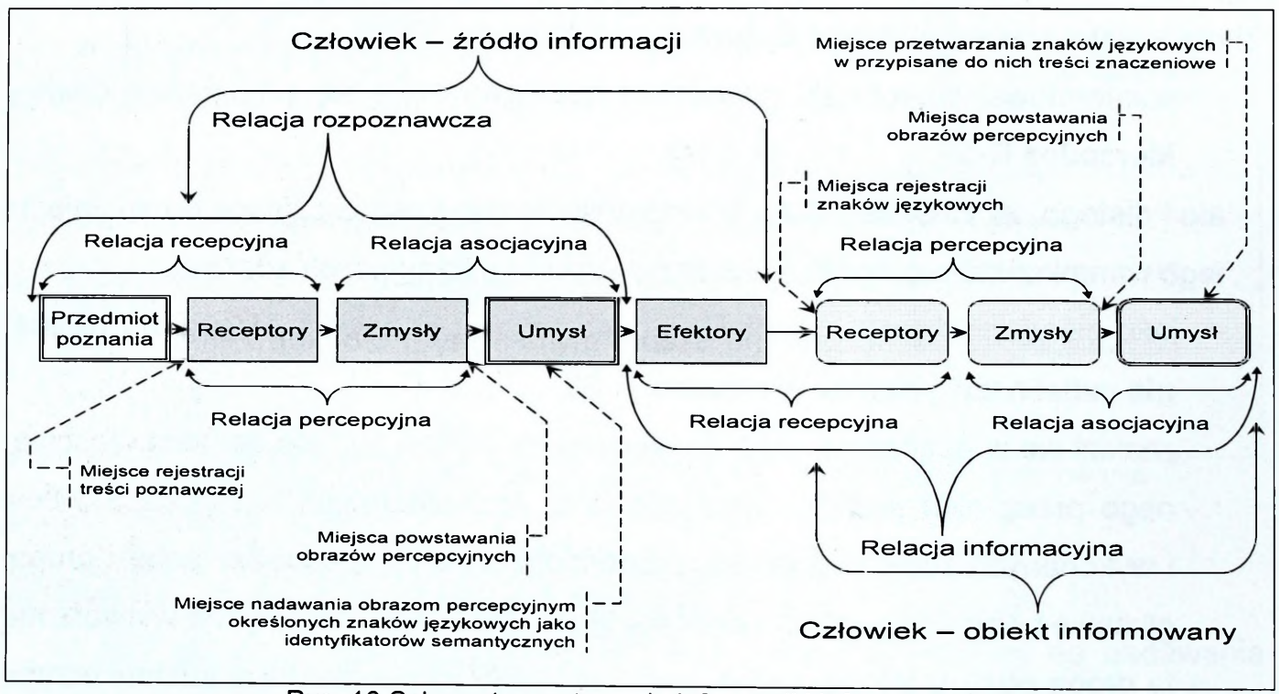
$H_{optyczny}$ – horyzont optyczny [km],
$h_{obiektu}$ – wysokość obiektu obserwowanego [m],
$h_{obserwatora}$ – wysokość obserwatora [m],
3,57 – współczynnik empiryczny.

[57] W tym wypadku wiązka światła jest postrzegana tylko w aspekcie teorii falowej – jako wycinek pola elektromagnetycznego charakteryzujący się określonym gradientem.

[58] **Treść recepcyjna** i **treść poznawcza** nie są tym samym. **Treść poznawcza** jest wartością obiektywnie istniejącą i najczęściej w całej rozciągłości nie jest dostępna dla ludzkich zmysłów. Treść ta jest immanentnie zespolona z konkretnym **przedmiotem poznania** – dotyczy wszystkiego co jest z tym przedmiotem związane. **Treść recepcyjna** jest natomiast wartością subiektywną – jest zawsze determinowana fizjologicznymi możliwościami receptorów konkretnego człowieka. Na przykład **treść recepcyjna** krótkowidza będzie diametralnie różna od treści recepcyjnej normalnie widzącego człowieka. Podobnie rzecz się ma do pozostałych receptorów.

[59] Obraz percepcyjny – to, jak wygląda otoczenie w następstwie użycia zmysłów (A. Morton, „Przewodnik po teorii poznania", Spacja, Warszawa 2002, s. 304).

Nawiązując do powyższego można przypuszczać, że na podobnej zasadzie kształtowały się wszystkie języki etniczne. Świadczyć mogą o tym chociażby odnalezione rysunki, rzeźby i malowidła jaskiniowe obrazujące różne stany sytuacyjne oraz zdarzenia, rzeczy i sceny, do których reprezentacji były prawdopodobnie przypisywane określone brzmienia głosowe (fonemy[60] i morfemy[61]) oraz gesty i zachowania symbolizujące ich treści znaczeniowe (semantykę), co z pewnością usprawniało zbiorowe porozumiewanie się i tym samym lepsze egzystowanie w hordach. Nie ulega zatem wątpliwości, że te odkrycia ikoniczne[62], są najstarszymi dowodami na kształtowania się **znaków językowych**[63] i tym samym wykorzystywanie informacji, o czym już wcześniej wspominano. Procedurę tę, w znacznym uproszczeniu, można wyrazić następującym zobrazowaniem schematycznym (rys. 18).



Rys. 18.Schemat powstawania informacji i informowania

Źródło: Opracowanie autorskie

---

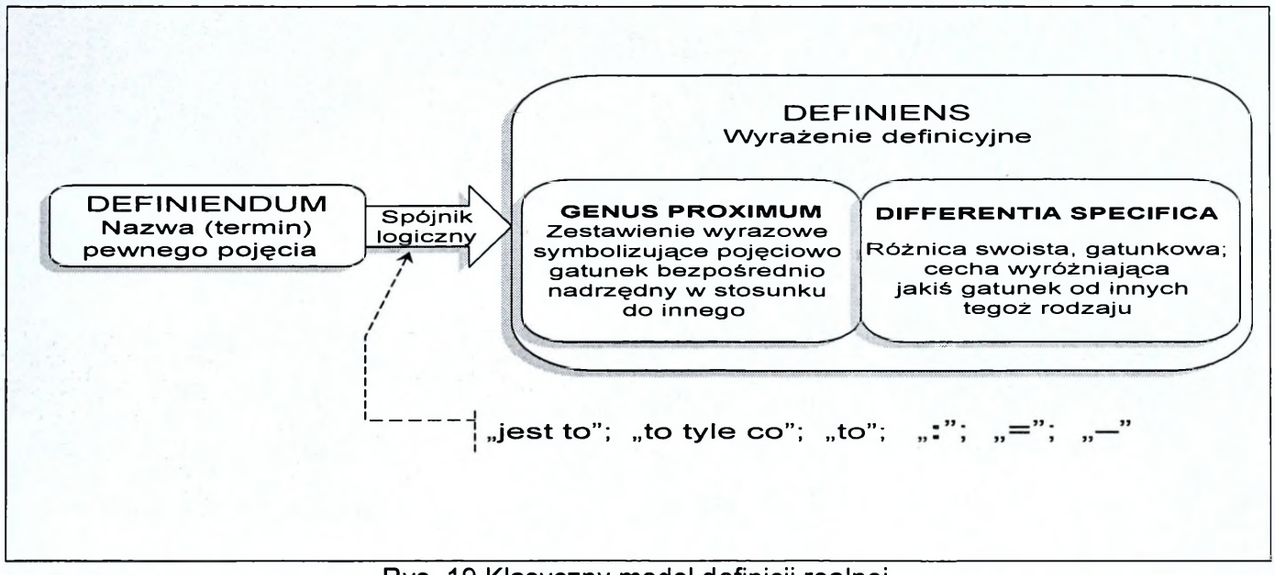
[60] Fonem – dźwięk, element systemu dźwiękowego języka pełniący funkcję dystynktywną, tj. funkcję różnicowania znaczeń wyrazów i form wyrazowych („Słownik języka polskiego", PWN, Warszawa 1978, tom I s. 601). Najmniejsza jednostka mowy rozróżnialna dla użytkowników danego języka; nie ma własnego znaczenia; służy do odróżniania elementów znaczeniowych morfemów (przypis autorski).

[61] Morfem – najmniejsza, znaczeniowo niepodzielna cząstka wyrazu. Morfem główny – rdzeń wyrazu. Morfem poboczny – przyrostek lub przedrostek („Słownik języka polskiego", PWN, Warszawa 1979, t. II s. 213) Najmniejsza grupa fonemów, która niesie ze sobą określone znaczenie i której nie można podzielić na mniejsze jednostki znaczeniowe (przypis autorski).

[62] Znaki ikoniczne (naturalne) – takie, które przypominają swoja postacią, to co oznaczają (piktogramy); nie muszą być wyłącznie obrazami – mogą przybierać formy dostosowane do wrażliwości percepcyjnej wszystkich zmysłów (przypis autorski).

[63] Znak językowy – wszystko co w języku posiada swoje znaczenie (semantykę); najmniejszym znakiem językowym jest morfem [najmniejsza grupa fonemów (najmniejsza jednostka mowy rozróżniana przez użytkowników danego języka), która posiada określone znaczenie i której nie można podzielić na mniejsze jednostki znaczeniowe], a największym – cały tekst; znaki językowe dzielą się na: wzrokowe, słuchowe, dotykowe, węchowe i smakowe (przypis autorski).

Stosując klasyczne zasady definiowania[64], elementy wyszczególnione na rysunku 26 należy interpretować (rys. 19)[65]:



Rys. 19 Klasyczny model definicji realnej

Źródło: Opracowanie autorskie na podstawie: K. Ajdukiewicz, „Zarys logiki", PZWS, Warszawa 1959, s. 44.

Relacja[66] **rozpoznawcza** – związek refleksyjny[67] występujący pomiędzy człowiekiem i dostrzeganym przez niego przedmiotem poznania.

gdzie:

- „relacja rozpoznawcza" – *definiendum,*
- „związek refleksyjny występujący pomiędzy człowiekiem i dostrzeganym przez niego przedmiotem" – *definiens,*
- „związek refleksyjny" – *genus proximum,*
- „występujący pomiędzy człowiekiem i dostrzeganym przez niego przedmiotem poznania" – *differentia specifica.*

Relacja informacyjna – związek asocjacyjny występujący pomiędzy znakiem językowym i jego semantycznym interpretatorem.

gdzie:

[64] Klasyczna definicja realna podaje dla definiowanego gatunku najbliższy jego rodzaj i różnicę gatunkową (Definitio fit per genus proximum et differentia specificam) [K. Ajdukiewicz, „Zarys logiki", PZWS, Warszawa 1959, s. 44].

[65] Istota definiowania sprowadza się do tego aby sformułować wyjaśnienie w takim zestawieniu wyrazowym (genus proximum i differentia specifica), które sprowadza się do wskazania innego wyrażenia przynależącego do danego języka i posiadającego w danym języku to samo znaczenie co wyrażenie, którego znaczenia poszukujemy [nie identycznie, ale w podobny sposób wyjaśnia istotę definiowania Tadeusz Kwiatkowski (T. Kwiatkowski, „Wykłady i szkice z logiki ogólnej", UMCS, Lublin 2002) – przypis autorski.

[66] Relacja (w rozumieniu logicznym) – wszelki związek czy zależność (stosunek) między dwoma (lub więcej) przedmiotami danego rodzaju, pojęciami, wielkościami itp. („Słownik języka polskiego", PWN, Warszawa 1981, tom III, s. 41).

[67] Refleksja (w rozumieniu filozoficznym) – poznanie skierowane na podmiot poznający („Słownik języka polskiego", PWN, Warszawa 1981, tom III, s. 32).

- „relacja informacyjna" – *definiendum,*
- „związek asocjacyjny występujący pomiędzy znakiem językowym i jego semantycznym interpretatorem" – *definiens,*
- „związek asocjacyjny" – *genus proximum,*
- „występujący pomiędzy znakiem językowym i jego semantycznym interpretatorem" – *differentia specifica.*

Relacja recepcyjna – związek fizyczny występujący pomiędzy receptorem i przedmiotem poznania.

gdzie:

- „relacja recepcyjna" – *definiendum,*
- „związek fizyczny występujący pomiędzy receptorem i przedmiotem poznania" – *definiens,*
- „związek fizyczny" – *genus proximum,*
- „występujący pomiędzy receptorem i przedmiotem poznania" – *differentia specifica.*

Relacja percepcyjna – proces mózgowy transformujący doznania recepcyjne w obrazy percepcyjne.

gdzie:

- „relacja percepcyjna" – *definiendum,*
- „proces mózgowy transformujący doznania recepcyjne w obrazy percepcyjne" – *definiens,*
- „proces mózgowy" – *genus proximum,*
- „transformujący doznania recepcyjne w obrazy percepcyjne" – *differentia specifica.*

Relacja asocjacyjna – związek pojęciowy występujący pomiędzy obrazem percepcyjnym i znakiem językowym symbolizującym ten obraz.

gdzie:

- „relacja asocjacyjna" – *definiendum,*
- „związek pojęciowy występujący pomiędzy obrazem percepcyjnym i znakiem językowym symbolizującym ten obraz" – *definiens,*
- „związek pojęciowy" – *genus proximum,*
- „występujący pomiędzy obrazem percepcyjnym i znakiem językowym symbolizującym ten obraz" – *differentia specifica.*

W aspekcie powyższego można się zgodzić z Marianem Mazurem, że *informacja to transformacja jednego komunikatu asocjacji informacyjnej w drugi komuni-*

kat tej asocjacji[68], ale pod warunkiem, że przez znak językowy, reprezentowany terminem **informacja**, będziemy rozumieli tylko **proces informowania**, czyli semantykę wynikającą z lemmy **informować**.

Informować – przekazywać treści znaczeniowe, za pomocą etnicznych[69] znaków językowych;

gdzie:

- „informować" – *definiendum,*
- „przekazywać treści znaczeniowe, za pomocą etnicznych znaków językowych" – *definiens,*
- „przekazywać treści znaczeniowe" – *genus proximum,*
- „za pomocą etnicznych znaków językowych" – *differentia specifica.*

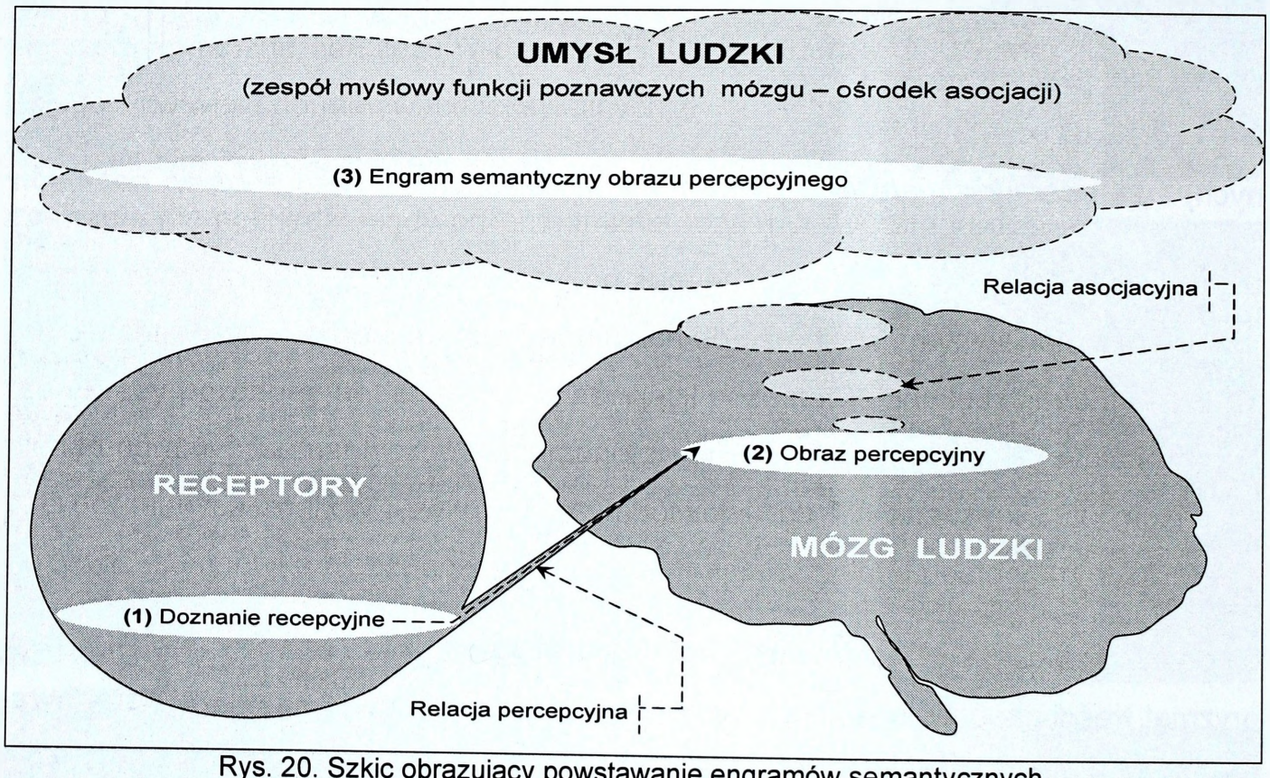
Oznacza to, że **informowanie** może się odbywać tylko w ramach komitywy językowej utrzymywanej w relacjach międzyludzkich. Jak akcentuje Tadeusz Kotarbiński, *tylko człowiek* jest dostosowany do ***komunikowania*** *treści myślowych* (asocjacyjnych)[70] *za pośrednictwem mowy mówionej lub pisanej, on tylko spośród gatunków stworów żywych na Ziemi*[71]. Podobnie procedurę tę postrzega Henryk Greniewski twierdząc, że *informację przekazuje tylko człowiek człowiekowi*[72], chociaż dodaje później, że *w cybernetyce używa się wyrazu informacja w rozumieniu dużo szerszym*[73]. Ludwig von Bertalanffy twierdzi natomiast, że *człowiek tworzy swój świat, nazywany kulturą*[74]. Dalej dodaje, że *wśród hipotez na temat jego ewolucji wyróżniamy dwa blisko ze sobą powiązane czynniki – język i kształtowanie pojęć*[75]. Konfrontując ten zapis z poprzednimi wynika, że i tu jest wyrażone podobne przekonanie co do roli funkcjonalnej spełnianej przez informację. Przejawia się to wyraźnie przez pryzmat treści znaczeniowej przypisanej do znaków językowych **język** i **kształtowanie pojęć**, co jest conditio sine qua non[76] zaistnienia **komunikowania** w ogóle. Zbli-

---

[68] M. Mazur, „Jakościowa teoria informacji", WNT, Warszawa 1970, s. 70 (patrz również tabela nr 1, poz. 14).
[69] Etniczny – związany z przynależnością do jakiegoś narodu („Słownik języka polskiego", PWN, Warszawa 1978, tom I, s. 558).
[70] Wyjaśnienie autorskie.
[71] T. Kotarbiński, „Traktat o dobrej robocie (wydanie siódme)", Ossolineum, Wrocław·▪ Warszawa·▪ Kraków·▪ Gdańsk· ▪ Łódź, 1982, s. 207-208.
[72] H. Greniewski, „Sprawy wszystkie i jeszcze inne (o logice i cybernetyce)", KiW, Warszawa 1970, s. 24-25 (patrz również tabela nr 1, poz. 13).
[73] Ibidem.
[74] L. von Bertalanffy, „Ogólna teoria systemów (podstawy, rozwój, zastosowania)", PWN, Warszawa 1984,
s. 299 (patrz również tabela 1, poz. 16).
[75] Ibidem.
[76] Conditio sine qua non – warunek niezbędny, nieodzowny.

żone do tego akcenty interpretacyjne, chociaż nie tak jednoznacznie wyrażone jak poprzednie, można odnaleźć w pracach H.J. Flechtnera[77], N. Wienera[78], R. Ketlińskiego[79] i w wielu normatywach leksykalnych[80].

W tym miejscu wydaje się być zasadne jeszcze raz zaakcentowanie, że **informacja** nie pochodzi nigdy od przedmiotu poznania. Od przedmiotu poznania pochodzą tylko **treści poznawcze** które, po zarejestrowaniu przez odpowiednie receptory i przetransformowaniu (percypowaniu) ich do ośrodków zmysłowych mózgu, tworzą **obrazy percepcyjne**, które drogą asocjacji pozostawiają w ludzkim umyśle określone engramy[81] semantyczne skojarzone z tymi obrazami, ale nie przypisane jeszcze do żadnych znaków językowych symbolizujących ich znaczenie, co można by nazywać „semantyką nieoznaczoną" lub „informacją w czystej postaci" (rys. 20).



Rys. 20. Szkic obrazujący powstawanie engramów semantycznych (semantyki nieoznaczonej)

Źródło: Opracowanie autorskie

[77] H.J. Flechtner, „Grundbegriffe der Kybernetik", Wissenschaftliche Verlagsgesellschaft, Stuttgart 1966 (patrz również tabela 1, poz. 11).
[78] N. Wiener, Cybernetyka i społeczeństwo", KiW, Warszawa 1960 (patrz również tabela 1, poz. 8).
[79] R. Kietliński, Aspekty problemu podejmowania decyzji" (art. w „Zeszycie Naukowym Uniwersytetu Łódzkiego nr 61, s. 55)", UŁ, Łódź 1969 (patrz również tabela 1, poz. 17).
[80] Patrz tabela 1, poz.: 2, 3, 5, 7.
[81] Engram – ślad pamięciowy, zmiana pozostawiona w układzie nerwowym przez określone przeżycie, działanie określonych bodźców, stanowiące podstawę późniejszego odtwarzania; w przypadku pamięci długotrwałej zmiana w biochemicznej strukturze neuronów („Nowy leksykon PWN", Wydawnictwo Naukowe PWN, Warszawa 1998, s. 444).

Engram semantyczny – ślad pamięciowy treści wyobrażeniowej spowodowany zewnętrznym lub wewnętrznym doznaniem człowieka;

gdzie:

- „engram semantyczny" – *definiendum,*
- „ślad pamięciowy treści wyobrażeniowej spowodowanej zewnętrznymi i wewnętrznymi doznaniami człowieka" – *definiens,*
- „ślad pamięciowy treści wyobrażeniowej" – *genus proximum,*
- „spowodowanej zewnętrznymi i wewnętrznymi doznaniami człowieka" – *differentia specifica.*

Semantyka nieoznaczona – engram semantyczny bez przypisanego mu znaku językowego (tylko osobnicze wyobrażenie) – synonim informacji potencjalnej;

gdzie:

- „semantyka nieoznaczona" – *definiendum,*
- „engram semantyczny bez przypisanego mu znaku językowego" – *definiens,*
- „engram semantyczny" – *genus proximum,*
- „bez przypisania mu znaku językowego (tylko osobnicze wyobrażenie)" – *differentia specifica.*

Czysta postać informacji – semantyka nieoznaczona bytująca w ludzkim umyśle bez przypisanego jej identyfikującego znaku językowego – synonim informacji potencjalnej.

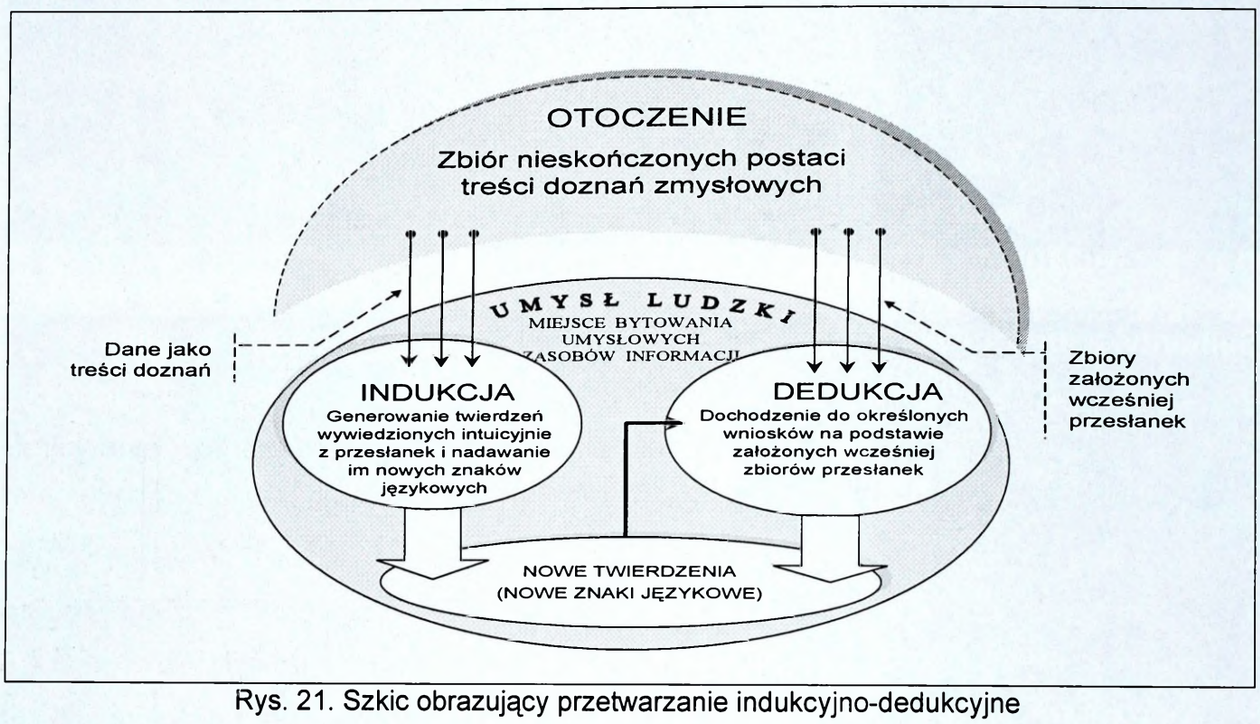
gdzie:

- „czysta postać informacji" – *definiendum,*
- „semantyka nieoznaczona bytująca w ludzkim umyśle bez przypisanego jej identyfikującego znaku językowego" – *definiens,*
- „semantyka nieoznaczona bytująca w ludzkim umyśle" – *genus proximum,*
- „bez przypisanego jej identyfikującego znaku językowego" – *differentia specifica.*

Semantyka nieoznaczona, jako ślad pamięciowy treści wyobrażeniowej[82] bytujący w ludzkim w umyśle, w oderwaniu od jakiegokolwiek symbolizującego ją znaku językowego, nie może spełniać **warunku informowania** wynikającego z definicji tego procesu i istoty komitywy językowej. Stanowi natomiast niezbędnie konieczną podstawę do przetwarzania indukcyjno-dedukcyjnego, w następstwie czego zostaje jakoby „opatrywana" stosownymi znakami językowymi, umożliwiającymi for-

[82] Wyobrażenie – wywołany w świadomości obraz przedmiotu lub sytuacji, które w danej chwili nie oddziałuje na narządy zmysłowe człowieka, opierający się na uprzednio poczynionych spostrzeżeniach i fantazji („Słownik języka polskiego", PWN, Warszawa 1981, tom III, s. 826).

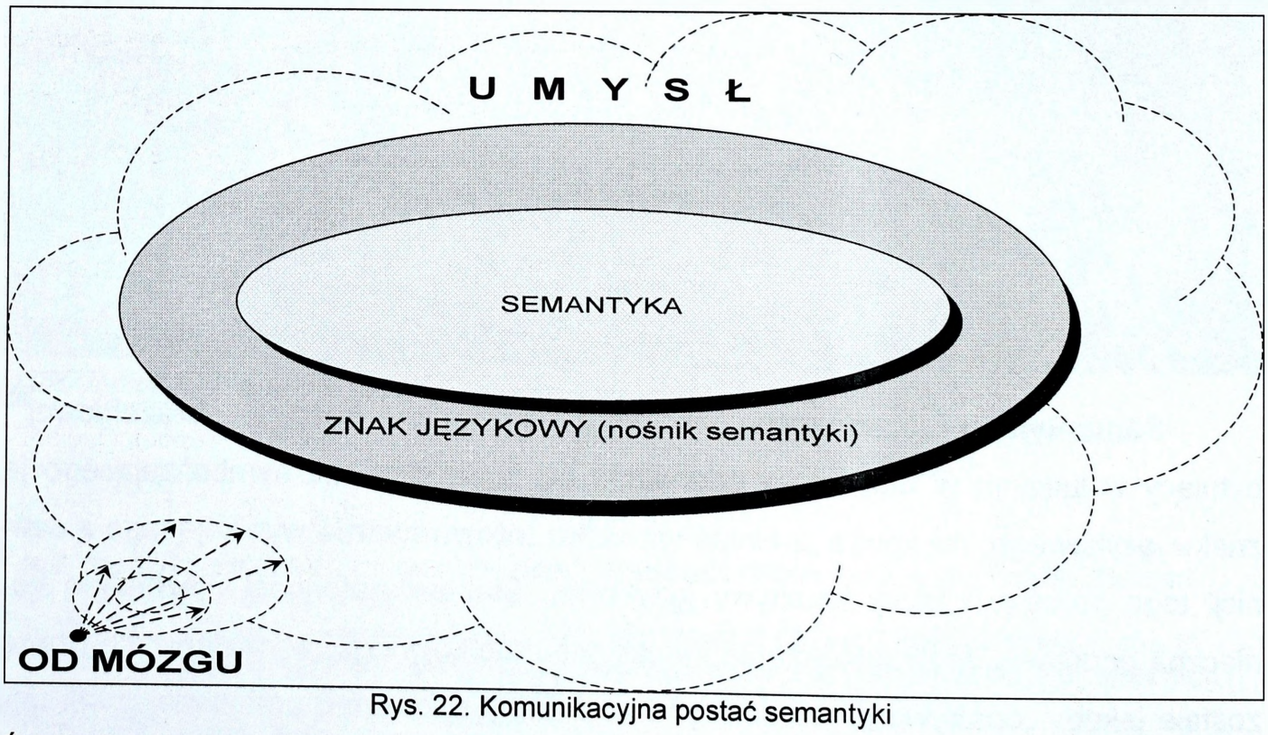
mułowanie twierdzeń, nazw i wyjaśnień z nią związanych, w postaci możliwej do zewnętrznego generowania – czyli do przekazywania jej treści znaczeniowych innym (rys 21).



Rys. 21. Szkic obrazujący przetwarzanie indukcyjno-dedukcyjne

Źródło: Opracowanie autorskie

Powoduje to, że w następstwie takiego postępowania „semantyka nieoznaczona" staje się „semantyką oznaczoną" i przyjmuje postać komunikacyjną (rys. 22).



Rys. 22. Komunikacyjna postać semantyki

Źródło: Opracowanie autorskie

Semantyka oznaczona – engram semantyczny z przypisanym znakiem językowym identyfikującym jego postać – synonim komunikacyjnej postaci semantyki;

gdzie:

- „semantyka oznaczona" – *definiendum,*
- „engram semantyczny z przypisanym znakiem językowym identyfikującym jego postać" – *definiens,*
- „engram semantyczny" – *genus proximum,*
- „z przypisanym znakiem językowym identyfikującym jego postać" – *differentia specifica.*

Komunikacyjna postać semantyki – engram semantyczny z przypisanym znakiem językowym identyfikującym jego postać – synonim semantyki oznaczonej;

gdzie:

- „komunikacyjna postać informacji" – *definiendum,*
- „engram semantyczny z przypisanym znakiem językowym identyfikującym jego postać" – *definiens,*
- „engram semantyczny" – *genus proximum,*
- „z przypisanym znakiem językowym identyfikującym jego postać" – *differentia specifica.*

Każda komunikacja, jako ruch polegający na utrzymywaniu łączności między odległymi od siebie miejscami[83], odbywa się zawsze w określonych relacjach charakteryzujących się też określonymi związkami i zależnościami komunikacyjnymi[84]. Podobnie rzecz się ma i z komunikacją semantyki. Opatrzona określoną nazwą (określonym znakiem językowym) staje się przygotowana do komunikowania, ale nadal może tylko bytować w ludzkim umyśle. Wygenerowana na zewnątrz, pod postacią określonego znaku językowego (nazwy, terminu), wiąże się zawsze z konkretnymi nośnikami materialnymi:

- środowiskiem sprężystym – podczas wyrażania znaków językowych słowami,
- kartką papieru – podczas wyrażania znaków językowych wyrazami,
- polem magnetycznym – podczas zapisywania znaków językowych na taśmie magnetofonowej lub płycie CD,
- itp.

---

[83] „Słownik języka polskiego", PWN, Warszawa 1978, tom I, s. 981.
[84] „Słownik języka polskiego", PWN, Warszawa 1981, tom III, s. 41 (parafraza autorska).

W ten sposób przyjmuje określone postaci relacyjne, które w uogólnieniu można wyrazić następującym zobrazowaniem (rys. 23).



Rys. 23. Relacyjna postać semantyki

Źródło: Opracowanie autorskie

Relacyjna postać semantyki – engram semantyczny zespolony ze znakiem językowym i nośnikiem materialnym znaku językowego;

gdzie:

- „relacyjna postać semantyki" – *definiendum,*
- „engram semantyczny zespolony ze znakiem językowym i z nośnikiem materialnym" – *definiens,*
- „engram semantyczny" – *genus proximum,*
- „zespolony ze znakiem językowym i z nośnikiem materialnym" – *differentia specifica.*

W procesie informowania każde zespalanie **znaku językowego**, reprezentującego określoną **semantykę**, z jego **fizycznym nośnikiem** sprowadza się zawsze do celowej „deformacji" **pierwotnej struktury tego nośnika** kodem danego znaku językowego, dostosowanym do określonych potrzeb sytuacyjnych. W komunikacji międzyludzkiej może to być naruszenie struktury środowiska sprężystego (w przypadku znaków językowych wyrażanych mową) lub struktury kartki papieru (w przypadku znaków językowych wyrażanych pisemnie) itp. Po dotarciu, w takim zespoleniu (w takiej postaci), do punktu docelowego (zawsze człowieka), a w rzeczy samej do określonego receptora ludzkiego i jego ośrodka zmysłowego, zostaje jak gdyby „oderwana" od fizycznego nośnika nazwy i jako przetworzona asocjacyjnie nazwa przechodzi ponownie do bytowania w ludzkim umyśle, pod postacią treści znaczeniowej (semantyki), ale już innego człowieka i trwa tam tak długo, jak pozwala na to

jego pamięć, powodując w tym czasie, wraz z innymi, nowe skojarzenia myślowe wynikające z przyrodzonego prawa asocjacji. Na tej zasadzie odbywa się, między innymi, uczenie i intelektualny rozwój człowieka.

W nawiązaniu do powyższego można już wysunąć tezę, że termin **informacja**, jako definiendum występujące w kanonicznej postaci rzeczownikowej[85], może być wyjaśnione poprzez definiens składający się z pięciu zwięzłych odpowiedzi na następujące pytania (tab. 2).

Pojęciowa interpretacja terminu „informacja" Tabela 2

Lp.	Pytania	Odpowiedzi
1.	Co to jest informacja?	Nazwa
2.	Czego nazwa?	Treści
3.	Jakich treści?	Doznań
4.	Jakich doznań?	Zmysłowych i umysłowych
5.	Czyich doznań	Człowieka

Źródło: Opracowanie autorskie.

Odczytując powyższe odpowiedzi, w kolejności zadawanych pytań, uzyskuje się definicję w następującym brzmieniu:

Informacja – nazwa treści doznań zmysłowych i umysłowych człowieka;
gdzie:
- „informacja" – *definiendum,*
- „nazwa treści doznań zmysłowych i umysłowych człowieka" – *definiens,*
- „nazwa treści" – *genus proximum,*
- „doznań zmysłowych i umysłowych człowieka" – *differentia specifica.*

Jak z pewnością dostrzegł to Czytelnik, definicja ta jest dwuczłonowym twierdzeniem predykcyjnym[86] łączącym w sobie dwa predykcyjne twierdzenia proste[87] wyrażone w postaci:

$F_1(x)$ – *informacja jest nazwą treści doznań zmysłowych człowieka,*

$F_2(x)$ – *informacja jest nazwą treści doznań umysłowych człowieka,*

co można zapisać:

$$F_1(x) \; i \; F_2(x)$$

gdzie:

x – *nazwa indywidualna określona mianem „informacja",*

[85] Kanoniczna postać rzeczownikowa – rzeczownik w pierwszym przypadku liczby pojedynczej.
[86] Predykacja to orzekanie.
[87] Predykcyjne twierdzenie proste to takie, które zawiera podmiot i predykat jednoargumentowy.

F_1 – predykat (orzecznik), że „informacja jest nazwą treści doznań zmysłowych człowieka”,

F_2 – predykat (orzecznik), że „informacja jest nazwą treści doznań umysłowych człowieka”,

Z powyższej treści definicyjnej, a konkretnie z fragmentu predykującego, że „informacja” jest tylko nazwą, wynika:

(1) Informacja, jako sama nazwa, nie może posiadać energii.

(2) Informacja, jako sama nazwa, nie może posiadać masy.

(3) Informacja, jako sama nazwa, może tylko posiadać wartość semantyczną w relacjach komunikacyjnych człowiek – człowiek.

(4) Informacja, jako nazwa „w czystej postaci” (w postaci niezwiązanej z nośnikiem), może powstawać i bytować tylko w ludzkim umyśle.

(5) Informacja, jako nazwa wygenerowana na zewnątrz, wiąże się zawsze z określonym nośnikiem materialnym (ze środowiskiem sprężystym – w przypadku mowy; z kartką papieru – w przypadku pisma itp.).

(6) Jeśli informacja, „w czystej postaci”, powstaje i bytuje tylko w ludzkim umyśle, to wynika z tego, że pierwotnym źródłem informacji może być tylko i wyłącznie człowiek, który w określonym czasie nadał danym treściom stosowne według siebie nazwy.

(7) Jeśli informacja, „w czystej postaci” powstaje tylko w umyśle ludzkim, jako stosowna według twórcy nazwa, to jako taka jest zawsze subiektywna – zawsze zależy od wcześniejszej wiedzy danego człowieka oraz jego predyspozycji intelektualnych, psychofizycznych i intencyjnych.

(8) Źródłem treści doznań zmysłowych i umysłowych człowieka jest zawsze jego zewnętrzne i wewnętrzne otoczenie, generujące nieskończoną ilość różnych postaci treści.

(9) Z faktu, że we wszystkich zewnętrznych relacjach komunikacyjnych „informacja” występuje zawsze w zespoleniu z określonym nośnikiem materialnym [patrz punkt (5)], wynika następstwo, iż w takiej postaci spełnia, w stosunku do człowieka, podwójną funkcję: a) sterującą – poprzez nośnik oddziałujący na układ zmysłów, b) semantyczną – poprzez nazwę oddziałującą na skojarzenia zachodzące w jego umyśle (w zespole myślowym funkcji poznawczych mózgu).
W stosunku do obiektów nie będących ludźmi, czynnikiem oddziałującym jest

tylko i wyłącznie postać nośnika, zdeformowana określonym kodem naruszającym strukturę naturalną tego nośnika – jego postać pierwotną.

Dostrzegać też trzeba, że „informacja", jako nazwa, symbolizuje pojęcia odnoszące się do dwóch rodzajów treści:

(1) materialnych – doznawanych, bezpośrednio[88] i pośrednio[89], poprzez układ zmysłowy człowieka, które można nazywać „treściami doznań zmysłowych",

(2) niematerialne – stanowiące wytwory ludzkiego myślenia, które można nazywać „treściami doznań umysłowych".

Przy takiej kategoryzacji, przez zestawienie wyrazowe „treść informacyjna", należy rozumieć wszelką semantykę odzwierciedlającą stany rzeczy wynikające z treści określonych doznań zmysłowych i umysłowych. Należy przy tym pamiętać, że treści doznania zmysłowego i doznania umysłowego nie są informacjami – są po prostu i tylko treściami doznań. Treściami informacyjnymi stać się mogą tylko nazwy identyfikujące, które w swoim wnętrzu semantycznym zawierają treści opisu identyfikujące dane doznanie. Zależność ta wynika z faktu, że każde doznanie ma tylko wartość poznawczą dla doznającego, Nazwy natomiast posiadają wartość informacyjną. Przy ich użyciu można informować innych o tym czego nigdy nie doznawali. Doznanie bez przypisanej temu nazwy jest tylko doznaniem dla doznającego i niczym więcej. Informacja, jako nazwa danego doznania zawiera dopiero pojęciowe elementy identyfikacyjne, które umożliwiają informować innych o stanie danego doznania. Dlatego też „informacja", jako nazwa, może się odnosić semantycznie do wszystkiego co jest związane z postrzeganiem zmysłowym „świata realnego" i wszystkiego co jest związane z myślowym odczuwaniem doznań powstających w „wirtualnym świecie" ludzkiego myślenia. Proponowana definicja uwzględnia to w zestawieniu wyrazowym: nazwa doznań zmysłowych i umysłowych człowieka.

W aspekcie formalnym, proponowana definicja spełnia dwa warunki – konieczny i wystarczający. W zaproponowanej postaci uwzględnia wskazania „rodzaju najbliższego" (genus proximum) i „cechy różnicujące" (differentia specifica). Z tego też względu zdaje się być realna i użyteczna w postrzeganiu funkcji komunikacyjnych

---

[88] Bezpośrednia identyfikacja zmysłowa występuje wówczas, kiedy pomiędzy obiektem poznawanym i układem zmysłowym człowieka nie występują żadne urządzenia pośrednie, rozszerzające zakres postrzegania zmysłowego (przypis autorski).

[89] Pośrednia identyfikacja zmysłowa występuje wówczas, kiedy pomiędzy obiektem poznawanym i układem zmysłowym człowieka występują jakieś urządzenia, które rozszerzają zakres postrzegania zmysłowego (przypis autorski).

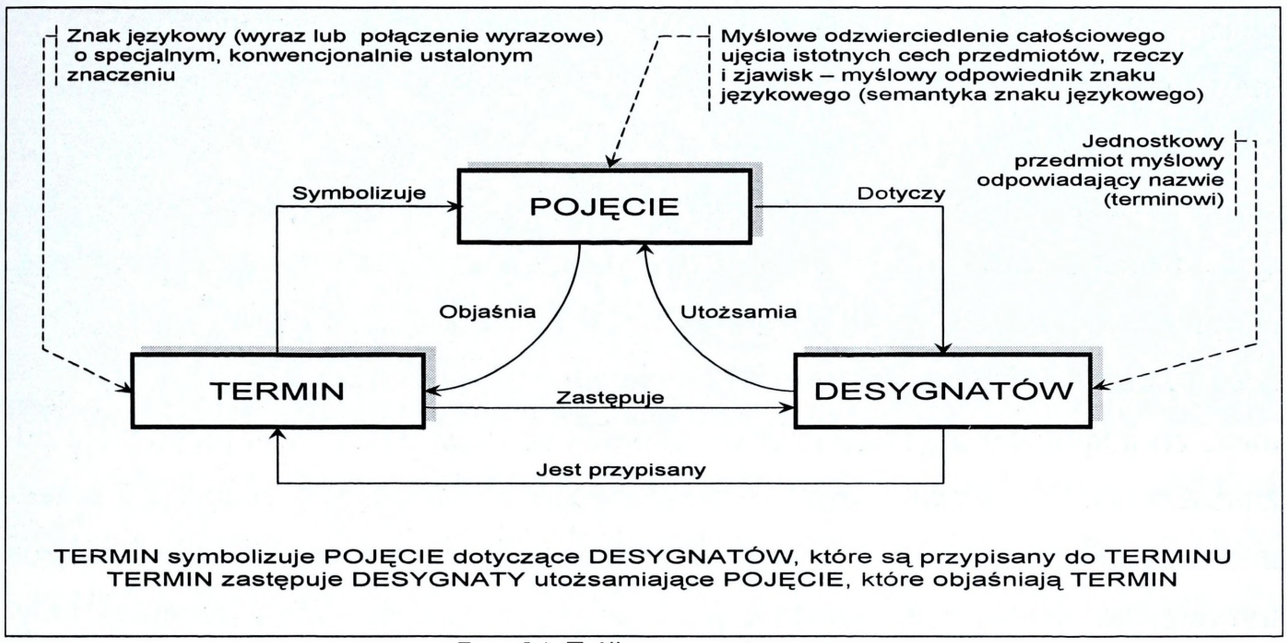
(sprawczych, regulujących i projektujących), a także i metodologicznych (słownikowych i semantycznych). Ponadto w jej treści wyjaśniającej nie występują elementy typu „ignotum per ignotum" (nieznane przez nieznane) co powoduje, że zakresy definiensu (wyrażenia definiującego) i definiendum (wyrażenia definiowanego) nie „krzyżują" się.

Podobny co do tego pogląd prezentuje Louis Couffignal twierdząc, że *informacja to zespół nośnika i semantyki, gdzie semantyka jest efektem psychicznym informacji, a* ***nośnik*** *jest* ***zjawiskiem fizycznym*** *skojarzonym z* ***semantyką*** *w celu utworzenia informacji*[90]. Nie jest to jeszcze wyjaśnienie zupełne, ale wyraźnie wskazujące, że **informacja**, w postrzeganiu autonomicznym, **nie jest wytworem materialnym**. Postać materialną (fizyczną) zachowuje tylko jej „środek transportowy" – „nośnik", na który nakłada się nazwa i jej semantyka, czyli informacja. Nośnik ten, podobnie jak pojazd pasażerowi, umożliwia jej przemieszczanie się w czasie i przestrzeni. Dlatego też „dokowanie" informacji w „maszynie cybernetycznej", w czystej postaci – w postaci niezwiązanej z nośnikiem – jest niemożliwe.

Interpretację merytorycznie zbliżoną do poprzedniej (do Louis'a Couffignal'a) można znaleźć w książce Norberta Wienera „Cybernetyka i społeczeństwo", gdzie autor wyjaśnia: *Informacja jest nazwą treści zaczerpniętej ze świata zewnętrznego, w miarę jak się do niego dostosowujemy i jak przystosowujemy doń swoje zmysły*[91]. Autor używając stwierdzenia, że **informacja** jest **nazwą treści** potwierdza tym samym, iż ta (informacja) może być tylko **semantyką** określonego **znaku językowego**, bo każdy znak językowy (termin) symbolizuję określoną treść znaczeniową – określone pojęcie, które jest tożsame znaczeniowo z semantyką (rys. 24). Co prawda Norbert Wiener nie akcentuje wyraźnie, że nadawanie nazw treściom doznań zmysłowych odbywa się w ludzkim umyśle, ale z całości wynika jednoznacznie, że chodzi tu tylko o człowieka i asocjacyjnie spełniane funkcje prze jego umysł, które są związane z nadawaniem nazw różnym doznaniom zmysłowym (obrazom percepcyjnym). W pewnym sensie potwierdza to też jego kolejne Jego stwierdzenie, że *proces otrzymywania i wykorzystywania informacji jest procesem naszego dostosowywania*

[90] L. Couffignal, „Les machines a penser", Les Editions de Minut, Paris 1964 (patrz również tabela 1, poz. 10).
[91] N. Wiener, „Cybernetyka i społeczeństwo", KiW, Warszawa 1960, s. 16 (patrz również tabela 1, poz. 8).

się do różnych ewentualności środowiska zewnętrznego oraz naszego czynnego życia w tym środowisku[92].



Rys. 24. Trójkąt semantyczny

Źródło: Opracowanie autorskie na podstawie: C.K. Ogden, I.A. Richards, „The Meaning of Meaning: A Study of the Influence of Languaage upon Thought and of the Science of Symbolism", Harcout, Brace & World, New York 1946

W nieco innej formie syntaktycznej i z nieco innym akcentem, ale merytorycznie zbieżnym z poglądami Louis'a Couffignal'a i Norberta Wienera, interpretuje informację Henryk Greniewski, w swojej książce „Sprawy wszystkie i jeszcze inne". Wyraża pogląd, że: *W języku potocznym wyraz informacja używamy jest zwykle w ten sposób, że spełniane są trzy warunki poniższe:*

a) *każda informacja jest wiadomością o czymś,*
b) *informację uzyskuje tylko człowiek (poprzez obserwację lub czynność umysłową),*
c) *informacje przekazuje tylko człowiek człowiekowi*[93]

Analizując ten pogląd techniką *porządkowania wstępującego*[94], to znaczy traktując go jako odpowiedzi na pytanie: czym jest informacja? można przypuszczać, że ich Autor postrzega rzeczowość tego terminu (znaku językowego) prze pryzmat semantyki i jej nośników językowych, transformujących jedne komunikaty asocjacji informacyjnej w kolejne komunikaty tej asocjacji. Świadczy o tym stwierdzenie, że *informacja*

[92] Ibidem.
[93] H. Greniewski, „Sprawy wszystkie i jeszcze inne", KiW, Warszawa 1970, s. 24 (patrz również tabela 1, poz. 13).
[94] Porządkowanie wstępujące – przekształcanie odpowiedzi, na jakieś pytanie dotyczące świata, w odpowiedź na pytanie dotyczące czyjegoś umysłu (A. Morton, „Przewodnik po teorii poznania", Spacja, Warszawa 2002, s. 305)

jest wiadomością, to znaczy, że jest jakąś treścią znaczeniową przekazywaną za pomocą określonych znaków językowych – to znaczy, że jest semantyką. Słuszność takiej interpretacji potwierdzają kolejne sformułowania odzwierciedlające pogląd, że *informację uzyskuje tylko człowiek* a także, że *informacje przekazuje tylko człowiek człowiekowi.*

Bardzo istotne, ale mogące też budzić i pewne wątpliwości, zdaje się być stwierdzenie zawarte w punkcie „b", odczytywane w zespoleniu z uzupełnieniem zamieszczonym w nawiasie tego punktu. Widnieje tam zapis, że *informację uzyskuje tylko człowiek (poprzez obserwację lub czynność umysłową).* Można zatem rozumieć, że informację uzyskuje również człowiek poprzez obserwację przedmiotu poznania co nie jest prawdą. Jak już akcentowano, w następstwie obserwacji **przedmiotu poznania** człowiek uzyskuje tylko określone **treści recepcyjne** powodujące wytwarzanie zmysłowych **obrazów percepcyjnych** którym, drogą **asocjacji** umysłowej są dopiero nadawane określone **nazwy**, jako nośniki **semantyki** tych doznań percepcyjnych[95]. Przypuszczać można, że Autorowi chodziło tylko o wyeksponowanie procedury informowania, co w taki rozumieniu jest to jak najbardziej słuszne[96], chociaż sama **obserwacja**, w dosłownym znaczeniu tego słowa, nie wyczerpuje możliwych form **informowania**. Jak też już wcześniej podkreślano, **recepcje**, **percepcje** i **asocjacje** nie odnoszą się tylko do wzrokowych **znaków językowych**. Jako komplementarne elementy struktury **układu informacyjnego** są dostosowane do transformowania wszystkich **treści recepcyjnych** w **obrazy percepcyjne** i w symbolizujące je **nazwy**, jako nośniki **semantyki**, odzwierciedlającej **pojęciowo** treści znaczeniowe, zarejestrowanych zmysłowo **obrazów percepcyjnych**. Ważne natomiast jest w tym punkcie (chodzi o punkt „b") uzupełnienie wyjaśniające, że **informację** może uzyskiwać człowiek również przez **czynność umysłową**. Wynika z tego – czego wyraźnie nie zaakcentował w swojej definicji Norbert Wiener – że **nazwy** nie są nadawane tylko **treściom poznawczym** pochodzącym ze świata zewnętrznego. Są również nadawane skojarzeniom pochodzącym z wewnętrznego „świata myśli", w następstwie toczącego się tam ciągle przetwarzania indukcyjno-dedukcyjnego i niekończącego się pasma asocjacji.

Jako, że „semantyka oznaczona", reprezentowana przez konkretny znak językowy (nazwę), powstaje zawsze w ludzkim umyśle, w następstwie asocjacji obrazów

---

[95] Patrz rys. 25 i 27 oraz przypisany do nich tekst.
[96] Patrz rys. 26 i 27 oraz przypisany do nich tekst.

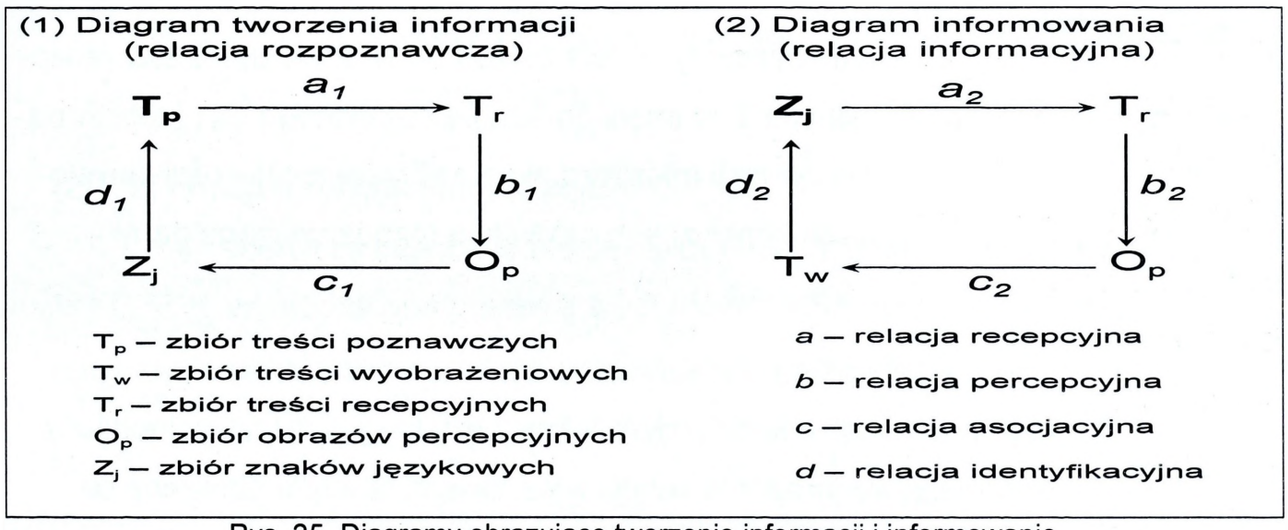
percepcyjnych i wyobrażeniowych ze stanem myślowym funkcji poznawczych mózgu. Dlatego też **źródłem** wszelkich **informacji** jest zawsze i tylko człowiek.

Źródło informacji – człowiek przekazujący treści znaczeniowe, za pomocą etnicznych znaków językowych;

gdzie:

- „źródło informacji" – *definiendum,*
- „człowiek przekazujący treści znaczeniowe, za pomocą etnicznych znaków językowych" – *definiens,*
- „człowiek przekazujący treści znaczeniowe" – *genus proximum,*
- „za pomocą etnicznych znaków językowych" – *differentia specifica.*

Nawiązując do wcześniejszych treści (tekstowych i rysunkowych), procedurę tworzenia informacji i procedurę informowania można również opisać językiem i symboliką stosowaną w *teorii kategorii*[97] i na kanwie dwóch prostych diagramów wykazać różnice występujące pomiędzy tymi procedurami (rys. 25).



Rys. 25. Diagramy obrazujące tworzenie informacji i informowanie

Źródło: Opracowanie autorskie

Na powyższych diagramach (rys. 25) wyraźnie widać, że:

(1) W relacji rozpoznawczej (diagram 1):

---

[97] Teoria kategorii – jest działem matematyki stosunkowo młodym. Popularność zaczęła zdobywać dopiero w latach sześćdziesiątych naszego wieku. Jej podstawowe pojęcia zostały sformułowane w 1945 roku przez amerykańskich matematyków S. Eilengerga i S. Mac Lane'a. Teoria kategorii proponuje spojrzenie na matematykę odmiennie od przyjętego w teorii mnogości. W teorii mnogości (1)zbiór, (2)element zbioru i (3)relacja $a \in A$ są fundamentalnymi pojęciami tej teorii, na których się opiera cała współczesna matematyka. W teorii kategorii elementy zbiorów schodzą na plan dalszy, najważniejsze są przekształcenia i złożenia przekształceń. Przekształcenie *f zbioru X w zbiór Y*, oznacza się symbolem $f: X \to Y$ lub $X \xrightarrow{f} Y$, traktowane jest w teorii kategorii jako „strzałka" (morfizm), której „początkiem" jest zbiór *X* (zwany też dziedziną), a „końcem" jest zbiór *Y* (zwany też kodziedziną przekształcenia *f*). Gdy rozważa się kilka przekształceń naraz, wtedy można je przedstawiać za pomocą jednego rysunku składającego się z symboli zbiorów i strzałek symbolizujących przekształcenia; rysunek taki nazywamy diagramem („Leksykon matematyczny", Wiedza Powszechna, Warszawa 1993, s. 619-639).

- Pierwszą dziedzinę[98] w czteroelementowym łańcuchu przekształceń, wyrażoną pod postacią a_1, stanowi zbiór treści poznawczych T_p, a kodziedzinę[99] – zbiór treści recepcyjnych T_r, co można zapisać:

$$a_1 : T_p \rightarrow T_r$$

gdzie:

a_1 – symbolizuje tylko taki zakres przekształcania treści poznawczych T_p w treści recepcyjne T_r, które w danej sytuacji mieszczą się w zakresie możliwości recepcyjnych konkretnego człowieka rozpoznającego dany przedmiot.

- Drugą dziedzinę przekształceń typu b_1 stanowią treści recepcyjne T_r, a kodziedzinę – obraz percepcyjny O_p, co można zapisać:

$$b_1 : T_r \rightarrow O_p$$

gdzie:

b_1 – symbolizuje tylko taki zakres przekształcania treści recepcyjnych T_r w treści obrazu percepcyjnego O_p, które w danej sytuacji mieszczą się w zakresie możliwości zmysłowych konkretnego człowieka rozpoznającego dany przedmiot.

- Trzecią dziedzinę przekształceń typu c_1 stanowią treści obrazu percepcyjnego O_p, a kodziedzinę – znak językowy Z_j odzwierciedlający osobnicze wyobrażenie asocjacyjne związane z tym obrazem, co można zapisać:

$$c_1 : O_p \rightarrow Z_j$$

gdzie:

c_1 – symbolizuje tylko taki zakres przekształcania treści obrazu percepcyjnego O_p w treści znaku językowego Z_j, który w danej sytuacji mieści się w intelektualnych możliwościach konkretnego człowieka rozpoznającego dany przedmiot.

---

[98] Dziedzina przekształcenia – zbiór stanowiący początek przekształcenia a_1 (początek „strzałki"); [„Leksykon matematyczny", Wiedza Powszechna, Warszawa 1993, s. 620].

[99] Kodziedzina przekształcenia – zbiór stanowiący koniec przekształcenia a_1 (koniec „strzałki"); [„Leksykon matematyczny", Wiedza Powszechna, Warszawa 1993, s. 620].

- Czwartą dziedzinę przekształceń typu d_1 stanowią treści znaku językowego Z_j, a kodziedzinę – zbiór treści poznawczych T_p, co można zapisać:

$$d_1 : Z_j \rightarrow T_p$$

gdzie:

d_1 – symbolizuje złożenie przekształceń występujące w relacji recepcyjnej, percepcyjnej i asocjacyjnej, co można zapisać:

$$d_1 = a_1 b_1 c_1$$

i interpretować, że każda informacja, jako nazwa treści doznań zmysłowych i umysłowych człowieka, jest zawsze subiektywna – zawsze zależy od wcześniejszej wiedzy konkretnego człowieka oraz jego predyspozycji intelektualnych i psychofizycznych, a często i od nastawienia intencjonalnego.

(2) W relacji informacyjnej (diagram 2):

- Pierwszą dziedzinę w czteroelementowym łańcucha przekształceń, wyrażoną pod postacią a_2, stanowi zbiór treści znaczeniowych Z_j skojarzonych ze znakiem językowym, a kodziedzinę – zbiór treści recepcyjnych T_r, co można zapisać:

$$a_2 : Z_j \rightarrow T_r$$

gdzie:

a_2 – symbolizuje tylko taki zakres przekształcania treści znaczeniowych Z_j w treści recepcyjne T_r, które w danej sytuacji mieszczą się w zakresie możliwości recepcyjnych konkretnego człowieka odbierającego dany znak językowy.

- Drugą dziedzinę przekształceń typu b_2 stanowią treści recepcyjne T_r, a kodziedzinę – obraz percepcyjny O_p, co można zapisać:

$$b_2 : T_r \rightarrow O_p$$

gdzie:

b_2 – symbolizuje tylko taki zakres przekształcania treści recepcyjnych T_r w treści obrazu percepcyjnego O_p , które w danej sytuacji mieszczą się w zakresie możliwości zmysłowych człowieka informowanego.

- Trzecią dziedzinę przekształceń typu c_2 stanowią treści obrazu percepcyjnego O_p, a kodziedzinę – treści wyobrażeniowe T_w odzwierciedlające osobnicze predyspozycje asocjacyjne osoby informowanej, co można zapisać:

$$c_2 : O_p \rightarrow T_w$$

gdzie:

c_2 – symbolizuje tylko taki zakres przekształcania treści obrazu percepcyjnego O_p w treści wyobrażeniowe T_w, który w danej sytuacji mieszczą się w intelektualnych możliwościach człowieka informowanego.

- Czwartą dziedzinę przekształceń typu d_2 stanowią treści wyobrażeniowe T_w, a kodziedzinę – zbiór treści znaczeniowych Z_j określonego znaku językowego, co można zapisać:

$$d_2 : T_w \rightarrow Z_j$$

gdzie:

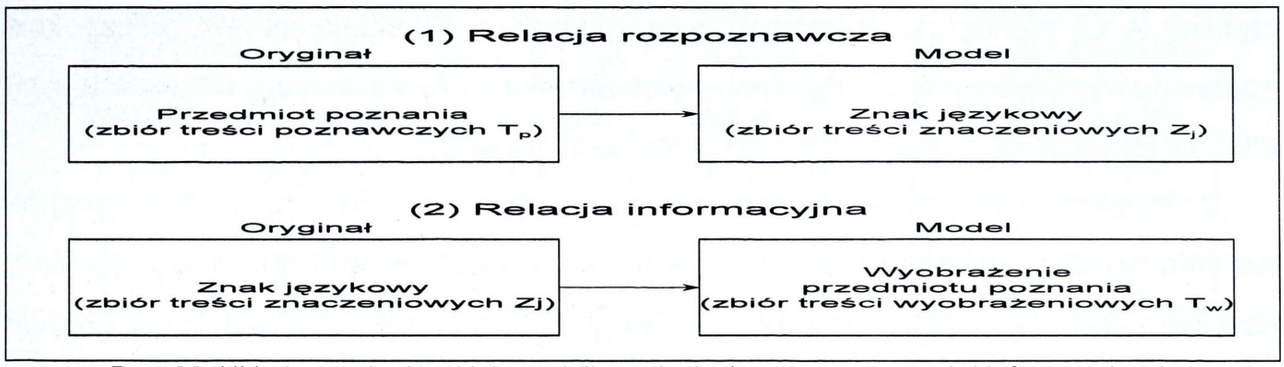
d_2 – symbolizuje złożenia przekształceń występujące relacji recepcyjnej, percepcyjnej i asocjacyjnej, co można zapisać:

$$d_2 = a_2 b_2 c_2$$

i interpretować, że ten sam proces informowania może powodować różne wyobrażenia, co jest związane z wcześniejszą wiedzą informowanego oraz z jego predyspozycjami intelektualnymi i psychofizycznymi.

Uogólniając można powiedzieć że, tak w relacjach rozpoznawczy, jak i w relacjach informacyjnych, każde złożenie przekształceń sprowadza się do konstrukcji umysłowej modelu odwzorowującego określony oryginał. W relacjach rozpoznawczych ory-

ginał stanowi zawsze przedmiot poznania, a jego model[100] – znak językowy nadany mu przez rozpoznającego. W relacjach informacyjnych dzieje się odwrotnie. Oryginał stanowi znak językowy, a jego model – treść wyobrażeniowa przedmiotu oznaczonego tym znakiem (rys. 26).



Rys. 26. Układy oryginałów i ich modeli w relacjach rozpoznawczych i informacyjnych

Źródło: Opracowanie autorskie

Jak już akcentowano, **informacja** w postaci semantyki oznaczonej[101] i nieoznaczonej[102] powstaje i bytuje tylko w ludzkim umyśle, jako **wyobrażeniowy wytwór funkcji poznawczych mózgu**[103], spowodowany określonymi doznaniami zewnętrznymi i wewnętrznymi. Mniemać można, że podobnie postrzegali ten problem etniczni twórcy języka łacińskiego, oznaczając ten rodzaj doznania znakiem języko-

---

[100] Model – Układ, którego zadaniem jest imitowanie wyróżnionych cech innego układu, zwanego oryginałem.

- Model może być elementem działającym analogicznie do oryginału lub myślowym przedstawieniem zależności występujących w oryginale.
- Model jest quasi-obiektem , imitującym obiekt w znacznym uproszczeniu, lecz z zachowaniem niektórych cech rzeczywistego obiektu, istotnych dla przyjętego punktu widzenia.
- Modele dzielimy na abstrakcyjne (matematyczne, logiczne, wyobrażeniowe itp.) i fizyczne (mechaniczne, hydrauliczne, chemiczne, elektromechaniczne, elektryczne itp.).
- Między obiektem modelowanym a jego modelem musi zachodzić co najmniej relacja homomorfizmu.
- Między modelem abstrakcyjnym i modelem fizycznym tego samego obiektu może występować relacja izomorfizmu odnośnie pewnych cech lub relacja homomorfizmu w różnych jej stopniach

[Maria Kempisty (redakcja), „Mały słownik cybernetyczny", WP, Warszawa 1973, s. 238]

Istnieje również odwzorowanie homeomorficzne, ale te różni się od odwzorowania homomorficznego tym, homomorficzne odnosi się do przekształceń algebraicznych, a homeomorficzne do topologicznych, to znaczy do działu matematyki poświęconej badaniu tych właściwości tworów geometrycznych (zbiorów, punktów), które nie ulegają zmianie przy pewnych przekształceniach – jak na przykład przy rozciąganiu czy kurczeniu się figur.

[101] Semantyka oznaczona – engram semantyczny z przypisanym znakiem językowym identyfikującym jego postać – synonim komunikacyjne postaci semantyki (przypis autorski).

[102] Semantyka nieoznaczona – engram semantyczny bez przypisanego mu znaku językowego (tylko osobnicze wyobrażenie) – synonim informacji potencjalnej (przypis autorski).

[103] Wyobrażenie – wywołany w świadomości obraz przedmiotu lub sytuacji, które w danej chwili nie oddziałuje na narządy zmysłowe człowieka, opierający się na uprzednio poczynionych spostrzeżeniach i fantazji („Słownik języka polskiego", PWN, Warszawa 1981, tom III, s. 826).

wym **informatio**[104], co w języku polskim przekształcono w termin **informacja**. Wynika też z tego, co zdaje się już być oczywiste, że w bezpośrednich relacjach komunikacyjnych „człowiek – człowiek" zasadniczą rolę spełniają treści znaczeniowe znaków językowych, czyli ich semantyka, a nie stan fizyczny nośników tych znaków, chociaż te są niezbędne w każdym komunikowaniu. Spełniają jednak, w aspekcie znaczeniowym, tylko rolę podrzędną – tylko „środka transportowego" dla określonych znaków językowych i zespolonej z tymi znakami semantyki.

W relacji „człowiek – urządzenie" jest nieco inaczej. Zasadniczą funkcję spełnia stan fizyczny **nośników** znaku językowego, a nie ich **semantyka** (nie treść znaczeniowe znaków). Żadne urządzenie i żadna „maszyna cybernetyczna" nie reagują na wartości semantyczne. Reaguje tylko na wartości fizyczne. Dlatego też deformacja pierwotnej struktury nośnika treściami określonego znaku językowego musi być dostosowana do wejścia konkretnego urządzenia. Na przykład w „maszynie cybernetycznej" (komputerze) funkcje takiego nośnika spełnia prąd elektryczny zasilający poszczególne układy tego urządzenia. Nośnik ten musi być zatem „zdeformowany" binarnymi ciągami prądowymi przebiegającymi zgodnie z zastosowanym kodem wektorowym danych.

Dane – elementarne treści znaczeniowe (fizyczne i semantyczne), przyjmowane za podstawę w szerszych zestawieniach procesowych i semantycznych;
gdzie:

- „dane" – *definiendum*,
- „elementarne treści znaczeniowe (fizyczne i semantyczne), przyjmowane za podstawę w szerszych zestawieniach procesowych i semantycznych" – *definiens*,
- „elementarne treści znaczeniowe (fizyczne i semantyczne)" – *genus proximum*,
- „przyjmowane za podstawę w szerszych zestawieniach procesowych i semantycznych" – *differentia specifica*.

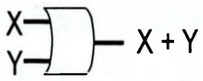
Na wejściach tych urządzeń, podobnie jak w ośrodkach zmysłowych człowieka, odbywa się proces „separacji" nośnika od binarnych ciągów prądowych. Odbywa się to według określonego programu, który **steruje** procedurami **przetwarzania danych**, poprze odpowiednio zestawione bramki, funkcjonujące według zasad klasycznej logiki dwuwartościowej (prawda → 1; fałsz → 0) – rys. 26. Żadna „maszyna cybernetyczna" (komputer) nie odczytuje zatem treści znaczeniowej tych ciągów (semantyki).

[104] Informatio – wyobrażenie [„Słownik łacińsko-polski", PWN, Warszawa 2003, tom 2, s. 69; Władysław Kopaliński, „Słownik wyrazów obcych i zwrotów obcych (wydanie dziewiąte)", WP, Warszawa 1975, s. 429].

Identyfikuje tylko i przetwarza wartości fizyczne według wcześniej wprowadzonego do niej program. Żadna maszyna nie myśli i nie nadaje nowych nazw treściom. Realizuje tylko ściśle zalgorytmizowane procedury przetwarzania fizycznych danych.

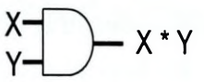
Alternatywa „OR"
[X lub Y (suma logiczna)]

Wejście		Wyjście
X	Y	Z = X OR Y
0	0	0
0	1	1
1	0	1
1	1	1



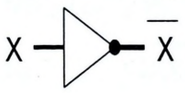
Koniunkcja „AND"
[X i Y (iloczyn logiczny)]

Wejście		Wyjście
X	Y	Z = X AND Y
0	0	0
0	1	0
1	0	0
1	1	1



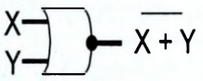
Negacja „NOT"
[nie X (negacja logiczna)]

Wejście	Wyjście
X	Y = NOT X
0	1
1	0



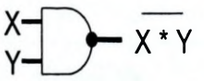
Negacja alternatywy „NOR"
[nie X lub Y (negacja sumy logicznej)]

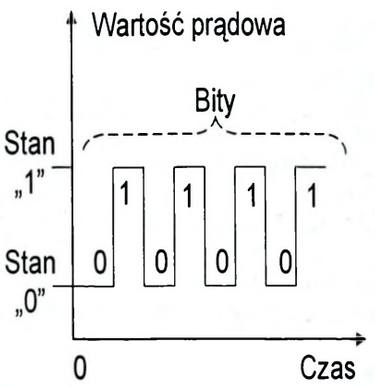
Wejście		Wyjście
X	Y	Z = X NOR Y
0	0	1
0	1	0
1	0	0
1	1	0



Negacja koniunkcji „NAND"
[nie X i Y (negacja iloczynu logicznego)]

Wejście		Wyjście
X	Y	Z = X NAND Y
0	0	1
0	1	1
1	0	1
1	1	0





Rys. 26. Szkic obrazujący funkcje logiczne bramek w przetwarzaniu danych binarnych

Źródło: Opracowanie autorskie

Istota tej procedury sprowadza się do tego, że **fonemy**[105], wykorzystywane w relacjach międzyludzkich do tworzenia **morfemów**[106], są zastępowane różnymi binarnymi zestawieniami prądowymi, odzwierciedlającymi umownie stany „0" i „1" które, w odpowiednim uporządkowaniu kodowym, odwzorowują **fonemy** (rys. 27).

[105] Fonem – najmniejsza jednostka mowy ludzkiej rozróżniana przez użytkowników danego języka etnicznego.
[106] Morfem – znak językowych składających się z niepodzielnego zbioru fonemów.

KODOWANIE W UKŁADZIE ÓSEMKOWYM (2^3=8)							
Kodowane cyfry							
0	1	2	3	4	5	6	7
Kod wektorowy cyfr							
000	001	010	011	100	101	110	111

KODOWANIE W UKŁADZIE SZESNASTKOWYM (2^4 = 16)															
Kodowane cyfry i fonemy															
0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Kod wektorowy cyfr i fonemów															
0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111

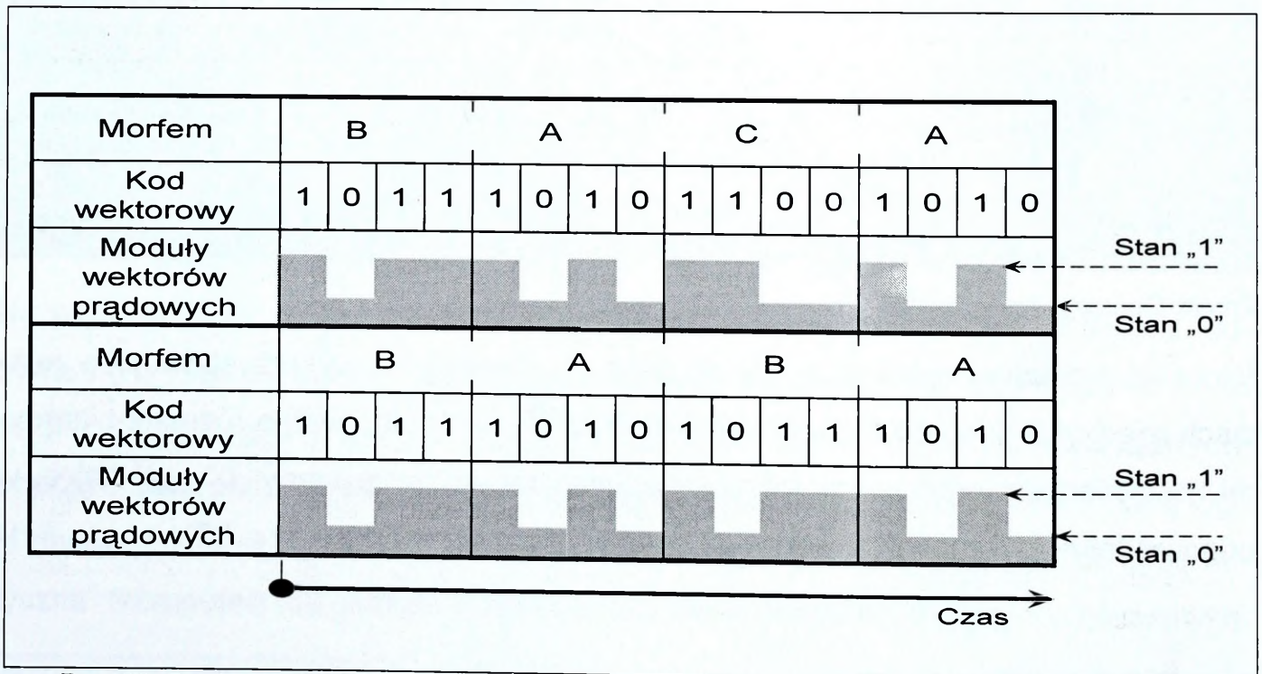
Rys. 27. Cyfrowy obraz kodu wektorowego w układzie ósemkowym i szesnastkowym

Źródło: Opracowanie autorskie

Przy takiej transformacji można na przykład, znaki języka etnicznego (morfemy) „baca" i „baba", zapisać w postaci następującego kodu wektorowego:

- baca → 1011 1010 1100 1010;
- baba → 1011 1010 1011 1010.

W „maszynie cybernetycznej" (komputerze) treści znaczeniowe tego zapisu będą natomiast odzwierciedlały przebiegi prądowe (moduły wektorów prądowych) w następującej postaci (rys. 28).



Rys. 28. Prądowy obraz kodu wektorowego odwzorowywanego w „maszynie cybernetycznej"

Źródło: Opracowanie autorskie

W tym miejscu wnikliwy Czytelnik może zarzucić, że we współczesnej cybernetyce procedury przetwarzania odbywają się już nie tylko na zasadach klasycznej logiki dwustanowej (prawda → 1; fałsz → 0), ale również na zasadach logiki rozmytej, gdzie pomiędzy „1" (prawdą) i „0" (fałszem) występują jeszcze stany pośrednie[107].

W umyśle człowieka liczba stanów pośrednich jest nieskończona i można powiedzie, że zachodzące w tej przestrzeni asocjacje, ukierunkowane na przetwarzanie i wytwarzanie informacji, charakteryzują się ciągłością rozkładów zmiennych losowych wykorzystywanych w kojarzeniu[108]. Dlatego też możliwości asocjacyjne umysłu ludzkiego należy pojmować jako procesy o nieskończonych możliwościach przetwarzania. W podobnym kontekście, aczkolwiek skierowanym do syntaktyki, sformułował definicję języka przytaczany już wcześniej Noama Chomsky wyrażając pogląd, że *język jest nieskończonym zbiorem zdań, generowanych za pomocą skończonej liczby reguł i słów*. W argumentacji tego przytoczył niezwykle wymowne zdanie: *Colorless green ideas sleep furiously*[109] (bezbarwne zielone idee wściekle śpią). Tym samym, na przykładzie surrealnej treści znaczeniowej (surrealnej semantyki), chociaż wynikającej z gramatycznie zestawionego znaku językowego (zdania), wykazał nieskończony zakres możliwości generowania przez człowieka przeróżnych informacji, co świadczy o ciągłości i nieskończoności asocjacyjnego przetwarzania zlokalizowanego w ludzkim umyśle, czego nie osiąga żadna „maszyna cybernetyczna" operująca na danych binarnych które, jako zmienne losowe, zachowują z natury rzeczy cechy charakterystyczne dla rozkładów dyskretny[110], nawet przy stosowaniu niezwykle gęstego próbkowania wartości prawdopodobieństwa w przedziale ⟨0 - 1⟩, które niezależnie od tej gęstości, to jednak zawsze pozostanie próbkowaniem skokowym (dys-

---

[107] Logika rozmyta (ang. fuzzy logic) – jedna z logik wielowartościowych (multi-valued logic) stanowiąca uogólnienie klasycznej logiki dwuwartościowej; jest ściśle powiązana z teorią „zbiorów rozmytych" i teorią prawdopodobieństwa; w logice rozmytej między stanem „0" (fałsz) i stanem „1" prawda rozciąga się szereg wartości pośrednich, które określają stopień przynależności (prawdopodobieństwo) określonego elementu do danego zbioru (przypis autorski).

[108] Ciągła zmienna losowa – to zmienna losowa ζ, dla której istnieje taka nieujemna funkcja f(x), że dystrybuanta zmiennej losowej ζ wyraża się wzorem

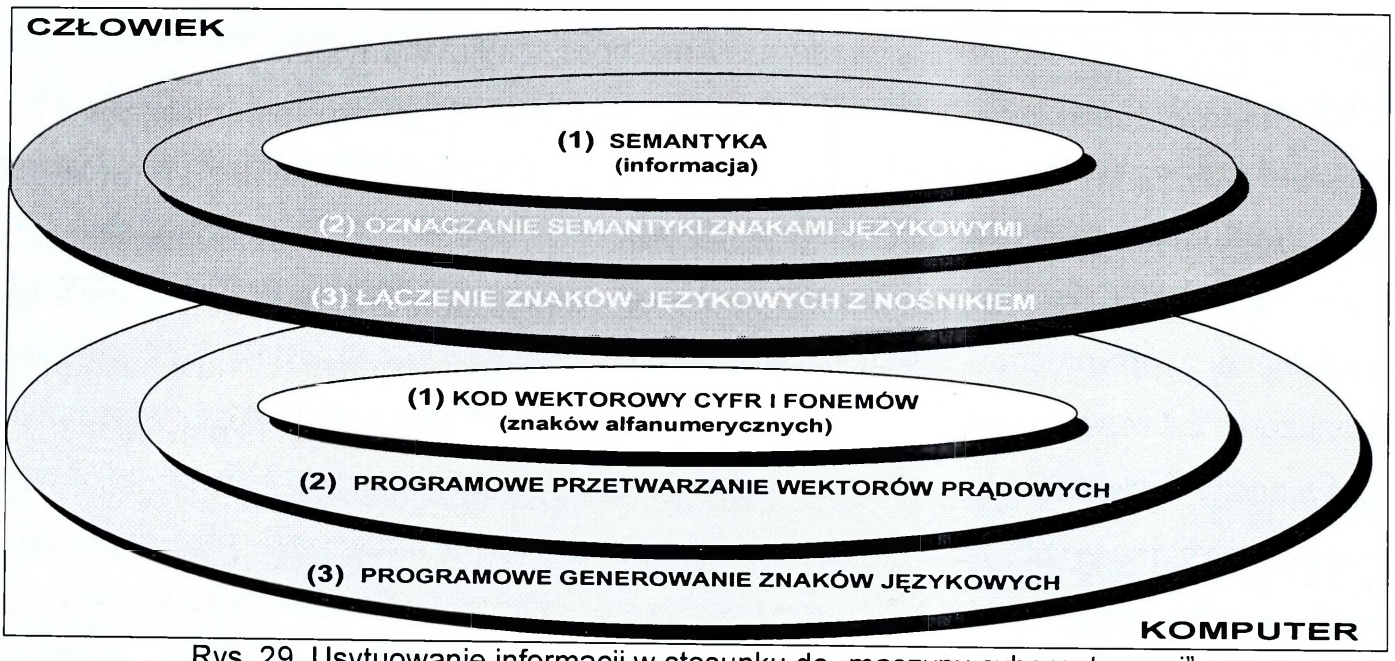
$$F(x) = P(\zeta < x) = \int_{-\infty}^{x} f(t)dt$$

i jest ciągła dla każdej rzeczywistej wartości *x*. Funka *f(x)* nazywa się funkcją gęstości prawdopodobieństwa zmiennej losowej ζ (Cz. Plat, „Problemy rachunku prawdopodobieństwa i statystki matematycznej", PWN, Warszawa 1978, s. 55-56).

[109] N.A. Chomsky, „Syntactic Structures", The Hague/Paris, Mouton 1957, s. 15.

[110] Dyskretna (skokowa) zmienna losowa – taka zmienna losowa, która może przyjmować tylko skończoną lub co najwyżej przeliczlną ilość wartości (równą ilości liczb naturalnych) [Cz. Plat, „Problemy rachunku prawdopodobieństwa i statystki matematycznej", PWN, Warszawa 1978, s. 36].

kretnym), a nie ciągłym. Wnika z tego, że w „maszynie cybernetycznej" nie odbywa się przetwarzanie informacji, rozumianej jako semantyki, a tylko przetwarzanie danych reprezentowanych przez binarne przebiegi prądowe, uporządkowane kodem wektorowym przypisanym tylko do konkretnych fonemów występujących w poszczególnych morfemach, czyli do symboli posiadających tylko reprezentacje dźwiękowe, ale pozbawionych jakiejkolwiek semantyki. Konfrontując to z obrazem przedstawiającym relacyjną postać semantyki (patrz rys. 31), można powiedzieć, że wejście do „maszyny cybernetycznej" poprzedzają jeszcze dwie warstwy transformacyjne, reprezentowane przez „środowisko kodu wektorowego fonemów i cyfr (znaków alfanumerycznych)" i „środowisko binarnych modułów wektorów prądowych" (rys. 29).

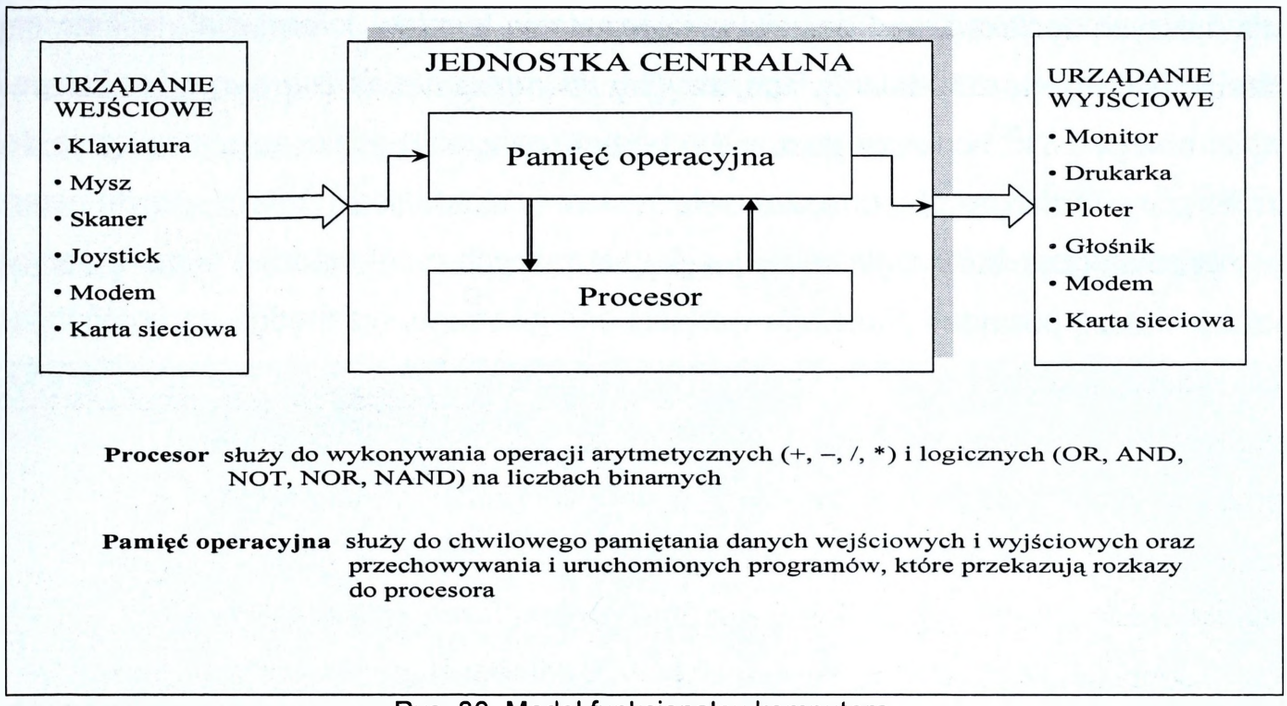


Rys. 29. Usytuowanie informacji w stosunku do „maszyny cybernetycznej"

Źródło: Opracowanie autorskie

Można zatem powiedzieć, że w cybernetyce, tak zwane „sieci asocjacyjne" są w rzeczywistości tylko surogatem[111] asocjacji umysłowej i nie uczestniczą w przetwarzaniu informacji jako semantyki (jako treści znaczeniowej znaku językowego), a tylko w przetwarzaniu danych fizycznych, to znaczy – prądowych reprezentacji kodu wektorowego przypisanego do odpowiednich cyfr i fonemów, a razem nazywając – znaków alfanumerycznych (rys. 30).

[111] Surogat – produkt, materiał zastępczy zbliżony w swoich podstawowych właściwościach do artykułu zastępowanego; namiastka („Słownik języka polskiego", PWN, Warszawa 1981, tom III s. 372.



Rys. 30. Model funkcjonalny komputera

Źródło: Opracowanie autorskie

Akcenty wątpliwości co do tego, że w „maszynie cybernetycznej" przetwarza się informacje, można odnaleźć w różnych pracach i publikacjach zaliczanych dziś do klasyki z tego obszaru. Na przykład Henryk Greniewski wyraża przekonanie, że *w cybernetyce używa się wyrazu informacja w rozumieniu dużo szerszy*, mimo tego, że wcześniej, w tej samej publikacji[112], stwierdza: *(1) każda informacja jest wiadomością o czymś; (2) informacje uzyskuje człowiek przez obserwację lub czynność umysłową; (3) informacje przekazuje tylko człowiek człowiekowi* – zastrzegając przy tym, że chodzi tu o język potoczny. Konfrontując to i bacząc na autorytet naukowy Autora nie można przypuszczać, iż wyrażony na ten temat pogląd jest małoznaczny. Wręcz odwrotnie. Należy sądzić, że stosując takie wyjaśnienia celowo sygnalizuje istnienie istotnego problemu, chociaż sam przechodzi dalej do spraw stricte cybernetycznych, co ze względu na tytuł wydawnictwa jest zrozumiałe. Istotność tego wynika natomiast z faktu, że we wszelki międzyludzkich relacjach komunikacyjnych jest ze wszech miar niepożądane aby tym samym znakiem językowym – w tym wypadku tym samym morfemem – symbolizować zróżnicowane treści znaczeniowe (przypisywać im zróżnicowaną semantykę). Nie identycznie w całym kontekście, ale we fragmentach swojego wywodu taki sam pogląd wyraża Marian Mazur. Również stwierdza, że *w cybernetyce używa się wyrazu informacja w rozumieniu dużo szerszym*[113]. Bardzo istotne

[112] H. Greniewski, „Sprawy wszystkie i jeszcze inne (o logice i cybernetyce)", KiW, Warszawa 1970, s. 24-25.
[113] M. Mazur, „Jakościowa teoria informacji, WNT, Warszawa 1970, s. 27.

dla dalszych dociekań, nad pojęciową interpretacją terminu „informacja", jest stwierdzenie Ludwiga von Bertalanffy'ego, że: *(...) informacji nie można wyrazić w kategoriach energii (...)*[114] i dalszy jego wywód z tym związany, gdzie autor nawiązuje do zróżnicowań istniejących pomiędzy zwierzęciem i człowiekiem[115]. Tym samym neguje cybernetyczne utożsamianie sygnałów sterujących z informacją, które z natury rzeczy muszą posiadać określone wartości energetyczne, niezbędne do uruchamiania procesów obliczeniowych w „maszynie cybernetycznej", czego informacja – jako semantyka – nie posiada i posiadać nie może. Von Hans-Joachim Flechtner jednoznacznie stwierdza, że *(...) sygnał (Signal) i informacja (Nachricht) to nie to samo chociaż w literaturze nie jest to wyjaśnione (...)*[116]. Dodaje do tego, że *(...) takie sama informacje mogą być przekazywane za pomocą różnych sygnałów (...)*[117] i to, że *(...) sygnał jest elementem fizycznym (...)*[118] natomiast *(...) informacja jest przeciwieństwem sygnału (...)*[119]

Uwzględniając powyższe można się zastanawiać czy „maszyna cybernetyczna" jest w ogóle w jakiś sposób związana z informacją czy też nie. Wiadomo, że przetwarza dane prądowe, ale nie semantykę jak to się dzieje w ludzkim umyśle. Zatem nie przetwarza informacji. Z drugiej zaś strony, na bazie prądowych reprezentacji znaków alfanumerycznych (cyfr i fonemów) dokonuje szeregu obliczeń i innych operacji, których wyniki, zgodnie z określonym programem, mogą być prezentowane na urządzeniach wyjściowych w postaci określonych znaków językowych, niosących już w sobie określone treści znaczeniowe czyli tak zwaną semantykę. Z pozoru zdaje się to przypominać procedury zachodzące w relacjach rozpoznawczych i relacjach informacyjnych. Różnica polega jednak na tym, że w tych relacjach, tak w jednym jak i drugim przypadku, finalnymi wytworami są umysłowe doznania asocjacyjne objawiające się, bądź to przypisywaniem określonych znaków językowy (nazw) do danych obrazów percepcyjnych (w relacjach rozpoznawczych), bądź to odwzorowywaniem treści znaczeniowych (semantyki) wynikających z odebranych znaków językowych w relacjach informacyjnych[120]. W maszynie cybernetycznej wszelkie procesy przebiegają na zasadzie programowo zdefiniowanego sterowania. Wielkie szybkość

---

[114] L. Bertalanffy, „Ogólna teoria systemów", PWN, Warszawa 1984, s. 73.
[115] Ibidem, s. 299 i 300.
[116] H. J. Flechtner, „Grundbegriffe der Kybernetik", Wissenschaftliche Verlagsgesellschaft M.B.H., Stuttgart 1967, s. 61.
[117] Ibidem.
[118] Ibidem.
[119] Ibidem, s. 62.
[120] Patrz rys. 26 i przypisany do nie tekst.

przetwarzania danych i wysoce zaawansowane techniki graficzne sprawiają tylko wrażenie **jak gdyby** w tych maszynach odbywało się **przetwarzanie informacji**. W rzeczywistości jest przecież inaczej. Dlatego też procedury te, oprócz przetwarzania danych, można również określać mianem przetwarzania **quasi-informacji**, gdzie pierwszy człon tej nazwy, według źródeł języka etnicznego (łacińskiego), oznacza: jakby, jak gdyby[121].

Quasi-informacja – informatyczny znak językowy, dostosowany do przetwarzania w maszynach cybernetycznych,

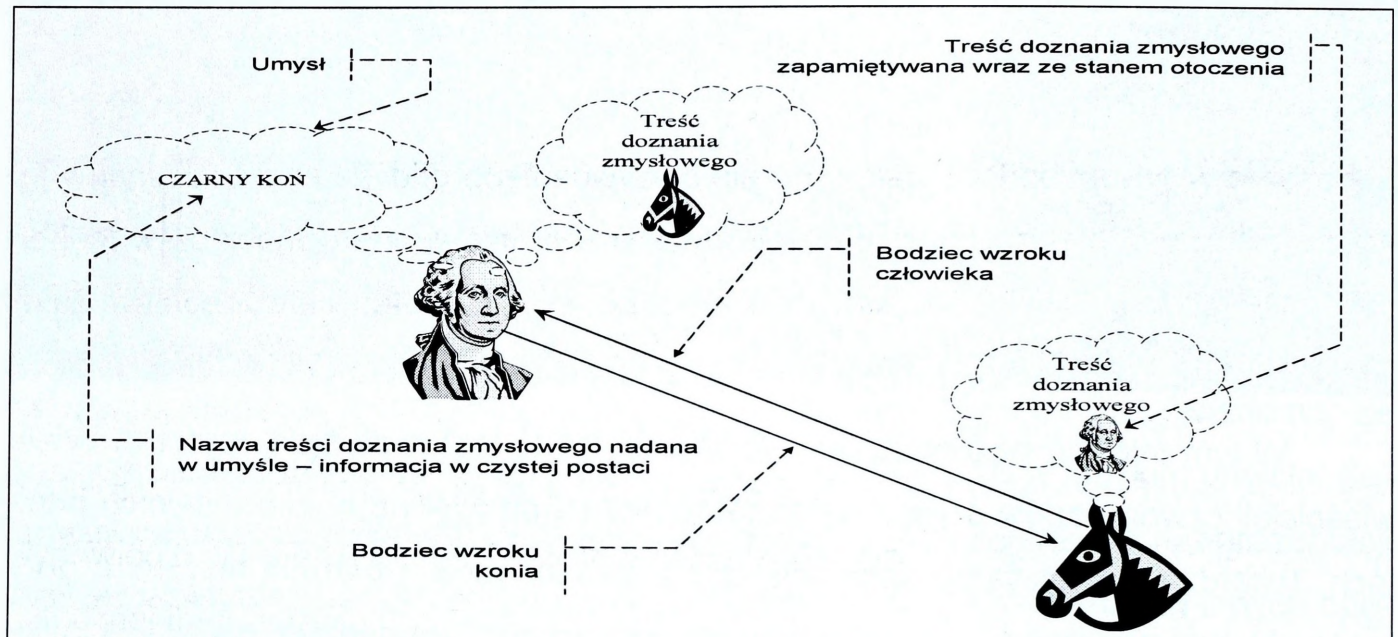
gdzie:

- „quasi-informacja" – *definiendum*,
- „informatyczny znak językowy, dostosowany do przetwarzania w maszynach cybernetycznych" – *definiens*,
- „informatyczny znak językowy" – *genus proximum*,
- „dostosowany do przetwarzania w maszynach cybernetycznych" – *differentia specifica*.

W tym miejscu pozostaje do wyjaśnienia jak to jest w świecie zwierząt. Wielu właścicieli czworonogów często wyraża nadmiernie pochlebne opinie o swoich pupilach. Twierdzą, że wszystko rozumieją co się do nich mówi i potrafią myśleć. Z góry można by odpowiedzieć – nie; bo gdyby tak było, to prawdopodobnie wszystkie zwierzęta rzeźne pozostałyby anorektykami, a inne zaczęłyby uprawiać sztukę. Problematykę tę z wielką dociekliwością opisał w swoich pracach między innymi Ludwig von Bertalanffy. Z ich treści wynika tylko, że zwierzęta mają zwykle lepiej rozwinięte od człowieka niektóre zmysły. Więcej zapamiętują doznań fizycznych i towarzyszących im stanów sytuacyjnych w otoczeniu, do czego sprowadza się istota naturalnej (gatunkowej) i sztucznej tresury. Zwierzęta nie potrafią myśleć i semantycznie odbierać mowy ludzkiej. Odbierają tylko fizyczne efekty nośnika mowy – drgania (zmiany) ciśnienia powodowane wypowiadaniem słów. Zapamiętują te efekty wraz z towarzyszącymi temu okolicznościami i po iluś powtórzeniach, odbierając podobne drgania, kojarzą to ze stanem otocznia, które wcześniej towarzyszyło tym drganiom. Podobnie dzieje się z gestami, czyli efektami widzenia. Zwierzęta mają też lepiej rozwinięty od człowieka zmysł węchu. Często też mają bardziej rozszerzony zakres widzenia niż człowiek. To wszystko pozwala im więcej i wcześniej doznawać tego co, z przyrodzonego prawa natury, zapewnia im trwanie w otoczeniu i to co stanowi zagrożenie.

[121] „Słownik łacińsko-polski", Wydawnictwo szkolne PWN, Warszawa 2003, tom II, s. 592.

Innymi słowy mogą szybko dostosowywać się do zmian zachodzących w otoczeniu, co jest warunkiem przetrwania. Wyrazistym przykładem mogą być chociażby węże, wyczuwające szybko fale sejsmiczne i niezależnie od warunków panujących na zewnątrz, opuszczają swoje podziemne ukrycia, unikając w ten sposób zagłady wynikającej z trzęsienia ziemi. Dlatego też często wydaje się człowiekowi mówiącymi do zwierzęcia, które podporządkowuje się wypowiadanym słowom, że rozumie ono sens wypowiedzi. W rzeczywistości jest to zawsze efekt tylko naturalnej (gatunkowej) lub sztucznej tresury (rys. 31).



Rys. 31. Szkic obrazujący reakcje człowieka i zwierzęcia na oddziaływanie bodźca wzroku

Źródło: Opracowanie autorskie

Zwierzęta nie reagują na semantyczną stronę znaków językowych, a tylko na fizyczne kształty ich nośników i na fizyczne stany otocznia, które z przyrodzonego gatunkowo prawa natury mieszczą się w zakresie ich fizycznego odczuwania. Sądzić można, że właśnie dlatego Norbert Wiener, odnosząc się do układów cybernetycznych, nie zatytułował swojego wielkiego dzieła inaczej, tylko: „Cybernetics: Or the Contro and Communication in the Animal and the Machine („Cybernetyka, czyli sterowanie i komunikacja **w zwierzęciu i maszynie**"[122]), akcentując poprzez to, że zarówno jeden, jak i drugi obiekt (zwierzę i „maszyna cybernetyczna") są dostosowane do odbierania i przetwarzania podobnych oddziaływań zewnętrznych. Dodając do tego słowo „control" (sterowanie) wyjaśnił, iż nie chodzi tu o oddziaływania informacyjne (semantyczne), ale o oddziaływania fizyczne – to znaczy o nośniki informacji, a

[122] N. Wiener, „Cybernetyka, czyli sterowanie i komunikacja w zwierzęciu i maszynie", PWN, Warszawa 1971.

nie o informację, który to we wszelkich swoich postaciach zachowują zawsze stan fizyczny.

Ludwig von Bertalanffy wyjaśnia natomiast[123], że: *(...) język jako wezwanie lub rozkaz można zaobserwować już w świecie zwierząt; przykładem jest tu śpiew ptaków, ostrzegawczy świst kozicy górskiej itp. Jednak język jako przedstawianie i komunikowanie faktów stanowi monopol człowieka. W szerszym znaczeniu język obejmuje nie tylko mowę oralną, ale również pismo oraz system symboli matematycznych. Są to systemy symboli nie odziedziczonych, lecz systemy symboli dowolnie tworzonych i tradycyjnych. Przede wszystkim wyjaśnia to specyfikę historii człowieka w odróżnieniu od ewolucji biologicznej: jest to tradycja w przeciwieństwie do dziedziczonych mutacji występujących tylko w długim okresie. Po drugie, fizyczną metodę prób i błędów, w dużej mierze charakteryzującą zachowania zwierząt, zastępuje się eksperymentem myślowym, czyli eksperymentowaniem przy użyciu symboli pojęciowych. Dlatego staje się możliwa prawdziwa kierunkowość docelowa. Kierunkowość docelowa i teologia w sensie metafizycznym, tzn. regulacja zdarzeń w znaczeniu podtrzymywania, produkcji i reprodukcji organicznej całościowości, stanowi ogólne kryterium życia. Z prawdziwej celowości wynika jednak, że działania są prowadzone z pełną świadomością ich celu, ich końcowego wyniku; rzeczywiście istnieje już koncepcja przyszłego celu i ona to wpływa na aktualne działanie. Odnosi się to do prymitywnych działań życia codziennego, a również do najwyższych osiągnięć ludzkiego intelektu w nauce i technice.*

Z treści przytoczonego tekstu jednoznacznie wynika, że istota porozumiewania się zwierząt to nie jest bynajmniej proces informacyjny, lecz tylko fizyczne pobudzanie do wcześniej zapamiętanych zachowań, kojarzących się z konkretną formą określonego pobudzania, co można interpretować jako zjawisko stanowiące następstwo „naturalnej tresury gatunkowej", ukierunkowanej na trwanie w określonych środowiskach.

Informacyjny – człon kontekstowy nazwy, oznaczający rzeczy, stany, procesy i zjawiska związane z informacją i informowaniem,

gdzie:

- „informacyjny" – *definiendum*,

[123] L. von Bertalanffy, „Ogólna teoria systemów (Podstawy, rozwój, zastosowania)", PWN, Warszawa 1984, s. 299-300

- „człon kontekstowy nazwy,
  oznaczający rzeczy, procesy i zjawiska związane z informacją i informowaniem" – *definiens,*
- „człon kontekstowy nazwy" – *genus proximum,*
- „oznaczający rzeczy, procesy i zjawiska
  związane z informacją i informowaniem" – *differentia specifica.*

Tresura naturalna – gatunkowe naśladownictwo w świecie zwierząt, powodowane warunkami istnienia w określonych środowiskach,

gdzie:

- „tresura naturalna" – *definiendum,*
- „gatunkowe naśladownictwo w świecie zwierząt,
  powodowane warunkami istnienia w określonych środowiskach" – *definiens,*
- „gatunkowe naśladownictwo w świecie zwierząt" – *genus proximum,*
- „powodowane warunkami istnienia w określonych środowiskach" – *differentia specifica.*

Tresura sztuczna – ludzkie działanie, świadomie ukierunkowane na przyzwyczajanie zwierząt do wykonywania określonych czynności,

gdzie:

- „tresura sztuczna" – *definiendum,*
- „ludzkie działanie, świadomie ukierunkowane na przyzwyczajanie zwierząt
  do wykonywania określonych czynności" – *definiens,*
- „ludzkie działanie" – *genus proximum,*
- „świadomie ukierunkowane na przyzwyczajanie zwierząt
  do wykonywania określonych czynnośc" – *differentia specifica.*

1.1.2. Funkcje informacji w działaniach celowych

Egzystencjalną sferę człowieka można interpretować jako zbiór wszelkich wpływów (materialnych i niematerialnych), które kształtują jego warunki bytu w istniejącym i rozwijającym się otoczeniu. Aktywności ludzkie, tak jednostkowe jak i zbiorowe, sprowadzają się zawsze do wytwarzania stanów, które – w zespoleniu z określonymi elementami otoczenia – mają sprzyjać tworzeniu się następstw pożądanych z punktu widzenia danego decydenta. Wynika z tego, że świadomie kształtowana aktywność ludzka jest następstwem niekończącego się pasma podejmowania decyzji o działaniu i zachowaniach własnych oraz o działaniu i zachowaniach innych.

Czym jest zatem decyzja?

W literaturze związanej z prakseologią oraz z teorią organizacji i zarządzania, jak również w normatywach leksykalnych związanych z tym przedmiotem, wymienia się, ze względu na określone cechy rozstrzygalności, wiele rodzajów decyzji. Wśród nich do najczęściej spotykanych daje się zaobserwować następujące wyróżnienia, jak chociażby:

A. W *Leksykonie zarządzania*[124]:

(1) ze względu na horyzont czasowy, w jakim się ujawniają skutki decyzji:
- decyzje strategiczne,
- decyzje taktyczne,
- decyzje operacyjne;

(2) ze względu na stanowisko, na których są podejmowane decyzje:
- decyzje kierownicze,
- decyzje niekierownicze;

(3) ze względu na wielkość luki informacyjnej:
- decyzje pewne,
- decyzje ryzykowne,
- decyzje niepewne;

(4) ze względu na nowość problemu decyzyjnego:
- decyzje programowane (powtarzalne),
- decyzje nieprogramowalne (podejmowane po raz pierwszy);

(5) ze względu na stopień opisania problemu decyzyjnego:
- decyzje dobrze ustrukturalizowane,
- decyzje słabo ustrukturalizowane;

(6) ze względu na stopień złożoności problemu decyzyjnego:
- decyzje proste,
- decyzje złożone;

(7) ze względu na wynik decyzji i sposób postępowania decydenta:
- decyzje racjonalne,
- decyzje nieracjonalne.

B. W *Encyklopedii organizacji i zarządzania*[125] podaje się, że w literaturze poświęconej problematyce decyzji jej istota jest tłumaczona w dwojakiego rodzaju kategoriach – (1) rezultatowej i (2) czynnościowej, gdzie:

---

[124] „Leksykon zarządzania", Difin, Warszawa 2004 r., s. 91-92.

(1) W aspekcie **rezultatowym** rozumiana jest jako akt wyboru celu lub sposobu działania, pożądanych z punktu widzenia systemu, w ramach którego wybór ten jest dokonywany, przy czym aktowi wyboru są stawiane lub nie określone wymagania. W konsekwencji do klasy pojęciowej „decyzja" zaliczane są wszystkie akty wyboru albo tylko niektóre z nich, np. jedynie takie, które są uświadomione przez podejmującego decyzję lub wyłącznie te, które opierają się na zracjonalizowanych w pewien sposób kryteriach, tj. akty wyboru nielosowe albo dokonywane tylko spośród dostępnych dla podejmującego decyzję celów lub sposobów działania. Niezależnie od różnic istotą takiego tłumaczenia pojęcia „decyzja" jest skupienie uwagi na rezultacie określonego ciągu zdarzeń lub czynności doprowadzających do aktu wyboru przyszłego działania.

(2) W aspekcie **czynnościowym** decyzja rozumiana jest jako szczególnego rodzaju aktywność ludzi, wyrażająca się w poszukiwaniu takich rozwiązań pojawiających się problemów, które mogą zapewnić realizację zamierzonych celów systemu.

Dalej Autorzy *Encyklopedii organizacji i zarządzania* wyjaśniają, że z punktu widzenia różnych kryteriów, wyróżnia się:

(1) ze względu na kryterium podstawowe:
   - decyzje kierownicze,
   - decyzje niekierownicze;

(2) ze względu na kryterium rozwoju czynności, których one dotyczą:
   - decyzje wynikające z porządku dziennego zajęć,
   - decyzje badawcze,
   - decyzje alokacyjne,
   - decyzje wykonawcze,
   - decyzje oceniające;

(3) ze względu na miejsce w hierarchii organizacyjnej:
   - decyzje scentralizowane,
   - decyzje zdecentralizowane;

(4) ze względu na długość horyzontu czasowego:
   - decyzje bieżące,

---

[125] „Encyklopedia organizacji i zarządzani", PWE, Warszawa 1982 r., s. 87-89.

- decyzje perspektywiczne;

(5) ze względu na stopień pewności sytuacji decyzyjnej:

- decyzje ryzykowne,
- decyzje niepewne;

(6) ze względu na formy decydowania:

- decyzje indywidualne,
- decyzje kolegialne,
- decyzje kolektywne;

(7) ze względu na rodzaj problemów:

- decyzje strategiczne,
- decyzje taktyczne,
- decyzje operacyjne.

C. W *Małej encyklopedii prakseologii i teorii organizacji*[126] termin „decyzja" jest interpretowany jako:

- czyn wewnętrzny będący wolnym wyborem jednego z możliwych przyszłych zachowań się,
- wynik będący przetwarzaniem zamiarów w cele,
- wybór jednego działania z pewnej ilości działań możliwych w danym momencie,
- wybór jednego działania z pewnej ilości działań, które wydają nam się możliwe w danym momencie lub świadome powstrzymywanie się od wyboru – co także jest wyborem.

Ponadto wymieniane są:

- decyzje skrępowane, kiedy wybór jest ograniczony do jednego wyjścia lub go odrzucenia,
- decyzje personalne, które dotyczą przyjęcia do pracy, awansów, nagród, kar itp.,
- decyzje podejmowane w skomplikowanych warunkach.

D. Henri Fayol w książce *Administracja przemysłowa i ogólna*[127] wyróżnia decyzje związane z realizacją funkcji:

- przewidywania i planowania,

---

[126] „Mała encyklopedia prakseologii i teorii organizacji", Zakład Narodowy im. Ossolińskich, Wrocław .Warszawa Kraków Gdańsk· 1978, s. 44-45.

[127] H. Fayol, „Administracja przemysłowa i ogólna", Poznań 1947, s. 37.

- organizowania,
- rozkazywania,
- koordynowania,
- kontrolowania.

E. Jan Zieleniewski w książce *Organizacja i zarządzanie* wymienia[128]:

- zespołowe decyzje kierownicze,
- jednoosobowe decyzje kierownicze,
- decyzje zbiorowe typu parlamentarnego,
- decyzje kolegialne.

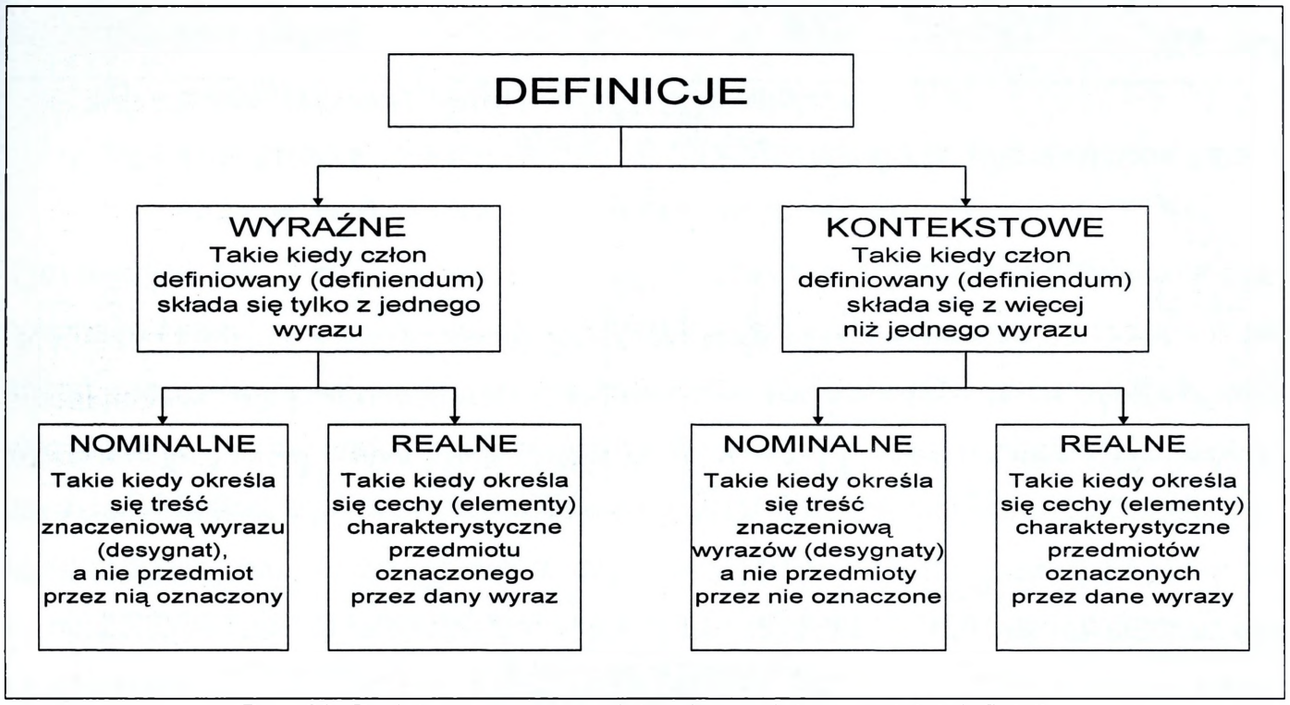
F. Jerzy Supernat w książce *Techniki decyzyjne i organizatorskie (wydanie 2)* wymienia natomiast aż ponad 30 rodzajów różnych typów decyzji, które systematyzuje w 10 grupach ze względu na kryteria dotyczące[129]:

(1) struktury podmiotu podejmującego decyzję,
(2) okoliczności podejmowania decyzji,
(3) kontekstu decyzyjnego,
(4) norm postępowania przy podejmowaniu decyzji,
(5) rodzaju rozwiązywanych problemów,
(6) wiedzy posiadanej przez decydującego,
(7) zmienności sytuacji decyzyjnej,
(8) stopnia trudności wynikającego z sytuacji decyzyjnej,
(9) typu wyniku uzyskanego w następstwie podjętej decyzji,
(10) horyzontu czasowego.

Podobne przykłady można przytaczać dalej. Niemniej jednak i te wystarczą już chyba do przekonania Czytelnika, że złożoność i powszechność decydowania powoduje, iż w międzyludzkich relacjach wszelkiego oddziaływania, zachowującego znamiona kierowania, można zawsze znaleźć jakieś nowe kryteria i według nich dokonywać nowych kategoryzacji, chociażby na użytek jakiejś grupy czy środowiska lokalnego. Dlatego też zbiór możliwych do wyróżniania typów decyzji należy uznawać za ciągle otwarty – a nade wszystko definiowanych kontekstowo. Konfrontując to z terminologią i zasadami podziału stosowanymi w logice można powiedzieć, że wymienione wcześnie definicje decyzji należą do grupy: bądź to **wyraźnych nominalnych**, bądź to **kontekstowych nominalnych** i **kontekstowych realnych** (rys 32).

[128] J. Zieleniewski, „Organizacja i zarządzanie (wydanie III)", PWN, Warszawa 1969, s. 475-477;
[129] J. Supernat, „Techniki decyzyjne i organizatorskie (wydanie 2)", Limited, Kolonia 2003 r., s. 20-27.

Brak jest natomiast definicji decyzji **wyraźnie realnej**, określającej cechy (elementy) charakterystyczne przedmiotu oznaczonego tym terminem[130], co w przedmiotowej sprawie, wynikającej z tytułu niniejszego podrozdziału, jest niezbędnie konieczne do przejrzystego naświetlenia funkcji informacyjnych spełnianych w procesach decyzyjnych.



Rys. 32. Podstawowe nazewnictwo i zasadniczy podział definicji
(wg terminologii stosowanej w logice)

Źródło: Opracowanie autorskie na podstawie: W. Marciszewski (redakcja), T. Kotarbiński (konsultacja), „Mała encyklopedia logiki", Zakład Narodowy im. Ossolińskich, Wrocław – Warszawa – Kraków 1970, s. 38-44; M. Omyła, „Zarys logiki", Wydawnictwa Szkolne i Pedagogiczne, Warszawa 1995, s. 102-104; S.J. Sokołowski, „Logika w dowodzeniu i kierowaniu", Wydawnictwo MON, Warszawa 1972, s. 92-95.

Dlatego też proponuje się aby tego rodzaju decyzję (decyzję wyraźnie realną) interpretować:

Decyzja – postanowienie lub rozstrzygnięcie, zawierające zbiór dezyderatów i ustaleń zmierzających do osiągnięcia owego postanowienia lub rozstrzygnięcia,

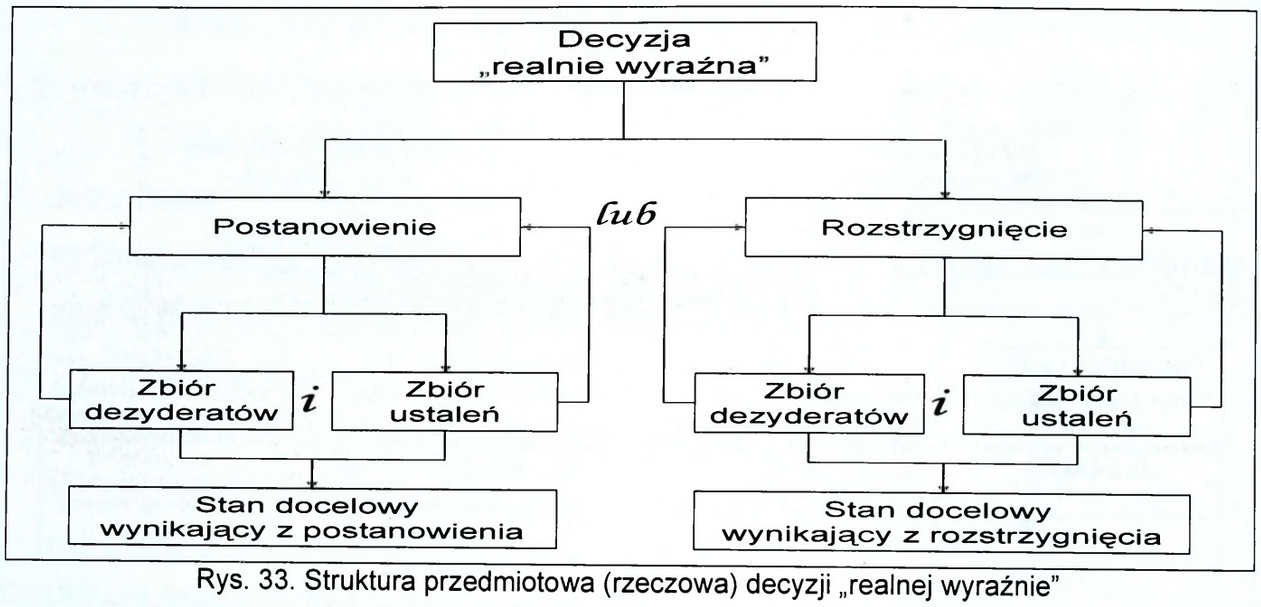
gdzie:

- „decyzja" – *definiendum,*
- „postanowienie lub rozstrzygnięci, zawierające zbiór dezyderatów i ustaleń zmierzających do osiągnięcia owego postanowienia lub rozstrzygnięcia" – *definiens,*
- „postanowienie lub rozstrzygnięcie" – *genus proximum,*

[130] W „Encyklopedii organizacji i zarządzania", PWE, Warszawa 1982, s. 87, zaraz po wyrazie „decyzja", są
w nawisie użyte terminy „postanowienie", „rozstrzygnięcie", co można w aspekcie „realności wyraźnej" odczytywać jako element definiens'u ale tylko odnoszący się do genus proximum. Brak jest natomiast wyjaśnienia odnoszącego się do cech różnicujących, czyli do differentia specifica.

- „zawierające zbiór dezyderatów i ustaleń zmierzających do osiągnięcia owego postanowienia lub rozstrzygnięcia" – *differentia specifica.*

gdzie strukturę przedmiotową (rzeczową) stanowią postanowienia lub rozstrzygnięcia przejawiające się pod postacią odpowiednio dobranych zbiorów dezyderatów i ustaleń, których realizacja zapewni osiągnięcie owego postanowienia lub rozstrzygnięcia (rys. 33).



Rys. 33. Struktura przedmiotowa (rzeczowa) decyzji „realnej wyraźnie"

Źródło: Opracowanie autorskie

W tym miejscu należy jednak dodać, że dezyderaty i ustalenia, jako strukturalne elementy decyzji „realnie wyraźnej", są zawsze określonymi alternatywami lub podzbiorami alternatów, które w procesie wypracowywania decyzji zostały wybrane ze zbioru alternatyw dopuszczalnych i według przekonań decydenta są najbardziej dostosowane do potrzeb wynikających z realizacji określonych dążeń ukierunkowanych na osiągnięcie wytyczonego wcześniej celu. Wynika z tego, że wartość jakościowa każdej decyzji objawia się zawsze przez pryzmat trafności doboru określonych dezyderatów i ustaleń do celu działań oraz stanu materialnego istniejącego w przestrzeni pola operacyjnego i stanu materialnego istniejącego w przestrzeni operatora podejmującego określone działanie. Każde zatem decydowanie jest wyborem określonego wariantu działania, a w rozumieniu rzeczowym (realnie wyraźnym) – – postanowieniem lub rozstrzygnięciem zawierającym zbiór owych dezyderatów i ustaleń będących następstwem wyboru określonego działania.

W praktyce zarządczej tak się zdarza, że podejmowane decyzje są często nadmiernie determinowane celami zbytnio oderwanymi od rzeczywistości istniejącej w przestrzeni materialnej pola operacyjnego i w przestrzeni materialnej operatora.

Oznacza to, że nie wszyscy decydenci zdają sobie sprawę, iż cel działania nie jest bynajmniej zmienną niezależną, ale zmienną zależną, co w największym uogólnieniu można wyrazić następującą funkcją:

$$C = f(M_1, M_2)$$

gdzie:

C – cel działania,

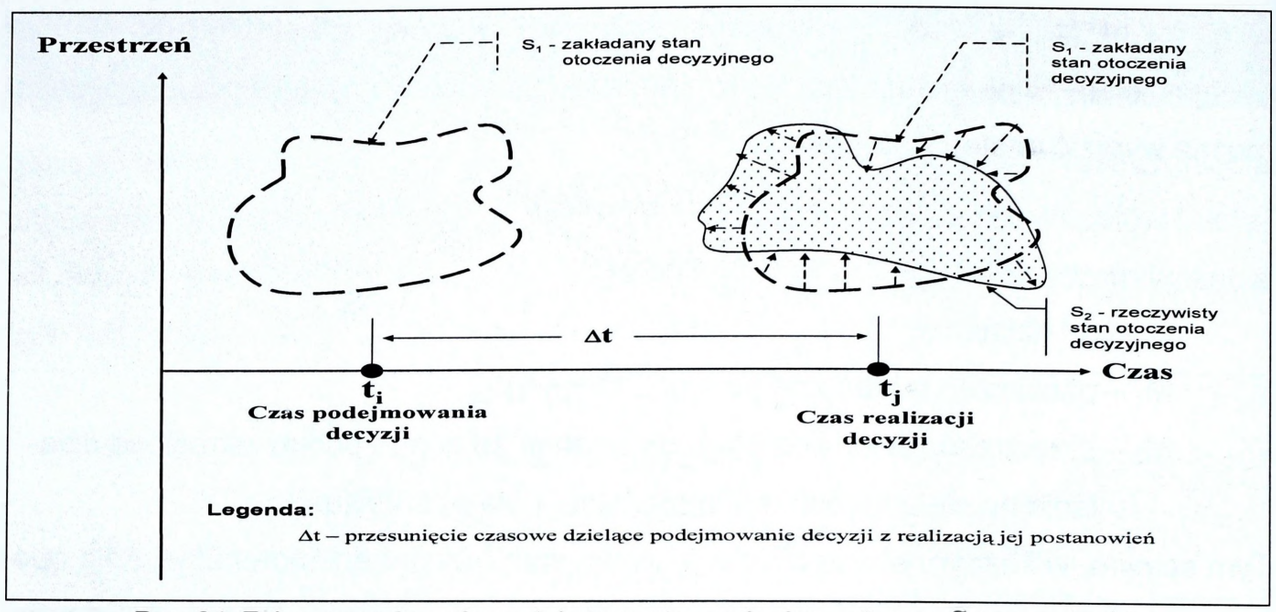
M_1 – przestrzeń materialna pola operacyjnego,

M_2 – przestrzeń materialna operatora zamierzającego podjąć określone działanie na ciele przestrzeni materialnej pola operacyjnego.

Tym samym, w każdym otoczeniu decyzyjnym stan przestrzeni materialnej pola operacyjnego i stan przestrzeni materialnej potencjalnego operatora stanowią sobą przestrzeń problemową determinującą wyznaczanie racjonalnych celów. Jakiekolwiek wychodzenie poza granice tejże przestrzeni powoduje zawsze negatywne następstwa decyzyjne objawiające się, bądź niemożliwością osiągnięcia wytyczonego celu, bądź osiągnięciem znacznie mniej tego co było możliwe do osiągnięcia. Problem ten komplikuje jeszcze dynamika czasoprzestrzennych zmienności sytuacyjnych występujących zarówno w przestrzeni pola operacyjnego, jak i w przestrzeni potencjalnego operatora. Oznaczając przez S_1 stan otoczenia decyzyjnego istniejący w czasie t_1 odpowiadającm wypracowywaniu decyzji, a przez S_2 stan otoczenia decyzyjnego występujący w czasie t_2 odpowiadającym realizacji decyzji, tak się zwykle zdarza, że w przedziale czasowym:

$$\Delta t = t_2 - t_1$$

następują mniejsze lub większe, ale zawsze pewne zmiany sytuacyjne powodowane różnymi czynnikami zewnętrznymi i wewnętrznymi (rys. 34).

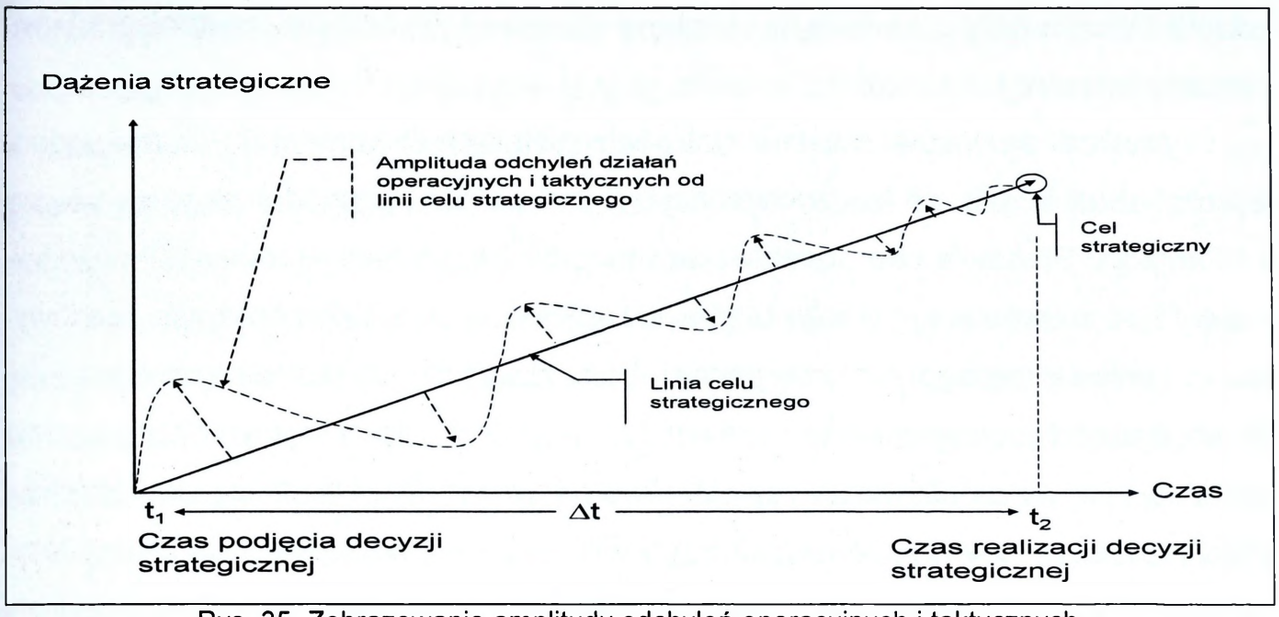


Rys. 34. Zobrazowanie zmienności stanu otoczenia decyzyjnego S w czasie Δt

Źródło: Opracowanie autorskie.

Można zatem powiedzieć, że istota ludzkich dążeń, objawiająca się przez pryzmat podejmowanych decyzji jest tym mniej dokładna im większy jest przedział czasowy Δt, dzielący czas podejmowania decyzji od czasu wdrażania w życie wynikających z tej decyzji postanowień lub rozstrzygnięć. Szczególnie daje się to dostrzegać przez pryzmat „amplitudy odchyleń" w strategicznym przedziale czasowym Δt. Mieszczące się w nim działania operacyjne i taktyczne muszą zatem podlegać ciągłemu monitorowaniu i korygowaniu aby, w miarę zbliżania się do strategicznego miejsca celu, amplituda ich odchyleń od strategicznej linii celu była jak najmniejsza i zachowywała przy tym jakoby cechy „fali gasnącej"[131] co jest bezpośrednio związane z częstotliwością dokonywania korekt, a pośrednio – ze stopniem dokładności i terminowością śledzenia zmian sytuacyjnych zachodzących w rzeczywistym otoczeniu decyzyjnym, które występują w czasie realizacji określonych postanowień i rozstrzygnięć decyzyjnych, a które pierwotnie (w czasie podejmowania decyzji) postrzegano w nieco innym kształcie merytorycznym jako odniesienie decyzyjne (rys. 35). W tym właśnie obszarze informacja wnosi wartości trudne do przecenienia.

[131] Termin używany w elektronice.



Rys. 35. Zobrazowanie amplitudy odchyleń operacyjnych i taktycznych od w strategicznej linii celu

Źródło: Opracowanie autorskie.

W następstwie różnych zastosowań i rozwiązań umożliwia monitorowanie i korygowanie bieżących stanów sytuacyjnych. Pozwala wykrywać i oceniać rodzące się zagrożenia i niebezpieczeństwa wynikające z pierwotnie powziętych decyzji. Można powiedzieć, że wkroczenie informacji w egzystencjalną sferę człowieka wyszło tym dążeniom naprzeciw. Spowodowało diametralne zmiany w antecedentnym[132] postrzeganiu przez człowieka dynamiki i prawidłowości zmian zachodzących w jego otoczeniu i w warunkach życia. Tym samym umożliwiło mu lepsze dostosowywanie się do nich, dzięki trafniej dobieranym antycypacjom[133].

Zastosowanie nowych wdrożeń technicznych i organizacyjnych w dużym zakresie przyczyniły się do pokonania istniejących wcześniej barier czasowych i dostępności informacyjnej. Umożliwiły szybsze i dokładniejsze identyfikowanie stanów otoczenia we wszystkich sferach aktywnego życia i tym samym stworzyły sprzyjające okoliczności do podejmowanie trafniejszych decyzji ukierunkowanych na bezpieczniejsze dostosowywanie się do funkcjonowania w zmieniającej się rzeczywistości. Umożliwiły stworzenie doskonałych narzędzi pracy i wkroczenie w wysoce wyspecjalizowane procedury operacyjne. Otworzyły szeroko drzwi dostępu do światowej wiedzy i personalnej komunikacji. Zracjonalizowały administrację i udoskonaliły zarzą-

[132] Antecedencje – okoliczności, zdarzenia poprzedzające jakiś fakt, co poprzedzało stan obecny („Słownik języka polskiego, PWN, Warszawa 1978, tom I, s. 59).

[133] Antycypacja – przedwczesne wystąpienie fazy jakiegoś procesu; przedwczesne realizowanie czegoś; wyprzedzenie („Słownik języka polskiego, PWN, Warszawa 1978, tom I, s.62). W prakseologii – wykonanie czegoś wcześniej co będzie potrzebne w przyszłości, ale wtedy nie będzie możliwości wykonania tego (przypis autorski).

dzanie. Wprowadziły człowieka, w nieznane mu wcześniej środowisko *społeczeństwa wiedzy i informacji*.

Analiza procesów rozwojowych najsilniejszych gospodarek świata jednoznacznie potwierdza, że kluczowymi czynnikami wzrostu gospodarczego są wiedza i informacja. Stanowią one podstawową bazę dla badań oraz kreowania innowacyjności i utrzymywania wysokiego tempa rozwojowego, przy jednoczesnym zachowywaniu konkurencyjnego poziomu jakości. W środowisku tym jest jeszcze istotne to, że *społeczeństwo wiedzy i informacji* nie pozostawia nikogo obojętnym. Zwykli ludzie dowiadują się o nowych możliwościach stylu pracy, rozwoju i wypoczynku. Intelektualiści i ludzie nastawieni poznawczo odkrywają szansę przezwyciężenia izolacji terytorialnej i zaściankowości. Politycy i menedżerowie, obawiając się rozgłosu i utraty zajmowanych pozycji, stają się bardziej wstrzemięźliwymi w poczynaniach wykraczających poza etyczne ramy przysługującego im statusu. W aspekcie społecznym jest jeszcze bardzo istotne to, że w środowisku tym występują samoistne, a nie narzucane z góry, przesłanki do korzystnych zmian w stylu życia. Szerokie możliwości usługowe stwarzają ludziom warunki do racjonalnego gospodarowania czasem, a rozwój współpracy międzynarodowej i wymiana informacji stwarzają okoliczności do kształtowania wspólnot i zacierania konfliktogennych różnic kulturowych i narodowościowych.

Patrząc optymistycznie, można przypuszczać, że w niedalekiej przyszłości zwiększy się wolność ludzkich wyborów, a człowiek zostanie w znacznej mierze „uwolniony" od przymusu pracy. Tym samym wystąpi nadmiar czasu wolnego, co będzie sprzyjało nieskrępowanemu rozwijaniu się ludzkich osobowości. Prawdopodobnie, w coraz większym tempie postępować będzie rozwój technologiczny i gospodarczy. Techniki informacyjne będą intensywnie wspierały biznes i gospodarstwa domowe. Uzewnętrzni się powszechność wykorzystywania systemów informatycznych i znacznie wzrośnie nacisk na edukację. Postęp stanie się jednostkowym i społecznym sukcesem człowieka, który przełoży się na zyski finansowe i niwelację nieporozumień, co spowoduje większe poczucie sensu aktywnego uczestniczenia w życiu społecznym i wzrost odpowiedzialność jednostki za kształtowanie dobrobytu ogólnego.

Patrząc mniej optymistycznie, chociażby przez pryzmat obecnej sytuacji kształtującej się w demokracji amerykańskiej (w USA), można zakładać, że zaawansowane techniki informacyjne będą coraz bardziej wiązane z kapitałem, produkcją

i komercją. Przemysł informacyjny może wzrastać znacznie szybciej niż dochód narodowy brutto. Techniki informacyjne znajdą szerokie zastosowanie w automatyzacji, w pracach biurowych, szkole i we wspomaganiu decyzji. Może jednak nastąpić regres w ochronie prywatności. Może się zmniejszyć udział rządów w kształtowaniu sytuacji rynkowych i egzystencjalnych człowieka.

Nie ulega wątpliwości że nowe technologie informacyjne niosą ze sobą poprawę życia. Szybki transport i nowoczesna telekomunikacja redukują bariery czasu i odległości. Zbliżają do siebie ludzi w skali globalnej i tym samym przyczyniają się do eliminowania wielu zagrożeń wynikających z niewiedzy i izolacjonizmu.

Generowana nowymi technologiami egzystencjalna rzeczywistość, mimo wielu niewątpliwych zalet, niesie z sobą również i potencjalne zagrożenia, jak chociażby dla kultur i tożsamości narodowych. Może też wpływać destrukcyjnie na spełnianie integrujących ról społecznych i środowiskowych przypisywanych tradycyjnie do państwa, kościoła, rodziny, szkoły, partii politycznych, zakładów pracy itp. Sprzyjać może tworzeniu się nowych form przestępczości i autorytaryzmu. Może też powodować ograniczanie prywatności i stwarzanie przesłanek do podejmowania negatywnych kooperacji w sferze informacyjnej, objawiających się generowaniem wirtualnych stanów otoczenia, trudnych do odróżnienia od rzeczywistości. Narzędzia te, opanowane przez niecne środowiska, mogą być wykorzystywane do manipulowania nastrojami oraz wytwarzania atmosfery zastraszenia i podtrzymywania rządów totalitarnych.

Bardzo refleksyjne, co do tego, zdają się być futurystyczne dywagacje George'a Orwell'a opublikowane w 1949 roku w powieści pod tytułem *Rok 1984*, gdzie autor przez pryzmat rządów „wielkiego brata" pesymistycznie szkicuje wizję przyszłości w roku 1984[134]. Akcentuje, że w następstwie zachodzących zmian w postępie technologicznym wzrośnie kryzys gospodarczy. Nasili się częstotliwość aktów terrorystycznych i gwałtownie rozszerzy się epidemia nowych chorób. Czynniki te spowodują społeczną akceptację dla rządów centralnych i autorytarnych. Ustanowione zostaną systemy polityczne oparte na wzmożonej dyscyplinie i inwigilacji. Pojawi się cenzura rządowa i ingerencja w prywatność życia obywateli. Kontroli podlegać będzie przemysł informacyjny. Techniki te (informacyjne) znajda zastosowanie głownie w biznesie i sprawowaniu władzy, natomiast nastąpi ich wyraźny regres w zastoso-

[134] G. Orwell, „Rok 1984", KIW, Warszawa 1988 r. (tłumaczenie polskie). Oryginał powieści ukazał się w języku angielskim w 1949 roku (rok przed śmiercią autora), a pierwsze wydanie polskie ukazało się w 1953 roku.

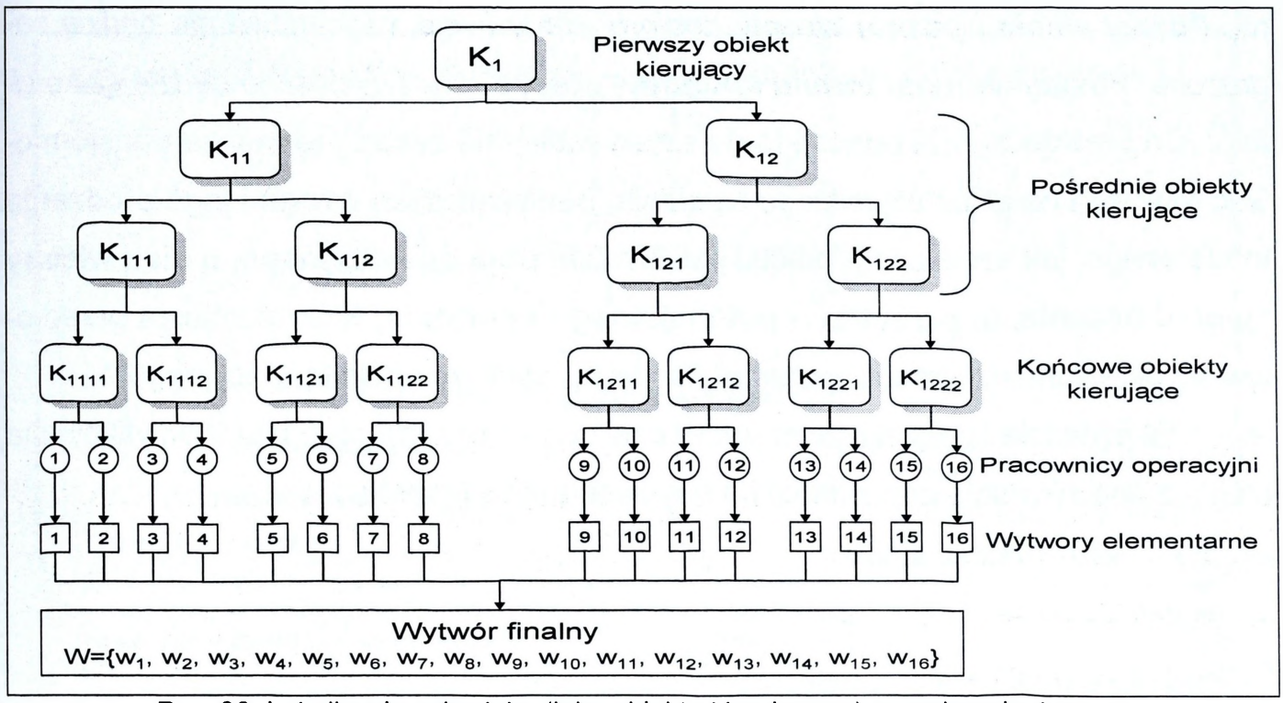
waniach indywidualnych. Ukształtuje się ostry podział pomiędzy posiadającymi i nieposiadającymi informacje. Większość obywateli będzie biernie nastawiona na wszelkie naruszenia prywatności, prezentując ksenofobiczną postawę ratowania „własnej skóry". Jednocześnie komputerowi hakerzy utworzą ruch wyrażający wzrastające niezadowolenie społeczne, co w efekcie doprowadzi do kolejnej rewolucji.

Oczywiście katastroficzna wizja przyszłości symbolicznego roku „1984" nie sprawdziła się. Niemniej jednak niektóre elementy zaistniały i rozwijają się. Można tu wymienić terroryzm, AIDS, inwigilację, postępujące ograniczanie prywatności i nadużycia informacyjne, których najgroźniejszym przejawem stała się walka informacyjna. Specjaliści z Pentagonu wyrażają się nawet, że ta forma zagrożenia, postrzegana przez pryzmat skutków, może być substytutem następstw zaistniałych podczas ataku japońskiego na Pearl Harbor. Zakładają nawet, że 30 komputerowych wirtuozów rozmieszczonych w różnych częściach świata, z budżetem około 10 mln. dolarów, mogłoby rzucić USA na kolana. Ten scenariusz stawia państwa wysokich technologii w obliczu nowego i bardzo realnego zagrożenia, a do tego jeszcze niezmiernie trudnego do wcześniejszego neutralizowania, ponieważ przeciwnikiem może być nie tylko państwo czy koalicja, ale również organizacja terrorystyczna czy zorganizowany gang kryminalny.

Co się zaś tyczy bezpośrednio funkcji informacyjnych spełnianych w procesach decyzyjnych, to rozpocząć trzeba, że obiektem kierującym, we wszelkich układach *względnie odosobnionych*[135] postrzeganych w aspekcie prakseologicznym, jest zawsze człowiek jako sprawca impulsu wywołującego określoną reakcję obiektu kierowanego. Jego funkcja kierownicza może być lokowana w różnych miejscach tego układu. Jest jednak regułą, że zawsze będzie na wejściu, ale oprócz tego może być też lokowana i w różnych miejscach jego wnętrza. Dlatego też tak usytuowanego człowieka, w prakseologicznym modelu (układzie) działania celowego, należy postrzegać jako: pierwotny obiekt kierujący, pośredni obiekt kierujący (różnych szczebli) i końcowy obiekt kierujący (rys. 36).

---

[135] Układ względnie odosobniony to: *(...) wszelki i tylko taki układ, który posiada obie poniższe własności:*
(1) reszta Wszechświata działa na nasz układ, ale oddziaływanie odbywa się tylko na pewnych, że tak powiem, „drogach", zwanych „wejściami" układu, (2) nasz układ wywiera wpływ na resztę Wszechświata, ale oddziaływanie to biegnie, że tak powiem, tylko pewnymi „drogami", mianowicie odbywa się za pośrednictwem „wyjść" naszego układu. (H. Greniewski, „Elementy cybernetyki sposobem niematematycznym wyłożone, PWE, Warszawa 1959, s. 11 i 12).



Rys. 36. Lokalizacja człowieka (jako obiektu kierującego) w prakseologicznym modelu (układzie) działania celowego

Źródło: Opracowanie autorskie.

Jak już wcześniej akcentowano, każda decyzja, pojmowana jako **wyraźnie realna**, to zawsze *określone postanowienie*[136] *lub rozstrzygnięcie*[137]*, zawierające zbiór dezyderatów*[138] *i ustaleń*[139] *ukierunkowanych na osiągnięcie owego postanowienia lub rozstrzygnięcia*. Trafność owych postanowień i rozstrzygnięć zależy od wielu czynników, ale nade wszystko od znajomości, przez decydującego, stanu otoczenia decyzyjnego, w którym kluczowe miejsce zajmuje *przestrzeń materialna pola operacyjnego i przestrzeń materialna potencjalnego operatora*[140]. Problematykę tę podobnie postrzegał, już XXVII wieków temu (544-496 p.n.e.), jeden z największych starożytnych myślicieli Dalekiego Wschodu, Sun Zi (można by nawet powiedzieć najstarszy prakseolog świata[141]) wyrażając intencje swoich myśli następującymi słowa-

---

[136] Postanowienie – rozporządzenie, zarządzenie, uchwała, orzeczenie. Postanowić – powziąć jakąś decyzję; zdecydować o kimś, o czymś („Słownik języka polskiego", PWN, Warszawa 1992, tom II, s. 841).

[137] Rozstrzygać – rozważywszy coś, postanawiać, decydować o czymś; wpływać na coś w sposób decydujący, ostateczny, być czynnikiem, od którego coś zależy („Słownik języka polskiego", PWN, Warszawa 1992, tom III, s. 119).

[138] Dezyderat – wyraźnie określone żądanie („Słownik języka polskiego", PWN, Warszawa 1992, tom I, s. 391).

[139] Ustalić – rozstrzygnąć, zdecydować o czymś, wyznaczyć coś. Ustalić normy, prawidła, reguły („Słownik języka polskiego", PWN, Warszawa 1992, tom III, s. 624).

[140] W literaturze przedmiotu, a szczególnie w prakseologicznej (krajowej i zagranicznej), poświecono wiele miejsca czynnikom wpływającym na trafność podejmowania decyzji. Dlatego też w niniejszej publikacji nie przytacza się tych zapisów w brzmieniu dosłownym, a chociażby i z tego względu, że nie wszystkie korespondują z treścią wynikającą z tytułu monografii.

[141] Tadeusz Kotarbiński wyraża pogląd: „Powodów do ukucia terminu *prakseologia* nagromadziło się dość, odkąd ludzie zaczęli się zastanawiać nad sprawnością własnych działań i odkąd w Europie za-

mi: ***Poznaj siebie** i **poznaj wroga**, dopiero wtedy twoje zwycięstwo nie będzie zagrożone. **Poznaj warunki terenu** i **pogody**, wtedy twoje zwycięstwo będzie całkowite*[142]. Co prawda Sun Zi odnosił to do sztuki walki, ale zasadę tę można transformować również i na grunt wszelkiego działania, ponieważ **stan wroga** i jego **otoczenie** to nic innego, jak szczególna postać **przestrzeni pola operacyjnego**, a **stan własny** i **jego otoczenie**, to **przestrzeń potencjalnego operatora**, który zamierza przeprowadzić określone działanie (operację) na ciele przestrzeni pola operacyjnego.

W aspekcie informacyjnym, przestrzeń pola operacyjnego jest identyfikowana poprzez poszukiwanie odpowiedzi na trzy zasadnicze pytania:

- co? → identyfikacja stanu,
- gdzie? → identyfikacja miejsca,
- kiedy? → identyfikacja czasu.

Znając odpowiedzi na powyższe pytania można dopiero formułować stosowne co do tego postanowienia i rozstrzygnięcia decyzyjne w postaci odpowiednio uporządkowanych zbiorów dezyderatów i ustaleń, korespondujących merytorycznie z odpowiedziami na dwa kolejne pytania:

- czym? → wybór instrumentarium i operatorów;
- w jaki sposób? → wybór wariantu działania.

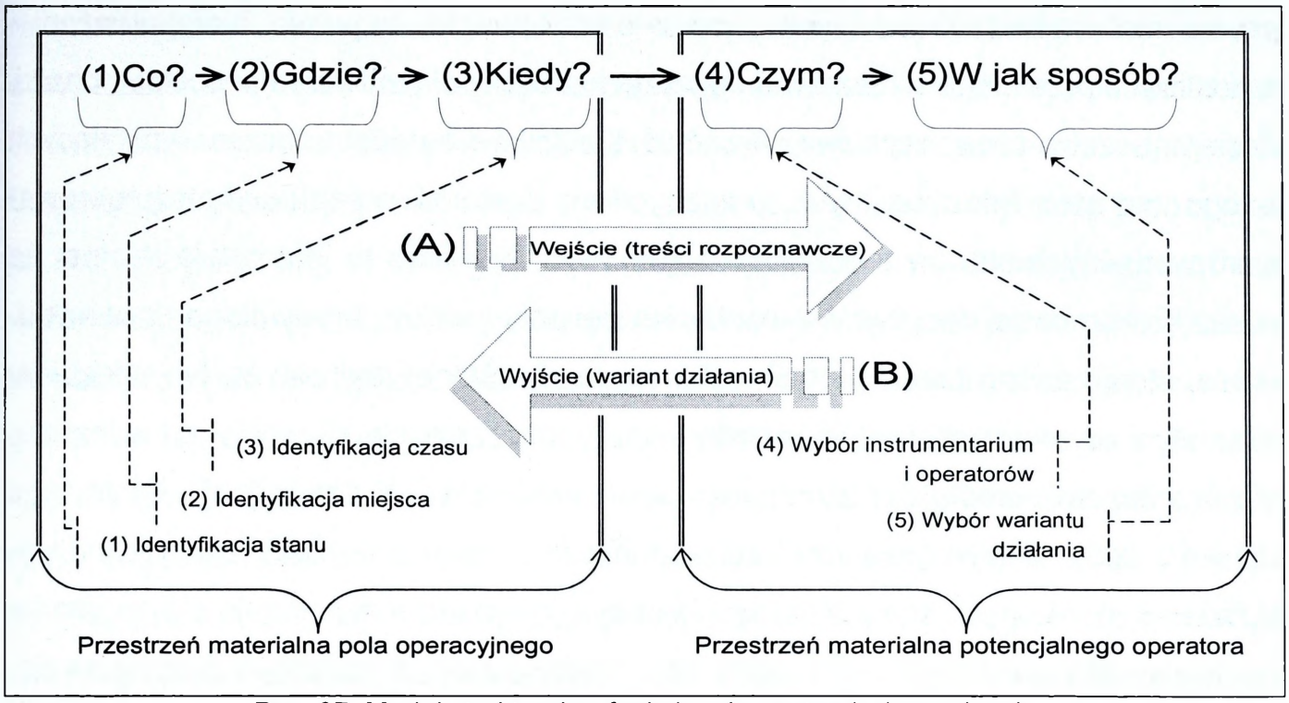
Zatem w aspekcie potrzeb odnoszących się do **treści rozpoznawczych** i **treści informacyjnych**, występujących w każdym otoczeniu decyzyjnym, model strukturalno-funkcjonalny tych potrzeb, jako *układ względnie odosobniony*[143], można wyrazić następującym zobrazowaniem (rys. 37).

---

domowił się zwyczaj sięgania po źródłosłowy greckie przy nadawaniu imion poszczególnym dyscyplinom badawczym. Nie wiem jednak o nikim, kto by miał użyć tego terminu przed rokiem 1890, kiedy to Alfred E s p i n a s na łamach *Revue Philosophique de la France et de l'Etranger* w artykule pt. *Les origines de la technologie* pisał co następuje: Kunszt jest bardziej zespołem reguł ustalonych niźli zbiorem inicjatyw wyrozumianych [...] Rzemieślnik majstruje, rolnik orze, marynarz żegluje, żołnierz walczy, kupiec handluje, profesor uczy, rządca administruje [...] Wszystko to mieści się w ramach reguł. A idzie tu nie o sztuki piękne, lecz o kunszty użyteczne. I otóż słowo *praktyka* nasuwa termi *prakseologia* dla oznaczenia nauki o faktach tego rodzaju rozważanych w ich całokształcie, nauki o formach najogólniejszych i zasadach najwyższych działania w świecie stworów żywych". [T. Kotarbiński, „Traktat o dobrej robocie (wydanie siódme)", Ossolineum, Wrocław – Warszwa – Kraków – Gdańsk – Łódź 1982, s. 332].

[142] Sun Zi, „Sztuka wojny (przekład K.A.M.)", Przedświt, Warszawa 1994, s. 8.

[143] „Mówiąc *układ względnie odosobniony* mamy na myśli wszelki i tylko taki układ, który posiada następujące właściwości: (1) reszta Wszechświata działa na nasz układ, ale oddziaływanie odbywa się tylko na pewnych powiem *drogach* zwanych *wyjściami* układu; (2) nasz układ wywiera wpływ na resztę Wszechświata, ale oddziaływanie to biegnie tylko pewnymi *drogami*, mianowicie odbywa się za pośrednictwem *wyjść* naszego układu". H. Greniewski, *Elementy cybernetyki sposobem niematematycznym wyłożone*, PWN, Warszawa 1959, s.11-12.



Rys. 37. Model strukturalno-funkcjonalny potrzeb decyzyjnych

Źródło: Opracowanie autorskie.

Treści[144] **rozpoznawcze** – treści recepcyjne i semantyczne, występujące w relacjach rozpoznawczych,

gdzie:

- „treści rozpoznawcze" – *definiendum,*
- „treści recepcyjne i semantyczne, występujące w relacjach rozpoznawczych" – *definiens,*
- „treści recepcyjne i semantyczne" – *genus proximum,*
- „występujące w relacjach rozpoznawczych" – *differentia specifica.*

Treści informacyjne – treści semantyczne, występujące w relacjach informacyjnych,

gdzie:

- „treści informacyjne" – *definiendum,*
- „treści semantyczne, występujące w relacjach informacyjnych" – *definiens,*
- „treści semantyczne" – *genus proximum,*
- „występujące w relacjach informacyjnych" – *differentia specifica.*

W procedurach pozyskiwania (zdobywania) *treści informacyjnych* i *treści rozpoznawczych,* a także w procedurach ich gromadzenia, opracowywania (przetwarzania), przechowywania i dystrybucji, obserwuje się coraz większy udział technik elektronicznych, a nade wszystko informatycznych. Wnosi to, bez wątpienia, pewien komfort i usprawnienia do żmudnej pracy analitycznej. Z drugiej zaś strony stwarza

[144] Treść – podstawowy, zasadniczy, najważniejszy element czegoś („Słownik języka polskiego", PWN, Warszawa 1981, tom III, s. 530).

pewne niebezpieczeństwa wynikające z kształtowania, zupełnie niepostrzeżenie, szkodliwych przekonań o niezawodnej wszechstronności i uniwersalności tej techniki. Zacierana jest w ten sposób wrażliwość użytkowników na postrzeganie wynikających z tego zagrożeń informacyjnych, mogących się materializować ukrytym generowaniem wirtualnych stanów otoczenia decyzyjnego. Zjawisko to jest o tyle istotne, że w każdym procesie decyzyjnym, osoby lub zespoły ludzkie, uprawnione do decydowania, stoją zawsze przed problemem wyboru określonej alternatywy lub podzbioru alternatyw ze zbioru alternatyw ich zdaniem dopuszczalnych. W praktyce i w literaturze przedmiotu określa się to mianem „wielowariantowości decyzyjnej". Istota tego wynika z faktu, o czym już wcześniej wspominano, że prawie nigdy aprioryczne wyobrażenia określonych stanów otoczenia decyzyjnego nie potwierdzają się aposteriorycznie w całej rozciągłości.[145] Można zatem powiedzieć, że wszelkie decyzje są podejmowane w warunkach **dysonansu poznawczego**. Złożoność tej problematyki i wynikające z tego następstwa jednoznacznie wyjaśnia Leon Festinger.[146] Stwierdza on: *(...) od czasu, a niekiedy nawet często zdarza się, że w naszej świadomości przejawia się rozbieżność czy sprzeczność miedzy przekonaniem, które w danym momencie akceptujemy, a jakimś innym przekonaniem, które w pewien sposób jest z nim sprzeczne. Ta rozbieżność czy sprzeczność, z którą związany jest stan napięcia, to nic innego jak właśnie* ***dysonans****, który jest przykry i którego chcemy się pozbyć, dążąc do jego redukcji, a tym samym do jego przeciwieństwa, jakim jest* ***konsonans***[147]. W kontekście powyższego wysuwa i udowadnia, licznymi badaniami, następującą hipotezę:[148]

(1) *Istnienie niewygodnego psychologicznie dysonansu motywuje osobę do prób jego zredukowania i osiągnięcia konsonansu*[149].

(2) *W sytuacji występowania dysonansu osoba będzie nie tylko próbowała go zredukować, ale będzie również w sposób aktywny unikała sytuacji oraz informacji, które mogłyby go zwiększyć.*

Uwzględniając powyższe i nie negując w najmniejszym stopniu ogromnych wartości wnoszonych przez elektronikę i informatykę do egzystencjalnej sfery współczesnego człowieka, a tym samy i do jego procedur decydowania, uwzględniać jed-

[145] Wróć do rys. 43 i przypisanego do niego tekstu.
[146] Dysonans poznawczy – sprzeczne ze sobą relacje w obrębie poznania (L. Festinger, „Teoria dysonansu poznawczego (A Theory of Cognitive Dissonance, wyd. 1957)", PWN, Warszawa 2007, s. 20).
[147] Ibidem, s. 13.
[148] Ibidem, s. 20-211 (s. 20 – hipoteza; dalsze strony – dowód).
[149] Konsonans – przeciwieństwo dysonansu (Ibidem, s. 13).

nak należy, że w następstwie podświadomego dążenia istoty ludzkiej do **konsonansów**, technika ta może również powodować, poprzez swoje wytwory, bardzo sugestywne, a zarazem i subiektywne wpływy na kształtowanie postanowień decyzyjnych. Sugestywność i subiektywność tego wynika z faktu, że wszelkie **wytwory** tego rodzaju technik powstają w następstwie przetwarzania **nie informacji**, ale **quasi-informacji**, która z natury rzeczy nie zawiera w swoim wnętrzu przedmiotowy treści **semantycznych**, ale tylko treści **energetyczne** (fizyczne), którym dopiero po programowo zaprojektowanej ekspozycji (tekst, obraz, wykres, zestawienie, wyliczenie itp.) przypisuje się wartości semantyczne – np. powszechnie stosowanym symulacjom. Sugestywność uzyskiwanych w ten sposób treści wynika z faktu, że tak elektronika, jak i maszyna cybernetyczna, mogą rejestrować i szybciej przetwarzać znacznie więcej danych niż mieści się to w możliwościach fizycznych człowieka. Z tej też przyczyn rodzi się często nieuzasadnione przekonanie, że ta przerasta człowieka. Rodzące się w ten sposób fascynacje doprowadzają często do deprecjonowania roli człowieka. Zdają się nie uwzględniać faktu, że są to tylko narzędzia, a ich twórcą jest właśnie On – Człowiek. Co się zaś tyczy niezawodności, to można przytaczać liczne katastrofy spowodowane niedoskonałością rozwiązań technicznych (elektronicznych i informatycznych), czemu można by poświęcić oddzielne opracowanie.

Odnosząc się do decyzji i decydowania, nie wyeksponowano jeszcze, że każda decyzja, rozumiana jako **wyraźnie realna** – zawierająca w sobie „rzeczy decyzyjne" wyrażone w formie postanowień lub rozstrzygnięć sformułowanych pod postacią konkretnych dezyderatów i ustaleń – to nic innego jak **zbiór wytworzonych informacji kierowniczych**, ukierunkowanych na uświadomienie podwładnym zakresu ich zadań związanych z osiąganiem określonego celu. Zbiory tych informacji mogą być przekazywane w ustawach, rozporządzeniach, zarządzeniach, dyrektywach, poleceniach, nakazach, zakazach, a w szczególnych przypadkach – w rozkazach. Nawiązując w tym kontekście do prakseologii, **za zasadnicze wskazanie dla decydentów, a nawet i za przedmiot badań dla naukowców zajmujących się problematyką zarządzania**, należy uznać wskazanie Tadeusza Kotarbińskiego wyrażone następującymi słowami: **„Chodzi o to, by człowiek ochoczo robił to, co robić musi, by tego, co robić musi, nie robił tylko dla tego, że musi; by w robieniu tego, co musi, znalazł upodobanie i dzięki temu pracę swą usprawnił wielokrotnie, oka-**

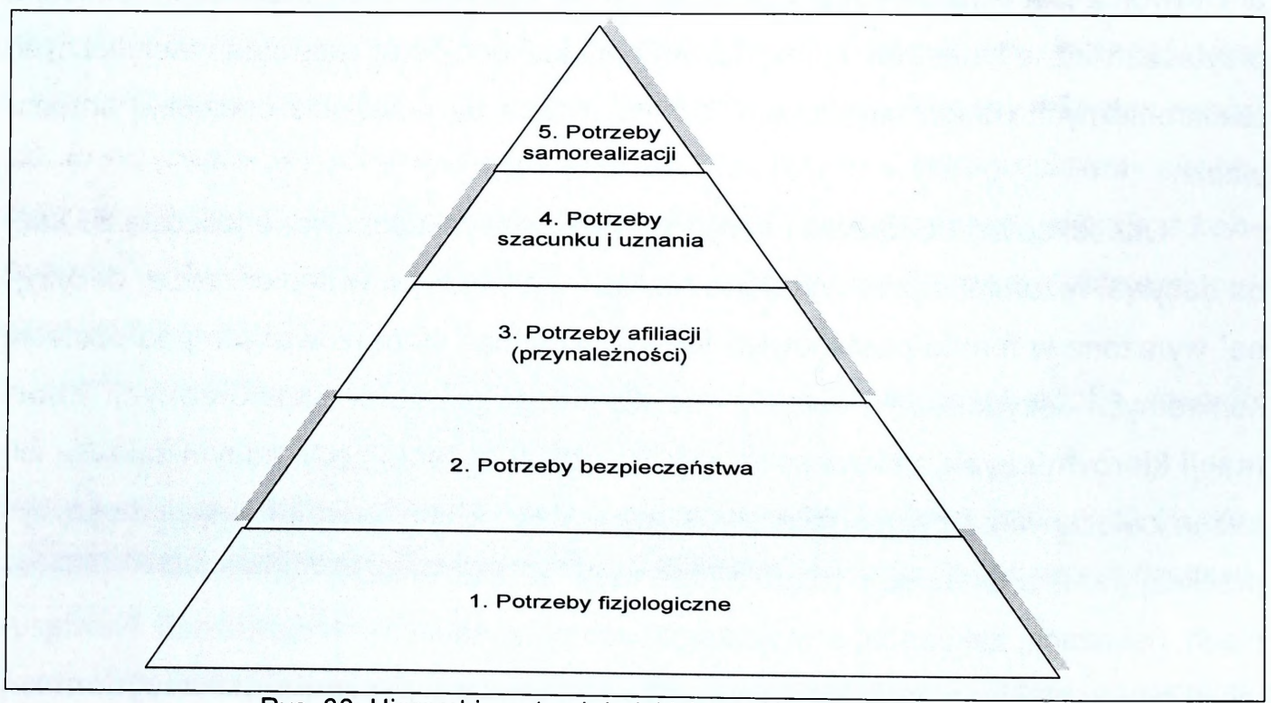
zując hojność w oddaniu się jej".[150] Oczywiście, że osiągnięcie tego dotyczy spełniania bardzo wielu i bardzo złożonych warunków. Tym samym, może to być wskazanie dla sceptyków wyrażających przekonania, że „zarządzanie" nie ma swojego przedmiotu poznania. Postrzegając najogólniej, a trafniej będzie – tylko poglądowo, można to skonstatować hierarchią potrzeb Abrahama Harolda Maslowa (rys. 38).

Co się zaś tyczy *zbioru wytwarzanych informacji kierowniczych* (informacji decyzyjnych), to ich wpływy organizacyjne należy postrzegać przez pryzmat „zasobów ludzkich".

Informacje decyzyjne – treści semantyczne wyrażone znakami językowymi, odzwierciedlające wolę decydenta w określonej sprawie,

gdzie:

- „informacje decyzyjne" – *definiendum,*
- „treści semantyczne wyrażone znakami językowymi, odzwierciedlające wolę decydenta w określonej sprawie" – *definiens,*
- „treści semantyczne wyrażone znakami językowymi" – *genus proximum,*
- „odzwierciedlające wolę decydenta w określonej sprawie" – *differentia specifica.*



Rys. 38. Hierarchia potrzeb ludzkich wg Abrahama Maslowa

Źródło: Opracowanie autorskie na podstawie: A. Maslow, „Motywacja i osobowość", PWN, Warszawa 2006, s. 115-119.

W literaturze przedmiotu zestawienie wyrazowe „zasoby ludzkie" jest różnie interpretowane. Zdarza się nawet, że w niektórych wydawnictwach (głównie star-

[150] T. Kotarbiński, „Traktat o dobrej robocie (wydanie siódme)", Ossolineum, Wrocław · Warszawa · Kraków · Gdańsk · Łódź 1982, s. 213.

szych i mniej autorytatywnych), a bardzo często w innych publikacjach (nagminnie w internetowych), ten kontekstowy termin jest definiowany przez pryzmat ludzkich zbiorowości, co jest semantycznie uwłaczające dla człowieka. Człowiek nie jest „zasobem", to znaczy *pewną ilością czegoś zebranego, nagromadzonego w celu wykorzystania w przyszłości*[151]. O skali rozpowszechniania błędnych interpretacji świadczyć też może fakt, że w „Wikipedii" przytacza się następujące wyjaśnienie: „Zasoby ludzkie (ang. *human resources*) – pojęcie mające dwojakie znaczenie. Pierwsze wywodzi się z nauk społecznych – głównie ekonomicznych – zgodnie z klasyczną szkołą ekonomii oznacza pracę (siłę roboczą) jako jeden z trzech środków produkcji. Drugie, bardziej powszechne, mieszczące się w zakresie zarządzania przedsiębiorstwem, odnosi się do indywidualnych pracowników oraz działu firmy, który zajmuje się rekrutacją, szkoleniem, motywowaniem oraz zwalnianiem pracowników (czyli polityką kadrową)"[152]. Wracając jednak do angielskiego źródłosłowu *human resources* wynika jednak, że ten oznacza, w tłumaczeniu dosłownym, *ludzkie bogactwo*, a w szerszym ujęciu kontekstowym – „bogactwo" człowieka objawiające się poprzez wszystko to co wypełnia jego wnętrze umysłowe, fizjologiczne i fizyczne.

Zasoby ludzkie – bogactwo człowieka, objawiające się przez wszystko co wypełnia jego wnętrze umysłowe, fizjologiczne i fizyczne,

gdzie:

- „zasoby ludzkie" – *definiendum*,
- „bogactwo człowieka, objawiające się przez wszystko co wypełnia jego wnętrze umysłowe, fizjologiczne i fizyczne" – *definiens*,
- „bogactwo człowieka" – *genus proximum*,
- „objawiające się przez wszystko co wypełnia jego wnętrze umysłowe, fizjologiczne i fizyczne" – *differentia specifica*.

W aspekcie powyższej definicji można dokonywać różnych detalizacji i wymieniać różne zasoby ludzkie. W aspekcie sprawy przedmiotowej, wynikającej z tytułu niniejszego podrozdziału i z przytoczonego wcześniej wskazania prakseologicznego, wynika jednak, że w tym kontekście należy nade wszystko uwzględniać zasoby: pojęciowe, intelektualne, mentalnościowe, umiejętnościowe i sprawnościowe.

Zasoby pojęciowe – zbiór myślowych odzwierciedleń, całościowych ujęć istotnych cech przedmiotów, rzeczy i zjawisk,

[151] Zasób – pewna ilość czegoś zebrana , nagromadzona w celu wykorzystania w przyszłości. („Słowni języka polskiego", PWN, Warszawa 1992, tom III, s. 960).
[152] http://pl.wikipedia.org/wiki/Zasoby_ludzkie (19.10.2009; godz. 01:25).

gdzie:

- „zasoby pojęciowe" – *definiendum,*
- „zbiór myślowych odzwierciedleń,
  całościowych ujęć istotnych cech przedmiotów, rzeczy i zjawisk" – *definiens,*
- „zbiór myślowych odzwierciedleń" – *genus proximum,*
- „całościowych ujęć istotnych cech przedmiotów, rzeczy i zjawisk" – *differentia specifica.*

Zasoby intelektualne – zbiór osobniczych predyspozycji umysłowych, dostosowanych do poznawania istoty bytu,

gdzie:

- „zasoby intelektualne" – *definiendum,*
- „zbiór osobniczych predyspozycji umysłowych,
  dostosowanych do poznawania istoty bytu" – *definiens,*
- „zbiór osobniczych predyspozycji umysłowych" – *genus proximum,*
- „dostosowanych do poznawania istoty bytu" – *differentia specifica.*

Zasoby mentalnościowe – zbiór swoistych sposobów osobniczego myślenia i ustosunkowywania się do rzeczywistości,

gdzie:

- „zasoby mentalnościowe" – *definiendum,*
- „zbiór swoistych sposobów osobniczego myślenia
  i ustosunkowywania się do rzeczywistości" – *definiens,*
- „zbiór swoistych sposobów osobniczego myślenia" – *genus proximum,*
- „i ustosunkowywania się do rzeczywistości" – *differentia specifica.*

Zasoby umiejętnościowe – zbiór predyspozycji osobniczych do transformowania wiedzy w praktyczne zastosowania,

gdzie:

- „zasoby umiejętnościowe" – *definiendum,*
- „zbiór predyspozycji osobniczych
  do transformowania wiedzy w praktyczne zastosowania" – *definiens,*
- „zbiór predyspozycji osobniczych" – *genus proximum,*
- „do transformowania wiedzy w praktyczne zastosowania" – *differentia specifica.*

Zasoby sprawnościowe – zbiór predyspozycji osobniczych do wykonywania określonych czynności fizycznych i umysłowych,

gdzie:

- „zasoby sprawnościowe" – *definiendum,*

- „zbiór predyspozycji osobniczych
  do wykonywania określonych czynności fizycznych i umysłowych" – *definiens*,
- „zbiór predyspozycji osobniczych" – *genus proximum*,
- „do wykonywania określonych czynności fizycznych i umysłowych" – *differentia specifica*.

W procedurach zarządzania, każdemu decydentowi chodzi o to (a przynajmniej chodzić powinno) aby jego postanowienia i rozstrzygnięcia, wyrażone w postaci odpowiednio uporządkowanych zbiorów dezyderatów i ustaleń (informacji decyzyjnych), powodowały jak największe zaangażowanie wykonawców w realizacji określonego dzieła. Zakres uzewnętrzniania się owego zaangażowania objawia się zawsze wkładem zasobów umiejętnościowych i sprawnościowych w wykonawstwo dzieła. Procedura z tym związana nie jest bynajmniej prosta. Można powiedzieć, że złożoność wynika z faktu, iż każda osoba znajdująca się w „łańcuchu wykonawczym" winna robić wszystko ochoczo i nie tylko dla tego, że musi. W tym tkwi istota dobrego zarządzania. O tym jednak często zapominają decydenci, przewartościowując siłę sprawczą przymusu ponad ochoczość wykonawstwa. Zapominają, bądź też nie zdają sobie sprawy, że zasoby ludzkie to wartości jednoznacznie spersonalizowane – że ich rzeczywistym dysponentem jest zawsze konkretny człowiek. Nikt nie jest w stanie wymusić na człowieku aby, wbrew swoim przekonaniom mentalnym, czynił wszystko do końca co mieści się w jego potencjalnych możliwościach. Znane są z historii liczne przykłady tego, że ludzie znosili tortury, tracili życie, ale nie wyrzekali się swoich przekonań. Jeśli nawet stwarzali pozory uległości, to we wnętrzu mentalnym pozostawali niezmienni i oczekiwali tylko na sprzyjające okoliczności aby pod różnymi postaciami, najczęściej ukrytymi, wymawiać symulowane podporządkowanie. Przykładami tego mogą być przeróżne formy sabotażu[153]. W uogólnieniu można powiedzieć, że najczęstszymi przyczynami tego staje się nadmierna hierarchizacja władzy, która z natury rzeczy prowadzi zawsze, do mniejszego lub większego, ale „totalitaryzmu organizacyjnego"[154], wynikającego zwykle z osobowościowej przywary zarządzającego do koncentrowania władzy, względnie z braku jego zaufania do podwładnych,

[153] Sabotaż – zamierzone dezorganizowanie pracy przez uchylanie się od niej lub wadliwe jej wykonywanie, a także niszczenie, uszkadzanie środków produkcji; zamaskowane działanie mające na celu przeszkadzanie w realizacji jakiegoś planu („Słownik języka polskiego", PWN, Warszawa 1992, tom III, s. 167).

[154] Totalitaryzm – system organizacji państwa polegający na ingerencji państwa we wszystkie dziedziny życia politycznego, społecznego i kulturowego oraz na sprawowaniu nad nimi kontroli („Słownik języka polskiego", PWN, Warszawa 1992, tom III, s. 516). Termin kontekstowy „totalitaryzm organizacyjny" został użyty w odniesieniu do organizacji mniejszych niż państwo, i tylko z intencją zaakcentowania niepożądanych wpływów wnoszonych, w podobny sposób przez przełożonych, do funkcjonowania organizacji (przypis autorski).

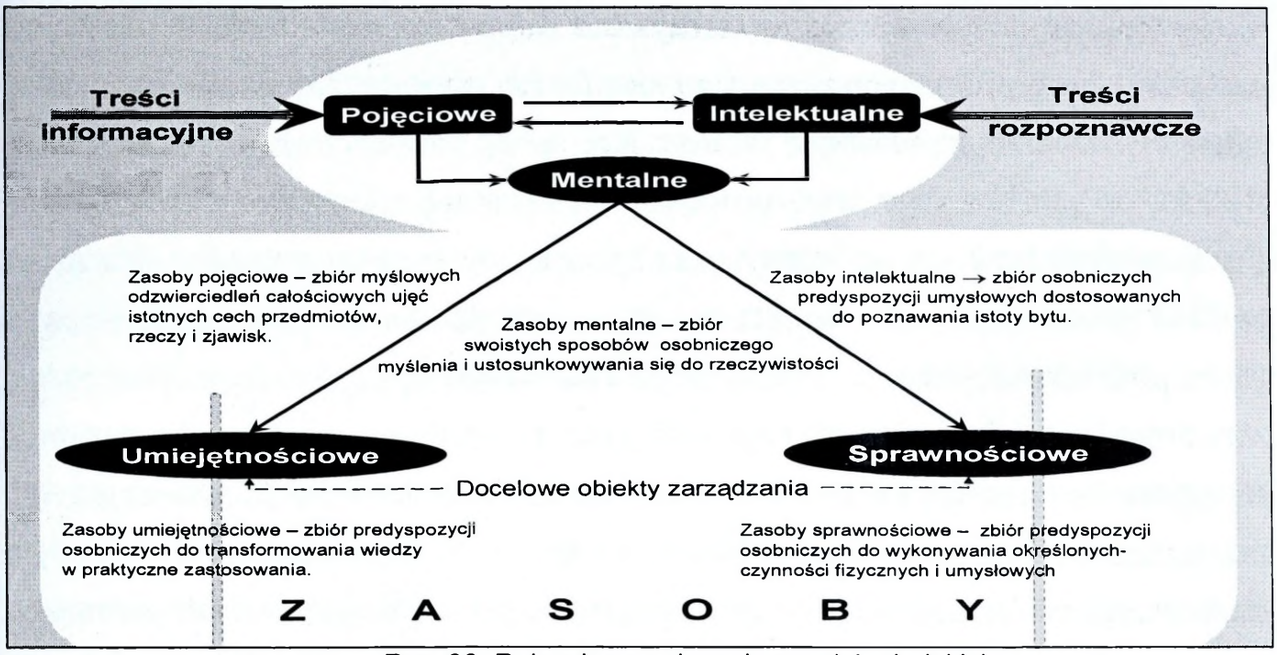
bądź też z postrzeganej przez siebie ich niechęci do własnej osoby. Może też zdarzać się, że zarządzający popada w megalomanię[155] zapominając, że sukces każdej organizacji to efekt synergiczny[156] całego zespołu, ale nigdy jednostki, chociażby miała być ona najdoskonalszą. Wynikające z tego tak zwane „popędzanie ludzi", nadmierny nadzór, zbyt szczegółowe zadania i nadmierne wytykanie błędów czy też ciągłe „patrzenie na ręce" prowadzą zawsze do zradzania się oporów i niechęci, co wcześniej lub później, ale zawsze odzwierciedla się negatywnymi następstwami dla organizacji i kreatora takiej formy zarządzania. W makroskali przykładami tego mogą być upadłe imperia, systemy państwowe czy partie polityczne, a w mniejszym zakresie – liczne przedsiębiorstwa i inne twory organizacyjne.

Wracając do przytaczanego już wskazania prakseologicznego Tadeusza Kotarbińskiego, **(...) by człowiek ochoczo robił to, co robić musi, (...)**, należy uwzględniać, że osiągnięcie takiego stanu w zarządzaniu, a do tego jeszcze w skali globalnej danej organizacji, jest z jednej strony niezmiernie pożądane, ale z drugiej zaś i niezmiernie trudne. Wyrażając się najogólniej można orzec, że trudność ta wynika ze złożoności wpływów oddziałujących na kształtowanie ludzkiej mentalności. Aby człowiek z pełnym zaangażowaniem czynił coś ochoczo, co zostało mu nakazane, musi nade wszystko być do tego mentalnie przekonany – musi się z tym nakazem identyfikować. W innym przypadku będzie czynił to co zostało mu nakazane, tylko dla tego, że zostało nakazane i z tej racji będzie bezemocjonalnym wykonawcą dzieła – będzie wykorzystywał swoje zasoby umiejętnościowe i sprawnościowe tylko w ograniczonym zakresie i tylko w takim, w jakim zostało to na nim wymuszone. Można zatem przyjmować, że mentalność człowieka stanowi sobą rzeczywiste „centrum" kierowania stanami ludzkich zachowań, które między innymi objawiają się poprzez pryzmat wykorzystywania zasobów umiejętnościowych i sprawnościowych człowieka. Istota tego wynika z faktu, że mentalność ludzka charakteryzuje się zindywidualizowanym sposobem osobniczego myślenia i zindywidualizowanym sposobem ustosunkowywania się człowieka do konkretnej rzeczywistości. W procedurach zarządzania kluczowe elementy stanowią **treści informacyjne** zawarte w postanowieniach decyzyjnych i **treści rozpoznawcze** pochodzące z otoczenia (rys. 39).

---

[155] Megalomania – przesadne przekonanie o swojej wartości, skłonność do przeceniania własnych możliwości, znaczenia, osiągania sukcesów; mania („Słownik języka polskiego", PWN, Warszawa 1992, tom II, s. 134).

[156] Synergia – współdziałanie, kooperacja czynników, skuteczniejsza niż suma ich oddzielnych działań (W. Kopaliński, „Słownik wyrazów obcych i zwrotów obcojęzycznych", WP, Warszawa 1967, 1994, s. 491).



Rys. 39. Relacyjne powiązania zasobów ludzkich

Źródło: Opracowanie autorskie.

Istotne wskazania, co do powyższego, można odnaleźć w pracach Davida Hume'a, Rene Descartes'a (Kartezjusza), Hansa Joachima Flechtner'a, Leona Festinger'a, Kazimierza Ajdukiewicza, wielokrotnie przytaczanego już Tadeusza Kotarbińskiego i innych. Sięgając jeszcze dalej można też je odnaleźć nie tylko w filozofii platońskiej i poplatońskiej, ale także i w filozofii przedplatońskiej. Chociaż akcentowana w nich problematyka była naświetlana w nieco innych kontekstach niż obecnie rozważany, to jednak z treści wybranych myśli wynika, że zagadnieniami kształtowania „zasobów mentalnościowych" zajmowano się już od wczesnego Antyku, chociaż nikt ich wtedy nie określał takim mianem. Występujące w tym zjawisku zależności, interpretowano głównie poprzez właściwości przypisywanych do „umysłu", „rozumu", „zmysłów" i „myśli". Systematyzując to, w sensie merytorycznym, na pierwszy plan zdają się wysuwać dociekania poznawcze Davida Hume'a, wyrażone słowami: *Wszelkie barwy poezyj, choćby najwspanialsze, nie mogą nigdy przyrody oddać w taki sposób, ażebyśmy opis wzięli za krajobraz rzeczywisty. Najżywsza myśl nie dorówna nigdy nawet najsłabszemu czuciu.*[157] Dalej dodaje: *Taką samą różnicę możemy zauważyć w odniesieniu do wszystkich innych percepcyi umysłu. Inaczej zachowuje się człowiek w napadzie gniewu, inaczej, gdy tylko myśli o tem uczuciu. Skoro mi ktoś powie, że jakaś osoba jest zakochana, łatwo zrozumiem myśl jego i utworzę sobie trafne wyobrażenie o stanie tej osoby; w żaden jednak sposób nie*

[157] D. Hume , „Badania dotyczące rozumu ludzkiego", De Agostini Polska Sp. z o.o., Warszawa 2001, s. 16 [Printed in Spain przekładu: J. Łukasiewicza i K. Twardowskiego, „An enquiry concerning Human Understanding", Wydawnictwa Polskiego Towarzystwa Filozoficznego (wydanie 2), Lwów 1919].

mogę wziąć tego wyobrażenia za rzeczywiste niepokoje i wzruszenia miłosne. Gdy zwracamy uwagę na minione uczucia i skłonności, myśl nasza jest wiernem zwierciadłem i odtwarza przedmioty z prawdą; lecz barwy, których używa, są blade i niewyraźne w porównaniu z temi, w których występowały percepcye pierwotne. Nie trzeba wielkiej bystrości ani głowy metafizycznej, by spostrzec między nimi różnice.[158] Wyjaśnia zatem, co w przedmiotowej sprawie jest bardzo istotne, że: *Możemy przeto podzielić wszystkie percepcye umysłu na dwie klasy czyli rodzaje, które różnią się od siebie stopniem swej siły i żywości. Słabsze i mniej żywe percepcye nazywają się zwykle* ***myślami*** *lub* ***ideami****. Dla drugiej kategoryi brak nazwy w naszym języku i w bardzo wielu innych; zdaje się dlatego, że tylko w celach naukowych trzeba było podporządkować je pod jakiś wyraz lub termin ogólny. Pozwólmy sobie zatem nazwać je* ***impresyami****, nadając słowu temu znaczenie cokolwiek odmienne od zwykłego. Przez wyraz impresya rozumiem więc wszystkie żywsze percepcye, które powstają, gdy słyszymy, widzimy, czujemy, kochamy, nienawidzimy, pożądamy lub chcemy. Impresye są zaś różne od idei, które są mniej żywemi percepcyami i które uświadamiamy sobie wtedy, gdy zastanawiamy się nad któremkolwiek z wymienionych powyżej wrażeń lub wzruszeń.*[159] W rozdziale trzecim (O kojarzeniu się idei) David Hume dodaje: *Jest rzeczą oczywistą, że istnieje jakieś prawo związku pomiędzy różnemi myślami czyli ideami umysłu i że występują one po sobie z pewnego rodzaju metodą i prawidłowością, gdy zjawiają się w pamięci lub wyobraźni. W poważniejszych rozmyślaniach i rozmowach jest fakt ten tak widoczny że każdą poszczególna myśl, która przerwie prawidłowy tok lub łańcuch idei, natychmiast spostrzegamy i usuwamy.*[160]

Z przytoczonych fragmentów tekstu wynika, że to co David Hume, ponad dwa wieki temu[161] – jeszcze na przełomie ery agrarnej i przemysłowej[162] – nazywał „my-

---

[158] Ibidem.
[159] Ibidem, s. 17.
[160] Ibidem, s. 21.
[161] Pierwsza edycja tego dzieła została wydana w Londynie 1748 roku pod tytułem: „Philosophical Essays concerning Human Understanding" (Szkice filozoficzne o rozumie ludzkim). Taki był pierwszy tytuł dzieła, które dopiero w wydaniu z 1758 roku otrzymało tytuł „Badania dotyczące rozumu ludzkiego".
[162] Wg Alvin i Heidi Toffler „era agrarna" (pierwsza fala), która uwidoczniła się około 10 000 lat temu, pojawieniem się wynalazków i umiejętności związanych z rolnictwem i osiadłym trybem życia. „Era przemysłowa" (druga fala) zaistniała około 300 lat temu, wraz z pojawieniem się druku i maszyny parowej. Przyniosła wytwarzanie stali, elektryczności, nowe środki transportu i komunikacji oraz standaryzację i unifikację. „Era obecna" (trzecia fala) rozpoczęła się wraz z powstawaniem nowych technologii umożliwiających nieograniczoną komunikację i odejście od masowej produkcji (Alvin i Heidi Toffler, „Trzecia fala", PIW, Warszawa 1997).

ślami" lub „ideami", to nic innego jak semantyka, a inaczej – „informacja" przekazywana pod postacią odpowiednio dobranych i zestawionych znaków języka etnicznego. Świadczy o tym chociażby użyty przez niego i przytaczany już zapis: *Wszelkie barwy poezyj, choćby najwspanialsze, nie mogą nigdy przyrody oddać w taki sposób, ażebyśmy opis wzięli za krajobraz rzeczywisty. Najżywsza myśl nie dorówna nigdy nawet najsłabszemu czuciu.* Można przypuszczać, iż Autor używając zestawienia wyrazowego *(...) barwy poezyj, chociażby najwspanialsze, nie mogą nigdy oddać w taki sposób, ażebyśmy opis wzięli za krajobraz rzeczywisty (...)*, chciał prawdopodobnie zaakcentować niedoskonałość przekazu informacyjnego dokonywanego za pomocą języka etnicznego i do tego jeszcze – poetyckiego, który z natury rzeczy jest najbardziej emocjonalny i tym samym najbardziej wpływowy na kształtowanie ludzkich uczuć. W tym też kontekście w pełni przekonujące, a szczególnie w aspekcie bieżącego kształtowania mentalności ludzkiej, zdają się być **treści rozpoznawcze**, które David Hume nazywa **impresjami** i lokuje je, pod względem skuteczności wpływów, przed **informacyjnymi**, używając do ich określenia bliskoznacznych terminów **myśli** i **idee**.

W poglądach Davida Hume'a daje się też dostrzec stwierdzenie, chociaż niezbyt wyraziste merytorycznie, ale bardzo istotne i konieczne do uwzględniania w procesach decyzyjnych. Autor wyrażając się, że *(...) każdą poszczególną myśl, która przerwie prawidłowy tok lub łańcuch idei, natychmiast spostrzegamy i usuwamy.* Dysponując dzisiejszą wiedzą, można by powiedzieć, że David Hume zaobserwował istotne zjawisko zachodzące w ludzkim umyśle (można również powiedzieć w ludzkiej mentalności), które po 209 latach Leon Festinger, w następstwie przeprowadzonych badań, nazwał **dysonansem poznawczym**[163]. W opublikowanej na ten temat teorii udowodnia dwie zasadnicze tezy[164]:

- *Istnienie niewygodnego psychologicznie dysonansu*[165] *motywuje osobę do prób jego zredukowania i osiągnięcia konsonansu*[166].

[163] Pierwsze wydanie dzieła D. Hume'a odbyło się w 1748 roku. Teorię dysonansu poznawczego L. Festinger opublikował w 1957 roku.
[164] L. Festinger, „Teoria dysonansu poznawczego", PWN, Warszawa 2007, s. 20.
[165] Dysonans – dwa elementy poznawcze są w relacji dysonansu, jeśli, przy uwzględnianiu tylko tych dwóch elementów, odwrotność jednego elementu wypływa z drugiego elementu (Ibidem, s. 198).
[166] Konsonans – dwa elementy poznawcze są ze sobą w konsonansie, jeżeli, przy uwzględnianiu tylko tych dwóch elementów, jeden element wynika z drugiego (Ibidem).

- *W sytuacji występowania dysonansu osoba będzie nie tylko próbowała go zredukować, ale będzie również w sposób aktywny unikała sytuacji oraz informacji, które mogłyby go zwiększyć.*

W dalszej części swojego wywodu poznawczego dokumentuje, że[167]:

- *Jeżeli dwa elementy poznawcze pozostają w jakimś związku, relacja między nimi jest albo dysonansem albo konsonansem.*
- *Wielkość dysonansu (lub konsonansu) wzrasta wraz z ważnością lub wartością elementu.*
- *Całkowita wielkość dysonansu między dwoma zbiorami elementów poznawczych jest funkcją ważonej proporcji wszystkich znaczących relacji między dwoma zbiorami pozostającymi w relacji dysonansu. Używam terminu „proporcja ważona", ponieważ każda znacząca relacja będzie ważona w zależności od ważności elementów wchodzących w tę relację.*

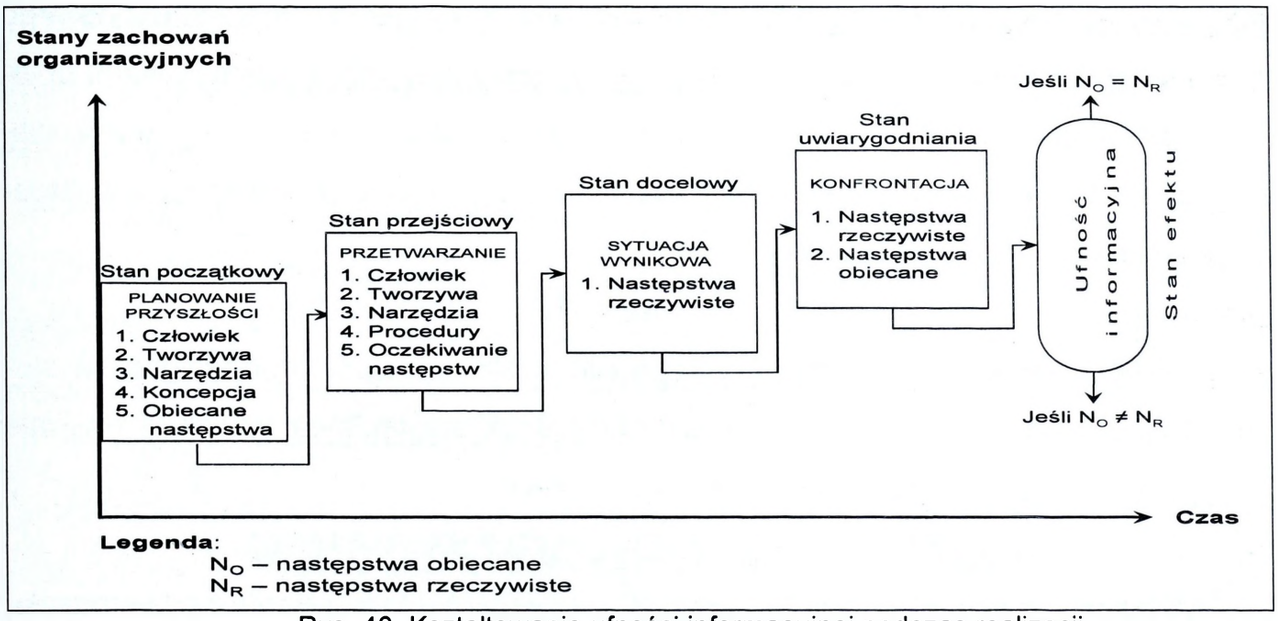
Autor powyższej teorii akcentuje również, że *(...) pojawiające się zdarzenia lub nowa informacja, z którą spotyka się osoba, mogą spowodować co najmniej chwilowy dysonans w stosunku do posiadanej wiedzy, procesów poznawczych lub przekonań, jeśli chodzi o zachowanie. Ponieważ osoba nie ma pełnej kontroli nad informacjami, jakie do niej docierają, ani też nad zdarzeniami, jakie mają miejsce w jej otoczeniu, taki dysonans może łatwo się pojawiać (...)*[168].

Uwzględniając powyższe i chronologię przyczyn przekładających się na stopień **ochoczego wykonawstwa**, w pierwszej kolejności pamiętać trzeba o przestrzeganiu zasad kształtowania **konsonansu poznawczego**, ukierunkowanych na zachowywanie spójności semantycznej pomiędzy treściami informacji decyzyjnych z treściami rozpoznawczymi docierającymi do wykonawców postanowień i rozstrzygnięć decyzyjnych, które według Adama Mortona nazywane są **obrazami percepcyjnymi**[169], a według Davida Hume'a – **impresjami**[170]. Pamiętać też trzeba, o czym przestrzega Leon Festinger[171], że stan osobowy każdej organizacji składa się z ludzi posiadających już określone doświadczenia życiowe – z ludzi, którzy w przeszłości doznawali, z przyczyn przełożonych, nie tylko satysfakcji, ale i rozczarowań (zawodów), co w różnym zakresie nadwątliło ich zaufanie do apriorycznej wiarygodności

[167] Ibidem, s. 31.
[168] Ibidem, s. 21.
[169] A. Morton, „Przewodnik po teorii poznania", Spacja, Warszawa 2002, s. 304.
[170] D. Hume, „Badania dotyczące rozumu ludzkiego", De Agostini Polska Sp. z o.o., Warszawa 2001, s. 16 i 17.
[171] L. Festinger, „Teoria dysonansu poznawczego", PWN, Warszawa 2007, s. 26, punkt 4.

informacji przekazywanych przez te osoby. Dlatego też każdy decydent jest ciągle obserwowany i oceniany pod tym względem przez podwładnych. Jest to powodowane ich mentalnymi dążeniami ukierunkowanymi na osiąganie konsonansu poznawczego w kwestii identyfikacji rzeczywistych intencji postępowania przełożonego (decydenta). Ta nieformalna, ale wielce znacząca procedura, rozpoczyna się zwykle od oceniania czy określony przełożony może być wiarygodnym reprezentantem interesów pracowniczych. W aspekcie tego brana jest zwykle pod uwagę znajomość podwładnych, stopień zainteresowania nimi, ich problemami, oczekiwaniami i aspiracjami. Oceniana jest również skromność jego zachowywania się oraz rzeczowość i etyczność postępowania. Ukształtowane w ten sposób przekonania uzupełniane są przeróżnymi impresjami poznawczymi odnoszącymi się do sfery czysto profesjonalnej, związanej z funkcjonowaniem organizacji. W ten sposób kształtowane są przekonania pracownicze nie tylko o intencjonalności, ale i merytorycznym przygotowaniu przełożonego do kompleksowego reprezentowania interesów organizacji.

W trakcie realizacji konkretnych zadań ufność informacyjna do postanowień decyzyjnych określonego przełożonego kształtowana jest głównie w czterech stanach zachowań organizacyjnych (rys. 40):



Rys. 40. Kształtowanie ufności informacyjnej podczas realizacji postanowień decyzyjnych

Źródło: Opracowanie autorskie.

(1) Stan początkowy wyznacza planowanie przyszłości. Jego strukturę stanowią ludzie, tworzywa, narzędzia, koncepcje i obiecane następstwa jako aprioryczne motywatory ludzkich zachowań. Ważne jest przy tym uwzględnianie, że każda decyzja jest zawsze ukierunkowywana na powodowanie określonych zmian, co

jakoby automatycznie wiąże się z przymusem wykonywania określonej pracy, to znaczy *(...) splotu czynów (w szczególnym przypadku – pasma czynów) mających charakter pokonywania trudności dla uczynienia zadość czyimś potrzebom istotnym*[172]. Z natury ludzkiej wynika natomiast, że każdy człowiek zobligowany do tego zwykle stawia sobie pytanie: A co ja z tego będę miał? Dlatego też każdy decydent, kierujący określone żądania wykonawcze, winien również uwzględniać, że takie pytania, chociażby nie wypowiadane głośno, to jednak istnieją w mentalności podległego mu stanu. Dlatego też właściwie wypośrodkowana, wyważona i akceptowana przez wykonawców informacja o następstwach wynikających z postanowień decyzyjnych stanowi sobą bardzo istotny element motywacyjny, co nie zawsze jest uwzględniane w praktyce zarządczej.

(2) Stan przejściowy wyznacza przetwarzanie. Jego strukturę nadal stanowią ludzie, tworzywa i narzędzia. W stosunku do stanu początkowego różnica polega na tym, że koncepcja przeistacza się już w konkretna procedurę działania (w konkretną pracę), a obiecane następstwa – w konkretne oczekiwania.

(3) Stan docelowy stanowi sytuacja wynikowa, obrazująca zakres realizacji postanowień decyzyjnych i stopień realizacji obiecanych przez decydenta następstw.

(4) Stan uwiarygodniania się decydenta w oczach podległego mu stanu osobowego następuje podczas konfrontacji następstw rzeczywistych z następstwami obiecanymi. W ramach tego może wystąpić dwojakiego rodzaju sytuacja wynikową. Może się darzyć, że następstwa obiecane (N_O) w pełni pokryją się z następstwami rzeczywistymi (N_R):

$$N_O = N_R$$

i wówczas stan efektu będzie powodował wzrost „ufności informacyjnej" w stosunku do decydenta. Może się też zdarzyć, że następstwa obiecane (N_O) nie pokryją się z następstwami rzeczywistymi (N_R):

$$N_O \neq N_R$$

W takiej sytuacji „ufność informacyjna" w stosunku do decydenta będzie malała, niezależnie od tego czy następstwa rzeczywiste (N_R) będą mniejsze czy też większe od następstw obiecanych (N_O).

Jeśli następstwa rzeczywiste (N_R) będą mniejsze od następstw obiecanych (N_O):

---

[172] T. Kotarbiński, „Traktat o dobrej robocie (wydanie siódme)", Ossolineum, Wrocław-▪ Warszawa-▪ Kraków-▪ Gdańsk- ▪ Łódź 1982, s. 80.

$$N_O > N_R$$

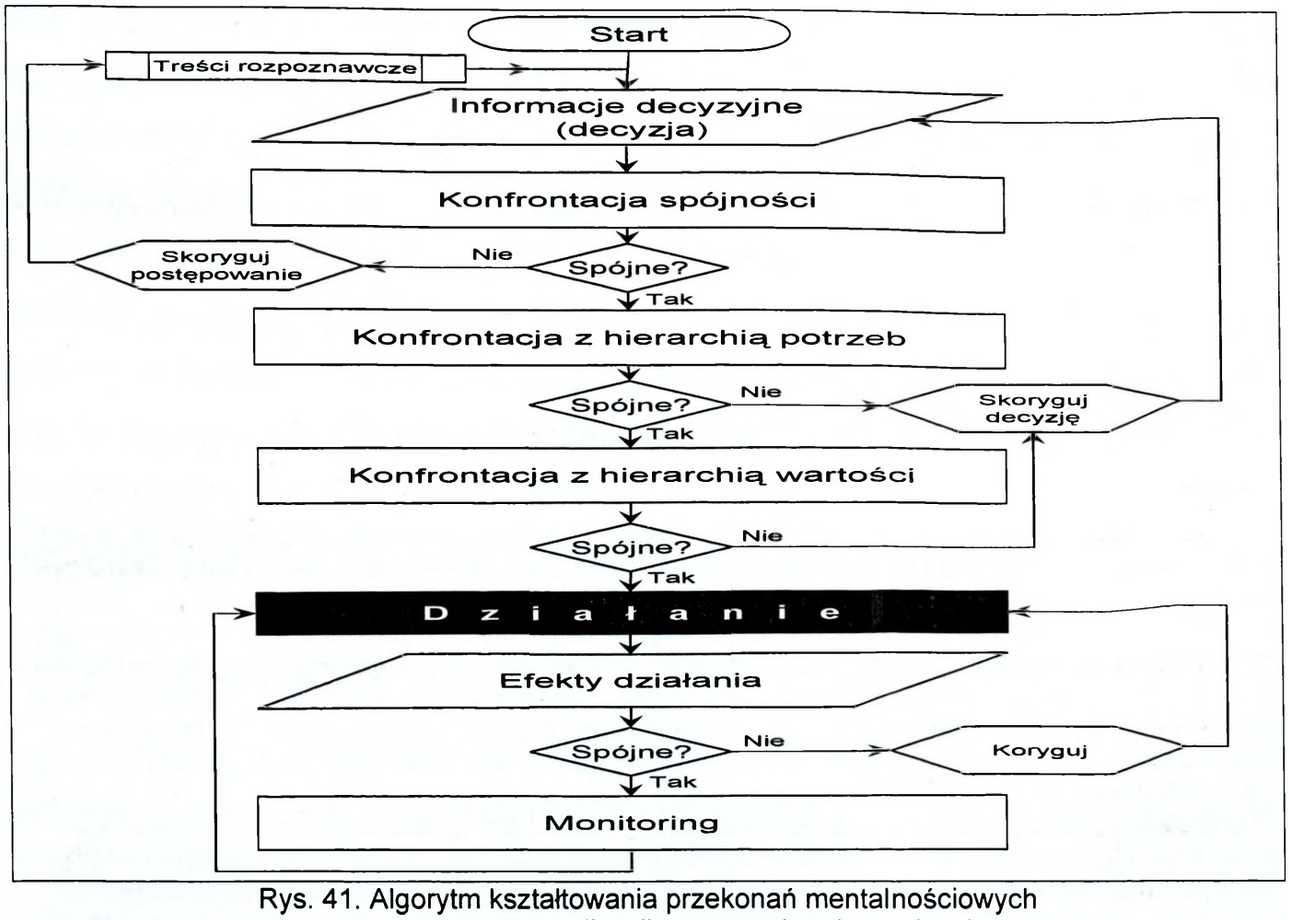
wówczas realizatorzy, którzy właściwie wykonali skierowane do nich postanowienia decyzyjne, poczują się oszukani przez decydenta i następnym razem będą angażowali swoje zasoby umiejętnościowe i sprawnościowe, w realizację nowego dzieła, tylko w takim zakresie w jakim będą musieli. Z pewnością nie będą podchodzili do jego wykonywania „ochoczo"

Jeśli natomiast okaże się, że następstwa rzeczywiste (N_R) przerosły swoim wymiarem następstwa obiecane (N_O):

$$N_O < N_R$$

wówczas również dla decydenta zaistnieje niekorzystna sytuacja. Wśród podległego stanu może się zrodzić przekonanie, że przełożony jest „asekurantem". Tak ukształtowana opinia może powodować w przyszłości generowanie nieuzasadnionych roszczeń pracowniczych, co z pewnością jest szkodliwe dla funkcjonowania każdej organizacji.

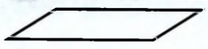
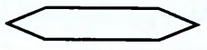
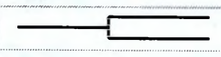
Wpływ informacji decyzyjnych i treści rozpoznawczych na kształtowanie przekonań mentalnościowych można wyrazić następującym algorytmem (rys. 41 i tab. 2).



Rys. 41. Algorytm kształtowania przekonań mentalnościowych w procesie realizacji postanowień decyzyjnych

Źródło: Opracowanie autorskie.

Symbole stosowane w sieciach działania Tabela 2

Nazwa operacji	Wyjaśnienie	Symbol
Przetwarzanie	Operacje lub grupa operacji, w wyniku których ulega zmianie wartość, postać lub miejsce zapisu danych	
Wprowadzenie, wyprowadzenie	Wprowadzenie lub (i) wyprowadzenie danych	
Decyzja	Operacje określające wybór jednej z alternatywnych dróg działania	
Przygotowanie	Modyfikacja rozkazu lub grupy rozkazów, powodująca zmianę w przebiegu procesu przetwarzania	
Droga przepływu danych	Więź operacyjna między poszczególnymi operacjami procesu przetwarzania	
Skrzyżowanie	Skrzyżowanie dróg przepływu danych bez powiązania między nimi	
Łączenie	Łączenie dróg przepływu danych	
Początek, koniec lub przerwa	Oznaczenie miejsca rozpoczęcia, zakończenia lub przerwania działania programu	
Komentarz	Oznaczenie miejsca na komentarz	
Proces zdefiniowany	Proces zdefiniowany poza programem	
Droga przepływu danych	Wskazanie kierunku przepływu danych, gdy kierunek ten nie jest jednoznacznie oznaczony	
Łącznik	Łącznik międzystronnicowy	
Łącznik stronicowy	Wejście lub wyjście z wyodrębnionych fragmentów schematu znajdujących się na jednej stronie – łącznik stronnicowy	

Źródło: Polska norma branżowa PN-75/E-01226.

Procedura postępowania przedstawiona na rysunku 41 rozpoczyna się, w sposób formalny, od przekazywania informacji decyzyjnych (decyzji). W sposób nieformalny docierają jednak do wykonawców jeszcze określone treści rozpoznawcze, które David Hume nazywa *impresjami*[173], a Bertrand Russell – *przestrzenią zjawiska*[174]. Ich interpretacje osobnicze mogą, ale nie muszą być spójne znaczeniowo z informacjami decyzyjnymi. Niespójność ta może wynikać bądź z przesłanek obiektywnie uzasadnionych bądź z przesłanek subiektywnych. Tak w jednym, jak i drugim przypadku zawsze wymaga to podjęcia określonej reakcji przez decydenta, sprowadzającej się generalnie do korygowania swojego postępowania. Może się to odnosić bądź do zmiany zachowania bądź do zmiany uzasadniania racji decyzyjnych. Ważne

[173] „Można przeto podzielić wszystkie percepcye umysłu na dwie klasy czyli rodzaje, które różnią się od siebie stopniem swej siły i żywotności. Słabsze i mniej żywe percepcje nazywają się zwykle myślami lub ideami. Do drugiej kategoryi brak nazwy w naszym języku i w bardzo wielu innych; zdaje się dlatego, że tylko w celach naukowych trzeba było podporządkować je pod jakiś wyraz lub termin ogólny. Pozwólmy sobie zatem nazwać je **impresyami**, nadając temu słowu znaczenie cokolwiek odmienne od zwykłego. Przez wyraz **impresya** rozumiem więc wszystkie żywsze percepcye, które powstają, gdy słyszymy, widzimy, czujemy, kochamy, nienawidzimy, pożądamy lub chcemy". [D. Hume (przekład: J. Łukasiewicz i K. Twardowski), „Badania dotyczące rozumu ludzkiego", De Agostini Polska Sp. z o.o., Warszawa 2001, s. 17].

[174] „**Przestrzeń rzeczywista** ma charakter publiczny, **przestrzeń zjawiska** stanowi prywatną własność tego, kto doznaje wrażeń. Ten sam przedmiot wydaje się mieć różne kształty w **prywatnych przestrzeniach** różnych ludzi; tak więc **przestrzeń rzeczywista**, w której ma on swój rzeczywisty kształt, musi się różnić od **przestrzeni prywatnych**. A zatem, przestrzeń taka, jaką proponuje ją nauka, choć powiązana z przestrzeniami, które widzimy i czujemy, nie jest z nim identyczna, a sposób tego powiązania wymaga zbadania. [B. Russell (przekład: W. Sady), „Problemy filozofii", PWN, Warszawa 2004, s. 35].

jest przy tym, że uzyskana w tym zakresie spójność zawsze powoduje uwiarygodnianie się przełożonego w oczach podległego mu stanu osobowego. Nie oznacza to jeszcze, że podjęta decyzja będzie realizowana „ochoczo". Do tego konieczne jest jeszcze uzyskanie spójności postanowień decyzyjnych z hierarchią potrzeb i z hierarchią wartości, które są ukształtowane w środowisku wykonawczym. Występujące w tym zakresie rozbieżności wymagają zawsze korygowania postanowień decyzyjnych, jeśli decydent chce uchodzić nie tylko za wiarygodnego, ale i rzeczywistego reprezentanta interesów pracowniczych, co w zespoleniu komplementarnym przekłada się na „ochoczość" wykonawstwa. Rezygnując z tego (z roli reprezentanta) i dążąc tylko usilnie do realizacji postanowień decyzyjnych musi stosować określone formy nieakceptowanego mentalnie przymusu i może tylko pozostać wiarygodnym, ale nie więcej niż satrapą, co w istotnym zakresie będzie zawsze powodowało ograniczanie wkładu umiejętnościowych i sprawnościowych zasobów ludzkich istniejących w środowisku wykonawczym i możliwych do wnoszenia w dzieło wynikające z postanowienia decyzyjnego.

Innym, nie mniej ważnym czynnikiem, który wpływa na „ochoczość" wykonawstwa – jak to nazywa Tadeusz Kotarbiński – jest *czytelność informacji*[175] zawarta w postanowieniach i rozstrzygnięciach decyzyjnych. Człowiek, jako element podmiotowy organizacji, występuje ciągle w roli obiektu informującego lub informowanego, względnie w roli jednego i drugiego razem, co wynika z ustalonej organizacyjnie zwierzchności. W określonym czasie, dysponuje również określonymi stanami swoich zasobów pojęciowych, intelektualnych, mentalnościowych, umiejętnościowych i sprawnościowych. Stany te nie są raz na zawsze ustalone. Zmieniają się w rytm czasu i panującego kształtu otaczającej go rzeczywistości. Ich poziom decyduje zawsze o określonych możliwościach człowieka i jego predyspozycjach predestynujących do funkcjonowania w określonych miejscach struktur organizacyjnych.

1.1.3. Wartościowanie informacji

Informacja, jako treść znaczeniowa znaku językowego (jako semantyka), nie posiada i posiadać nie może trwale ustalonej wartości. Jej cena objawia się zawsze

[175] „Następne miejsce w naszym wyliczaniu walorów **dobrej informacji** zajmie jej **czytelność**, a mamy tu na myśli coś więcej niż to, co się rozumie przez ten wyraz w mowie potocznej. Idzie nam o zespół cech wypowiedzi informacyjnej, przyczyniających się do tego, że jej treść zostaje trafnie ujęta przez odbiorcę powiadomienia". [T. Kotarbiński, „Traktat o dobrej robocie (wydanie siódme)", Ossolineum, Wrocław▪ Warszawa▪ Kraków▪ Gdańsk▪ ▪ Łódź 1982, s. 206/207].

w komplementarnym zespoleniu z konkretnymi potrzebami użytkownika. Ta sama informacja może być dla kogoś wysoce wartościowa, dla innej osoby niewiele znacząca, a jeszcze dla innej – zupełnie bezwartościowa. Jest to zawsze związane z konkretnymi potrzebami danego użytkownika, a konkretnie – z antecedentnie[176] podejmowanymi przez niego wysiłkami ukierunkowanymi na osiągnięcie określonego celu. Wyrażając to innymi słowy można powiedzieć, że cena informacji wynika z różnicy funkcji spodziewanych zysków i funkcji poniesionych nakładów:

$$I_C = f(Z) - f(N)$$

gdzie:

I_C – *cena informacji,*

Z – *spodziewane zyski,*

N – *poniesione nakłady.*

Uwzględniając antecedentność, nakładów w stosunku do zysków, jakoby automatycznie narzuca się skojarzenie, że cena informacji najbardziej wyraziście unaocznia się w procedurach decydowania, gdzie w ślad za konkretnymi postanowieniami i rozstrzygnięciami kryją się określone zmiany realizowane kosztem skonkretyzowanych nakładów, które – w mentalności decydenta – kojarzą się z następstwami w postaci określonych zysków. Jak już akcentowano wcześniej, uwzględniane w decyzjach stany przyszłości nie są jednak zdarzeniami pewnymi. Są zawsze tylko stanami prawdopodobnymi. Z tej też przyczyny i podejmowane decyzje przyjmują zwykle postać wielowariantową, dostosowaną kształtem strukturalno-funkcjonalnym do dających się przewidywać stanów przyszłości. Wynika z tego, że funkcja zysków jest niczym innym, jak tylko esperancją[177]:

$$E(X) = x_1 p_1 + x_2 p_2 + \ldots + x_n p_n$$

gdzie:

x_i – korzyści wynikające z realizacji określonego postanowienia lub rozstrzygnięcia decyzyjnego,

p_i – prawdopodobieństwo wystąpienia określonego stanu otoczenia podczas realizacji określonego postanowienia lub rozstrzygnięcia decyzyjnego.

---

[176] Antecedencje – okoliczności, zdarzenia poprzedzające jakiś fakt.

[177] Esperancja – [fr. *espérance* (nadzieja)] *mat.* średnia wartość oczekiwana jako wynik rachunku prawdopodobieństwa dla zmiennej losowej przy nieskończonej liczbie prób.

Oznaczając przez:

D_i – kształt strukturalno-funkcjonalny i-tej decyzji,

S_j – stan j-tego otoczenia decyzyjnego występujący w czasie realizacji i-tej decyzji

k_{ij} – korzyści wynikające z realizacji i-tej decyzji w czasie zaistnienia j-tego stanu otoczenia decyzyjnego,

$P(S_j)$ – prawdopodobieństwo zaistnienia j-tego stanu otoczenia decyzyjnego,

K_i – korzyści wynikające z realizacji i-tej decyzji,

wówczas średnią wartość korzyści oczekiwanych (esperancję) można wyrazić równaniem:

$$E(K_i) = \sum_{j=1}^{n} P(S_j) k_{ij} ,$$

a model wyboru wariantu decyzyjnego – zestawieniem tabelarycznym (tab. 3):

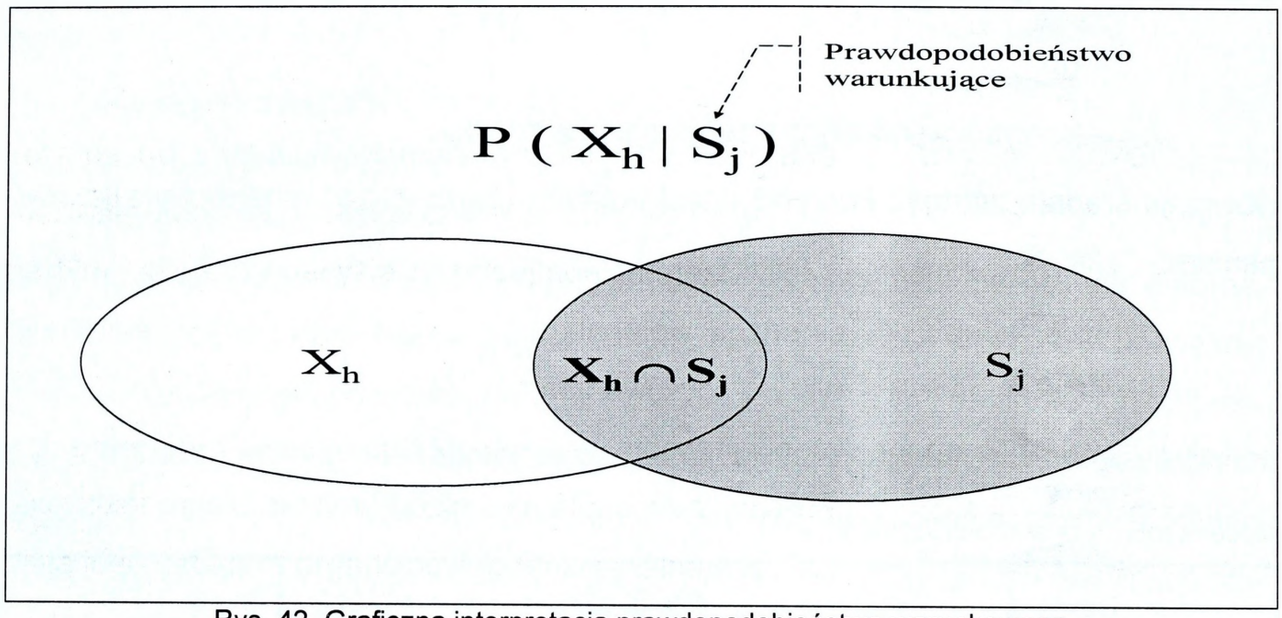
Model wyboru wariantu decyzyjnego Tabela 3

D_i	$P(S_J)$				$E(K_i)$
	$P(S_1)$	$P(S_2)$	...	$P(S_n)$	
D_1	k_{11}	k_{12}	...	k_{1n}	$E(K_1)$
D_2	k_{21}	k_{22}	...	k_{2n}	$E(K_2)$
D_3	k_{31}	k_{32}	...	k_{3n}	$E(K_3)$
...	...	...	...	...	...
D_n	k_{n1}	k_{n2}	...	k_{nn}	$E(K_n)$

Źródło: Opracowanie na podstawie: W. Sadowski, „Decyzje i prognozy", PWE, Warszawa 1977, s. 132

Tak jak każda z podejmowanych decyzji D_i posiada zawsze określoną strukturę organizacyjno-funkcjonalną, tak i każdy stan otoczenia decyzyjnego S_j, występujący w trakcie realizacji decyzji D_i, charakteryzuje się podobnymi właściwościami. W procedurze decydowania istota rzeczy sprowadza się do tego aby apriorycznie formułowana struktura organizacyjno-funkcjonalna danej decyzji D_i była jak najbardziej dosto-

sowana do struktury organizacyjno-funkcjonalnej stanu otoczenia decyzyjnego S_j, możliwego do zaistnienia w czasie wdrażania jej do praktyki. Trudność polega jednak na tym, że każda decyzja D_i podejmowana jest tylko w stosunku do prawdopodobnych stanów otoczenia S_j, jako przedmiotów poznania[178] zidentyfikowanych wcześniej w określonych relacjach rozpoznawczych[179], ale tylko na podstawie jakichś przesłanek X_h. Dlatego też każdy stan otoczenia decyzyjnego S_j należy traktować jako zbiór zawierający w sobie określone elementy podzbioru X_h, które odzwierciedlają jego strukturę organizacyjno-funkcjonalną (rys. 42),



Rys. 42. Graficzna interpretacja prawdopodobieństwa warunkowego

Źródło: Opracowanie autorskie

a informacje o nich – podstawę do identyfikacji stanu otoczenia decyzyjnego, co można wyliczać z zależności:

$$P(X_h|S_j) = \frac{P(X_h \cap S_j)}{P(S_j)} \quad gdzie \quad P(S_j) > 0$$

i odczytywać: jeśli zaistnieje stan otoczenia decyzyjnego S_j to prawdopodobieństwo wystąpienia zdarzenia należącego do zbioru X_h jest równe ilorazowi iloczynu tych zdarzeń do prawdopodobieństwa warunkującego to zdarzenie. Z przekształcenia tego równania wynika też, że iloczyn takiego zdarzenia stanowi liczba:

$$P(X_h \cap S_j) = P(X_h|S_j) \times P(S_j).$$

Przyjmując, że stany otoczenia decyzyjnego S_j tworzą zupełny układ zdarzeń w przestrzeni $\Omega = 1^*$, jeśli:

[178] Patrz rys. 18 (Schemat powstawania informacji i informowania).
[179] Ibidem

- $S_j \cap S_k = 0^*$ dla $j \neq k$,
- $P(S_j) > 0$ dla $j \in \{1,2,...,n\}$,
- $S_1 \cup S_2 \cup ...S_n = \Omega$,

to dla dowolnego $X_h \subset \Omega$ prawdopodobieństwo całkowite można wyliczać z zależności:

$$P(X_h) = P(X_h|S_1) \times P(S_1) + P(X_h|S_2) \times P(S_2) + ... + P(X_h|S_n) \times P(S_n).$$

PRZYKŁAD

Dane wyjściowe

W procesie podejmowania decyzji są uwzględniane tylko dwa stany otoczenia zewnętrznego S_j, które mogą wystąpić z prawdopodobieństwem:

- $P(S_1) = 0,4$,
- $P(S_2) = 0,6$,

i po trzy zdarzenia X_h identyfikujące stany otoczenia zewnętrznego S_j, które mogą wystąpić z prawdopodobieństwem:

- $P(X_1|S_1) = 0,2$,
- $P(X_2|S_1) = 0,3$,
- $P(X_3|S_1) = 0,5$,

- $P(X_1|S_2) = 0,4$,
- $P(X_2|S_2) = 0,25$,
- $P(X_3|S_2) = 0,35$.

R o z w i ą z a n i e

Dysponując powyższymi danymi i znając struktury organizacyjno-funkcjonalne podjętych decyzji D_i każdy decydent prawdopodobnie w pierwszej kolejności przeprowadzi kalkulacje, a przynajmniej powinien takie przeprowadzić, które pozwolą mu ustalić korzyści wynikające z realizacji podjętych decyzji w warunkach wystąpienia znanych mu już stanów otoczenia zewnętrznego S_j – to znaczy w sytuacji kiedy nie

będzie korzystał z dodatkowych informacji o tych stanach otoczenia zewnętrznego podczas realizacji określonej decyzji.

Przyjmując, że decydent dokonał takiej kalkulacji i wynikło z niej, że największych korzyści może się spodziewać po wdrożeniu do realizacji decyzji pierwszej D_1, która zapewnia korzyści w wysokości 6,4 jednostek umownych (tab. 4).

Zestawienie kalkulacyjne dotyczące wyboru decyzji bez korzystania z dodatkowych informacji o stanach otoczenia zewnętrzne — Tab. 4

D_i	$P(S_j)$		$E(K_i)$
	$P(S_1) = 0,4$	$P(S_2) = 0,6$	
D_1	$k_{11} = 10$	$k_{12} = 4$	$E(K_1) = 6,4$
D_2	$k_{21} = 4$	$k_{22} = 6$	$E(K_2) = 5,2$
D_3	$k_{31} = 2$	$k_{32} = 8$	$E(K_3) = 5,6$

Źródło: Opracowanie autorskie

Decydent, chcąc się jednak upewnić czy powyższe rozwiązanie jest najlepsze z możliwych, zdecydował się na przeprowadzenie jeszcze kalkulacji ukierunkowanej na unaocznienie korzyści wynikających z sytuacji kiedy mógłby korzystać z dodatkowych informacji o stanach otoczenia zewnętrznego S_j podczas wdrażania do realizacji poszczególnych decyzji D_i. Korzystając z zależności::

$$P(X_h \cap S_j) = P(X_h|S_j) \times P(S_j)$$

wyliczył, że:

- $P(X_1 \cap S_1) = P(X_1|S_1) \times P(S_1) = 0,2 \times 0,4 = 0,08$,
- $P(X_2 \cap S_1) = P(X_2|S_1) \times P(S_1) = 0,3 \times 0,4 = 0,12$,
- $P(\bar{X}_3 \cap S_1) = P(X_3|S_1) \times P(S_1) = 0,5 \times 0,4 = 0,20$,
- $P(X_1 \cap S_2) = P(X_1|S_2) \times P(S_2) = 0,4 \times 0,6 = 0,24$,
- $P(X_2 \cap S_2) = P(X_2|S_2) \times P(S_2) = 0,25 \times 0,6 = 0,15$,

- $P(X_3 \cap S_2) = P(X_3|S_2) \times P(S_2) = 0{,}35 \times 0{,}6 = 0{,}21$,

Podstawiając powyższe wyniki do równania:

$$P(X_h) = P(X_h|S_1) \times P(S_1) + P(X_h|S_2) \times P(S_2) + ... + P(X_h|S_n) \times P(S_n)$$

wyliczył również, że prawdopodobieństwo wystąpienia zdarzeń X_h należących do zbioru S_j wynosi::

- $P(X_1) = P(X_1|S_1) \times P(S_1) + P(X_1|S_2) \times P(S_2) = 0{,}08 + 0{,}24 = 0{,}32$,
- $P(X_2) = P(X_2|S_1) \times P(S_1) + P(X_2|S_2) \times P(S_2) = 0{,}12 + 0{,}15 = 0{,}27$,
- $P(X_3) = P(X_3|S_1) \times P(S_1) + P(X_3|S_2) \times P(S_2) = 0{,}20 + 0{,}21 = 0{,}41$.

Sumując to według zależności:

$$\sum_{h=1}^{3} P(X_h) = 0{,}32 + 0{,}27 + 0{,}41 = 1*$$

uzyskał prawdopodobieństwo równe jedności, co przekonało go o poprawności postępowania i całość dociekań ujął zestawieniu reprezentującym aprioryczną identyfikację stanów otoczenia decyzyjnego (tab. 5).

Aprioryczna identyfikacja stanów otoczenia decyzyjnego — Tabela 5

$P(S_j)$		$P(X_h\|S_j)$			$P(X_h \cap S_j)$		
S_j	p	x_1	x_2	x_3	x_1	x_2	x_3
S_1	0,40	0,20	0,30	0,50	0,08	0,12	0,20
S_2	0,60	0,40	0,25	0,35	0,24	0,15	0,21
$P(X_h)$					0,32	0,27	0,41

Źródło: Opracowanie autorskie na podstawie

W dalszych dociekaniach uwzględnił jednak, że aprioryczna identyfikacja stanów otoczenia decyzyjnego S_j oparta jest tylko na przypuszczeniach i w takiej postaci nie stanowi jeszcze wystarczającej podstawa do wartościowania informacji.

Uwzględniając natomiast, że stany otoczenia decyzyjnego $S_1, S_2, ..., S_n$ tworzą zupełny rozkład zdarzeń w przestrzeni Ω i $P(X_h) > 0$, stosując twierdzenie *Bayesa*:

$$P(S_j|X_h) = \frac{P(X_h|S_j) \times P(S_j)}{P(X_h)}$$

obliczył jakie jest aposterioryczne prawdopodobieństwo, że wykryte zdarzenie X_h pochodzi ze zbioru S_j, co w zespoleniu z treścią zawartą w tabeli 5 umożliwiło wykonanie zestawienia obrazującego aprioryczne i aposterioryczne możliwości identyfikacji stanów otoczenia zewnętrznego S_j (tab. 6).

Aprioryczna i aposterioryczna identyfikacja stanów otoczenia zewnętrznego — Tabela 6

$P(S_j)$		$P(X_h\|S_j)$			$P(X_h \cap S_j)$		
S_j	p	x_1	x_2	x_3	x_1	x_2	x_3
S_1	0,40	0,20	0,30	0,50	0,08	0,12	0,20
S_2	0,60	0,40	0,25	0,35	0,24	0,15	0,21
$P(X_h)$					0,32	0,27	0,41
$P(S_1\|X_h)$					0,25	0,44	0,49
$P(S_2\|X_h)$					0,75	0,56	0,51

Źródło: Opracowanie autorskie

Bazując na danych zawartych w tabeli 6 oraz wcześniejszych kalkulacjach odnoszących się do ustalania korzyści przypisanych do i-tej decyzji i j-tego stanu otoczenia zewnętrznego, które według apriorycznej wiedzy decydenta zostały oszacowane w wysokości (wróć do tab. 4):

- k_{11} = 10 jednostek umownych – dla pierwszej decyzji D_1 i pierwszego stanu otocznia zewnętrznego S_1,
- k_{12} = 4 jednostki umowne – dla pierwszej decyzji D_1 i drugiego stanu otocznia zewnętrznego S_2,
- k_{21} = 4 jednostki umowne – dla drugiej decyzji D_2 i pierwszego stanu otocznia zewnętrznego S_1,

- k_{22} = 6 jednostek umownych – dla drugiej decyzji D_2 i drugiego stanu otocznia zewnętrznego S_2,
- k_{31} = 2 jednostki umowne – dla trzeciej decyzji D_3 i pierwszego stanu otocznia zewnętrznego S_1,
- k_{32} = 8 jednostek umownych – dla trzeciej decyzji D_3 i drugiego stanu otocznia zewnętrznego S_2.

Podstawiają powyższe wartości do aposteriorycznie ustalanych stanów otoczenia zewnętrznego $P(S_j|X_h)$ i wykorzystując dane zawarte w tabeli 6 decydent wykonał zestawienie umożliwiające oszacowanie korzyści wynikających z posiadania dodatkowych informacji o stanach otoczenia zewnętrznego S_j podczas realizacji poszczególnych postanowień decyzyjnych D_i, czego wynikło, że te $E(K_{\inf})$ kształtują się w wysokości 6,7182 jednostek umownych (tab. 7).

Zestawienie umożliwiające szacowanie korzyści wynikających z posiadania dodatkowych informacji o stanach otoczenia zewnętrznego występujących podczas realizacji postanowień decyzyjnych Tabela 7

		$P(X_1) = 0,32$	
D_i	$P(S_j\|X_1)$		$E(K_i)$
	$P(S_1\|X_1)=0,25$	$P(S_2\|X_1)=0,75$	
D_1	$k_{11}=10$	$k_{12}=4$	$E(K_1)=5,50$
D_2	$k_{21}=4$	$k_{22}=6$	$E(K_2)=5,50$
D_3	$k_{31}=2$	$k_{32}=8$	$E(K_3)=6,50$
		$P(X_2) = 0,27$	
D_i	$P(S_j\|X_2)$		$E(K_i)$
	$P(S_1\|X_2)=0,44$	$P(S_2\|X_2)=0,56$	
D_1	$k_{11}=10$	$k_{12}=4$	$E(K_1)=6,64$
D_2	$k_{21}=4$	$k_{22}=6$	$E(K_2)=5,12$
D_3	$k_{31}=2$	$k_{32}=8$	$E(K_3)=5,36$
		$P(X_3) = 0,41$	
D_i	$P(S_j\|X_3)$		$E(K_i)$
	$P(S_1\|X_3)=0,49$	$P(S_2\|X_3)=0,51$	
D_1	$k_{11}=10$	$k_{12}=4$	$E(K_1)=6,94$
D_2	$k_{21}=4$	$k_{22}=6$	$E(K_2)=5,02$
D_3	$k_{31}=2$	$k_{32}=8$	$E(K_3)=5,06$

$$E(K_{\inf}) = \sum_{h=1}^{n} P(X_h) \times E(K_{\max}) = 0,32 \times 6,5 + 0,27 \times 6,64 + 0,41 \times 6,94 = 6,7182$$

Źródło: Opracowanie autorskie

O d p o w i e d ź

Konfrontując spodziewane korzyści $E(K_1) = 6{,}4$, możliwe do osiągnięcia bez korzystania z dodatkowych informacji o stanach otoczenia zewnętrznego S_j podczas realizacji postanowień decyzyjnych (tab. 4), z korzyściami $E(K_{\inf}) = 6{,}7182$ spodziewanymi do osiągnięcia przy korzystaniu z dodatkowej informacji o stanach otoczenia zewnętrznego S_j, podczas realizacji postanowień decyzyjnych (tab. 7) i uwzględniając, że cena informacji wynika z zależności:

$$I_C = f(Z) - f(N)$$

gdzie:

I_C – cena informacji,

Z – spodziewane zyski,

N – poniesione nakłady,

można powiedzieć, że funkcję zysków $f(Z)$ stanowią korzyści $E(K_{\inf})$, spodziewane do osiągnięcia przy korzystaniu z dodatkowej informacji o stanach otoczenia zewnętrznego S_j, a funkcję nakładów $f(N)$ – korzyści $E(K_i)$, spodziewane do osiągnięcia bez korzystania z dodatkowych informacji o stanach otoczenia zewnętrznego S_j. W następstwie tego cenę informacji wyznacza zależność:

$$I_c = E(K_{\inf}) - E(K_i)$$

pod warunkiem, że:

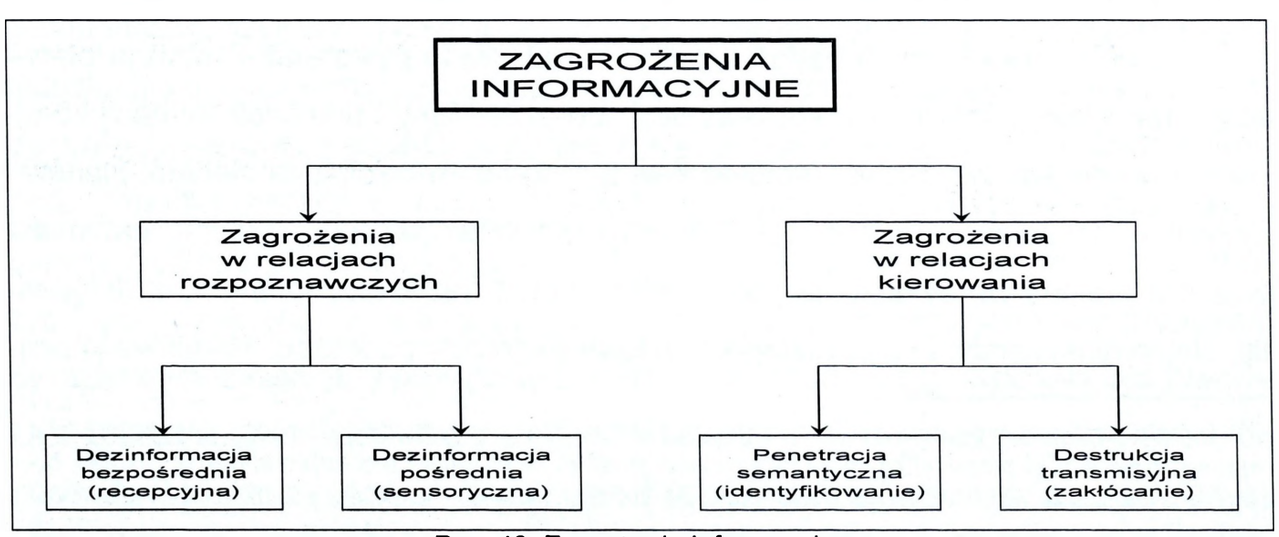
$$E(K_{\inf}) - E(K_i) > 0 .$$

W niniejszym przykładzie cenę informacji wyznacza wartość:

$I_c = E(K_{\inf}) - E(K_i) = 6{,}7182 - 6{,}4 = 0{,}3182$ jednostek umownych.

2. ZAGROŻENIA INFORMACYJNE W SIECIACH TELEINFORMATYCZNYCH

Z dociekań zawartych w rozdziale pierwszym jednoznacznie wynika, że bezpieczeństwo i ochronę informacji w sieciach teleinformatycznych, należy postrzegać przez pryzmat negatywnych oddziaływań na procedury tworzenia informacji i negatywnych oddziaływań na procedury informowania[1]. Postrzegając ten problem w takim aspekcie można też przyjmować, że negatywne oddziaływania (zagrożenia) na procedury tworzenia informacji to przede wszystkim dezinformacja, unaoczniająca się celowym deformowaniem stanów rzeczy w przestrzeni zainteresowania poznawczego, wpływająca negatywnie na semantykę wytwarzaną w bezpośrednich (recepcyjnych) i pośrednich (sensorycznych) relacjach rozpoznawczych[2]. Negatywne oddziaływania (zagrożenia) na relacje kierowania można natomiast postrzegać przez pryzmat penetracji semantycznej (identyfikowanie) i destrukcyjne oddziaływania (zakłócanie) transmisyjne funkcjonujące w relacjach informacyjnych[3] (rys. 43).



Rys. 43. Zagrożenia informacyjne

Źródło: Opracowanie autorskie

[1] Patrz rys. 25 na s. 51 i przypisany do niego tekst.
[2] Patrz rys. 18, s. 36 i przypisany do niego tekst.
[3] Ibidem.

2.1. Zagrożenia informacyjne w relacjach rozpoznawczych

We współczesnym świecie informacja stała się jedną z podstawowych potrzeb człowieka. Coraz szersze masy, a wręcz całe społeczeństwa domagają się ciągle nowych informacji. Zaspokojenie tej potrzeby stało się możliwe dzięki osiągnięciom współczesnej techniki, a przez to rozwojowi nowoczesnych środków masowego przekazu. Informacja z odległego zakątka kuli ziemskiej niemal błyskawicznie dociera do każdego, kto jej pożąda. Łatwość dostępu oraz mnogość informacji powodują pewne zagrożenia dla potencjalnych odbiorców. Zagrożeniem tym jest świadome i celowo wysyłana, obok informacji prawdziwej, dezinformacja[4]. W takim natłoku wiadomości masowy odbiorca nie jest w stanie odróżnić informacji prawdziwej od fałszywej, przez to staje się ofiarą organizatorów współcześnie przygotowywanej i prowadzonej dezinformacji. Każda informacja może stać się orężem walki, który w wyniku globalnego zasięgu i możliwości oddziaływania na ogromne masy ludzi przybierze znaczenie strategiczne. Prowadzona przez centralne kierownictwo państwa w sposób zorganizowany i w określonym celu – staje się elementem walki psychologicznej[5].

2.1.1. Dezinformacja jako element zagrożenia – identyfikacja ogólna

Z przeprowadzonych badań wynika, że od czasu powstania i rozwoju pierwszych form zorganizowanych społeczności, ich przywódcy i dowódcy formacji zbrojnych – w celu wprowadzenia przeciwników w błąd co do swoich zamierzeń, planów i działań – stosowali dezinformację. Nie używano wówczas tego terminu, natomiast wszelkie metody wprowadzenia przeciwnika w błąd nazywano fortelem, podstępem itp. Najoryginalniejsze i najbardziej pomysłowe przykłady podstępu, kłamstwa w poli-

[4] W pojęciu wojskowym dezinformacja to rozpowszechnianie nieprawdziwych wiadomości i dokumentów dla wprowadzenia w błąd przeciwnika co do faktycznego zamiaru. organizacji i prowadzenia operacji (walki, bitwy), a także składu wojsk własnych i charakteru ich działania; jest ona jednym z podstawowych sposobów realizacji zadań maskowania strategicznego, stanowi również jeden z elementów maskowania operacyjnego (Leksykon Wiedzy Wojskowej - Wyd MON, Warszawa 1979).

[5] Wojna psychologiczna to system oparty na specjalnych metodach i sposobach oddziaływania dywersji polityczno-propagandowej na żołnierzy i społeczeństwo przeciwnika w celu osłabienia ich odporności psychicznej. Głównym elementem w.p. jest dywersja ideologiczna stosowana przy jednoczesnym nacisku dyplomatycznym i ekonomicznym, a nawet szantażu militarnym, sabotażu i terrorze, dezinformacji i prowokacji (Leksykon Wiedzy Wojskowej - Wyd. MON, Warszawa 1979).

tyce i w walce zbrojnej były zbierane, uogólniane i opisywane przez historyków i teoretyków wojskowych. Pierwszym, który na podstawie doświadczeń wojennych z przełomu VI i V w. p.n.e. dokonał takiej analizy przedsięwzięć dezinformacyjnych był chiński filozof, uczony mąż i doradca Sun Zi[6]. Pisał on „wojna to droga kłamstwa, dlatego jeśli coś możesz – pokazuj, że nie możesz; jeśli korzystasz z czegoś – pokazuj, że nie korzystasz; jeśli jesteś blisko – pokazuj, że daleko; jeśli znajdujesz się daleko – pokazuj, że jesteś blisko; zwabiaj przeciwnika korzyściami, spowoduj u niego dezorganizacje i bierz go; przyjąwszy pokorny wygląd, wzbudź w nim pewność siebie; napadaj przeciwnika, kiedy nie jest przygotowany; pojawiaj się tam, gdzie on ciebie nie oczekuje". W wyniku uogólnień i przeprowadzonej analizy Sun Zi określił pięć głównych metod stosowania fortelu, tj.: działania pozorujące; oddziaływanie na psychikę; dezorganizowanie szeregów; usypianie czujności; wykorzystywanie błędów, niedoskonałości, nie przygotowania i nieostrożności przeciwnika.

Początki zorganizowanej na szeroką skalę dezinformacji, na przykład w wykonaniu rosyjskim, sięgają pierwszych lat istnienia ZSRR. Pierwszy schemat organizacyjny CzK zawierał wydział prowokacji, który jest uważany za pierwszą komórkę organizacyjną zajmującą się dezinformacją. W latach 1921-1927 OGPU[7] prowadził jedną z najefektowniejszych operacji dezinformacyjnych pk. "Trust"[8], której celem było ukrycie prawdziwego oblicza państwa oraz pozyskanie zachodniego kapitału. Lenin w 1921 roku zapowiedział światu odejście od wojującego komunizmu na rzecz stopniowego nawrotu do gospodarki rynkowej i liberalizacji sfery polityczno-gospodarczej, czyli tzw. Nową Ekonomiczną Politykę. Idea NEP-u polegała na demonstracji odwrotu komunizmu od polityki konfrontacji na rzecz współpracy z Zachodem. Akcją kierował Feliks Dzierżyński, który za pośrednictwem utworzonej organizacji "Trust" przekazywał dezinformacyjne wiadomości do służb wywiadowczych państw Zachodu. W ramach tego planu Dzierżyński założył m.in. pewną liczbę "opozycyjnych" gazet (np. "Nową Rosję"). Zadaniem tych gazet było szerzenie propagandy szerokich zmian w życiu polityczno-ekonomicznym kraju. Kadrowi pracownicy OGPU organizowali spotkania z rosyjskimi pisarzami na emigracji, namawiali ich do powrotu. Redaktorzy "opozycyjnych" gazet przeprowadzali wywiady ze zwolnionymi

[6] Sun Zi - "Sztuka wojny" , Przedświt, Warszawa 1994.

[7] OGPU (Objedinionnoje Gosudarstwiennoe Polityczeskoje Uprawlenije) - Zjednoczony Państwowy Zarząd Polityczny, 1922-1934 naczelny organ radzieckich władz bezpieczeństwa (Encyklopedia Popularna PWN, wydanie siódme, Warszawa 1985).

[8] E.J.Epstein - „Postęp" niewidzialna wojna między KGB a CIĄ rozdział II pt. Trust (Oficyna Wydawnicza SCRIPTAMENENT - Krosno 1993).

więźniami politycznymi, informowali o zawieszeniu cenzurowania książki i sztuk teatralnych. W atmosferze "głasnosti" Związek Radziecki otworzył się również dla zachodniego biznesu. Problemem było jednak przekonanie zachodnich biznesmenów, pamiętających zabór ich własności bez odszkodowania w 1917 roku, że obecne inwestycje będą bezpieczne. W tym celu posłużono się Armandem Hammerem, który otrzymał fikcyjną koncesję i rozgłosił ten fakt w Ameryce. Do roku 1925 Hammerowi udało się pozyskać dla sprawy inwestowania w przedsiębiorstwa radzieckie wiele prestiżowych korporacji, w tym Ford Motor Company. Po osiągnięciu założonych celów, w roku 1929 NEP upadła, wszystkie prywatne przedsiębiorstwa znacjonalizowano, większość inwestycji uległa konfiskacie bez odszkodowania, ponownie wprowadzono cenzurę, stłumiono ruchy opozycyjne, zamknięto niepartyjne gazety.

We współczesnych warunkach celem dezinformacji jest stałe utrzymywanie w niepewności potencjalnego przeciwnika, wprowadzenie go błąd co do faktycznych zamierzeń, planów kierownictwa politycznego i wojskowego oraz przedsięwzięć realizowanych w państwie i w siłach zbrojnych. Natomiast w czasie prowadzenia działań bojowych dezinformacja będzie odgrywać główną rolę w uzyskaniu zaskoczenia w skali operacyjno-taktycznej.

Dezinformacja w skali globalnej może funkcjonować w sferze politycznej, ekonomicznej, naukowo-technicznej i militarnej. W zależności, w której jest stosowana, można podzielić ją na: polityczną, ekonomiczną, naukowo-techniczną i wojskową. Dezinformację polityczną może prowadzi państwo. W sferze wewnętrznej jej obiektem może być własne społeczeństwo. Dezinformacja może więc być narzędziem służącym ukształtowaniu pożądanych postaw, opinii i zachowań własnego społeczeństwa. Może się objawiać w ustawodawstwie, systemie kształcenia i wychowania młodzieży, w systemie informacji społecznej, a nawet w programach naukowo-badawczych. W sferze zewnętrznej może być skierowana przeciw innym państwom. Jej celem może być kształtowanie pozytywnej opinii o własnym państwie na arenie międzynarodowej W wypadku prowadzenia polityki wywołującej krytykę czy sprzeciw międzynarodowej opinii społecznej celem dezinformacji może być ukrywanie prawdziwych zamiarów. Rząd poprzez dezinformację może dążyć do uzyskania akceptacji i wsparcia społeczności międzynarodowej dla swojej działalności.

Historia rozwoju społeczeństwa, stosunków międzypaństwowych oraz doświadczenia minionych wojen wskazują, że znaczenie dezinformacji stawało się coraz większe. Początkowo odgrywała ona główną rolę w polityce i w sferze militarnej,

a następnie objęła dziedziny ekonomii i sfery naukowo-techniczne. Realizacja przedsięwzięć z zakresu dezinformacji w dziedzinie ekonomicznej państwa, tj. przedsięwzięć dezinformacji gospodarczej, może mieć na celu wprowadzenie przeciwnika w błąd co do osiągnięć ekonomiczno-gospodarczych, dotyczących możliwości obronnych państwa, a w tym: rozmieszczenia obiektów, posiadających ważne znaczenie dla obronności; czasu, metod i sposobów konwersji produkcji przemysłowej na potrzeby wojska; mocy produkcyjnych oraz rodzajów i typów wytwarzanej produkcji wojskowej. Z tym obszarem dezinformacji wiąże się ściśle obszar nauki i techniki. Działalność dezinformacyjną na tym polu można określić jako dezinformację w dziedzinie naukowo-technicznej. Celem tego rodzaju dezinformacji może być wprowadzenie potencjalnego przeciwnika lub konkurencji w błąd co do rzeczywistych osiągnięć, odkryć naukowych na rzecz zdolności obronnej państwa i sił zbrojnych, zgromadzonych doświadczeń w zakresie operacyjnego-bojowego wyszkolenia wojsk, zmian w teorii sztuki wojennej, nowych modeli techniki wojskowej i uzbrojenia, ich parametrów taktyczno-technicznych i możliwości bojowych, sposobów ich wykorzystania oraz perspektyw rozwoju i możliwości wejścia do uzbrojenia wojsk. Obszarem dezinformacji najbardziej istotnym z punktu widzenia sił zbrojnych i obronności państwa jest z pewnością dezinformacja wojskowa. Najogólniej ujmując, obiektami tej dezinformacji będzie: przeciwnik, wojska własne oraz otoczenie, w którym następuje styczność obu stron. Oddziaływanie na przeciwnika może być skierowane na dwa elementy – na system dowodzenia i kierowania oraz na system rozpoznania. W tej sytuacji jej istotą będzie przekazywanie przez system rozpoznania przeciwnika fałszywych informacji do jego centrum decyzyjnego. Natomiast istotą dezinformacji w stosunku do wojsk własnych może być powodowanie takiego ich działania, aby umacniało przeciwnika w przekonaniu o słuszności jego wniosków z rozpoznania. Taki sam cel może mieć dezinformacja w stosunku do otoczenia (do ludności cywilnej, członków ruchów partyzanckich, jeńców, pracowników wywiadu, obserwatorów i obcokrajowców). Reasumując, można użyć stwierdzenia, że dezinformacja wojskowa to zamierzone rozpowszechnianie, odpowiednio dobranymi kanałami, fałszywych informacji, pogłosek, dokumentów oraz demonstrowanie działań wojsk, których celem jest wprowadzenie w błąd przeciwnika odnośnie prawdziwych zamierzeń i przeprowadzonych przedsięwzięć o znaczeniu militarnym.

W trakcie przygotowywania i prowadzenia operacji dezinformacja wojskowa może być jednym z elementów uzyskania zaskoczenia, a tym samym osiągania po-

wodzenia w walce. Obecnie może się stać wyjątkowo rozgałęzioną i wielostronną dziedziną strategii wojennej[9] i wojskowej państwa, będącej w ścisłym związku z polityką, gospodarką oraz nauką i techniką.

Dezinformacja wojskowa ze względu na zakres, rolę, charakter i treść może być prowadzona w skali strategicznej, operacyjnej i taktycznej. Dezinformację w skali strategicznej powinny organizować i prowadzić centralne organy kierowania państwem. Bezpośrednim organizatorem i koordynatorem przedsięwzięć dezinformacyjnych powinno być naczelne dowództwo, odpowiedzialne za funkcjonowanie systemu obronnego państwa i wypracowanie strategii użycia sił zbrojnych zgodnie z doktryną wojenną. Swoim zakresem powinna obejmować własne państwo, w tym siły zbrojne oraz jego otoczenie międzynarodowe. Prowadzić ją można w sferze politycznej, dyplomatycznej, ekonomicznej, naukowo-technicznej i innych - np. wywiadu i kontrwywiadu.

W czasie pokoju przedsięwzięcia dezinformacji wojskowej w skali strategicznej mogą obejmować zagadnienia dotyczące: szkolenia, struktur organizacyjnych, dyslokacji, stanu gotowości bojowej, sposobów i terminów mobilizacyjnego i operacyjnego rozwinięcia sił zbrojnych; zadań strategicznych; planów i sposobów prowadzenia pierwszej operacji; składu wyposażenia i gotowości bojowej zgrupowań wojsk rozwiniętych w czasie pokoju; stopnia operacyjnego przygotowania terytorium państwa oraz systemu kierowania i dowodzenia siłami zbrojnymi.

W czasie narastania sytuacji kryzysowej i prowadzenia działań bojowych dezinformacja wojskowa może obejmować zagadnienia dotyczące: składu zgrupowań wojsk; charakteru, sposobów i kierunków działań bojowych; treści wykonywanych zadań; obiektów, na które planuje się wykonać uderzenia, rejonów i terminów wysadzenia desantów; kierunków oraz terminów wprowadzenia do walki drugich rzutów i odwodów.

Przedsięwzięcia dezinformacyjne mogą być realizowane zgodnie z planem dezinformacji naczelnego dowództwa. Przedsięwzięcia z zakresu dezinformacji wojskowej w skali operacyjnej mogą być potwierdzeniem i logicznym ciągiem fałszywych informacji, przekazywanych przeciwnikowi w skali strategicznej. Mogą dotyczyć sposobu przygotowania i prowadzenia operacji zaczepnych i obronnych; wykorzystania

[9] Strategia wojenna - najważniejsza dziedzina sztuki wojennej, obejmująca teorię i praktykę obronnego przygotowania państwa, sił zbrojnych, planowania i prowadzenia na skalę strategiczną działań wojennych oraz kierowanie nimi. Częścią składową strategii wojennej jest strategia wojskowa, tj. zbiór założeń i zasad odnośnie tworzenia i wykorzystania sił zbrojnych (Leksykon Wiedzy Wojskowej - Wyd MON, Warszawa 1979).

związków taktycznych oraz rodzajów sił zbrojnych; gotowości i zdolności bojowej wojsk; rozmieszczenia punktów dowodzenia i węzłów łączności; zasad organizacji zabezpieczenia operacyjnego i logistycznego. W trakcie bezpośredniego przygotowania operacji główny wysiłek dezinformacji można skupiać na ukryciu: faktu prowadzenia przygotowań do operacji i planu operacji; stanu gotowości planowanych do użycia wojsk, rejonów ześrodkowania odwodów lub prowadzonej mobilizacji; gotowości środków rażenia; rejonów rozwijania stanowisk dowodzenia oraz reżimu pracy środków łączności, kierunków ruchu wojsk i przewozów zabezpieczenia logistycznego.

Przedsięwzięcia z zakresu dezinformacji wojskowej w skali taktycznej wydaje się, że powinny być realizowane wyłącznie na mocy zarządzenia przełożonego. Prowadzić je można przede wszystkim w związkach taktycznych i oddziałach, będących w bezpośredniej styczności z przeciwnikiem lub w pasie przyfrontowym. Celem tych działań może być potwierdzenie rozpowszechnionych w skali operacyjnej, a czasami i strategicznej fałszywych informacji i tym samym utwierdzenie przeciwnika o ich prawdziwości.

Dezinformacja wojskowa w skali strategicznej, może być realizowana potencjałem sił zbrojnych i państwa, zgodnie z centralnie opracowanym planem. Powinna być organizowana zarówno w czasie pokoju, jak i w czasie wojny. Potwierdzeniem działań pozornych i fałszywych informacji organizowanych na szczeblu strategicznym, powinny być działania dezinformacyjne w skali operacyjnej i taktycznej. W czasie przygotowania dezinformacji wojskowej powinno się uwzględniać zamierzenia planu maskowania operacyjnego, WRE i zwalczania elementów rozpoznawczych przeciwnika.

W celu skutecznego przeciwdziałania rozpoznaniu przeciwnika, wprowadzenia go w błąd, a przez to zapewnienia osiągnięcia celu, dezinformacja powinna spełniać określone wymagania. Powinna być:

- scentralizowana,
- kompleksowa,
- spójna,
- wiarygodna,
- nieszablonowa,
- oparta na znajomości planów przeciwnika,

- skryta,
- terminowa,
- ciągła,
- dublowana,
- elastyczna.

Centralizacja powinna polegać na tym, że zadania poszczególnych organów dowodzenia będą ściśle rozgraniczone. Sztab niższego szczebla będzie wykonywał tylko i wyłącznie zadania otrzymane od przełożonego. Wszelka inicjatywa w prowadzeniu dezinformacji wojskowej ze strony niższych szczebli może być dopuszczalna jedynie wyjątkowo i wyłącznie za zgodą przełożonego. Wynika to z tego, że niższy szczebel, nie znając zamiaru i planu przełożonego, podczas realizacji pozornego przedsięwzięcia z własnej inicjatywy mógłby zakłócić plan działania przełożonego. Z analizy minionych wojen wynika, że każde pozorne przedsięwzięcie i działanie realizowane z własnej inicjatywy, w celu wprowadzenia przeciwnika w błąd, bez zgody wyższego przełożonego, w większości wypadków nie osiągało swojego celu i pozwalało przeciwnikowi na rozpoznanie prawdziwych informacji i działań. Dlatego, dla uniknięcia sprzeczności w planowaniu i realizacji przedsięwzięć dezinformacyjnych, kierowanie nimi powinno skupić się w centralnym organie dowodzenia siłami zbrojnymi.

Kompleksowość winna się sprowadzać do stosowania różnorodnych form, metod i sposobów, przy całościowym wykorzystywaniu dostępnych sił i środków oraz kanałów do transmisji dezinformacji we wszystkich dziedzinach, które wiążą się z działaniem sił zbrojnych. Spełnienie wymogu kompleksowości nabiera szczególnego znaczenia w okresie pokoju i w czasie narastania konfliktu, gdyż przedsięwzięcia dezinformacyjne są na tym etapie łatwe do zdemaskowania. Aby odniosły cel, powinny być prowadzone przez wszystkie szczeble dowodzenia siłami zbrojnymi i administracji państwa.

Spójność winna wynikać ze zgodności celu dezinformacji z celem polityki zewnętrznej państwa i militarną działalnością sił zbrojnych. Wymóg ten oznacza, że przedsięwzięcia dezinformacyjne powinny być prowadzone w sposób systemowy, tzn. aby wysyłane fałszywe informacje i prowadzone działania demonstracyjne były dla przeciwnika logicznym ciągiem. Cel polityki zewnętrznej kierownictwa państwowego winien być elementem nadrzędnym, z którego wynika celowość działania sił

zbrojnych, i dopiero na podstawie tych czynników można określić cele dezinformacji. Powstaje więc zależność, że cele operacji militarnych zależą od celu, jaki państwo zamierza osiągnąć poprzez wojnę, natomiast cel dezinformacji wojskowej zależy głównie od celu danej konkretnej operacji.

Wiarygodność polega na prowadzeniu dezinformacji tak, aby z dużym prawdopodobieństwem oddawała charakter działań rzeczywistych. Oznacza to, że przeciwnik powinien uwierzyć w przekazywane mu informacje i podjąć oczekiwane działania. W tym celu podczas przygotowywania fałszywych informacji należy umieścić w nich część rzeczywistych danych, natomiast fałszywe informacje dobierać tak, ażeby na tle ogólnej sytuacji i konkretnych okoliczności wydawały się prawdopodobnymi. Osiągać to można przez przekazywanie informacji już znanych przeciwnikowi, bądź drugorzędnych, nieaktualnych i takich, których poufność w najbliższym czasie zdezaktualizuje się. Dla spełnienia wymogu wiarygodności przekazywane informacje powinny być logiczne, a ich konstrukcja tak zbudowana, aby w wypadku wykrycia przez przeciwnika prawdziwych danych zostałyby one uznane za fałszywe. Przykładem wiarygodności dezinformacji może być plan przeprowadzenia przez Niemców pierwszej zaskakującej operacji przeciwko Francji, w początkowym okresie pierwszej wojny światowej, który zakładał wprowadzenie francuskiego dowództwa w błąd co do kierunku głównego uderzenia. Plan Schlieffena przewidywał koncentrację wojsk na lewym skrzydle przeciw francuskim umocnieniom w Ardenach. Ponieważ niemieckie dowództwo wiedziało, że informacjami na temat kierunku ich głównego uderzenia był zainteresowany również wywiad rosyjski, zostały stworzone wszelkie warunki, ażeby ten plan trafił w ich ręce. Opracowano więc ideę oszukania Francuzów przy pomocy rosyjskiego dowództwa. Podczas opracowywania planu zostały świadomie włączone takie dane, które zostały potwierdzone przez rosyjski wywiad. Pozorując przygotowanie głównego uderzenia przez Ardeny, Niemcy przegrupowali swoje główne zgrupowanie na prawe skrzydło w celu wykonania uderzenia z północnego zachodu w kierunku na Paryż, obchodząc francuskie umocnienia w Ardenach.

Nieszablonowość może polegać na unikaniu wcześniej użytych metod i ciągłym zmienianiu sposobów jej stosowania. Szczególnie szeroką różnorodność metod ukazuje nam analiza przypadków dezinformacji prowadzonej przez dowództwo Armii Czerwonej w drugiej wojnie światowej. W jednych z operacji, natychmiast po przekazaniu przeciwnikowi fałszywych danych, dokonywano pod obserwacją rozpoznania przeciwnika pozornego przegrupowania wojsk. Szczególnie szeroko praktykowana

była imitacja pozornych obiektów, demonstracja przegrupowań wojsk poprzez przesunięcie do linii frontu pustych lub z niewielką liczbą wojsk, składów kolejowych i kolumn samochodowych. Następnie, kiedy przeciwnik przekonywał się o ich realności i umacniał dany kierunek kosztem własnych odwodów bądź innych odcinków frontu, dowództwo rosyjskie dokonywało bezpośrednio przed rozpoczęciem operacji zaczepnej faktycznego przegrupowania i koncentracji wojsk na kierunku uderzenia - np. operacja ,,Bagration"[10]. W innych operacjach dokonywano faktycznego przegrupowania wojsk, skupiając wysiłek na tym, aby przeciwnik uznał to za pozorowanie[11]

Znajomość planów przeciwnika to warunek, który może bardzo ułatwiać przeprowadzenie skutecznej dezinformacji. Ustalenie jakimi przedsięwzięciami, obiektami i rejonami interesuje się wywiad przeciwnika oraz na zdobycie jakich informacji skupiają główny wysiłek jego elementy rozpoznawcze pozwala na właściwe, wiarygodne i skuteczne zorganizowanie przedsięwzięć dezinformacyjnych. Dysponując takimi wiadomościami można niejako „pomóc" przeciwnikowi w zdobyciu pożądanych informacji, przekazując je w spreparowanej postaci.

Skrytość powinna się sprowadzać do utrzymania przedsięwzięć w tajemnicy przed przeciwnikiem, ale też przed własnymi wojskami realizującymi te przedsięwzięcia i otoczeniem zewnętrznym. W celu zapewnienia skrytości przedsięwzięć zarówno w czasie pokoju jak i podczas przygotowania oraz prowadzenia operacji należy dążyć do ograniczenia kręgu osób, znających plan przedsięwzięć dezinformacyjnych. Przykładowo plan dezinformacji Schlieffena znał Wilhelm II, szef Sztabu Generalnego feldmarszałek Moltke oraz szef wywiadu. Natomiast agent, któremu zlecono przekazanie tego planu Rosjanom, nawet się nie domyślał się, że przekazywany dokument był fałszywy. W czasie przygotowania wielu operacji w drugiej wojnie światowej do kierowania realizacją przedsięwzięć z zakresu dezinformacji przeciwnika wyznaczono osoby funkcyjne oraz sztaby, o działalności których nie wiedzieli nawet oficerowie sztabów frontów i armii, natomiast wykonawcy tych zadań nie wiedzieli, że

---

[10] "Bagration" - strategiczna operacja białoruska Armii Radzieckiej przeprowadzona w okresie 23.06-31.07.44 na obszarze Białorusi, Litwy i wsch. Polski przeciwko wojskom niemieckim (Encyklopedia II wojny światowej, Wyd MON, Warszawa 1975).

[11] Pozorowanie to sztuczne tworzenie obrazu zbliżonego do rzeczywistości dla wprowadzenia przeciwnika w błąd, wykonywane w ramach maskowania operacyjnego. Pozorowanie obejmuje: stosowanie obiektów pozorowanych, działania demonstracyjne, pozorne przedsięwzięcia organizacyjne, imitujące rzeczywistą działalność wojsk i sztabów; dokonywanie pozornych przemarszów i przewozów wojsk, sprzętu technicznego i środków materiałowych; tworzenie dowództw i sztabów sugerujących obecność oddziałów i związków (Leksykon Wiedzy Wojskowej - Wyd MON, Warszawa 1979).

są to przedsięwzięcia dezinformacyjne, gdyż tylko wtedy, gdy wykonawcy przedsięwzięć dezinformacyjnych nie będą znać ich prawdziwego sensu, zachowają pożądaną w ich działaniach naturalność.

Terminowość oznacza, że efektywność przedsięwzięć dezinformacyjnych będzie wysoka tylko wtedy, gdy zostaną one dostarczone przeciwnikowi z takim wyliczeniem, aby zdołał on jeszcze zareagować na otrzymane informacje. Przekazanie przeciwnikowi fałszywych danych i nie potwierdzenie ich w zaplanowanym czasie innymi działaniami dezinformującymi, a niekiedy działaniami rzeczywistymi, ograniczy jego czas na podjęcie decyzji o przeprowadzeniu kontrprzedsięwzięć. Podjęte przez przeciwnika działania są dla prowadzącego dezinformację potwierdzeniem jej skuteczności.

Ciągłość działań dezinformujących wiąże się ściśle z czynnikiem czasu. Wysyłanie fałszywych danych powinno przebiegać systematycznie. Intensywność dezinformacji nie powinna narastać przed rozpoczęciem operacji bojowej czy innych aktywnych działań, gdyż wzbudzi podejrzenia przeciwnika i zmobilizuje go do podjęcia intensywniejszych działań rozpoznawczych. Ciągłość dezinformacji nie może też wyglądać na narzucanie rozpoznaniu i dowództwu przeciwnika wniosków bądź określonego obrazu działań. To on sam powinien, na podstawie ciągłych, otrzymywanych z różnych źródeł i różnymi kanałami informacji, ocenić sytuację i podjąć oczekiwane przez dezinformującego działania.

Dublowanie przedsięwzięć dezinformacyjnych jest niezbędnym elementem potwierdzenia już przekazanych przeciwnikowi fałszywych informacji. Szczególnie ważnym jest, dla potwierdzenia wiarygodności, demonstrowanie przeciwnikowi działań wojsk, które wydają się przeciwnikowi prawdopodobnymi. W skali strategicznej, dublowanie przedsięwzięć dezinformacji wojskowej realizuje się nie tylko przy pomocy sił i środków sił zbrojnych, ale również z szerokim wykorzystaniem politycznych, dyplomatycznych, ekonomicznych, naukowo-technicznych i innych oficjalnych i nieoficjalnych kanałów.

Elastyczność dezinformacji polega na uściśleniu we właściwym czasie i stosownie do zmian zachodzących w sytuacji polityczno-wojskowej na arenie międzynarodowej, a w czasie działań zbrojnych również w położeniu strategiczno-operacyjnym wojsk - przedsięwzięć, zadań i czasu ich wykonania, a w miarę potrzeb, na zmianie wykonawców zadań. Aby sprostać temu wymogowi organ kierujący dezinformacją powinien prowadzić ciągłą analizę jej skutków.

Dezinformację wojskowa; ze względu na formę objawiającą się przez pryzmat metod, sposobów, stosowania środków, kanałów transmisyjnych danych oraz przekazywanych treści i podejmowanych działań pozornych; można zgrupować w trzech przestrzeniach funkcjonalnych: przekazu, dokumentu i działania.

W ramach przekazu mogą być stosowane trzy metody – ustna, pisemna i sensoryczna. W przekazie ustnym, w celu dostarczenia przeciwnikowi dezinformujących danych, może być wykorzystywany stan osobowy wojsk własnych, miejscową ludność, dyplomaci, przedstawiciele firm państwowych i prywatnych, jak również telewizję, radio oraz wojskowe i cywilne środki łączności. Mogą być też wykorzystywane środki pozorujące mieszczące się w dostępności penetracji sensorycznej stosowanej przez przeciwnika.

W ramach dokumentacji dezinformowanie może polegać na odpowiednio usystematyzowanym dostarczeniu przeciwnikowi fałszywych: dyrektyw, rozkazów, zarządzeń bojowych, meldunków, map decyzji, roboczych dokumentów operacyjnych, planów zabezpieczenia działań bojowych, współdziałania, obiektów wojskowych, schematów obrony, łączności, ognia, rozmieszczenia celów, obserwacji, pól minowych; harmonogramów uderzeń, przelotów i przegrupowań wojsk. itp. Uzupełnieniem mogą być treści dezinformacyjne publikowane w wojskowych czasopismach, dziennikach, broszurach, ulotkach propagandowych i plakatach.

W ramach działania ważnym elementem dezinformacyjnym są odpowiednio spreparowane ruchy wosk i akcje bojowe pozorujące sytuacje ujawnione wcześniej w ramach przekazu i dokumentacji. Można przyjmować, że dezinformacja osiągnie swój cel wówczas, gdy przeciwnik obserwując działania pozorujące uzna je za realne. Z analizy doświadczeń wojennych wynika jednak, że osiągnięcie tego staje się możliwe, kiedy wszystkie formy dezinformacyjne składają się na spójną realnie całość. Klasycznym przykładem tego może być przygotowywanie przez państwa zachodnie desantu w Normandii. Celem wprowadzenia niemieckiego wywiadu i kierownictwa polityczno-wojskowego w błąd co do desantu przez kanał La Manche, na szeroką skalę wykorzystywano środki radiowe. Celowo prowadzono rozmowy radiowe przez fikcyjną armię Pattona, pozorując jej koncentrację naprzeciw cieśniny Pas de Calais. W celu większego uwiarygodnienia tej sytuacji, sam generał Patton niejednokrotnie pojawiał się w tym rejonie. Również niemieccy agenci, rozpracowani przez angielski kontrwywiad, przekazywali do centrali dane potwierdzające koncentrację. Niemieckie dowództwo uznało więc wszystkie napływające informacje za praw-

dopodobne i w dalszym ciągu utrzymywało na tym kierunku 15. Armię w rejonie Calais oraz cztery dywizje pancerne odwodu Dowództwa "Zachód".

Innym przykładem zastosowania dezinformacji w technicznych środkach łączności była agresja Izraela na Egipt w 1967 roku. Dowództwo Izraela, znając szyfry oraz robocze częstotliwości egipskich radiostacji obrony powietrznej, dokonało dezinformacji poprzez przekazanie fałszywego rozkazu, co doprowadziło do obniżenia czujności i zmniejszenia gotowości bojowej oddziałów sił powietrznych i OPL armii egipskiej. W rezultacie przeprowadzona przy pomocy środków radiowych dezinformacja zapewniła dużą skuteczność zmasowanych uderzeń izraelskiego lotnictwa na wojska, lotniska, stacje radiolokacyjne i środki OPL Egiptu. Można przypuszczać, że w dobie obecnej znaczenie tego sposobu, wraz z globalnym zasięgiem współczesnych środków łączności, nabierze jeszcze większego znaczenia. Wysoko rozwinięte państwa, dysponujące najnowocześniejszymi środkami łączności i WRE, są w stanie zablokować każdą informację, lub stworzyć wrażenie istnienia fikcyjnych zdarzeń i przez to kształtować opinię całych społeczności.

Duże znaczenie może mieć dezinformacja prowadzona poprzez publikację fałszywych informacji w prasie cywilnej i wojskowej. Działalność ta może być ukierunkowana na kształtowanie przychylnej dla kierownictwa danego państwa opinii własnego społeczeństwa, dotyczącej np. konieczności zwiększenia wydatków na zbrojenia lub potrzeb związanych z obecnością wojskową w różnych regionach świata, uzasadnianych obroną strategicznych interesów państwa. Z tym sposobem dezinformacji ściśle wiąże się fałszowanie dokumentów, które służą potwierdzeniu rozpowszechnianych w prasie i innych środkach masowego przekazu informacji. Fałszowanie dokumentów łączy się z kolejnym sposobem dezinformacji, tj. zamierzonym "zagubieniem" fałszywych lub odtajnionych dokumentów. W tym celu można organizować ,,nieszczęśliwe wypadki" lub "przypadkowe zapomnienia" dokumentów w torbach polowych, walizkach dyplomatycznych czy nie zamkniętych sejfach. Tym sposobem posłużyło się angielsko-amerykańskie dowództwo w maju 1943 roku, w celu zatajenia przygotowań do operacji ,,Husky"[12] – dla potwierdzenia dezinformacji prowadzonej w środkach masowego przekazu, dostarczyło na okręcie podwodnym do brzegów Hiszpanii trupa w mundurze majora angielskiej armii. Do zwłok była celowo

[12] Morska operacja desantowa sił sprzymierzonych pk. "Husky" przeciwko wojskom niemieckim i włoskim, przeprowadzona (10-17.07.1943) w celu opanowania Sycylii i przygotowania warunków do inwazji na Włochy (Encyklopedia II wojny światowej Wyd. MON, Warszawa 1975).

przymocowana teczka z egzemplarzem planu fikcyjnej operacji i oryginalne listy przełożonych, w których wspomniano o przygotowaniu pozornych operacji inwazji na Francję, Bałkany i Norwegię. Angielskie dowództwo przejawiając aktywnie i celowo zaniepokojenie z powodu śmierci oficera w katastrofie lotniczej i zaginięcia teczki z dokumentami, zwróciło się z zapytaniem do Hiszpanii. Po upewnieniu się, że teczka została spenetrowana przez niemiecki wywiad, Anglicy opublikowali w gazecie "Times" informację o pogrzebie "zmarłego" majora Martina.

W ramach temu podobnych działń mogą być sterowane wystąpienia i oświadczenia przywódców politycznych i wojskowych, przedstawiające fałszywe dane. Na przykład, przed przystąpieniem do realizacji planu "Barbarossa"[13], kierownictwo polityczno-wojskowe faszystowskich Niemiec w wystąpieniach radiowych i prasowych dążyło do wprowadzenia w błąd kierownictwa ZSRR, celem odwrócenia jego uwagi od przygotowań do rozpoczęcia wojny na Wschodzie. Celem dezinformacji było przedstawienie działań przygotowawczych jako przygotowań do wojny przeciw Anglii.

Konflikt zbrojny Izraela z Egiptem w 1967 r. był również przykładem stosowania tego sposobu dezinformacji w wojnach lokalnych. Rząd Izraela i dowództwo sił zbrojnych niejednokrotnie występując w radiu i telewizji wszelkimi sposobami starały się upozorować przygotowywanie uderzenia na Syrię. Dla większej wiarygodności izraelski parlament, miesiąc przed rozpoczęciem agresji, jawnie udzielił rządowi pełnomocnictw do przeprowadzenia operacji przeciwko Syrii. Przeprowadzono w sposób jawny mobilizację wojsk i demonstracyjną koncentrację ich części przy granicy syryjskiej. Kiedy minister obrony Izraela mówił w radiu o potrzebie poszukiwania pokojowych rozwiązań, lotnictwo izraelskie otrzymało rozkaz do wykonania uderzenia na obiekty egipskie.

Bardzo skutecznym sposobem dezinformacji przeciwnika może być przygotowanie działań pozorujących. Przedsięwzięcia z zakresu przygotowania i realizacji działań pozorujących, jak wskazują doświadczenia drugiej wojny światowej, były prowadzone zarówno przed rozpoczęciem rzeczywistych operacji, jak i równocześnie z nimi. Ich celem było wprowadzenie przeciwnika w błąd co do zamiaru i planu tych operacji, odwrócenie zainteresowania przeciwnika szczególnie ważnymi kierunkami i rejonami przyszłych działań wojsk. Przykładem takiego planowania operacji

[13] „Barbarossa" - kryptonim niemieckiego planu agresji dokonanej w 1941 r. na ZSRR. Ogólne wytyczne do przygotowania planu agresji Hitler wydał feldmarsz. W. Brauchitschowi i gen. F. Halderowi w lipcu 1940r. wyznaczając początek działań na wiosnę 1941 r. (Encyklopedia II wojny światowej Wyd. MON, Warszawa 1975).

był plan dezinformacji „Bodygard", który w następnej kolejności przerodził się w plan specjalnej operacji pozorującej ,,Dywan", zakładający przeprowadzenie serii pozornych przedsięwzięć i działań wojsk angielsko-amerykańskich przed wysadzeniem desantu w Normandii. W początkowym okresie przygotowania tej operacji dowództwo amerykańsko-brytyjskie wykorzystywało wszystkie kanały, w których rozpowszechniano informacje o wszechstronnym przygotowywaniu inwazji wojsk sprzymierzonych w innych rejonach kontynentu europejskiego. Kiedy maskowanie znacznej liczby wojsk i okrętów na południu Anglii stało się niemożliwe, główny wysiłek dezinformacji został skierowany na wprowadzenie niemieckiego dowództwa w błąd co do prawdziwego rejonu wysadzenia desantu i kierunku głównego uderzenia. W tym celu została opracowana operacja desantowa ,,Bigot", zakładająca wysadzenie desantu przez cieśninę Pas de Calais. Wszystkie przekazywane dane – zarówno fałszywe jak i prawdziwe, były potwierdzane poprzez tworzenie pozornych koncentracji okrętów i wojsk oraz prowadzenie ćwiczeń na kierunkach Calais i Boulogne. W przeddzień operacji pozorowano ogniowe przygotowanie w pozornych rejonach z większą intensywnością niż w rzeczywistym rejonie wysadzenia desantu, dodatkowo skierowano w ten rejon dużą liczbę rybackich barek, pozorujących zbliżanie się desantu morskiego. Ważną rolę w dezinformowaniu niemieckiego dowództwa odegrała uruchomiona w kwietniu 1944r., nadająca w niemieckim języku tajna radiostacja „Soldatensender Calais"[14]. Głównym celem szerzonej przez radio propagandy[15] było usypianie czujności sztabów i wojsk niemieckich we Francji, stworzenie pozorów spokoju, zręczne sugerowanie, że inwazja na kontynent jest wciąż jeszcze czymś bardzo odległym, bowiem Wał Atlantycki, wzniesiony na zachodnich wybrzeżach „fortecy Europy" skutecznie paraliżuje wszelką myśl o ataku od strony morza.

Analogiczne przedsięwzięcia w celu dezinformacji niemieckiego dowództwa były prowadzone także przed inwazją wojsk amerykańskich i angielskich w północnej i północno-zachodniej Afryce. Idea operacji „Solo-I" polegała na tym, aby stworzyć wiarygodne wrażenie przygotowań do inwazji na Norwegię. W tym celu w wojskach przeprowadzono ćwiczenia o tematyce górskiej, wydano ludziom mundury arktyczne,

[14] Kozaczuk Wł. - Wojna w eterze, rozdz. pl. Overlord i ostanie miesiące wojny, s. 193-200 (Wyd Radia i Telewizji, Warszawa 1977).

[15] Propaganda - to ściśle określone działanie, polegające na przemyślanym rozposzechnianiu, za pomocą wszelkich środków przekazu, doktryn. idei, faktów, argumentów, informacji, sądów lub wystąpień w celu poparcia strony zaprzyjaźnionej, względnie osłabienia przeciwnika (Regulamin Wojny Psychologicznej Sił Lądowych Stanów Zjednoczonych, Warszawa 1987).
Według Leksykonu Wiedzy Wojskowej - Wyd. MON, Warszawa 1979 - propaganda to upowszechnianie, szerzenie wiedzy naukowej, politycznej, wojskowej, technicznej i innej, a także idei, doktryn i poglądów.

powielano mapy topograficzne Norwegii, zakupiono norweskie słowniki i rozmówki, poszukiwano wśród składu osobowego wojsk i ludności cywilnej osób władających językiem norweskim.

K o n s t a t a c j a

Doświadczenia minionych wojen światowych i lokalnych dowodzą, że do prowadzenia dezinformacji mogą być użyte różne siły i środki będące w dyspozycji organów państwowych i wojskowych. Skala ich użycia jest oczywiście zależna od sytuacji polityczno-wojskowej, siły przeciwnika, głównego kierunku zainteresowania wywiadu i rozpoznania przeciwnika oraz ich możliwości, jak również od zakresu i treści głównych przedsięwzięć dezinformacyjnych.

Siły i środki dezinformacji to przede wszystkim ludzie jako nośnicy informacji oraz sprzęt, którym się posługują w czasie jej transmisji. W zależności od sytuacji, wykorzystywanych kanałów i środków oraz terminu przeprowadzenia pozorujących przedsięwzięć mogą być zaangażowane następujące grupy ludzi: działacze państwowi i wojskowi; pracownicy ambasad i misji; przedstawiciele różnych delegacji; ludność miejscowa; korespondencji prasy, radia i telewizji; telefoniści, radziści i radiotelegrafiści węzłów oddziałów i pododdziałów łączności; skład osobowy wojsk własnych i przeciwnika; zbiegowie i jeńcy wojenni; agenci i dywersanci; partyzanci i pracownicy podziemia. Podstawą wykorzystania tych sił powinna być zasada szczególnie ścisłego przestrzegania tajności treści przedsięwzięć dezinformacyjnych i przedsięwzięć pozorujących. Osoby rozpowszechniające informacje lub realizujące działania pozorujące nie powinny wiedzieć, że są narzędziem dezinformacji.

Przydatnym nośnikiem fałszywej informacji może być miejscowa ludność. Zarówno w minionych wojnach, jak i podczas przygotowywania współczesnych operacji wojskowych, każdy wywiad z pewnością będzie doceniał rolę miejscowej ludności przygranicznych rejonów dla zdobywania informacji, tworząc w tym środowisku agenturę. Zatem miejscowa ludność może być jednym z ważniejszych źródeł pozyskiwania przez wywiad informacji. Dlatego też umiejętnie wykorzystując to środowisko można prowadzić skuteczną dezinformację.

Kolejną grupą ludzi, dostosowaną do spełniania tej roli, może być partyzantka i podziemie. Szczególnie istotną rolę mogą one odgrywać w czasie konfliktu zbrojnego. Mogą rozpowszechniać fałszywe pogłoski wśród miejscowej ludności, zamieszkującej terytorium okupowane przez przeciwnika. Jest to istotne o tyle, że w środowi-

sku tym mogą działać agenci wywiadu oraz dywersanci, którzy zbierając informacje spotkają się z dezinformacją. Aby dezinformacja była skuteczna, należy też dążyć do rozpracowania ludzi pracujących dla przeciwnika, a następnie, za ich pośrednictwem, dostarczać mu fałszywych informacji. Klasycznym przykładem wykorzystania rozpracowanego agenta był fakt zdemaskowania w Algierze, przez kontrwywiad aliantów, francuskiego pułkownika, jako agenta niemieckiego. Wiedząc o tym, że Niemcy przestali mu wierzyć i nie traktują poważnie jego informacji, dowództwo aliantów postanowiło przekazać przez niego informacje o tym, że inwazja wojsk amerykańskich i angielskich w Europie rozpocznie się od wysadzenia desantu w Normandii 5, 6 lub 7 czerwca 1944 r. Meldunek tej treści od agenta, który stracił zaufanie, stał się dla Niemców dowodem na to, że inwazja nastąpi w każdym dniu oprócz 5, 6 lub 7 czerwca i w każdym innym miejscu, ale nie w Normandii. Tymczasem operacja „Overlord" rozpoczęła się 6.06.1944 r.

Następną grupą za pośrednictwem której można rozpowszechniać fałszywe informacje mogą być zbiedzy i jeńcy wojenni. W czasie drugiej wojny światowej niemieckie dowództwo specjalnie dobierało ludzi, którzy otwarcie wyrażali swoją niechęć do faszyzmu i po określonym „przygotowaniu", tj. dostarczeniu im różnych fałszywych informacji celowo organizowano ich ucieczkę z obozów koncentracyjnych lub tajne przekroczenie linii frontu. Przygotowanie wytypowanej osoby nie polegało na bezpośrednim instruowaniu jej przez specjalistów od dezinformacji, lecz na przekazywaniu określonych informacji poprzez podstawionych współwięźniów. Takie informacje przyszły zbieg mógł zdobywać od przygotowanej ochrony, podsłuchując rozmowy lub obserwując działania perorujące. Pozorująca rozbudowa obozu mogła świadczyć o spodziewanym napływie nowych jeńców, tj. o przygotowywanej operacji zaczepnej.

Wymienione grupy, traktowane jako siły dezinformacyjne, korzystają z różnych środków technicznych, zwanych środkami dezinformacji. Środki te można podzielić na dwa rodzaje. Pierwszy stanowić mogą środki masowej informacji, do których zalicza się: prasę wojskową i cywilną, w tym codzienną i periodyczną; broszury informacyjne, literaturę techniczną i popularnonaukową, plakaty i ulotki, filmy dokumentalne, popularnonaukowe, o tematyce technicznej i wojskowej oraz reklamowe; radio, telewizję, sprzęt krótkofalowy, telefony, dyktafony, magnetofony, magnetowidy, korespondencję pocztową, tj. telegramy, listy i karty pocztowe. Środki masowego przekazu mogą być również wykorzystywane w działaniach dezinformacyjnych poprzez po-

dawanie informacji tendencyjnych. Takie informacje można preparować poprzez: podawanie wiadomości całkowicie fałszywych, których odbiorca nie może zweryfikować; dobór informacji, z których każda jest prawdziwa, ale są tak ustawione, aby stworzyć określoną intencję, mieszanie informacji prawdziwych i fałszywych; po prawdziwej informacji podanie ukierunkowanego komentarza; umieszczanie prawdziwej informacji w kontekście wyczerpującym jej sens; wtrącenie informacji tendencyjnej do informacji prawdziwej, dotyczącej czegoś całkiem innego; nadanie nieproporcjonalnie dużej rangi lub zniekształcenie prawdziwej informacji tak, żeby wywołać u odbiorcy określone emocje; podanie nieprawdziwej informacji w kontekście rzeczywistego wydarzenia. Informowanie tendencyjne jest również wtedy, gdy środki masowego przekazu poświęcą tyle samo czasu, przy znikomym zainteresowaniu odbiorców, dla nieistotnej, mało znaczącej informacji, co dla ważnej, interesującej zdecydowaną większość. Fortel polegać może na tym, aby pewne argumenty rozwijać bardziej przekonująco niż inne, poświęcać więcej miejsca określonym aspektom rzeczywistości i umieszczać w całym tekście pewne, ledwo zauważalne, wpływające znacząco na kierunek myślenia odbiorcy informacji. W tym celu stosuje się m.in. następujące techniki: „przypadkowe" umieszczenie jednego zdania wtrąconego w treści informacji, co wystarczy jednak do odpowiedniego jej zabarwienia; użycie wieloznacznego słowa lub sformułowania; podanie krótkiego tekstu, umieszczonego w ramce, obok informacji, którą chce się ukryć, gdyż krótki, uwypuklony tekst jest łatwiej odbierany; operowanie „przypadkowym" sąsiedztwem, gdzie dezinformacja jest zamieszczona obok informacji prawdziwej, w podobnej formie i objętości; posługiwanie się rysunkiem satyrycznym, który nie wymaga czytania tekstu, a jednoznacznie oddaje treść informacji.

Do drugiego rodzaju środków dezinformacji można zaliczyć środki wojskowe, takie jak: łączności telefonicznej, radiowej i telegraficznej. W toku działań wojennych, oprócz wymienionych, rozpowszechnianie dezinformacji na tyłach i w rejonach działań bojowych przeciwnika realizowano poprzez ulotki, dokumenty i innych materiały zawierające fałszywe treści. W tym celu wykorzystano: środki wojsk rakietowych i artylerii (rakiety kasetowe, pociski artyleryjskie); środki sił powietrznych (rakiety skrzydlate, kasetowe bomby lotnicze, samoloty bezpilotowe, szybowce); środki sił morskich, a technikę bojową i specjalną wykorzystywano do imitacji i demonstracji działań pozornych.

Z przeprowadzonej analizy faktów wynika, że dezinformację należy postrzegać jako

dwustronny proces, w którym pozornym informacjom i działaniom jednej strony są przeciwstawiane takie same informacje i działania strony przeciwnej. Z analizy tej wynika także, że w zamiarach udanych operacji dezinformacyjnych były zawsze uwzględniane działania pozorne i rzeczywiste, precyzyjnie zsynchronizowane z przekazem i dokumentacją treści dezinformacyjnych. Analizując problem w takim kontekście dostrzeżono też, że strategiczne planowanie przedsięwzięć dezinformacyjnych obejmowało zawsze sfery: polityczną, ekonomiczną, naukowo-techniczną i militarną. W opracowaniu planów dezinformacji uczestniczyli naczelni przedstawiciele, formalnie kompetentni do kształtowania stanów w tych przestrzeniach. Na podstawie tego były doiero opracowane szczegółowe plany dezinformacji politycznej, ekonomicznej, naukowo-technicznej i wojskowej. W interesie sił zbrojnych, w planach dezinformacji politycznej, ekonomicznej i naukowo-technicznej, były uwzględniane wytyczne politycznych władz wojskowych. Dopiero na tej podstawie poszczególne sztaby wojskowe, w kolejności hierarchicznej, opracowywały spójne co do tego plany swojego działania, składające się na jednolicie skoordynowaną całość dezinformacyjną prowadzoną w wymiarze strategicznym.

Kierowanie systemami dezinformacji wojskowej odbywało się z poziomu politycznego kierownictwa wojskowego. Na podstawie wytycznych, napływających danych wywiadowczych, podjętych decyzji i opracowanego planu do prowadzenia dezinformacji następowało łączenie, koordynacja i ukierunkowywanie działalności sztabów niższego szczebla na terminową i pełną realizację postawionych zadań w zakresie dezinformacji. Stosownie do zaistniałych sytuacji wdrażano określone przedsięwzięcia dezinformacyjne w rodzajach sił zbrojnych i zgrupowaniach wojsk, zarówno w okresie narastania sytuacji kryzysowej, jak i w czasie rozpoczynania konfliktu zbrojnego. Tak centralizowane kierowanie umożliwiało: rozgraniczanie funkcji i utrzymywanie hierarchiczności oddziaływania; zabezpieczanie koordynacji pozornych i rzeczywistych przedsięwzięć pod względem celu, miejsca i czasu; prawidłowy podział sił i środków według zadań oraz osiągnie skrytości i jak największej wiarygodności. Jako organy robocze były zwykle powoływane odpowiednie grupy operacyjne składające się z pożądanych, w danym czasie i miejscu, specjalistów.

Do zadań centralnych grup operacyjnych należało: planowanie ogólnego kompleksu przedsięwzięć z zakresu dezinformacji, maskowania i walki z działalnością wywiadowczą w skali globalnej; opracowanie fałszywych materiałów i dokumentów, planów pozornych operacji, bezpośrednie kierowanie pozornymi przedsięwzięciami i

działaniami wojsk; organizacja i sprawowanie kontroli nad terminowością, jakością przygotowania, przeprowadzania i skutecznością ich oddziaływania na przeciwnika.

Ważną funkcję w kierowaniu dezinformacją spełniała zawsze kontrola. Sprowadzała się zwykle do sprawdzania i ustalania: jakości i kompleksowości przedsięwzięć dezinformacyjnych; terminowości i precyzji przekazu fałszywych informacji i demonstrowania działań pozornych; stanu przygotowania i gotowości sił i środków, angażowanych do realizacji przedsięwzięć dezinformacyjnych; oznak demaskujących działania dezinformacyjne; stanu efektywności oddziaływania dezinformacyjnego; potrzeb w zakresie poprawek i korekt do wcześniej zaplanowanych przedsięwzięć dezinformacyjnych.

Kontrole dezinformacyjne były prowadzone w układzie ciągłym i okresowym. Stałej kontroli podawane były przedsięwzięcia pozorne realizowane w czasie pokoju, ukierunkowane na długofalowe oddziaływanie. Zwykle koncentrowały się na problematyce odnoszącej się do: zagadnień dotyczących zdolności obronnej państwa; rozmieszczenia i możliwości przemysłu zbrojeniowego; gotowości bojowej i mobilizacyjnej sił zbrojnych; kierunku operacyjnego przygotowania sztabów oraz zaopatrzenia sił zbrojnych w technikę bojową i uzbrojenie, jak również i perspektyw ich rozwoju; rozbudowy terytorium kraju i teatrów wojennych pod względem operacyjnym.

Kontrolom okresowym podlegały zwykle przedsięwzięcia odnoszące się do zakresu dezinformacji, których czas trwania był ograniczany konkretnymi sytuacjami, zarówno pod względem terminów przeprowadzenia, jak i oddziaływania na przeciwnika. Kontrole takie odnosiły się przede wszystkim do przygotowywania i realizacji przedsięwzięć dezinformacyjnych dotyczących: tematyki, zamiaru stron, przerabianych zagadnień w ćwiczeniach z wojskami, treningów dowódczo-sztabowych i gier wojennych; prowadzonych prób z uzbrojeniem, techniką bojową i specjalną.

Ważne miejsce w kontrolowaniu przedsięwzięć dezinformacyjnych zajmowało określanie skuteczności ich oddziaływania na przeciwnika. Stosowano przy tym: osobistą kontrolę i obserwację; wysłuchiwanie przekazów fałszywych informacji; badanie i analizowanie referatów, meldunków i informacji niższych szczebli o działaniach przeciwnika; sondowanie miejscowej ludności; przesłuchiwanie jeńców i dezerterów; przechwytywanie dokumentów, ich badanie i ocenę; przechwytywanie i przesłuchiwanie rozmów przeciwnika za pośrednictwem technicznych środków łączności.

Do prowadzenia kontroli przedsięwzięć dezinformacyjnych byli wyznaczani: funkcjonariusze naczelnych organów kierowania państwem oraz odpowiednio przy-

gotowani oficerowie. Pośrednią rolę w sprawowaniu kontroli spełniali: pracownicy ambasad, konsulatów, misji wojskowych i innych przedstawicielstw, w tym również i nielegalnych. Dostarczone przez nich meldunki były ważnym materiałem, służącym do oceny skuteczności dezinformacyjnej.

W czasie zagrożenia wybuchem konfliktu zbrojnego i przygotowań do prowadzenia pierwszej operacji uwzględniano zawsze, że przedsięwzięcia dezinformacyjne mogą umożliwić uzyskanie zaskoczenia w skali globalnej. Planowanie dezinformacji wojskowej w warunkach narastania sytuacji kryzysowej mogło związane z planowaniem pierwszej operacji. Główne kierunki dezinformacji, w czasie przygotowywania pierwszej operacji, były zwykle koncentrowane na zmobilizowaniu sił zbrojnych i przygotowywaniu planu. W zakresie przygotowania sił zbrojnych dezinformacja odnosiła się głównie do zniekształcania rzeczywistego obrazu: wyposażenia i uzbrojenia wojsk; organizacji szkolenia operacyjnego i przygotowania sztabów związków operacyjnych, taktycznych i oddziałów; doskonalenia struktur organizacyjnych sił zbrojnych; dowozu zasobów środków materiałowych, niezbędnych do prowadzenia pierwszej operacji; przygotowania terenu działań wojennych oraz prowadzenia rozpoznania. Natomiast w zakresie przygotowania operacji dezinformacja koncentrowała się na: przedsięwzięciach mobilizacyjnego rozwiania wojsk; tworzenia zgrupowań sił zbrojnych na teatrze działań wojennych, niezbędnych do prowadzenia pierwszych operacji; pracy uświadamiającej w siłach zbrojnych; organizacji polowego systemu dowodzenia.

W czasie przygotowywania pierwszej operacji jednym z ważniejszych zadań dezinformacyjnych było wprowadzanie przeciwnika w błąd co do wyposażenia sił zbrojnych w najnowsze rodzaje broni i techniki wojskowej. Realizacja tego polegała zwykle na oddziaływaniu poprzez przedsięwzięcia rozpoczynające się już w momencie rozpoczęcia prac naukowo-badawczych nad nowym prototypem broni. W celu wprowadzenia w błąd, w sposób skoordynowany były rozpowszechniane pogłoski i informacje o opóźnieniach badań i niepomyślnych próbach z prototypami oraz podejmowaniu praktycznych pracach nad doskonaleniem starych rodzajów broni. Do rozpowszechniania takich informacji i pogłosek w znacznym stopniu były wykorzystywane środki masowego przekazu. W wypadku gdy wywiad przeciwnika dowiadywał się o prowadzonych pracach w tej dziedzinie, przedsięwzięcia dezinformacyjne y były ukierunkowywane na przedstawianie nowych modeli jako już przestarzałych, zawierających wiele wad konstrukcyjnych i znacznie ustępujących, pod względem

podstawowych parametrów, modelom zagranicznym. Takie postępowania były zwykle stosowane, kiedy rzeczy dotyczące konstrukcji środków walki były oparte na nowych zasadach fizycznych.

Ważnym zadaniem dezinformacji było też ukrywanie zakładowych, poligonowych i wojskowych prób z nowymi środkami walki. Produkcja nowych modeli uzbrojenia, a tym bardziej ich testowanie, odbywa się pod przykrywką produkcji i badań nad techniką niezbędną dla gospodarki narodowej. Próby poligonowe i wojskowe nowych modeli uzbrojenia, techniki bojowej i specjalnej odbywały się pod pozorem rutynowych, codziennych zajęć i różnego rodzaju ćwiczeń itp. Dla „przykrycia" prób, zawczasu i zgodnie z planem dezinformacji były opracowywane legendy dla każdego rodzaju broni i techniki wojskowej. W celu uwiarygodnienia informacji i dokumentów na temat praktycznych działań wojsk, według wcześniej opracowanego lub uściślonego na dany czas scenariusza były prowadzone pozorne pokazy maskujące rzeczywiste działania, poprzez imitację i demonstrację przestarzałych rodzajów uzbrojenia. Informacja o terminach przeprowadzenia, przebiegu i wynikach pozorowanych prób broni i techniki za odpowiednim pozwoleniem, w sposób zamierzony były przekazywana zarówno za granicę, jak i w kraju. Dezinformacja dotyczyła też parametrów taktyczno-technicznych i bojowych, liczby i jakości zastosowanego rodzaju uzbrojenia oraz sposobów jego użycia bojowego. Rozpowszechniając w tym celu fałszywe pogłoski i dokumenty, za pośrednictwem środków masowego przekazu, ropowsechniano wśród wojsk i miejscowej ludności treści informacyjne, które w sposób zamierzony i skoordynowany deformowały prawdziwe dane, ujawniające możliwości bojowe i techniczne wdrażanego uzbrojenia. Podczas przeprowadzania prób wojskowych w okresie przygotowywania operacji z nowymi rodzajami broni i techniki bojowej przedstawiano zwykle zmodernizowane egzemplarze starego sprzętu. jako udoskonalony prototypy, przewidywane do wprowadzenia do wojsk.

Celami dezinformacji było też rozpowszechnianie pogłosek i fałszywych informacji demonstrujących wysokie osiągnięcia w dziedzinie prac naukowo-badawczych. Umiejętnie przygotowane reklamy, filmy dokumentalne i fabularne o tematyce wojskowej pokazywały przewagę własnej broni i techniki bojowej, ich wysoką jakość i nowoczesność. Główny cel takiej dezinformacji sprowadzał się do tego, aby unaoczniać przewagę własnej broni i techniki i tym samym zwiększyć zapotrzebowania innych państw na zakup uzbrojenia i sprzętu wojskowego lub utrzymać potencjalnego przeciwnika w niepewności i poprzez to „odstraszyć" go od agresywnych zamiarów.

Kolejnym zadaniem dezinformacji w czasie przygotowywania sił zbrojnych do pierwszej operacji było prowadzenie działań o charakterze pozornym, odnośnie przygotowania sztabów i wojsk do prowadzenia działań bojowych. W ten sposób wywiad przeciwnika był wprowadzany w błąd co do rzeczywistego stanu odnoszącego się do organizacji wojsk, techniki bojowej i uzbrojenia oraz rzeczywistych kierunków, tematyki i bojowego przygotowywania wojsk. Wykorzystując te możliwości dezinformowano przeciwnika. W tym celu przedsięwzięcia takie uwzględniano i prezentowano, zarówno w planach corocznych jak i perspektywicznych. W celu upowszechnienia informacji o przebiegu przygotowań i samych ćwiczeniach byli powiadamiani korespondenci prasy, radia i telewizji, którzy mogli szeroko komentować niektóre zagadnienia i wydarzenia z każdego etapu ćwiczeń. Konkretny wykaz zagadnień, podlegający upublicznieniu przez środki masowego przekazu i media wojskowe, był ujmowany w planie dezinformacji lub opracowanych legendach. Na jego podstawie były opracowywane konkretne treści wystąpień, artykułów, raportów, komunikatów, rozmów oraz przekazów radiowych, telefonicznych i telewizyjnych, przeznaczonych do opublikowania w gazetach i dziennikach. Szczególną uwagę zwracano przy tym na szczegółowe przygotowanie i przeprowadzenie takich działań wojsk, które potwierdzałyby wcześniej przekazane już fałszywe informacje.

W celu pomyślnej realizacji przedsięwzięć dezinformacyjnych uwzględniano w trakcie opracowywania ćwiczeń i ich prowadzeniu wszystkie oznaki demaskujące charakter ćwiczenia. Praktyka ćwiczeń na wyższych szczeblach wskazuje, że oznaką demaskującą były zwykle działania punktów dowodzenia. Dzięki systemowi rozpoznania kosmicznego, radioelektronicznego i radiotechnicznego, który obserwuje wyjście z miejsc stałej dyslokacji i przemieszczanie się punktów dowodzenia w trakcie ćwiczenia, można z łatwością określić charakter ćwiczenia, skład wojsk, a także z dużym prawdopodobieństwem zagadnienia szkoleniowe ćwiczenia. Na przykład przemieszczenie stanowisk dowodzenia na początku ćwiczenia w głąb terytorium, a następnie przesunięcie ich do granicy państwowej, z jednoczesnym postawieniem wojsk w stan pełnej gotowości oraz włączeniem ich do ćwiczenia, z zadaniem wykonania natarcia z marszu, na przedni skraju przeciwnika, połączone z forsowaniem przeszkody wodnej, pozwala z dostateczną precyzją określić, że w czasie ćwiczenia doskonali się nie zagadnienia o charakterze obronnym, lecz ofensywnym. Tę oznakę oznakę dezinformacji ukrywano też opracowując maskujące scenariusze ćwiczeń. Ich istota sprowadzała się do tego, że maskowanie działań zaczepnych rozpoczynło

się od rozmieszczania stanowisk dowodzenia w rejonach przygranicznych państwa, a następnie, pod pozorem nieudanych działań obronnych, zostały przemieszczone w głąb terytorium, z jednoczesnym zarządzeniem pełnej gotowości bojowej związków ćwiczących, przewidzianych do prowadzenia operacji zaczepnej. W celu uniknięcia rozpoznania prowadzonego zamiaru ćwiczenia przestrzegano, aby wszystkie zagadnienia o charakterze zaczepnym były prowadzone z jednego punktu dowodzenia. W celu dezinformacji co do składu ćwiczących wojsk i sztabów były organizowane pozorne dowództwa, sztaby i grupy operacyjne, ze środkami łączności, a także demonstrację działań wojsk przebywających w centrach szkoleniowych i na poligonach. W takich sytuacjach praca na technicznych środkach łączności, tj. przekazywanie radiogramów, komend i sygnałów oraz przemieszczanie wojsk w nowe rejony odbywało się zgodnie z realnymi i specjalnie opracowanymi w tym celu legendami.

Uogólniając można oceniać, że tak dezinformacja, jak i maskowanie działań stanowiły, stanowią i stanowić będą komplementarny kompleks zmagań przeciwnie ukierunkowanych sobie sił zbrojnych. Ścisła kontrola nad przygotowaniem i realizacją tych przedsięwzięć, zarówno prawdziwych jak i pozornych, scentralizowane planowanie oraz szczegółowe przygotowanie sił i środków zawsze ogranicza „przeciek" informacji demaskujących i stworzy sprzyjające warunki do wprowadzenia przeciwnika w błąd, co również zawsze prowadzi do osiągnięcia nad nim określonej przewagi.

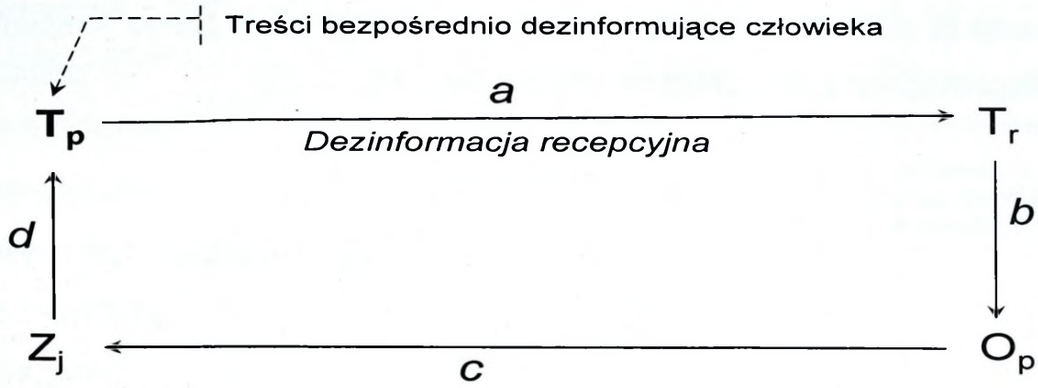
Z przeprowadzonej analizy i zaprezentowanej konstatacji wynika, że wszelkie przedsięwzięcia dezinformacyjne można usystematyzować w dwóch najbardziej uogólnionych grupach – jako dezinformację bezpośrednią mogącą przyjąć nazwę recepcyjna i dezinformację pośrednią mogącą przyjąć nazwę sensoryczna.

2.1.2. Dezinformacja bezpośrednia (recepcyjna)

Dezinformacja bezpośrednia to w istocie rzeczy dezinformacja recepcyjna, oddziałująca bezpośredni na ludzkie receptory. Stosując co do tego opisaną już wcześniej teorię kategorii[16] można tę formę wpływów interpretować jako celowe manipulowanie zbiorami treści poznawczych, ukierunkowane na wprowadzanie tak zestawionych treści poznawczy do układu recepcyjnego obserwatora, które po percepcji zmysłowej i asocjacji umysłowej utwierdzą go w przekonaniu o realności stanów

[16] Patrz rys. 25 na s. 51 i tekst na s. 51-54.

rzeczy sytuacyjnych, które w rzeczywistości nie istnieją. Wyrażając to innymi słowy, można powiedzieć, że zasadniczy proces dezinformowania zachodzi w relacji recepcyjnej (rys. 44).



T_p – zbiór treści poznawczych
T_w – zbiór treści wyobrażeniowych
T_r – zbiór treści recepcyjnych
O_p – zbiór obrazów percepcyjnych
Z_j – zbiór znaków językowych

a – relacja recepcyjna
b – relacja percepcyjna
c – relacja asocjacyjna
d – relacja identyfikacyjna

Rys. 44. Diagram obrazujący dezinformację recepcyjną (bezpośrednią)

Źródło: Opracowanie autorskie

Treści poznawcze mogą stanowić stany sytuacyjne przekładające się na obrazy percepcyjne, jak również odpowiednio spreparowane treści informacyjne wyrażane słownie, językiem pisanym i innymi znakami językowymi. Zasadniczy warunek, kwalifikujący procedury do tego rodzaju dezinformowania, sprowadza się do faktu, że pomiędzy treściami poznawczymi i receptorami człowieka nie mogą występować żadne elementy pośredniczące i z tej też przyczyny może być zamiennie nazywana dezinformowaniem bezpośrednim.

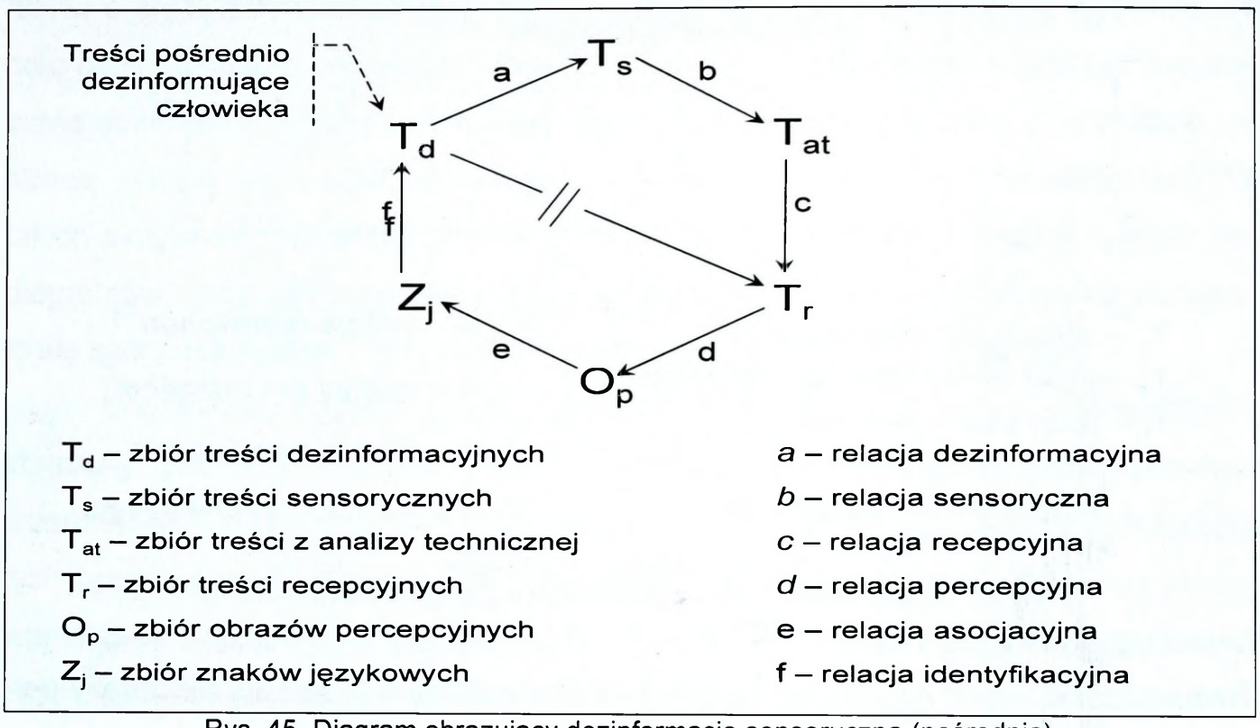
Dezinformacja bezpośrednia (recepcyjna) – celowo zniekształcona struktura sytuacyjna, znajdująca się w zasięgu bezpośredniej dostępności recepcyjnej dla obserwatora,

gdzie:

- „dezinformacja bezpośrednia (recepcyjna)" – *definiendum*,
- „celowo zniekształcona struktura sytuacyjna, znajdująca się w zasięgu bezpośredniej dostępności recepcyjnej dla obserwatora" – *definiens*,
- „celowo zniekształcona struktura sytuacyjna" – *genus proximum*,
- „znajdująca się w zasięgu bezpośredniej dostępności recepcyjnej dla obserwatora" – *differentia specifica*.

2.1.2. Dezinformacja pośrednia (sensoryczna)

Dezinformacja pośrednia, zwana sensoryczną, różni się tym od dezinformacji bezpośredniej (recepcyjnej), że pomiędzy przedmiotem poznania i receptorami człowieka występują jeszcze urządzenia techniczne (sensory i różnego rodzaju przetworniki) wspomagające jego układ recepcyjny (rys. 45).



T_d – zbiór treści dezinformacyjnych	*a* – relacja dezinformacyjna
T_s – zbiór treści sensorycznych	*b* – relacja sensoryczna
T_{at} – zbiór treści z analizy technicznej	*c* – relacja recepcyjna
T_r – zbiór treści recepcyjnych	*d* – relacja percepcyjna
O_p – zbiór obrazów percepcyjnych	e – relacja asocjacyjna
Z_j – zbiór znaków językowych	f – relacja identyfikacyjna

Rys. 45. Diagram obrazujący dezinformację sensoryczną (pośrednią)

Źródło: Opracowanie autorskie

Dezinformacja pośrednia (sensoryczna) – celowo zniekształcona struktura sytuacyjna, znajdująca się poza zasięgiem bezpośredniej dostępności recepcyjnej dla obserwatora,

gdzie:

- „dezinformacja pośrednia (sensoryczna)" – *definiendum*,
- „celowo zniekształcona struktura sytuacyjna, znajdująca się poza zasięgiem bezpośredniej dostępności dla obserwatora" – *definiens*,
- „celowo zniekształcona struktura sytuacyjna" – *genus proximum*,
- „znajdująca się poza zasięgiem bezpośredniej dostępności dla obserwatora" – *differentia specifica*.

Sensorami[17] (czujnikiem) nazywa się wszelkie urządzenia, które przetwarzają nieelektryczne wartości fizyczne w sygnały elektryczne. Ich członami wykonawczymi są natomiast różne urządzenia przetwarzające (przetworniki), nazywane też „aktorami", które przetwarzają zarejestrowane sygnały elektryczne w nieelektryczne wiel-

[17] Sensor – od angielskiego sensors.

kości fizyczne. Ze względu na rodzaj dostosowania wejść i wyjść tych urządzeń (sensorów i aktorów) można, ze względu na wielkości fizyczne z odpowiadającymi im rodzajami energii, wyróżniać osiem następujących grup tych urządzeń:

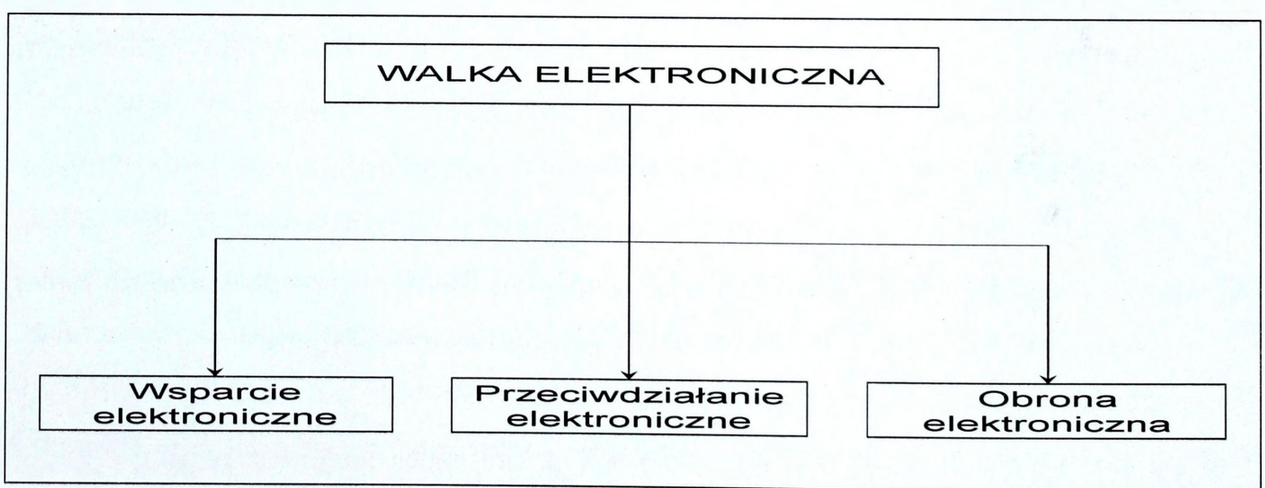
- elektryczne,
- chemiczne,
- biochemiczne,
- magnetyczne,
- elektromagnetyczne,
- mechaniczne,
- radiacyjne,
- termiczne.

Wszystkie te urządzenia niepomiernie rozszerzają możliwości układu recepcyjnego człowieka. Dzięki ich zastosowaniu staje się możliwe obserwowanie stanów rzeczy niedostępnych bezpośrednio człowiekowi. Można obserwować obiekty fizyczne znajdujące się poza horyzontem optycznym, niezależnie od pory doby i warunków atmosferycznych. Rejestrować efekty akustyczne występujące w tak zwanej „strefie ciszy" – poza dolnym i górnym progiem ludzkiego słuchu. Identyfikować stany sejsmiczne powodowane ruchem na powierzchni Ziemi. Obserwować ukryte obiekty przez pryzmat emisji termicznych. Odtwarzać stany infrastruktury i zgrupowań ludzkich poprzez stany chemiczne i biochemiczne ich otoczenia. Identyfikować źródła i stany sytuacyjne związane z generowaniem emisji elektromagnetycznych i radiacyjnych. Identyfikować rejony zgrupowań techniki przez pryzmat naruszeń wartości pola geomagnetycznego. Technika ta, w ramach walki zbrojnej, staje się ogromnym atrybutem w rozpoznawaniu przeciwnika. Z drugiej zaś strony stanowi sobą również i zagrożenia. Wszelkie tego typu urządzenia, z natury rzeczy, spełniają zawsze i tylko ściśle określone funkcje techniczne, skupione jednoznacznie wokół wartości konstrukcyjnie dostępnych. Strona przeciwna, znająca wcześniej parametry techniczne tych urządzeń, jest zawsze w stanie wytwarzać pozorne sytuacje tylko w oparciu o generowanie stosownych efektów, dostępnych technicznie dla poszczególnych sensorów monitorujących. Może też destrukcyjnie oddziaływać na procedury przetwarzania danych, uszkadzając energetycznie procesory funkcjonujące w konkretnych przetwornikach (aktorach) czy też wprowadzać do nich „złośliwe oprogramowania" i w ten sposób i w ten sposób przekształcać informację w dezinformację

2.2. Zagrożenia informacyjne w relacjach kierowania

Zasadnicze zagrożenia w relacjach kierowania stanowią przedsięwzięcia wynikające z „walki elektronicznej". Dowodząc tę tezę należy rozpocząć od faktu, że fakt ten został wykreowany przez postęp naukowo-techniczny odnotowany w sferze elektroniki. Uzyskane w tym zakresie efekty poznawcze zostały wykorzystane do tworzenia nowego typu urządzeń wykorzystywanych obecnie w tej walce, której zasadniczym celem jest, między innymi, negatywne oddziaływanie na teleinformatyczne sieci systemu informacyjnego przeciwnika, przy jednoczesnej ochronie procesów i systemów własnych. Obecnie prawie każda działalność wojskowa ma związek z operacjami informacyjnymi.

Według poglądów natowskich, do zasadniczych rodzajów działań, mających wpływ na operacje informacyjne, należy „walka elektroniczna", obejmująca spektralną sferę widma elektromagnetycznego i koncentrująca się w tej przestrzeni funkcjonalnej na poszukiwaniu, przechwytywaniu i identyfikowaniu emisji elektromagnetycznych, wraz ze źródłami ich generowania i „nałożonymi" na nie treściami semantycznymi. Jako element negatywnej kooperacji wzajemnej, jest jednocześnie ukierunkowywana na przeciwdziałanie temu ze strony przeciwnika. Generalnie uwzględnia się, że walka ta (walka elektroniczna) obejmuje: wsparcie elektroniczne, przeciwdziałanie elektroniczne i ochronę elektroniczną (rys. 46) [18].



Rys. 46. Podział walki elektronicznej

Źródło: Opracowanie autorskie

Walka elektroniczna, w ramach operacji informacyjnych, umożliwia uzyskiwanie danych niezbędnych do planowania, wykonywania i monitorowania skutków ope-

[18] Nie identyczną, ale merytorycznie zbliżoną interpretację można odnaleźć w AAP-6 - NATO Glossary of terms and definitions (english and french), NATO Standardization Agency (NSA), 2004.

racji informacyjnych. Kompleksowo analizuje systemy dowodzenia przeciwnika, pod kątem ich podatności na zakłócanie ofensywnymi działaniami elektronicznymi. W działaniach tych wykorzystuje identyfikację i wirtualizację pola walki. Wykorzystywana jest też do atakowania węzłów dowodzenia przeciwnika. Uniemożliwienia ich użycie w zasadniczych momentach operacji.

Wsparcie elektroniczne jest ukierunkowywane na zdobywanie i przetwarzanie tych informacji o przeciwniku, których nośnikami są fale elektromagnetyczne (wraz z informacją w nich zawartą – z semantyką) wypromieniowane przez źródła przeciwnika oraz inne efekty uboczne towarzyszące działaniom wojennym. Wyniki rozpoznania pozwalają określać jej zadania objawiające się przez zakłócenia i dywersję elektroniczną. Mogą również służyć do opracowania danych do rażenia ogniem elementów systemu dowodzenia przeciwnika. Postęp naukowo-techniczny pozwolił na skonstruowanie wielu rozpoznawczych urządzeń elektronicznych, które pozwalają na postrzeganie pola walki poprzez widmo promieniowania elektromagnetycznego, fale sprężyste (akustyczne i sejsmiczne) oraz przez pole magnetyczne i skład chemiczny środowiska. W połowie lat 70-tych XX wieku, w połączonych siłach zbrojnych NATO przyjęto program kompatybilnego rozwoju systemów działających w oparciu o elektronikę i określono go skrótem „C^3I"[19]. Było to rezultatem przeprowadzonych badań, które jednoznacznie wykazały, że eksploatowane systemy są przestarzałe i nie spełniają wymogów ówczesnego pola walki. Po przebudowie w ramach przyjętego programu „C^4I^2"[20], nowoczesne systemy elektroniczne integrują szereg różnych funkcji w jedną całość i zapewniają między innymi:

- zdobywanie danych o przeciwniku,
- kontrolę własnych wojsk,
- komputerowe wspomaganie procesów decyzyjnych,
- niezawodnie funkcjonującą łączność.

Skład, struktura organizacyjna, rozmieszczenie przestrzenne elementów takiego systemu oraz więzi informacyjne i funkcjonalne występujące między nimi, pozwalają na realizację następujących zadań:

- usprawnienie przegrupowania i manewru wojsk,
- automatyzację kierowania środkami walki,

---

[19] „C^3I", ang. Command, Control, Communication and Intelligence. Jest programem w znaczeniu rzeczowym i procedurą w znaczeniu czynnościowym (nie jest systemem).
[20] „C^4I^2" ang. Command, Control, Communications, Computers, Intelligence and Information.

- kontrolę wykonania postawionych zadań i przebiegu walki.

Przeciwdziałanie elektroniczne to zespół skoordynowanych przedsięwzięć i działań ukierunkowanych na dezorganizację pracy systemów oraz urządzeń elektronicznych przeciwnika, funkcjonujących w środowisku elektromagnetycznym (procesów informacyjnych przeciwnika). Działania te są prowadzone we wszystkich rodzajach sił zbrojnych, w każdych warunkach terenowych i meteorologicznych. Stosuje się co do tego różne techniki i sposoby poprzez odpowiednio dobrane emisje sygnały zakłócające. Przeciwdziałanie elektroniczne uniemożliwia lub ogranicza efektywne wykorzystanie przestrzeni elektromagnetycznej przez przeciwnika, przez co wpływa na wykluczanie lub ograniczanie sprawności jego systemów dowodzenia, rozpoznania i kierowania środkami walki.

Obrona elektroniczna jest rodzajem zabezpieczenia działań wojsk własnych i realizuje się ją na wszystkich szczeblach dowodzenia. Jest to zespół organizacyjnych i techniczno-eksploatacyjnych przedsięwzięć, zapewniających stabilną pracę własnym środkom i systemom elektronicznym. Jest ukierunkowana na zabezpieczanie dowodzenia wojskami i sterującymi środkami podczas prowadzenia walki w warunkach negatywnych oddziaływań elektronicznych stosowanych przez przeciwnika. Obrona ta jest ukierunkowywana stwarzanie dogodnych warunków do zachowywania ciągłości kierowania (dowodzenia i sterowania) własnymi siłami i środkami elektronicznymi.

2.2.1. Penetracja semantyczna (identyfikowanie)

Informacyjna penetracja semantyczna w relacjach kierowania sprowadza się w istocie rzeczy do prowadzenia rozpoznania elektronicznego. Atrybutem tego rodzaju rozpoznania jest fakt, że może być prowadzone bez względu na istniejącą sytuację polityczno-militarną, warunki atmosferyczne, czas, miejsce oraz położenie wojsk, nie powodując istotnego zróżnicowania wartości uzyskiwanych efektów (wyników rozpoznania). Jest to najszybszy, najtańszy, najbardziej manewrowy i skryty oraz najbezpieczniejszy rodzaj rozpoznania wojskowego. Rozpoznanie elektroniczne jest pasywną formą zdobywania informacji o obiektach elektronicznych przeciwnika promieniujących energię elektromagnetyczną, poprzez ich poszukiwanie, przechwytywanie, śledzenie, namierzanie oraz analizowanie. Z tego też względu

stanowi istotny ważny element systemu rozpoznania wojskowego. Jej właściwości charakteryzują je następujące cechy:

- pracuje bez bezpośredniego kontaktu z rozpoznawanymi obiektami,
- obejmuje wielkie odległości i przestrzenie – zasięgi ograniczają tylko właściwości fizyczne rozchodzenia się fal radiowych,
- może funkcjonować nieprzerwanie w różnych porach roku, w różnych godzinach i przy dowolnej pogodzie,
- zabezpiecza otrzymywanie prawdziwej informacji, pochodzącej bezpośrednio od przeciwnika (z wyłączeniem przypadków radiodezinformacji),
- uzyskuje wielką ilość informacji o różnorodnym charakterze i treści,
- otrzymuje informacje w krótkim czasie i najczęściej w trybie on-line,
- przechwytuje informacje niemożliwe do zdobycia innymi sposobami,
- pracuje w sposób skryty i bezpieczny – przeciwnik nie może stwierdzać faktu takiej działalności (pasywne urządzenia, możliwość działania z własnego obszaru i spoza strefy bezpośredniego oddziaływania środków rażenia przeciwnika).

Rozpoznanie elektroniczne w zależności od przeznaczenia zadaniowego dzieli się na globalne, strategiczne i taktyczne.

Rozpoznanie (wywiad) globalny zabezpiecza globalny dostęp do systemów masowej komunikacji. Kraje anglojęzyczne, będące sygnatariuszami porozumienia UKUSA[21] prowadzą wspólnie wywiad elektroniczny. Starają się o uzyskanie dostępu do większości światowych łączy międzynarodowych – chodzi tu o nieautoryzowany przechwyt sygnałów z satelitów komercyjnych, dalekosiężnych łączy radiowych, podwodnych kabli na dnie morza oraz z Internetu. Obecnie ponad 120 systemów satelitarnych znajduje się w ciągłym działaniu zbierając informacje. System stworzony przez UKUSA, często nazywany ECHELON, zajmuje się przetwarzaniem informacji, jest w dużym stopniu zautomatyzowany. Oprócz organizacji UKUSA istnieje przynajmniej 30 innych działających narodowych organizacji wywiadu elektronicznego. Największe to rosyjska i chińska, której dwie stacje skierowane na Rosję współpracują ze Stanami Zjednoczonymi. Większość bliskowschodnich i azjatyckich narodów zainwestowało w sposób istotny w wywiad elektroniczny, w szczególności Izrael, Pakistan i Indie.

[21] Porozumienia UKUSA ustanowiły w 1947 roku Wielka Brytania oraz USA, później dołączyły trzy inne anglojęzyczne państwa: Kanada, Australia i Nowa Zelandia.

Rozpoznanie strategiczne jest prowadzone na zamówienie organów władzy państwowej i wyższych sztabów wojskowych z celem pozyskiwania informacji wszechstronnej o rozpoznawanym kraju przez jego środki radioelektroniczne. Informacja taka jest niezbędna dla przygotowania sił zbrojnych i zasobów kraju do wojny, podjęcia decyzji o rozpoczęciu działań wojennych i umiejętnego prowadzenia operacji strategicznych.

Rozpoznanie operacyjne stanowi jedno z podstawowych źródeł zabezpieczających wojska w informacje drogą ciągłego śledzenia promieniowania elektromagnetycznego wielu wojskowych urządzeń i systemów przeciwnika. Jest ono w stanie zdobywać ważne wiadomości do rozpoczęcia działań bojowych przez siły związków, jednostek i pododdziałów.

Rozpoznanie taktyczne prowadzi się w strefie bezpośredniej styczności wojsk, w strefie walki obronnej lub zaczepnej oddziałów i związków taktycznych. Jego głównym celem jest wsparcie informacyjne dowódców podejmujących decyzje o użyciu wojsk i sposobie rozegrania walki. Obejmuje ono rozpoznanie naziemne oraz powietrzne. Na szczeblu taktycznym, nowoczesny system rozpoznania elektronicznego może zapewniać pozyskiwanie, weryfikację, gromadzenie i dystrybucję danych rozpoznawczych ze środowiska elektromagnetycznego i zjawisk ubocznych towarzyszących walce zbrojnej. W taktycznym rozpoznaniu elektronicznym zazwyczaj wykorzystuje się:

- samoloty, śmigłowce i środki bezpilotowe wyposażone w rozpoznawcze urządzenia radiowe, zestawy czujnikowe, aparaturę fotograficzną, urządzenia noktowizyjne i techniki podczerwieni oraz kamery telewizyjne;
- polowe środki rozpoznania elektronicznego takie jak: aparatownie odbioru i analizy emisji radiowych różnych zakresów częstotliwości, namierniki radiowe, stacje rozpoznania systemów radiolokacyjnych, stacje rozpoznania łączności radioliniowej i satelitarnej, stanowiące wyposażenie pododdziałów rozpoznania i walki elektronicznej;
- różnego rodzaju artyleryjskie środki rozpoznania radiolokacyjnego i dźwiękowego;
- polowe stacje radiolokacyjne obserwacji pola walki wojsk lądowych, rozwijane w ugrupowaniu bojowym batalionów i brygad.

Rozpoznanie elektroniczne, ze względu na środowisko lokacji, dzieli się na: naziemne, morskie, powietrzne i kosmiczne. W celu uzyskania informacji środkami

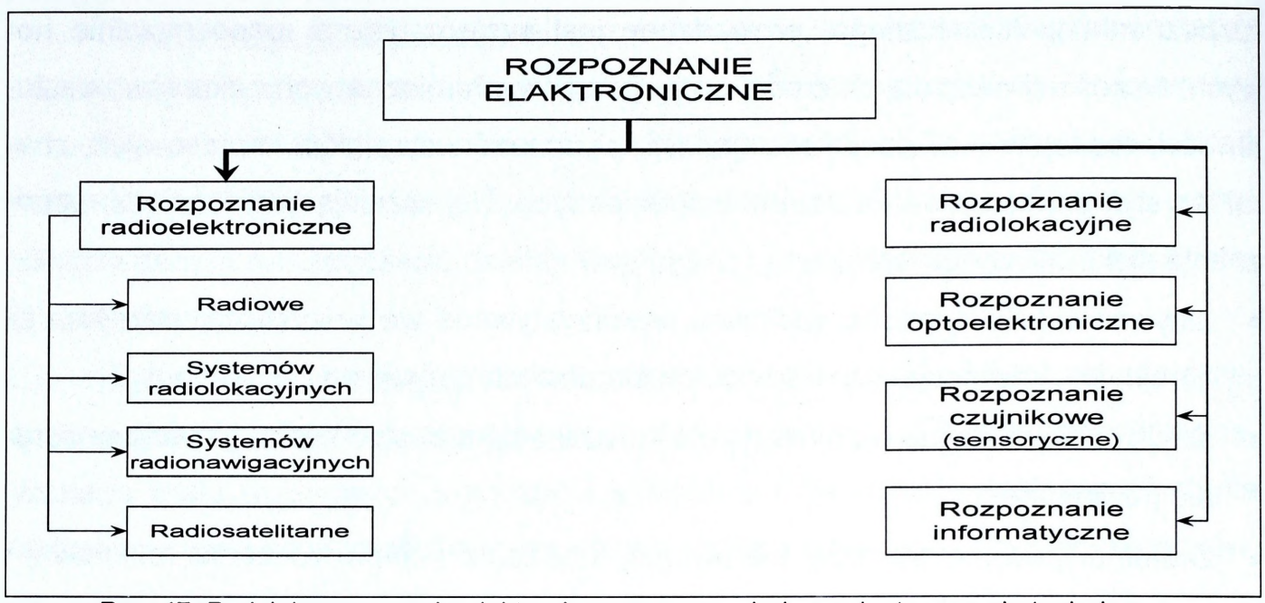
rozpoznania elektronicznego, prowadzone jest systematyczne rozpoznawanie nowych, wcześniej nieznanych źródeł audycji radiowych, nieznanych zakresów częstotliwości, rodzajów modulacji i manipulacji, parametrów sygnałów impulsowych, charakterystyk promieniowania anten i innych danych. Najważniejszymi źródłami rozpoznania elektronicznego są:

- aktywne środki łączności radiowej, wykorzystywane we wszystkich rodzajach sił zbrojnych i interesujących komórkach kierujących państwem,
- stacje radiolokacyjne różnych typów i przeznaczenia, stosowane głównie w obronie powietrznej,
- zautomatyzowane systemy kierowania, śledzenia i naprowadzania rakietowej i przeciwrakietowej broni, a także obiektów kosmicznych,
- systemy radionawigacyjne, wykorzystywane w morskiej, powietrznej i kosmicznej nawigacji.
- różnorodne telemetryczne systemy transmisji danych.

W skład środków technicznych rozpoznania elektronicznego wchodzą urządzenia:

- anteny odbiorcze – kierunkowe i dookolne,
- odbiorniki radiowe,
- radionamierniki,
- skanery do analizy panoramicznej,
- analizatory widmowe odbieranych sygnałów,
- urządzenia automatycznego odczytu częstotliwości i kierunku namiarów,
- urządzenia wyjściowe dla odbioru sygnałów telefonicznych i telegraficznych zagęszczonych kanałów łączności radiowej,
- urządzenia końcowe do odbioru słuchowego (telefon, głośniki),
- urządzenia do zapisu i dokumentowania sygnałów,
- przyrządy do obróbki, gromadzenia i ochrony odebranej informacji,
- środki kierowania, łączności i przekazu zdobytej informacji.

Rozpoznanie elektroniczne, ze względu na dostosowania techniczne, dzieli się na: radioelektroniczne, radiolokacyjne, optoelektroniczne, czujnikowe i informatyczne (rys. 47).



Rys. 47. Podział rozpoznania elektronicznego ze względu na dostosowanie techniczne

Źródło: Opracowanie autorskie

W procesie rozpoznania elektronicznego wszystkie dane o obiektach elektronicznych stają się informacjami rozpoznawczymi, które stanowią podstawę do analizy operacyjnej, a część z nich, jako cele elektroniczne – do analizy technicznej. Informacje te są wykorzystywane do oceny sytuacji militarnej w procesie podejmowania decyzji (rozpoznanie sytuacyjne), określania parametrów technicznych i przedsięwzięć organizacyjnych, niezbędnych do przeprowadzenia skutecznego przeciwdziałania elektronicznego (rozpoznanie celów elektronicznych) oraz organizowania obrony elektronicznej, a także koordynacji kolejnych zadań rozpoznawczych. Rozpoznanie sytuacyjne i rozpoznanie celów elektronicznych podlegają wszelkim regułom i zasadom obowiązującym w procesie działalności rozpoznawczej. Rozpoznanie to umożliwia wykrywanie bezpośredniego zagrożenia wojsk, zapewnia podjęcie działań uprzedzających (aktywnych i pasywnych) ograniczających skutki oddziaływania potencjalnego przeciwnika.

Rozpoznanie radioelektroniczne[22] ma na celu zdobywanie i przetwarzanie tych informacji o przeciwniku, których nośnikami są fale elektromagnetyczne (wraz z informacją w nich zawartą) – wypromieniowane przez źródła przeciwnika. Współczesne środki rozpoznania radioelektronicznego powinny być przystosowane zarówno do odbioru fal elektromagnetycznych emitowanych przez źródła (urządzenia nadawcze przeciwnika) jak i do prowadzenia analizy technicznej. Wartość rozpoznawczą poszczególnych źródeł należy określać na podstawie określonych, w procesie rozpo-

[22] J. Pieniak., *Określenie kryterium wiarygodności rozpoznania radiowego*, projekt publikacji do Zeszyty Naukowe AON, Warszawa 2005 r. (J. Pieniak współpracuje naukowo od wielu lat z autorem niniejszej pracy).

znania radioelektronicznego ich cech rozpoznawczych (informacyjnych). Źródłami rozpoznania radioelektronicznego są wszystkie środki pracujące w zakresie widma elektromagnetycznego od dolnej granicy podzakresu radiowego, do górnej granicy podzakresu optycznego.

Metodami zdobywania danych w rozpoznaniu radioelektronicznym są: poszukiwanie (search), przechwytywanie (intercept), śledzenie aktywności źródeł, namierzanie (direction finding DF) oraz analiza techniczno-operacyjna (anlysis).

Poszukiwanie jest podstawowym procesem rozpoznawczym, który ma na celu wykrycie sygnałów wypromieniowanych przez źródła rozpoznania i wyselekcjonowanie tych, którymi prowadzący rozpoznanie jest zainteresowany. Aby mogło nastąpić wykrycie źródła sygnału muszą być spełnione następujące warunki dostępności:

1. czasowo-przestrzenny - tzn. w tym samym czasie musi nastąpić spotkanie charakterystyk antenowych nadajnika sygnału i odbiornika urządzenia rozpoznawczego;
2. energetyczny - tzn. moc sygnału na wejściu urządzenia rozpoznawczego M_{we} musi być nie mniejsza od jego realnej czułości M_{cz}:

$$M_{we} > M_{cz}$$

3. częstotliwościowy – tzn. odbiornik urządzenia rozpoznawczego musi być nastrojony na częstotliwość pracy (nośną) źródła sygnału f_s, z odpowiednią dokładnością:

$$\frac{\Delta f}{2} \leq f_s \leq f_0 + \frac{\Delta f}{2};$$

gdzie:

f_0 – częstotliwość na którą jest nastrojony odbiornik,

Δf – szerokość pasma przepuszczania odbiornika,

f_s - częstotliwość nośna sygnału.

W trakcie poszukiwania realizowanego za pomocą odpowiednich urządzeń, każdy wykryty sygnał zazwyczaj zostaje poddany wstępnej identyfikacji i klasyfikacji. Poszukiwanie sygnałów prowadzi się w częstotliwości, kierunku lub równocześnie w częstotliwości i kierunku.

Poszukiwanie w częstotliwości polega na przestrajaniu urządzenia odbiorczego w całym jego zakresie lub określonym podzakresie i ustaleniu tych często-

tliwości na których występują poszukiwane sygnały. Jedną z form poszukiwania w częstotliwości jest jednoczesny odbiór w kilku przedziałach częstotliwości przy użyciu odbiorników wielokanałowych. Te ostatnie są szczególnie przydatne przy poszukiwaniu emisji rozproszonych typu FH[23].

Nowoczesne urządzenia rozpoznawcze, realizujące poszukiwanie w częstotliwości, są bardzo szybkie. Prędkość przestrajania osiąga wartości około 20 do 40 GHz na sekundę, dlatego wykrywanie sygnałów emisji FH nie stanowi dla nich problemu. Zazwyczaj urządzenia te są wyposażone w anteny o charakterystyce dookolnej, sektorowej lub kierunkowej. Po wykryciu i identyfikacji sygnału następuje namierzanie jego źródła.

W procesie poszukiwania prawdopodobieństwo wykrycia pracy pojedynczego źródła, określa funkcja kryterium:

$$f(p) \geq \frac{T_p}{T_s} \geq 1;$$

gdzie:

$f(p)$ –funkcja kryterium skutecznego przeszukiwania,

T_p – czas pracy poszukiwanego źródła,

T_s – czas przeszukiwania przydzielonego pasma.

Czas przeszukiwania przydzielonego pasma składa się z czasu przestrajania urządzenia odbiorczego przy poszukiwaniu oraz czasu identyfikacji źródła przez operatora. Na prawdopodobieństwo wykrycia pojedynczej emisji zasadniczy wpływ posiada szerokość przydzielonego do poszukiwania pasma częstotliwości, a także sprawność operatora i doskonałość wykorzystywanego sprzętu (odbiorników i analizatorów). Czas identyfikacji źródła zależy od tego, czy na stanowisku rozpoznawczym znajduje się operator czy też identyfikacja odbywa się automatycznie. W tym czasie winna zostać dokonana identyfikacja, czyli analiza techniczno-operacyjna[24] sygnału oraz namiar (lokalizacja źródła).

Przechwytywanie polega na odbiorze sygnałów nadawanych przez wykryte źródła rozpoznania i rejestrowaniu bądź samych sygnałów, bądź zawartych w nich informacji. Polega na dostrojeniu urządzenia rozpoznawczego do częstotliwości pra-

[23] Emisja typu FH od ang. Freqency Hopping polega na permanentnej zmianie wykorzystywanych częstotliwości radiowych (typowa szybkość ok. 200-300 zmian w ciągu sekundy).
[24] Analiza techniczno-operacyjna obejmuje określenie częstotliwości, rodzaju emisji oraz określenie typu przesyłanej informacji (fon, dalekopis, dane);

cy rozpoznawanego źródła i ciągłej rejestracji nadawanych informacji lub zmian parametrów nadawanego sygnału. Kryterium wyboru źródła do przechwytywania stanowi jego wartość informacyjna oraz ranga i miejsce obiektu które to źródło obsługuje.

Śledzenie polega na okresowym sprawdzaniu pracy rozpoznawanych źródeł. Śledzi się te źródła, których sygnały nie wymagają przechwytywania lub których wartość informacyjna w danej sytuacji jest drugorzędna.

Namierzanie to proces lokalizacji źródła promieniowania elektromagnetycznego za pomocą namierników[25] (stacji namierzania). Lokalizacji można dokonać za pomocą kilku namierników. W tym przypadku rozróżnia się trzy sposoby namierzania:

- automatyczne (synchronicznie) – polega na jednoczesnym określeniu azymutów na źródło rozpoznania przez wszystkie namierniki pracujące w systemie,
- na komendę – polega na określaniu azymutów na źródło przez wszystkie namierniki, które dostraja się do częstotliwości źródła, po otrzymaniu zadania ze stanowiska kierowania namierzaniem lub bezpośrednio ze stanowiska rozpoznawczego,
- według zadań stałych – polega na określaniu azymutów na pracujące źródła zgodnie z wcześniej opracowanym harmonogramem (planem).

Analiza techniczno-operacyjna polega na określeniu charakterystycznych cech sygnałów odebranych od źródeł, które wyróżniają je spośród innych i pozwalają na ich identyfikację przy kolejnych namiarach. W tym procesie dokonuje się również logicznego uporządkowania informacji o rozpoznawanych obiektach. Ocenia się ich skład i rozmieszczenie, stan ilościowo-jakościowy, rodzaj działalności i zamierzenia ich użytkowników.

Ze względu na rodzaje środków, w rozpoznaniu radioelektronicznym szczebla taktycznego możemy wyróżnić:

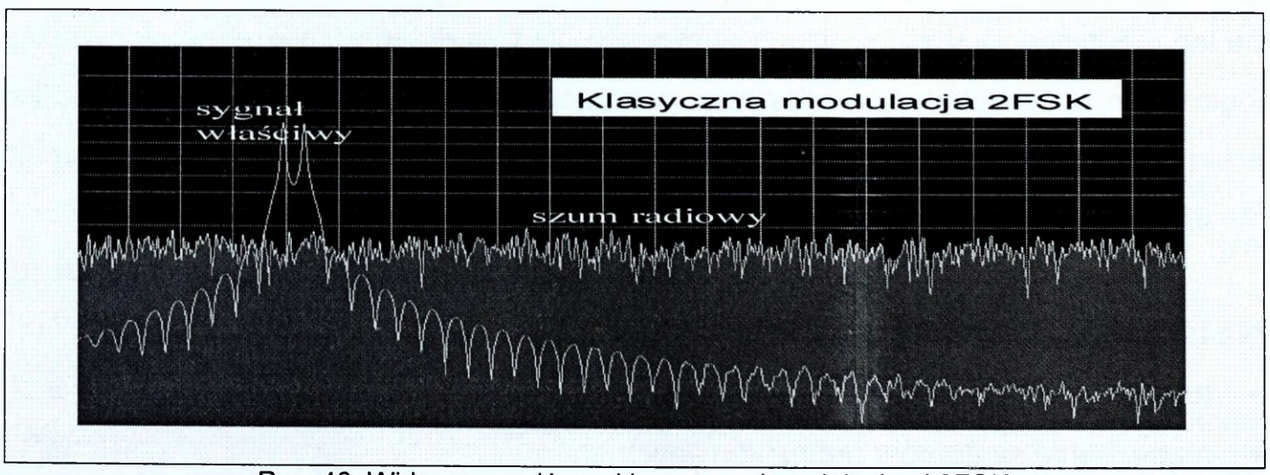
- rozpoznanie radiowe;
- rozpoznanie systemów radiolokacyjnych;
- rozpoznanie systemów radionawigacyjnych.
- rozpoznanie radiosatelitarne

[25] Określenie „namiernik" jest używane zamiennie z nazwą „pelengator".

Rozpoznanie radiowe[26] jest rodzajem rozpoznania radioelektronicznego, które obejmuje środki łączności radiowej i środki zakłócające tę łączność. Ma na celu zdobycie informacji o stanie ilościowym i jakościowym tych środków, miejscu ich rozmieszczenia i sposobach wykorzystania.

Głównym zadaniem tworzonych systemów łączności radiowej jest wiarygodne przekazywanie jak największej ilości informacji w jak najkrótszym czasie, przy minimalnych kosztach i maksymalnym bezpieczeństwie. Działające współcześnie systemy łączności w szerokim zakresie wykorzystują modulacje i metody nadawania ograniczające możliwość wykrycia i przechwytu informacji (LPI/LPD)[27]. Dzięki rozpraszaniu widma sygnału oraz skróceniu do niezbędnego minimum czasu przekazywania informacji, prawdopodobieństwo jej wykrycia i przechwytu, przy zastosowaniu klasycznych środków i narzędzi rozpoznania radioelektronicznego, jest bardzo niskie – wręcz zerowe. Przykładowo, gdy tą samą informację przekazujemy raz klasyczną podwójną manipulacją częstotliwości - 2FSK, a następnie podwójną manipulacją fazy - 2PSK z wykorzystaniem cyklicznego, pseudolosowego kodu rozpraszającego, to w drugim przypadku poziom nadawanego sygnału jest mniejszy od poziomu szumów.

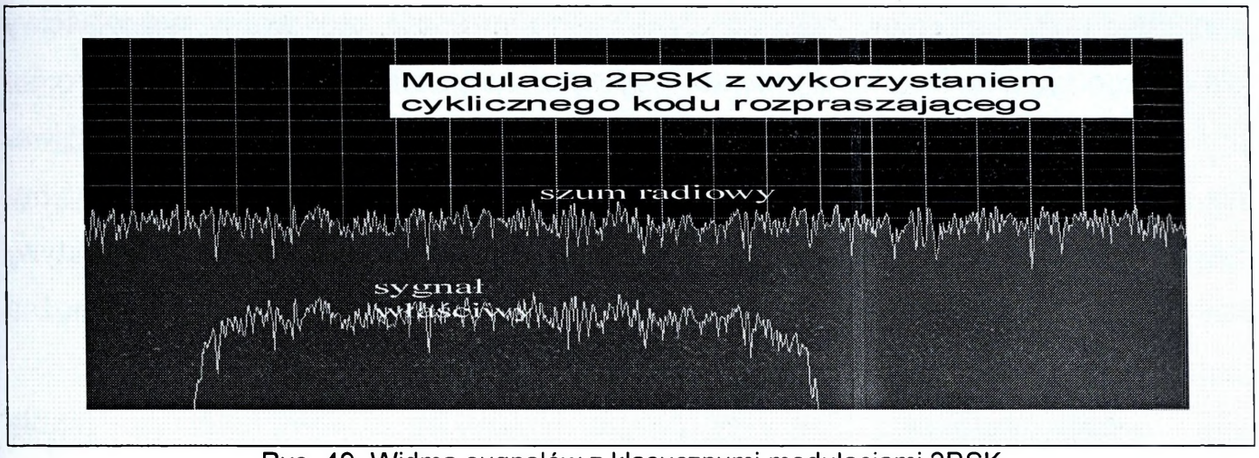
Kolejnym utrudnieniem, z punktu widzenia rozpoznania, wynikającym z powszechnego stosowania techniki cyfrowej w systemach łączności, stała się możliwość wykorzystania transmisji zwielokrotnionej (TDM)[28]. Takie rozwiązanie umożliwia łączenie i przenoszenie wielu, stosunkowo wolnych, kanałów informacyjnych jednym szybkim strumieniem danych (rys. 48 i 49).



Rys. 48. Widma sygnałów, z klasycznymi modulacjami 2FSK

Źródło: J. Pieniak , „Prowadzenie rozpoznania elektronicznego w ramach walki informacyjnej". Sesja Naukowa 100. rocznicy urodzin Mariana Rajewskiego, Warszawa 2005.

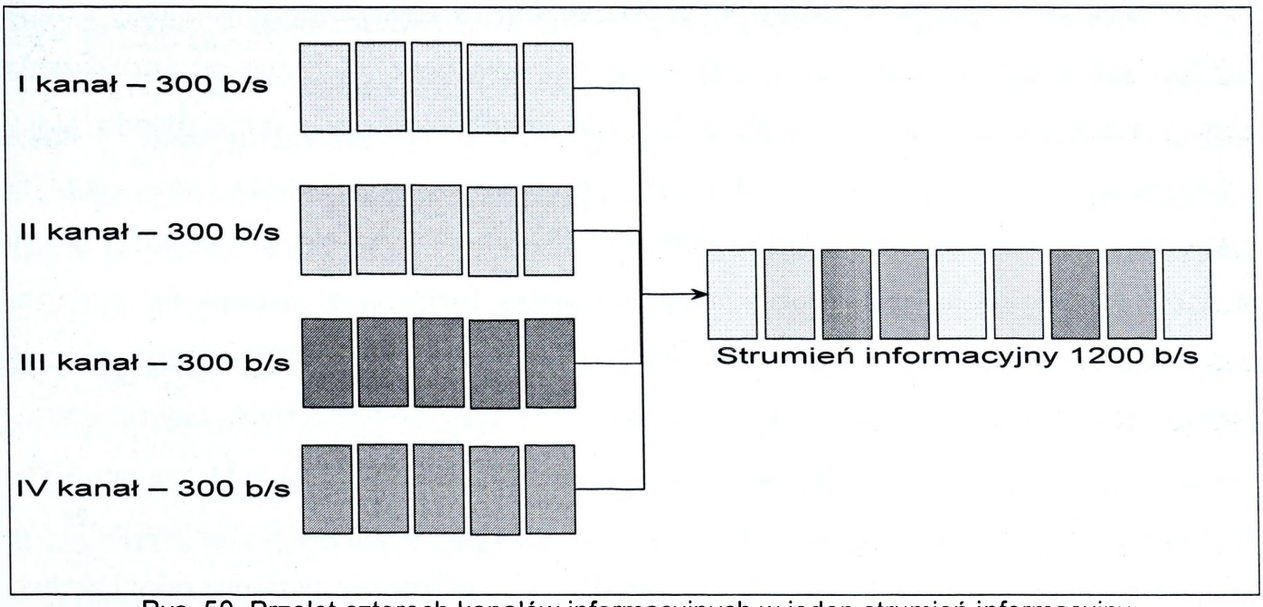
[26] Pieniak J., *Prowadzenie rozpoznania elektronicznego w ramach walki informacyjnej*. Sesja Naukowa 100. rocznicy urodzin Mariana Rajewskiego, Warszawa 2005 r.
[27] Low-Probability-of-Intercept/Low-Probability-of-Detection.
[28] Time Division Multiplexing.



Rys. 49. Widma sygnałów z klasycznymi modulacjami 2PSK

Źródło: J. Pieniak , „Prowadzenie rozpoznania elektronicznego w ramach walki informacyjnej". Sesja Naukowa 100. rocznicy urodzin Mariana Rajewskiego, Warszawa 2005.

Informacje z poszczególnych kanałów są przeplecione ze sobą, co w zasadniczy sposób utrudnia określenie intensywności ich wykorzystania, zwłaszcza przy braku informacji co do reguł przeplotu (rys.50).



Rys. 50. Przelot czterech kanałów informacyjnych w jeden strumień informacyjny

Źródło: J. Pieniak , „Prowadzenie rozpoznania elektronicznego w ramach walki informacyjnej". Sesja Naukowa 100. rocznicy urodzin Mariana Rajewskiego, Warszawa 2005.

Ilość pracujących jednocześnie środków radioelektronicznych oraz obecność zakłóceń atmosferycznych i przemysłowych w paśmie częstotliwości jest tak duża, że spełnienie wymogów pewnego i wiarygodnego przekazywania informacji narzuca konieczność stosowania wyrafinowanych sposobów jej kodowania. Stosowane obecnie kody umożliwiają rozpraszanie błędów grupowych, powstających w wyniku zaników czy zakłóceń odbieranego sygnału, a następnie ich automatyczną korekcję. W ten sposób rośnie odporność na zakłócenia kanału łączności, a ilość błędów w transmisji radykalnie maleje. Dodatkowo, aby mieć pewność, że informacja dotrze

zgodnie z przeznaczeniem tylko do określonego adresata, stosowany jest właściwy dla danego systemu łączności protokół kryptograficzny.

Uwzględniając przedstawione wyżej uwarunkowania, rozpoczęto poszukiwania innych sposobów prowadzenia rozpoznania radiowego, które wykorzystywać będą omówione wcześniej metody (poszukiwania, przechwytywania, śledzenia aktywności źródeł, namierzania oraz analizy techniczno-operacyjnej). Sposoby te można podzielić na: szeregowe i równoległe.

Sposób szeregowy, klasyczny, polega na tym, że prowadzenie rozpoznania radiowego realizuje się na określonej ilości stanowisk rozpoznawczych, na których poszukuje się sygnałów w całym zakresie lub określonym podzakresie i ustala się te częstotliwości na których one występują. Po wykryciu i identyfikacji sygnału następuje namierzanie jego źródła, które polega na ustawieniu się w szeregu do systemu namierzania i korzystanie z niego zgodnie z przydzielonym priorytetem.

W procesie poszukiwania prawdopodobieństwo wykrycia pracy pojedynczego źródła, zależy od czasu pracy poszukiwanego źródła oraz od czasu przeszukiwania przydzielonego pasma. Czas przeszukiwania przydzielonego pasma składa się z czasu przestrajania urządzenia odbiorczego przy poszukiwaniu oraz czasu identyfikacji źródła przez operatora. Na prawdopodobieństwo wykrycia pojedynczej emisji zasadniczy wpływ posiada szerokość przydzielonego do poszukiwania pasma częstotliwości, a także sprawność operatora i doskonałość wykorzystywanego sprzętu (odbiorników i analizatorów). Czas identyfikacji źródła zależy od tego, czy na stanowisku rozpoznawczym znajduje się operator, czy też identyfikacja odbywa się automatycznie. W czasie identyfikacji jest dokonana analiza techniczno-operacyjna[29] sygnału oraz namiar – czyli lokalizacja źródła. W przypadku gdy prawdopodobieństwo wykrycia pracy sygnałów radiowych określonej modulacji, będzie większe od 0,75 zostanie osiągnięty właściwy efekt poszukiwania. Gdy warunek ten nie jest spełniony należy przydzielić dodatkowo kilka stanowisk rozpoznawczych.

Sposób równoległy, zasadniczo zwiększa możliwości i automatyzuje system rozpoznania radiowego. Bazuje na nowoczesnych technologiach, wprowadza zasadniczo inne podejście do procesów rozpoznania radioelektronicznego tj. wykrywania, przechwytu i namierzania relacji radiowych pracujących w interesującym nas zakresie.

---

[29] Analiza techniczno-operacyjna obejmuje określenie częstotliwości, rodzaju emisji oraz określenie typu przesyłanej informacji (fon, dalekopis, dane);

Komercyjnym rozwiązaniem jest automatyczny system ACOS[30]. W skład systemu wchodzą trzy zasadnicze komponenty:

- zestaw szerokopasmowych namierników radiowych,
- centrum monitoringu,
- oprogramowanie systemowe zawierające bazy danych wynikowych oraz programy sterujące i zarządzające systemem.

Zastosowane w systemie ACOS szerokopasmowe namierniki radiowe charakteryzują się bardzo dużą wydajnością i szybkością namierzania. Dzięki swej nowoczesnej konstrukcji są w stanie namierzyć każdy sygnał, który pojawi się w badanym zakresie częstotliwości na czas dłuższy od 0,5 s. Dlatego też, oprócz funkcji lokalizacji źródeł promieniowania, namierniki pełnią rolę elementu wykrywającego te źródła. Każdy z namierników prowadzi samoczynnie wykrywanie i namierzanie według ustalonego przez użytkownika scenariusza, a wyniki namierzania przesyłane są do bazy danych wyników namierzania.

Centrum monitoringu to zespół szeroko- i wąskopasmowych odbiorników radiowych (z własnym systemem antenowym) powiązanych z wysokowydajnym systemem komputerowym o architekturze wieloprocesorowej. Centrum monitoringu połączone jest siecią LAN z bazą danych wyników namierzania. Każde wykryte i namierzone źródło promieniowania przekazywane jest do centrum, gdzie następuje proces automatycznej klasyfikacji wykrytych sygnałów na znane i nieznane. Dla sygnałów znanych, automatycznie przydzielany jest właściwy demodulator i dekoder, a otrzymane wyniki analizy i demodulacji rejestrowane w bazie danych wynikowych. Sygnały nierozpoznane są tylko rejestrowane do dalszej analizy przez specjalistów w sposób nieautomatyczny. Oprogramowanie zawiera specjalistyczne narzędzia, nie tylko do ręcznej analizy sygnałów, ale również do tworzenia nowych demodulatorów i dekoderów. Dzięki temu, sygnały pierwotnie nierozpoznane, przy powtórnym napotkaniu przez system mogą być przetwarzane w sposób automatyczny. Dzięki zastosowaniu wieloszczeblowego buforowania strumienia informacji, wszelkie procesy decyzyjne związane z namierzaniem, klasyfikacją sygnałów, wyborem demodulatorów i dekoderów są realizowane w sposób bezstratny. Oznacza to, że przechwyt informacji z danego źródła może odbywać się już w momencie wykrycia.

[30] Firmy niemieckiej PLATH GmbH, www.plath.de.

Bazy danych, jako trzeci element automatycznego systemu rozpoznania ACOS są połączone siecią komputerową z grupami użytkowników. Zastosowana technologia baz danych służy nie tylko do przechowywania danych wynikowych, ale również do konfigurowania i sterowania systemem. Pozwala na dynamiczne dostosowywanie realizowanych zadań rozpoznawczych do zaistniałej sytuacji radioelektronicznej. Bazy danych posiadają wiele wyspecjalizowanych narzędzi do wizualizacji otrzymywanych wyników w postaci zestawień, wykresów, tabel i zobrazowań na mapach. Istnieje również oprogramowanie do monitorowania poprawności działania całego systemu ACOS, jego konfiguracji i testowania poszczególnych podsystemów ze stanowiska administratora.

Duża elastyczność i wydajność systemu ACOS wskazuje na możliwość niezależnego wykorzystania tego systemu przez różne grupy użytkowników, bez wzajemnego oddziaływania.

Rozpoznanie radiowe obejmuje środki pracujące w systemach łączności radiowej krótkofalowej (KF) i ultrakrótkofalowej (UKF), łączności radioliniowej (horyzontowej i pozahoryzontowej) oraz łączności satelitarnej.

Łączność radiowa KF, którą traktuje się jako rezerwową, w dalszym ciągu nie straciła na znaczeniu w dowodzeniu wojskami. W latach 70. wykorzystanie łączności radiowej KF na szczeblach taktycznym i operacyjnym wynosiło około 37%, w latach 80. około 28% natomiast w połowie lat 90. około 20%. Nie oznacza to zmniejszenia się ogólnej liczby wykorzystywanych radiostacji, lecz mniejszego stopnia ich wykorzystania. Mimo tendencji do pomniejszania jej roli, stanowi nadal dla rozpoznania radioelektronicznego jedno z zasadniczych źródeł rozpoznania, co wynika głównie z propagacji fal krótkich, których zasięg jest w zasadzie nieograniczony.

Łączność radiowa UKF wykorzystywana jest przez wszystkie szczeble dowodzenia. Stanowi podstawowy rodzaj łączności do brygady włącznie. Natomiast od szczebla dywizji wzwyż, służy do wewnętrznych połączeń na stanowiskach dowodzenia. Ponadto jest wykorzystywana do współdziałania wojsk lądowych z lotnictwem taktycznym w relacjach ziemia-samolot. Łączność radiowa UKF wojsk lądowych (20 - 88 MHz) i sił powietrznych (220 - 400 MHz), jest jednym z podstawowych źródeł rozpoznania na szczeblu taktycznym.

Łączność radioliniowa, jeden z podstawowych elementów eksploatowanych systemów łączności, umożliwia tworzenie wielokanałowych magistrali wymiany da-

nych. Może stanowić ważne pod względem informacyjnym źródło rozpoznania. Rozpoznanie łączności radioliniowej obejmuje przedsięwzięcia polegające na wykrywaniu sygnałów przekazywanych w kierunkach radioliniowych oraz przechwytywaniu i analizowaniu danych przesyłanych w kanałach horyzontowych i pozahoryzontowych, Środki rozpoznania łączności radioliniowej są instalowane w specjalnych aparatowniach, które poszukując sygnałów poruszają się po drogach rokadowych, bądź na statkach powietrznych (pilotowych i bezpilotowych) latających w strefach dyżurowania nad własnym ugrupowaniem. W przypadku rozpoznania łączności horyzontowej anteny stacji radioliniowych i urządzenia rozpoznawczego muszą być w zasięgu optycznym (muszą się „widzieć"). Rozpoznanie łączności pozahoryzontowej wykorzystuje natomiast rozproszenie wiązki na niejednorodnościach troposfery (stąd potoczna nazywa radiolinii troposferycznych), nie wymaga warunku bezpośredniej widoczności, w tym przypadku anteny stacji radioliniowej i urządzenia rozpoznawczego mogą się znajdować w znacznej odległości od siebie (poza zasięgiem optycznym).

Rozpoznawanie łączności satelitarnej rozpoczęło się wraz z rozwojem systemów łączności satelitarnej. W następstwie tego ukształtował się nowy rodzaj rozpoznania elektronicznego. Rozpoznanie to obejmuje przedsięwzięcia prowadzące do zdobywania danych dotyczących środków i systemów łączności wykorzystujących sztuczne satelity Ziemi. Proces rozpoznawania systemów łączności radiowej obejmuje następujące etapy:

- poszukiwania źródła promieniowania w przestrzeni i częstotliwości,
- analizę techniczną sygnału radiowego,
- przechwyt informacji,
- analizę informacji i parametrów technicznych,
- wnioskowanie operacyjne.

Po wykryciu źródła promieniowania i ustaleniu jego częstotliwości pracy następuje kolejny etap rozpoznania, którym jest analiza techniczna sygnału radiowego. Celem jej jest ustalenie sposobu odbioru nadawanych informacji lub w przypadku stosowania utajniania informacji, ustalanie charakterystycznych cech technicznych pozwalających klasyfikowanie nadawania. Analiza techniczna obejmuje:

- określanie parametrów sygnału odbieranego (poziom sygnału, częstotliwość, zwielokrotnienie - FDM, rodzaj i parametry modulacji);

- selekcję kanału częstotliwościowego – pomiar parametrów (częstotliwości, pasma);
- demodulację – określanie sposobu i parametrów kodowania, dla systemów modulacji cyfrowej ustalana jest również szybkość transmisji danych, sposób kodowania i korekcji błędów;
- dekodowanie i „rozplatanie" sygnałów;
- określanie kodu transmisyjnego i przechwyt wiadomości (danych) nieszyfrowanych;
- określanie sposobu szyfrowania i deszyfrowania wiadomości;
- wskazanie metod przechwytu informacji dla nadawań jawnych.

Systemy łączności działają w oparciu o satelity telekomunikacyjne, w zależności od rodzaju, na orbicie rozmieszcza się od trzech do dziewięciu satelitów geostacjonarnych, które pokrywają swym zasięgiem niemalże cały glob ziemski (za wyjątkiem rejonów podbiegunowych). Do rozpoznania łączności satelitarnej wykorzystuje się urządzenia odbiorcze, których anteny ustawia się w kierunku możliwego rozmieszczenia satelitów. Położenie orbit i satelitów geostacjonarnych jest zazwyczaj znane, co znacznie ułatwia proces poszukiwania w kierunku. Zasadniczym problemem w procesie wykrywania jest więc poszukiwanie w częstotliwości.

Oprócz satelitów geostacjonarnych, w globalnych systemach łączności wykorzystuje się również satelity na tzw. średnich orbitach MEO (10 - 16 tys. km). Proces rozpoznania w tym przypadku jest o wiele bardziej złożony. Urządzenia rozpoznawcze muszą prowadzić poszukiwanie w azymucie, elewacji i częstotliwości, a po ich wykryciu ruchome anteny urządzeń rozpoznawczych muszą podążać za wykrytym obiektem, do momentu jego zniknięcia za linią horyzontu.

Rozpoznawanie systemów łączności satelitarnej, działających w oparciu o satelity na niskich orbitach LEO (poniżej 2 tys. km), jest problemem złożonym. Systemy te wykorzystują od 14 do 66 satelitów poruszających się z bardzo dużą prędkością kątową wynoszącą ok. 3,6°/min (czas obiegu jednego satelity wokół Ziemi wynosi około 100 minut).

Systemy łączności radiowej, radioliniowej i satelitarnej, mogą stanowić niewyczerpane źródła danych rozpoznawczych, które może uzyskiwać dobrze zorganizowane rozpoznanie radioelektroniczne. Jeśli uda się wykryć i zarejestrować pracę źródła, rozpoczyna się proces analizy sygnałów. W pierwszej kolejności jest określa-

ny zwykle rodzaj modulacji i jej parametry techniczne. W przypadku prostych modulacji analogowych (AM, FM, SSB, CW) odbiór informacji jest możliwy prawie natychmiast. Dla modulacji cyfrowych, prawidłowe określenie jej rodzaju umożliwia zastosowanie właściwego demodulatora. Po demodulacji uzyskuje się strumień informacyjny dostosowany do dalszej analizy. Może się wówczas okazać, że sposób kodowania tego strumienia odpowiada jednemu ze znanych sposobów, więc po procesie dekodowania otrzymuje się czystą informację. Współcześnie zdarza się to jednak bardzo rzadko. Najczęściej strumień informacyjny nie ma określonej struktury i jest odporny na badania statystyczne. Taki materiał źródłowy staje się wówczas obiektem badań kryptoanalitycznych.

Strumień cyfrowy otrzymany w wyniku demodulacji sygnału radiowego musi być poddany analizie w celu poprawnego określenia systemu kodowania nadmiarowego. We współczesnej telekomunikacji kodowanie jest stosowane w celu detekcji i korekcji błędów, jakie występują w sygnale otrzymanym po stronie odbiorczej. Współczesne kody są bardzo skomplikowane i trudne do identyfikacji na podstawie samego sygnału. Poprawne zdekodowanie strumienia danych jest zadaniem niezbędnym do rozpoczęcia procesu właściwej kryptoanalizy. Pomimo, iż kody detekcyjno-korekcyjne nie są traktowane jako zabezpieczenie kryptograficzne, to stanowią problem o podobnym stopniu złożoności.

Rozpoznanie radiolokacyjne to wykrywanie obiektów nieruchomych i ruchomych na lądzie, morzu i w powietrzu za pomocą stacji radiolokacyjnych. Rozpoznanie systemów radiolokacyjnych obejmuje zdobywanie danych dotyczących: systemów i środków radiolokacyjnych rozpoznania pola walki, artylerii i środków napadu powietrznego, przez poszukiwanie (wykrywanie), przechwytywanie, śledzenie i analizę sygnałów wypromieniowanych przez te środki oraz ich namierzanie. Obiekty, takie jak: infrastruktura naziemna, okręty, samoloty, rakiety, chmury itp., nazywane są celami radiolokacyjnymi[31], zaś sygnały odbite od tych obiektów – echem radarowym lub echem radiolokacyjnym. Badania aktualnego stanu oraz tendencji rozwojowych radiolokacji pozwalają stwierdzić, że do wykrywania obiektów pola walki wykorzystywane jest głównie pasmo 3 cm (8-12 GHz), natomiast środki napadu powietrznego wykorzystują pasma 2 i 3 cm (8-20 GHz). Dzięki temu, że energia elektromagnetyczna w zakresie mikrofalowym rozprzestrzenia się prostoliniowo i ze stałą prędkością -

[31] W wojskach radiotechnicznych przedmioty wykryte przez stacje radiolokacyjne nazywane są obiektami. Obiekty niezidentyfikowane lub obce (nieprzyjacielskie) nazywa się celami.

w środowisku jednorodnym, możliwe jest określanie współrzędnych rozpoznawanych obiektów, ich parametrów ruchu (prędkości i kierunku) oraz wielkości bryłowej.

Rozpoznanie radiolokacyjne jest prowadzone przez służby wojskowe i cywilne, które kontrolują przede wszystkim przestrzeń powietrzną, ale także obszar lądowy i morski, zarówno w czasie pokoju, konfliktu jak i wojny. Z tego względu, rozpoznanie radiolokacyjne obejmuje wszelkie rodzaje wojsk i służb, w których wykorzystywane są systemy i środki radiolokacyjne, obejmuje ono:

- systemy rozpoznania obszaru powietrznego,
- systemy nadzorowania pola walki,
- systemy kierowania ogniem,
- systemy obrony przeciwlotniczej,
- systemy rozpoznania powierzchni ziemi i inne.

Rozpoznaniem obejmowane są systemy wykorzystujące naziemne, brzegowe i okrętowe stacje radiolokacyjne, jak również samoloty wyposażone zarówno w klasyczne stacje radiolokacyjne i stacje obserwacji bocznej. Wykrycie pracującego źródła promieniowania radiolokacyjnego wymaga spełnienia warunków podobnych, jak to ma miejsce w przypadku rozpoznania radiowego, tzn. energetycznego, częstotliwościowego, przestrzennego oraz czasowego. Warunki te, określają możliwości prowadzenia rozpoznania systemów radiolokacyjnych oraz wpływają, w sposób zasadniczy, na rozwiązania konstrukcyjne i sposoby działania urządzeń rozpoznawczych. Szczególne znaczenie dla możliwości poszukiwania i wykrywania stacji radiolokacyjnych mają warunki przestrzenny i częstotliwościowy, ponieważ wykrycie źródła emisji następuje w kierunku i w częstotliwości.

Identyfikacja wymaga wykonania dwóch operacji:

- ukształtowania wektora cech na podstawie wiadomości uzyskanych przy odbiorze (a posteriori) i porównania go z wektorem cech, ukształtowanym w oparciu o dane zgromadzone wcześniej w „banku danych" (a priori).
- rozpoznania rodzaju urządzenia i określenia jego danych taktyczno-technicznych, które przeprowadza się na podstawie analizy wykrytych sygnałów.

Analiza odebranych sygnałów obejmuje szereg kolejnych operacji, z których najważniejsze to: rejestracja sygnału, pomiar parametrów sygnału, przetworzenie otrzymanych informacji z celem określenia typu, rodzaju i egzemplarza rozpoznawanego urządzenia radiolokacyjnego. Wszystkie te operacje wykonywane są przy sze-

rokim wykorzystaniu automatycznych i półautomatycznych analizatorów i rejestratorów.

Opracowywanie i tworzenie baz danych, w tym wzorców sygnałów rzeczywistych oraz metryk stacji radiolokacyjnych, jest jednym z podstawowych zadań prowadzonego w czasie pokoju rozpoznania stacji i systemów radiolokacyjnych.

Rozpoznanie radiolokacyjne może być prowadzone na małą (do 50 km) i dużą (do 500 km) głębokość, niezależnie od pory doby i roku oraz warunków meteorologicznych. Powietrzne rozpoznanie radiolokacyjne prowadzone jest z dużych wysokości (od 5 do 12 tysięcy metrów) i obejmuje swoim zasięgiem duże obszary przestrzeni powietrznej, morskiej i lądowej.

Wyróżniane są dwa sposoby prowadzenia rozpoznania radiolokacyjnego: pasywne i aktywne.

Pasywne rozpoznanie radiolokacyjne polega na odbiorze energii elektromagnetycznej emitowanej przez obiekty w sposób niezamierzony i zamierzony. Do sygnałów takich zalicza się:

- promieniowanie termiczne obiektów o temperaturze wyższej od zera bezwzględnego (0°K = -273,16°C),
- promieniowanie w zakresie fal radiowych, powstające przy pracy silników rakietowych, reakcjach jądrowych i wyładowaniach atmosferycznych,
- promieniowanie zamierzone różnych urządzeń radiowych znajdujących się na pokładach wykrywanych celów.

Podstawową zaletą urządzeń radiolokacji pasywnej jest ich niewykrywalność. Wynika to z faktu, że nie mają one żadnych urządzeń nadawczych, których sygnały mogłyby być odbierane przez urządzenia odbiorcze przeciwnika.

Aktywne rozpoznanie radiolokacyjne wykorzystuje własne środki emitujące w sposób zamierzony energię elektromagnetyczną. W radiolokacji aktywnej wykorzystuje się sygnały impulsowe i ciągłe. Do zalet pracy w metodzie impulsowej należy zaliczyć możliwość generacji sygnału bardzo dużej mocy (rzędu megawatów) w postaci impulsu o czasie trwania rzędu milisekund, przy stosunkowo małej mocy średniej nadajnika. Poza tym praca impulsowa daje możliwość jednoczesnego wykrywania i pomiaru współrzędnych dużej liczby obiektów oraz wykorzystywania jednej anteny do nadawania i odbioru sygnałów. Radiolokację aktywną realizują urządzenia w skład których wchodzą: nadajnik wytwarzający sygnały radiolokacyjne, odbiornik odbierający sygnały echa radiolokacyjnego oraz urządzenie zobrazowania. Ze względu

na sposób uzyskiwania sygnału echa wyróżnia się następujące rodzaje tej radiolokacji:

- z pasywną odpowiedzią,
- z aktywną odpowiedzią,
- półaktywne.

Radiolokacja aktywna z pasywną odpowiedzią polega na wykorzystaniu zjawiska odbijania fal radiowych od obiektu, a więc zdolności do pasywnej odpowiedzi. Odbity sygnał radiolokacyjny (echo) może zawierać dane o położeniu celu (współrzędne dwu - lub trójwymiarowe), parametrach ruchu (prędkości), a także o takich własnościach fizycznych, jak wymiary i kształt celu, jego przewodność itd. Radiolokacja aktywna z pasywną odpowiedzią umożliwia wykrycie obiektu, który nie promieniuje energii elektromagnetycznej. Wykryty zostanie każdy obiekt, który odbija fale elektromagnetyczne, dlatego też ten rodzaj rozpoznania należy do najczęściej spotykanych w praktyce.

Radiolokacja aktywna z aktywną odpowiedzią polega na współpracy urządzenia radiolokacyjnego lub specjalnego urządzenia wywoławczego (zapytującego) z zainstalowanym na wykrywanym obiekcie urządzeniem odzewowym (odpowiadającym). Jest to urządzenie nadawczo-odbiorcze wraz z anteną, które po odebraniu słabych sygnałów wywoławczych powoduje automatyczne nadawanie sygnałów odzewowych o stosunkowo dużej mocy, nie koniecznie na tej samej częstotliwości. Metodę tę wykorzystuje się do określenia przynależności państwowej samolotów tzw. określenie „swój - obcy" lub też w systemach radionawigacyjnych. W przypadku gdy nosiciel urządzenia zapytującego wyśle sygnał zapytania to urządzenie (radiolatarnia) odpowie na zapytanie wysyłając sygnał zwrotny. Układy przeliczające określą wówczas miejsce położenia obiektu.

Radiolokacja półaktywna polega na stosowaniu dwu lub więcej stacji radiolokacyjnych, z których jedna przeznaczona jest do „oświetlania" celu a druga do odbioru odbitych przezeń sygnałów (radiolokacja bistatyczna lub multistatyczna)[32]. Tego rodzaju urządzenia wykorzystywane są do specjalnych zastosowań jak np. dla ułatwienia naprowadzania pocisków kierowanych na cel lub wykrywania obiektów w technologii „stealth". Naziemna stacja radiolokacyjna może zawierać kilka urządzeń

[32] Radiolokacja bistatyczna - to zespół dwóch urządzeń z czego jednym jest nadajnik a drugim odbiornik wraz z urządzeniem wskaźnikowym. Radiolokacja multistatyczna to zespół co najmniej trzech urządzeń z czego jednym musi być nadajnik a dwa pozostałe to odbiorniki z urządzeniami wskaźnikowymi. W obydwu przypadkach nadajnik i odbiornik muszą być zsynchronizowane w czasie i w przestrzeni.

odbiorczych. Czym większa ilość urządzeń odbiorczych tym większe prawdopodobieństwo wykrycia obiektu o bardzo małej powierzchni skutecznego odbicia. Sygnały odbite docierają do odbiorników radiolokacyjnych, gdzie, po synchronizacji sygnałów można dokładne określić położenie obiektu, jego prędkość i kierunek poruszania. Podobne zjawisko występuje w pociskach kierowanych, gdzie sygnały odbite od obiektu odbierane są przez urządzenie odbiorcze w pocisku i wykorzystywane są do jego naprowadzania na obiekt (cel).

Cechą charakterystyczną urządzeń radiolokacyjnych pracujących impulsowo jest duża różnica mocy między sygnałami wysyłanymi przez nadajnik i sygnałami odbieranymi – odbitymi od celu o znikomej mocy. Wykorzystuje się również urządzenia radiolokacyjne pracujące na fali ciągłej, w których następuje jednoczesne wysyłanie sygnałów i odbiór echa. Wyodrębnienie odbitego sygnału następuje dzięki temu, że w punkcie odbioru ma on w danej chwili inną częstotliwość lub fazę od sygnału nadawanego.

Urządzenia pracujące na fali ciągłej można podzielić na:

- urządzenia z falą ciągłą niemodulowaną,
- urządzenia z falą ciągłą modulowaną.

Od dawna realizowana jest tendencja do wprowadzenia cyfrowych metod formowania sygnałów radiolokacyjnych (sondujących). Technika cyfrowa[33] pozwala na uproszczenie sterowania funkcjami generatorów sygnałowych z losową (pseudolosową) modulacją amplitudową, częstotliwościową oraz fazową manipulacją zapewniając kompensację zniekształceń przy nadawaniu i odbiorze odbitych sygnałów.

Rozpoznanie radiolokacyjne w systemie obrony powietrznej stanowi podstawowy rodzaj rozpoznania obiektów powietrznych.[34] Jest prowadzone przez posterunki radiolokacyjne wyposażone w aktywne systemy rozpoznania radiolokacyjnego oraz w systemy opracowania i zobrazowania informacji. Główne wysiłki są koncentrowane na prowadzeniu rozpoznania radiolokacyjnego przestrzeni powietrznej oraz dystrybucji informacji o sytuacji powietrznej w standardach transmisji kompatybilnych z funkcjonującymi w innych systemach.

---

[33] Wprowadzenie techniki cyfrowej miało wpływ na konstrukcją anten, w których do kształtowania charakterystyki kierunkowej wykorzystywano przesuwniki fazowe (anteny z tzw. szykiem fazowym), a ponadto na rozwój specjalizowanych procesorów cyfrowych pozwalających podejmować problemy cyfrowej obróbki sygnałów w czasie rzeczywistym. Następnie konstruowano anteny z tzw. cyfrowym szykiem fazowym, w których uzyskuje się sygnały cyfrowe bezpośrednio na wyjściu każdego elementu antenowego.

[34] Grzybowski M., *Posterunek radiolokacyjny, podstawowy komponent bojowy Wojsk Radiotechnicznych WLOP*, Przegląd WLOP, sierpień 2003 r.

Wojska Radiotechniczne[35] wykorzystują stacje radiolokacyjne o zróżnicowanych możliwościach wykrywania. Ugrupowanie wojsk tworzyć będą zarówno elementy stacjonarne, jak i manewrowe. Wyposaża się ten rodzaj wojsk w sprzęt najnowszej generacji. Są to nowoczesne radary typu N, które stanowią trzecią generację urządzeń radiolokacyjnych. Do rodziny tej należą stacje: ostrzegawcza i wysokościomierze oraz trójwspółrzędne o zwiększonym zasięgu i pułapie wykrywania.

Rozpoznanie optoelektroniczne jest stosunkowo nowym rodzajem rozpoznania elektronicznego. Jest przeznaczone do zdobywania oraz przetwarzania tych informacji o przeciwniku, których nośnikami są fale elektromagnetyczne pasma optycznego[36]. Do pracy w tym paśmie skonstruowano całą rodzinę urządzeń optoelektronicznych[37] pozwalających na prowadzenie rozpoznania w ultrafiolecie, w zakresie promieniowania widzialnego oraz w zakresie bliskiej, średniej i dalekiej podczerwieni. Wykorzystywane są tu urządzenia:

- telewizyjne,
- termowizyjne,
- noktowizyjne,
- oraz laserowe.

Telewizja stanowi dział telekomunikacji obejmujący całokształt zagadnień związanych z przekazywaniem na odległość ruchomych obrazów, zwykle z towarzyszącym im dźwiękiem, za pomocą urządzeń elektronicznych i torów telekomunikacyjnych W celu przetworzenia obrazu optycznego na sygnał elektryczny wykorzystuje się zjawisko fotoelektryczne, natomiast dla odwrotnego przetworzenia wykorzystuje się zjawisko katodoluminescencji.

Termowizja jest dostosowana do postrzegani obrazów w widmie promieniowania podczerwonego (aktualnie wykorzystywane są tylko dwa pasma tego widma (3μm i 10–13 μm). Zjawiska wykorzystywane w termowizji, podobne są do wykorzystywanych w noktowizji pasywnej. Różnica polega tylko na tym, że termowizja posiada jeszcze urządzenie skanujące, zamieniające obraz widziany w podczerwieni na ciąg impulsów elektrycznych (noktowizor pasywny z urządzeniem skanującym nazy-

[35] Wojska Radiotechniczne, http://www.wojsko.pl/index.html

[36] Pasmo optyczne (zakres optyczny) widma elektromagnetycznego stanowią promieniowania: ultrafioletowe (długość fali: 0,01-0,38μm), widzialne (długość fali: 0,38-0,76μm) i podczerwone (długość fali: 0,76-1000μm).

[37] Optoelektronika - to dział elektroniki, którego przedmiotem jest łączne wykorzystanie optycznego jak i elektrycznego sposobu przetwarzania i przekazywania sygnałów. Podstawą optoelektroniki są fizyczne procesy warunkujące przetwarzanie sygnałów elektrycznych na optyczne i sygnałów optycznych na elektryczne oraz procesy wytwarzania, przesyłania, przetwarzania i magazynowania informacji niesionych przez światło.

wany jest też termowizorem). Z drugiej strony aparatura termowizyjna jest odmianą telewizji wrażliwej na fragment zakresu promieniowania podczerwonego. Tworzenie obrazu polega na rejestracji przez kamerę promieniowania emitowanego przez obserwowany obiekt, a następnie przetworzeniu na kolorową mapę temperatur. System termowizyjny jest więc rodzajem „niezwykłego" termometru, który pozwala mierzyć temperaturę na odległość, w wielu miejscach jednocześnie. Innymi słowy, termowizja to badanie śladu cieplnego. Dzięki niemu ustala się obecność osób żywych w danym miejscu, bądź też zwłok (np. zakopanych), a także urządzeń z silnikami spalinowymi, broni palnej itp. Temperatura takich obiektów jest z reguły wyższa od temperatury środowiska, w jakim przebywają.

Badania termowizyjne pozwalają w sposób nieinwazyjny sprawdzić poprawność wykonania prac izolacyjnych na budynku, poszukiwać wad technologicznych błędów w ociepleniu, zawilgoceń, filtracji powietrza, wycieków i nieszczelności, zwiększonej rezystancji dla rozdzielni wszystkich napięć, transformatorów, szafek elektrycznych, uszkodzonych bezpieczników, linii wysokiego napięcia i wszelkich złączy elektrycznych, złego stanu izolacji cieplnej, przewodów doprowadzających gazy itp.

Noktowizja sprowadza się do zastosowań techniki optoelektronicznej umożliwiającej widzenie w widmie promieniowania o długości 0,76–1000μm. Zakres ten podzielono na podczerwień: bliską (0,76–1μm), średnią (1,5–5,6μm) i daleką (5,6–1000μm). Obserwacja różnych obiektów w podczerwieni może być realizowana przez wykorzystywanie promieniowania własnego (wszystkie ciała, których temperatura jest wyższa od zera bezwzględnego, wysyłają własne niekoherentne promieniowanie podczerwone) lub odbitego. W związku z tym przyrządy noktowizyjne dzieli się na:

- Pasywne (bierne) – detektor rejestruje promieniowanie podczerwone wysyłane przez przedmioty. Jeśli nie są one oświetlone przez inne źródła podczerwieni, to ich promieniowanie zależy od ich temperatury. Zasada ta umożliwiła zbudowanie termowizora, który pozwala widzieć w ciemności obiekty cieplejsze od otoczenia. Na tej zasadzie działa pirometr służący do zdalnego pomiaru temperatury.
- Aktywne (czynne) – polegające na emisji podczerwieni i kierowaniu jej na obserwowany obiekt oraz obserwacji zwróconego sygnału. Najpopularniejszym źró-

dłem podczerwieni są ciała rozgrzane, fotodioda LED, ale czasami wykorzystuje się też półprzewodnikowe lasery podczerwone.

Laser[38] – nazwa została utworzona jako akronim od *Light Amplification by Stimulated Emission of Radiation*. Jego istota funkcjonalna sprowadza się do wzmacnianie światła, poprzez wymuszoną emisję promieniowania. Jest to generator światła, wykorzystujący zjawisko emisji wymuszonej. Otrzymywane światło ma charakterystyczne właściwości, trudne lub wręcz niemożliwe do osiągnięcia w innych typach źródeł światła, mianowicie – bardzo małą szerokość linii emisyjnej – co jest równoważne bardzo dużej mocy w wybranym obszarze widma, spolaryzowane wiązki światła, spójność wiązki w czasie i przestrzeni, monochromatyczność, bardzo małą rozbieżność. W laserach impulsowych można uzyskać bardzo dużą moc w impulsie oraz szybkie narastanie impulsu. Specjalne lasery gazowe, wytwarzające ultrafiolet o możliwie jak najmniejszej długości fali, używane są do produkcji półprzewodnikowych układów scalonych, w stomatologii i dermatologii, a w tym do usuwania tatuaży, znamion oraz włosów. Natomiast półprzewodnikowe diody laserowe małej mocy są używane we wskaźnikach laserowych, drukarkach laserowych, a dużej mocy – wykorzystuje się w przemyśle do cięcia i spawania (o mocach do 10 kW). Lasery znalazły zastosowanie w nowoczesnej poligrafii do naświetlarkach filmów poligraficznych, offsetowych form drukowych, w cyfrowych kserokopiarkach itp. Lasery znalazły również zastosowanie przy znakowaniu produktów. Używa się ich przy liniach produkcyjnych posiadających bardzo wysokie wydajności, a także gdy chcemy uzyskać ładny i estetyczny nadruk. Nadruki można wykonywać na: etykietach produktów poprzez usuwanie warstwy farby, butelkach PET poprzez trwałe naniesienie znaków oraz elementach metalowych i innych.

W wojskach stawia się obecnie na broń laserową. Dokonano już przechwycenia i zestrzelenia laserem pocisku lecącego z prędkością naddźwiękową[39]. Konstruowana jest bardzo kosztowna broń laserowa, w której laser ma być zainstalowany na samolocie. Ma on być zdolny do niszczenia rakiet balistycznych we wczesnej fazie lotu, w każdym miejscu potencjalnego konfliktu na Ziemi. Systemy naprowadzania broni oparte są m.in. na elektrooptycę, ultrafiolecie, podczerwień i podczerwieni. Opracowano specjalny laser, który może być antyterrorystyczną bronią obronną w

[38] Encyklopedia Wikipedia, http://pl.wikipedia.org/wiki/Laser
[39] http://www.technologialaserowa.republika.pl/aktualnosci.html

zastosowaniach cywilnych i militarnych[40]. Niewielki laser błyskawicznie wykrywa ładunki wybuchowe, zagrożenie skażeniem chemicznym i ostrzega przed ewentualną groźbą katastrofy. Jest to kwantowy laser kaskadowy, który może pracować w trybie ciągłym w temperaturze pokojowej, emitując fale o długości głębokiej podczerwieni (9.5 mikrona i światło o mocy około 100mW). Każda substancja chemiczna ma specyficzną, niepowtarzalną własność pochłaniania światła o określonej częstotliwości, a większość chemikaliów mogących mieć zastosowanie jako niszczycielska broń „operuje" w przedziale długości fal od 8 do 12 mikronów.

Rozpoznanie czujnikowe (sensoryczne) jest również jednym z nowszych rodzajów rozpoznania elektronicznego. Ma na celu zdobywanie i przetwarzanie danych o przeciwniku, których nośnikami są fale sprężyste, tj. zakresu promieniowania innego niż radiowe (np. infradźwięki[41], ultradźwięki[42]) oraz wszelkiego rodzaju uboczne efekty i zjawiska towarzyszące działaniom bojowym, na przykład: akustyczne, termiczne, sejsmiczne, naciskowe, magnetyczne, fizyczne, chemiczne, zapachu itp. Do postrzegania tego rodzaju zmian środowiska wykorzystuje całą rodzinę urządzeń czujnikowych z szerokim zastosowaniem elektronicznej przemiany rejestrowanych efektów.

W zakresie fal sprężystych jest stosowane rozpoznanie akustyczne (z zakresem infradźwięków i ultradźwięków) oraz rozpoznanie sejsmiczne. Innym rodzajem rozpoznania czujnikowego (sensorycznego) jest rejestracja efektów zmian pola magnetycznego Ziemi oraz zjawisk chemicznych. Informacje o przeciwniku i środowisku pola walki, uzyskiwane z rozpoznania czujnikowego, mogą dotyczyć:

- nadzorowania aktywności przeciwnika w wybranych rejonach zainteresowania;
- natężenia ruchu wzdłuż wybranych tras,
- nadzorowania planowanych rejonów zrzutu desantów taktycznych,
- rejestracji zmian w obrębie stanowisk i punktów dowodzenia,
- rejonów ogniowych artylerii i stanowisk startowych rakiet.

Nowe generacje czujników (sensorów) są miniaturyzowane gabarytowo i wagowo. Mogą być zrzucane przez bezzałogowe statki powietrzne i samoloty. Należy

[40] http://oemagazine.com, 2005-08-23.

[41] Infradźwięki - fale sprężyste o częstotliwościach mniejszych niż 16 Hz, w więc leżące poniżej zakresu ludzkiej słyszalności. Fale te są słabo tłumione i dlatego rozprzestrzeniają się na duże odległości od źródła. Mogą być wykorzystane do rejestracji efektów sejsmicznych oraz eksplozji na polu walki.

[42] Ultradźwięki - drgania i fale sprężyste o częstotliwościach większych iż 20 kHz, a więc leżące powyżej zakresu ludzkiej słyszalności. Mogą być wykorzystane do rejestracji efektów akustycznych (odgłosów) pola walki.

się liczyć, że przyszłe rozwiązania będą zawierały również wiele innych czujników (sensorów), jak: hydroakustyczne, podczerwieni, magnetyczne, termalne, laserowe, optyczne, chemiczne, biologiczne, spektro-radiometryczne, do pomiaru częstotliwości nośnej, promieniowania i rezonansu elektronicznego. Czujniki te będą mogły działać zarówno w dzień jak i w nocy oraz w szerokim zakresie warunków meteorologicznych.

Rozpoznanie czujnikowe (sensoryczne) może być perspektywicznym rodzajem rozpoznania na szczeblu taktycznym, bowiem umożliwia pozyskiwanie danych z rejonów niedostępnych innym rodzajom rozpoznania w czasie zbliżonym do rzeczywistego.

Rozpoznanie informatyczne jest perspektywicznym rodzajem rozpoznania elektronicznego, z uwagi na masowy rozwój sieci informatycznych o zasięgu globalnym i lokalnym. Może być prowadzone na wszystkich szczeblach dowodzenia. Sieci informatyczne mogą być bogatymi źródłami danych o siłach i środkach potencjalnego przeciwnika. Podobnie jak w rozpoznaniu elektronicznym można prowadzić rozpoznanie w sieciach informatycznych wykorzystując omówione już wcześniej sposoby: poszukiwania, przechwytywania, śledzenia, namierzania i analizy techniczno-operacyjnej[43]. Poszukiwanie danych, np. w globalnej sieci jaką jest Internet, może polegać na posługiwaniu się różnego rodzaju wyszukiwarkami. Kolejnym sposobem pozyskiwania danych może być śledzenie. W tym wypadku śledzenie może być rozumiane jako analiza przepływu danych w sieciach i wyłapywanie tych niebezpiecznych programów, które zagrażają bezpieczeństwu danych lub awarii systemu komputerowego. Śledzenie może być wykorzystywane także do analizy dróg przepływu danych do potencjalnego przeciwnika. Ściśle z tym związany jest sposób namierzania intruza. Pozyskuje się w sieci dane dotyczące potencjalnych włamywaczy i wykorzystywanych przez nich metod włamań i dróg ucieczki. Efektem analizy tych danych staje się zidentyfikowanie włamywacza. Jest to kolejny sposób pozyskiwania danych nazywany często w rozpoznaniu analizą operacyjno-techniczną przechwyconych sygnałów.

Oprócz sieci globalnej nie mniej istotnymi są sieci o ograniczonym zasięgu (w tym sieci wojskowe), które również mogą być intensywnie inwigilowane. Systemy komputerowe mogą być atakowane od wewnątrz i z zewnętrz. W ataku zewnętrz-

[43] Scheffs W., *Rozpoznanie informatyczne nową płaszczyzną prowadzenia walki elektronicznej*, XI Konferencja naukowa - Automatyzacja dowodzenia, 2003,

nym, wykonanym spoza sieci przez osobę nieuprawnioną do korzystania z zasobów danej sieci, najczęściej są stosowane takie metody jak:

- podsłuch,
- analiza „ruchu" użytkowników systemów,
- przechwytywanie emisji ujawniających,
- udawanie uprawnionych użytkowników systemu,
- omijanie mechanizmów uprawnień,
- sterowanie dostępem.

Ataki wewnętrzne występują głównie ze strony legalnych użytkowników systemu i polegają głównie na omijaniu mechanizmów uprawnień.

Wykonanie skutecznego ataku na systemy komputerowe pozbawione ochrony kryptograficznej jest łatwe, ze względu na zwykle standardowy sprzęt wykorzystywany do ih budowy oraz standardowe procedury wymiany informacji między obiektami systemu. Eliminowanie skutków udanego ataku wymaga natomiast specjalnych działań – zwykle dość kosztownego.

Przed rozpoczęciem ataku na określony system komputerowy wykonawca musi najpierw zdobyć o nim niezbędne dane. Związane z tym działania poprzedzające zwykle obejmują:

- analizę „ruchu" informatycznego,
- analizę przesyłanych pakietów,
- analizę emisji ujawniających (sygnałów elektromagnetycznych przenikających do otoczenia z przewodów i konstrukcji metalowych, możliwych do przechwytywania).

Dopiero po ustaleniu zasad pracy systemu i jego użytkowników następuje właściwym atak. Przykładowym sposobem pozyskiwania danych z komputerów sterowanych podczerwienią, jest przechwyt danych wysyłanych i odbieranych przez wiązkę podczerwieni. Tego typu przechwytywanie może być realizowane z niewielkich odległości. Podobny sposób pozyskiwania danych może być realizowany w sytuacji przekazu sygnałów droga radiową, nazywany zwcajowo „bluetooth'em". Po uzyskaniu dostępu do systemu komputerowego istnieje możliwość różnorodnego oddziaływania na system, w szczególności polega to na stosowaniu:

- powtórzeń – ponownym nadawaniu informacji, komunikatów lub ich części, w celu wytworzenia efektu, że stacja ta posiada większe uprawnienia niż rzeczywiste,

- modyfikacji – polegających na niedostrzegalnej zmianie treści semantycznych transmitowanych danych,
- „maskarady" – stwarzanie pozorów innego komputera niż rzeczywisty (jest często stosowana w połączeniu z innym formami ataku, a szczególnie z powtórzeniami i modyfikacjami komunikatów.

  Celem „maskarady" dokonywanej z zewnątrz może być:
  - zdobywanie chronionej informacji i zdezorganizowanie pracy systemu,
  - zwiększanie swoich uprawnień,
  - tworzenie fałszywych źródeł informacji,
  - tworzenie fałszywych „upływności" informacji,
  - symulowanie pokwitowań wiadomości,
  - wprowadzanie do systemu fałszywych informacji,
  - przenoszenie kosztów swojej działalności w sieci na innego użytkownika.
- „wjazdu na barana" – polega na wprowadzeniu do kanału transmisyjnego własnych danych, w czasie trwania transmisji między uprawnionymi użytkownikami,
- odmowy usługi – komputer nie wypełnia przewidzianych dla niego funkcji lub działa w sposób uniemożliwiający poprawną pracę innego komputera (likwiduje komunikaty kierowane do adresata, generuje sztuczny ruch),
- „potrzasku" – sprowadzającego się do zmiany oprogramowania, które umożliwia atakującemu wytworzenie. na odpowiedni sygnał, szkodliwych dla użytkownika efektów i sekwencji zdarzeń (powodują to różnego rodzaju wirusy komputerowe i konie trojańskie, które mogą już być instalowane podczas: produkcji urządzeń, instalowania i w czasie pracy komputera).

Bardzo bogatym i niezmiernie wartościowym źródłem danych rozpoznawczych jest samo promieniowanie niezabezpieczonego komputera. Emisja ujawniająca jest wykrywana w procesach przetwarzania i przesyłania informacji niejawnej. W urządzeniu takim jak komputer, promieniują prawie wszystkie elementy, z których się składa (procesor, dysk twardy, stacja dyskietek, klawiatura, monitor). Złe obudowy, odkryte łącza krawędziowe komputerów i urządzeń peryferyjnych (np. drukarek), mogą być „antenami" emitującymi, w czasie przetwarzania danych, promieniowanie elektromagnetyczne. Promieniowanie to może mieć zróżnicowany zasięg i w zależności od zastosowanych elementów rozchodzi się w promieniu 50.- 1500 m. Istnieją udokumentowane przypadki przechwytywania przez specjalne urządzenia, oddalone

nawet o kilkaset metrów, informacji wyświetlanych na monitorze lub przekazywanych łączami telefonicznymi[44].

Rozpoznanie systemów radionawigacyjnych polega na wykrywaniu i identyfikacji systemów i środków radionawigacyjnych. System radionawigacyjny to zespół współpracujących ze sobą urządzeń rozmieszczonych na ziemi i na obiektach ruchomych (samoloty, okręty, sztuczne satelity Ziemi), przeznaczonych do prowadzenia ruchomych obiektów po wyznaczonych trasach, naprowadzania ich na określone punkty terenowe oraz do kontroli położenia, dowiązywania stanowisk i obiektów itp. Systemy radionawigacyjne można klasyfikować między innymi ze względu na: zasięg, dokładność i miejsce lokalizacji, zakresy wykorzystywanych pasm częstotliwości oraz parametry sygnałów.

Ze względu na zasięg, naziemne systemy radionawigacyjne dzielą się na:

- bliskiej nawigacji – obejmujące środki radiotechniczne rozmieszczone na lądzie, aparatach latających i okrętach, które mają promień działania ograniczony do kilkuset kilometrów (pracują w zakresie fal krótkich i ultrakrótkich, charakteryzują się stosunkowo dużą dokładnością),
- dalekiej nawigacji – obejmujące środki radiotechniczne rozmieszczone na lądzie, aparatach latających i okrętach, które mają promień oddziaływania rzędu kilku tysięcy kilometrów (pracują w zakresie fal średnich, długich i bardzo długich i są mniej precyzyjne od bliskiej nawigacji).

Ogólnie systemy radionawigacyjne dzielą się na:

- autonomiczne – w których środki radioelektroniczne umieszczone są tylko wewnątrz poruszających się obiektów i umożliwiają określanie położenia niezależnie od urządzeń zewnętrznych (zaliczane są do nich radiowysokościomierze i dopplerowskie stacje radiolokacyjne),
- nieautonomiczne – które wykorzystują urządzenia odbiorcze lub odbiorczo-zapytujące współpracujące z naziemnymi lub satelitarnymi źródłami sygnałów nawigacyjnych.

[44] W trakcie międzynarodowego zjazdu hackerów w Almere (Holandia), w którym uczestniczyło ponad 2000 osób, prof. E. Moeller z politechniki w Aachen pokazał, jak za pomocą zwykłego telewizora, prostej anteny oraz nieco zmodyfikowanego odbiornika, można bez trudu, z odległości kilkuset metrów, odczytywać dane wyświetlane na monitorze komputera. Odczyt z monitora nie nastręczał żadnych trudności nawet wtedy, kiedy obok siebie pracowało kilka komputerów. Do pokazu wykorzystywano zwykły analogowy, czarno - biały telewizor bez żadnych przeróbek. Przystawka do odbioru wykonana była z powszechnie dostępnych części, a koszt jej wykonania nie przekroczył 2000 DEM.

Wywiad elektroniczny jest ukierunkowywany głównie na pozyskiwanie informacji wojskowych i dyplomatycznych przesyłanych pomiędzy stolicami i misjami zagranicznymi. Działania te obejmują również monitorowanie handlu narkotykami, pranie brudnych pieniędzy, terroryzm oraz przestępczość zorganizowaną. Zbieranie danych przez wywiad elektroniczny jest możliwe wtedy, gdy zostanie uzyskany dostęp do interesujących kanałów i zostaną „złamane" kody dostępu. Informacje o środkach dostępu i metodach łamania kodów są najbardziej chronionymi informacjami w obrębie każdej organizacji wywiadu elektronicznego.

Rozpoznanie sygnałów radiowych krótkofalowych to kolejny rodzaj zagrożeń. Krótkofalowe sieci radiowe do 1960 roku stanowiły najpowszechniejszej wykorzystywane rozwiązania komunikacyjne w utrzymywaniu łączności międzynarodowej pomiędzy geograficznie oddalonymi krajami. Ważną cechą, z punku widzenia komunikacyjnego i rozpoznawczego jest to, że fale krótkie odbijają się od jonosfery i powierzchni Ziemi, zapewniając tym samym utrzymywanie łączności na odległościach tysięcy kilometrów i tym samym stwarzają podobne warunki do ich przechwytywania przez elementy rozpoznania radioelektronicznego.

Rozpoznawanie łączności mikrofalowej stanowi istotny element informacyjny. Wynika to z faktu, że technika mikrofalową zapewnienia łączność o dużej pojemności i jest wykorzystywna telefonii, telegrafii i telewizji. Łączność mikrofalowa wykorzystuje nadajniki małej mocy oraz anteny paraboliczne umieszczone wysoko na masztach. Anteny mają zwykle średnice o wielkości 1-3 metrów, umieszczane są w miejscach tzw. widoczności optycznej, czyli wymaga się, aby stacje nadawczo-odbiorcze znajdowały się co 30-50 km. Dalekosiężne łącza mikrofalowe wymagają wielu stacji retransmisyjnych i odbiorczych. Każda pośrednicząca stacja odbiorcza odbiera tylko małą część transmitowanego sygnału, jego większość przechodzi poza horyzont i trafia w przestrzeń kosmiczną, gdzie mogą go przechwycić krążące po orbicie satelity. Powyższe własności były już wykorzystane w latach 60-tych przez wywiady elektroniczne. Pierwsze satelity wywiadowcze rozmieszczano blisko orbit geostacjonarnych i były sterowane z punktów naziemnych. Efekty tego okazały się znacznie większe niż oczekiwano pierwotnie. W związku z tym ciągle są projektowane i stosowane co do tego nowe rozwiązania techniczne i organizacyjne. Jest ono procesem ciągłym, realizowanym bez względu na stan stosunków politycznych pomiędzy poszczególnymi państwami, a jego intensywność jest zawsze zależna od konkretnych potrzeb organizatora. Jest jednoczenie jednym z najważniejszych źródeł zdobywania

informacji wojskowych i polityczno-wojskowych o zasięgu globalnym, a jednocześnie stanowiącym obiektywne narzędzie weryfikacji polityki i bezpieczeństwa narodowego.

Do podstawowych środków rozpoznania strategicznego w przestrzeni kosmicznej zalicza się satelity rozpoznawcze, które charakteryzują się dużą autonomicznością funkcjonowania i znaczną odpornością na przeciwdziałanie. Satelity rozpoznawcze, niskoorbitowe mogą skupiać się na przechwycie określonych obiektów. Oprócz tych satelitów istnieją ponadto tzw. satelity quasi geostacjonarne, umieszczone są na orbicie 42 tysięcy km. W przeciwieństwie do satelitów geostacjonarnych mają rozrzut wysokości pomiędzy 39 tysięcy km do 42 tysięcy km i promienia pomiędzy 30 tysięcy km do 33 tysięcy km. Poruszają się po ciągłej eliptycznej orbicie, co umożliwia im pokrycie większej powierzchni Ziemi podczas dniowego kursu i lokalizowanie źródeł emisji radiowych. Przechwycone sygnały są transmitowane do stacji odbiorczej przez silnie kierunkowe środki łączności na tzw. połączeniu 24 godzinnym. Naziemne stacje przechwytu[45] są obsługiwane i chronione głównie przez wojsko. W stacjach są wykorzystywane różne typy anten, każda w innym kształcie i z przeznaczeniem dla konkretnego zastosowania. Wysokie teleskopy w wielkośrednicowym kole (anteny Wullenweber) oraz okrągłe instalacje anten rombowych (antena Pusher) są używane do lokalizacji sygnałów radiowych. Anteny dookolne, wyglądające jak gigantyczne anteny TV służą do przechwytu niekierowanych sygnałów radiowych. Do odbioru sygnałów satelitarnych używane są tylko anteny paraboliczne. Większość anten parabolicznych jest ukryta pod sferycznym płaszczem. Chroni on antenę, a także i kierunek jej pracy. Jeśli w miejscu przechwytywania jest jedna antena paraboliczna to można być pewnym, że przechwytuje ona sygnał z satelitów, chociaż nie wiadomo jakie są to sygnały. Anteny odbiorcze na terenie stacji przechwytywania, mogą być używane do:

- łączności wojskowej,
- celów wywiadowczych,
- przechwytywania.

O przeznaczeniu anten może mówić jedynie ich średnica. Względy techniczne decydują o minimalnej średnicy dla anten odbiorczych. Pierwsze generacje satelitów wy-

[45] Campbell Duncan - IPTV Ltd.- Edinburgh, Part 2/5:The state of the art in communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband ulti-language leased or common carrier systems, and its applicability to COMINT targetting and selection, including speech recognition, STOA Programme, European Parliament, EP/IV/B/STOA/98/1401.

magały anten o średnicy 25-30 m, dzisiaj wystarczy 15-20 m. Jakość odbieranego sygnału poprawia komputerowe filtrowanie, dla celów wywiadowczych wybierane są jednak anteny największe, ze względu na dążenia związane ze zwiększaniem czułości przechwytu.

Satelity rozpoznania telekomunikacyjnego wykorzystują zjawisko polegające na tym, że, mikrofalowe sygnały radiowe wypromieniowane z powierzchni Ziemi, nie są odbijane od jonosfery tylko przechodzą bezpośrednio w przestrzeń kosmiczną. Właściwość ta jest wykorzystywana zarówno do zapewnienia łączności globalnej jak i do przechwytu tej łączności, zarówno w przestrzeni kosmicznej jak i na lądzie. Największa konstelacja satelitów telekomunikacyjnych jest nadzorowana przez międzynarodową organizację satelitów telekomunikacyjnych „Intelsat". Dla zapewniania permanentnej łączności punkt - punkt lub dla celów rozsiewczych, satelity umieszczone są na orbitach geostacjonarnych, dla obserwatorów z Ziemi znajdują się one na tej samej pozycji na niebie.

W okresie od 1967 do 1985 roku została stworzyła drugą, nowocześniejsza klasa satelitów wywiadowczych, dostosowanych do sterowania z punktów naziemnych. Wykorzystywały one duże anteny paraboliczne rozmieszczane w przestrzeni kosmicznej. Przechwytywał sygnały w pasmach UKF i mikrofalowym. Trzecią klasę satelitów rozmieszczono na wysoko położonych orbitach eliptycznych, w pobliżu biegunów, gdzie możliwe było ich „zawieszanie" na długi okres czasu, nad wysoko położonymi północnymi równoleżnikami. Umożliwiało to odbieranie sygnałów z: nadajników rozmieszczonych na północnych równoleżnikach, słabo monitorowanych przez oraz sygnałów przesyłanych do satelitów komunikacyjnych na tych samych orbitach.

Rozpoznawanie kabli podwodnych i podziemnych to kolejne zagrożenie informacyjne. Wynika to z faktu, że niezawodne systemy łączności międzynarodowej, o dużej pojemności, realizowane są poprzez podwodne i podziemne kable telefoniczne. Pierwsze systemy umożliwiały łączenie do kilkuset jednocześnie aktywnych kanałów telefonicznych, najnowsze systemy światłowodowe przesyłają do 5 Gb/s sygnału cyfrowego. Odpowiada to w przybliżeniu około 60.000 jednoczesnych rozmów telefonicznych. W tym celu są wykorzystywane zminiaturyzowane, indukcyjne urządzenia podsłuchowe. Nie mogą być natomiast podsłuchiwane tą techniką kable światłowodowe, ponieważ nie promieniują sygnałów o częstotliwości radiowej, co uniemożliwia wykorzystanie właściwości fizycznych pętli indukcyjnych. Badania dotyczące możliwości podsłuchu kabli światłowodowych, pochłonęły dużo funduszy, jednak

do tej pory osiągnięto bardzo mizerne rezultaty. Dalekosiężne kable światłowodowe są teoretycznie podatne na podsłuch, ale dostęp do nich jest możliwy tylko poprzez manipulowanie optoelektronicznymi wzmacniakami, które wzmacniając sygnał umożliwiają przesyłanie go na duże odległości. Wynika z tego, że dowolny podmorski system kablowy wykorzystujący zatapiane wzmacniaki optoelektroniczne jest podatny na przechwyt informacji.

Wywiad elektroniczny wymaga obecnie bardziej skomplikowanych środków technicznych do zbierania danych, a ich przetwarzanie może być w przyszłości jeszcze bardziej kosztowne i bardziej ograniczone niż obecnie. W okresie od 1950 roku do wczesnych lat 80-tych, wielokanałowe systemy analogowe, o dużej pojemności, były eksploatowane poprzez pracę w oddzielnych kanałach telekomunikacyjnych, na różnych częstotliwościach. Sygnał złożony, który mógł zawierać do 2000 i więcej kanałów rozmownych, był „multipleksem" (sygnał z podziałem częstotliwościowym FDM był przenoszony na wiele wyższe częstotliwości – na przykład w pasmo mikrofalowe. Tym samym metody analogowe zostały przekształcone w prawie uniwersalnie systemy cyfrowe. Podstawowym stał się wielokanałowy przekaz cyfrow z podziałem czasowym TDM. W systemie telefonicznym, z podziałałem czasowym, przekształcono w postać cyfrową indywidualne kanały rozmowne, dostosowane do sekwencyjnego przekazywania w szczelinach czasowych pętli TDM. Fakt ten wymaga ttworzenia określonych standardów dotyczących łączności cyfrowej. Najnowsze systemy cyfrowe wykorzystują kable światłowodowe o bardzo dużej pojemności, które przenoszą zsynchronizowane sygnały. Zsynchronizowanie sygnałów pozwala na to, że pojedyncze sygnały mogą być łatwo wydzielone z łączy o dużej pojemności. Do 1970 roku większość systemów telekomunikacyjnych wykorzystywało metody analogowe. Od 1990 roku prawie wszystkie łącza są cyfrowe i zapewniają większą pojemność. Systemy o największej pojemności wykorzystywane są przez Internet i działają przy szybkości transmisyjnej 155 Mb/s (ekwiwalent przesyłania 3 milionów słów na sekundę, czyli objętość prawie tysiąca książek na minutę). Dynamiczny wzrost znaczenia Internetu i związanych z nim form łączności cyfrowej wywołał dyskusje na temat wykorzystania go przez agencje wywiadu elektronicznego. We wczesnych latach dziewięćdziesiątych zostały opracowane szybkie i skomplikowane systemy wywiadu elektronicznego, które zbierają, filtrują i analizują formy szybkiej łączności cyfrowej wykorzystywanej przez Internet. Standardowe informacje internetowe są składane w pakiety zwan „datagramami". Datagramy zawierają liczby reprezentujące zarówno

ich źródło jak i ich przeznaczenie i są nazywane „adresem IP". Adresy są charakterystyczne dla każdego komputera podłączonego do Internetu. Są one łatwo identyfikowalne jeśli chodzi o kraj i miejsce pochodzenia oraz miejsce przeznaczenia. Ruch internetowy może być dostępny zarówno z międzynarodowych łączy telekomunikacyjnych wchodzących do do danego państwa, jak i z głównych miejsc wymiany internetowej. Obydwie metody posiadają swoje zalety. Dostęp do systemów łączności może zostać utajniony, natomiast dostęp do miejsc wymiany internetowej może być wykrywalny. Zaletą tej drugiej metody jest zapewnienie łatwiejszego dostępu do większej ilości danych i prostszych metod sortowania. Ilość danych jest ogromna.

Duża część ruchu internetowego posiada małe znaczenie wywiadowcze lub może być obrabiana w inny sposób. Na przykład wiadomości z grup dyskusyjnych są rozsyłane do każdego odbiorcy, który tylko chce je uzyskać. Agencje wywiadowcze posiadają dostęp do nich i baz danych zawierających wiadomości z poprzednich dni. Bezcelowe jest ich zbieranie w sposób utajniony. Podobnie sprawa się ma ze stronami World Wide Web (www), z których większość jest dostępna w sposób otwarty. Strony www są badane ciągle poprzez „przeszukiwarki", które generują katalogi ich zawartości. W tym zakresie są również wykorzystywane roboty do zbierania danych będących w obszarze zainteresowania.

Ruch internetowy pochodzący zza zagranicy, a znajdujący się w wywiadowczym zainteresowaniu, składający się z: poczty elektronicznej, transferu plików, prywatnych sieci wirtualnych działających na bazie Internetu oraz innych informacji, stanowi najwyżej kilka procent ruchu w miejscach wymiany internetowej i łączach głównych (backbone). Ocenia się, że ważniejsze agencje nagrywają codziennie około 500 milionów godzin rozmów we wszystkich językach świata i z coraz większym trudem „przekopują" się przez stale rosnącą górę informacji. Świat wysyła około 36 miliardów e-maili dziennie i liczba ta podwajać co dwa lata[46].

Stosowanie silnych i efektywnych systemów kryptograficznych znacznie ograniczy możliwości agencji wywiadu elektronicznego w przetwarzaniu zebranych informacji. „Prawo Moora" mówi, że koszt mocy obliczeniowej zmniejsza się o połowę co 18 miesięcy. Ma to wpływ zarówno na pracę agencji jak i ich celów. Tanie komputery osobiste mogą skutecznie wykonywać obliczenia matematyczne niezbędne do efek-

[46] Rybarczyk M., *Ślepe ucho Pentagonu*, Przekrój z 29.12.2005 r.

tywnej kryptografii. Przy braku nowych odkryć w dziedzinie matematyki i fizyki prawo Moora faworyzuje kryptografów a nie kryptologów.

Od połowy lat 90-tych agencje wywiadu elektronicznego spotkały się ze znacznymi trudnościami w utrzymywaniu globalnego dostępu do systemów telekomunikacyjnych. Te trudności będą się jeszcze powiększać. Zasadniczym powodem staje się przechodzenie na światłowodowe sieci telekomunikacyjne o dużej pojemności. Pozyskiwanie informacji wymaga fizycznego dostępu do kabla, co w przypadku przechodzenia sieci światłowodowych przez państwa nie współpracujące, może być dokonywane jedynie poprzez manipulacje przy wzmacniakach optoelektronicznych (gdy są zainstalowane). Rozmiar niezbędnego wyposażenia potrzebnego do przesyłania przechwyconego ruchu telekomunikacyjnego, wraz z zasilaniem, łączami oraz systemami rejestrującymi powoduje, że skryta działalność jest ryzykowna i niepraktyczna.

Ocenia się, że organizacje wywiadu elektronicznego w ostatnich 15 latach straciły dominację w technologii komputerowej i informacyjnej. Ich główne systemy komputerowe równają się lub nawet są gorsze w stosunku do tych, które wykorzystują organizacje przemysłowe czy akademickie. Posiadają jedynie lepsze zabezpieczenia chroniące przed promieniowaniem sygnałów radiowych, które mogą być poddawane analizie. Podobnie sprawa wygląda z cywilną i komercyjną kryptografią. Społeczność akademicka i przemysłowa jest wysoce wykwalifikowana w kryptografii i kryptologii. Próby ograniczania kryptografii opóźniły wprowadzenie efektywnych kryptograficznych systemów bezpieczeństwa. Przyjmuje się, że przyszłe trendy w dziedzinie wywiadu elektronicznego będą prawdopodobnie ukierunkowywane na:

- ograniczanie inwestycji dotyczących zbierania informacji z przestrzeni,
- większego, niż w przeszłości, wykorzystania agentów do zakładania urządzeń podsłuchowych i pozyskiwania kodów,
- intensyfikowaniu ataków, na zagraniczne systemy komputerowe, za pomocą Internetu,
- stosowanie innych środków umożliwiających w szczególności uzyskanie dostępu do chronionych plików lub informacji przed tym jak zostaną zaszyfrowane.

Rozpoznanie szerokopasmowe i analiza sygnałowa jest stosowane tam, gdzie dostęp do sygnałów jest utrudniony. W tym celu są specjalnie konstruowane pojedyncze urządzenia lub zestawy tych urządzeń.

Jednym z podstawowych urządzeń jest system przetwarzania komputerowego, o wielkości walizki. W rzeczywistości jest to zminiaturyzowana wersja komputera „słownikowego", umożliwiająca selekcję łączności niefonicznej z szerokiego zakresu sygnałów wejściowych, zgodnie z wcześniej ustalonymi kryteriami wyboru. Sygnały szerokopasmowe są zwykle przechwytywane z satelitów lub kabli w formie sygnałów zwielokrotnionych na wysokich częstotliwościach. Pierwszym krokiem w przetwarzaniu takich sygnałów, dla celów wywiadu elektronicznego, jest „wydzielanie szerokopasmowe", polegające na badaniu i analizie nowo pozyskanych systemów. Stosuje są przy tym:

- odzewowy sprzęt badawczy, który identyfikuje i klasyfikuje łącza satelitarne,
- demodulatory,
- dekodery,
- demultipleksery,
- mikrofalowe analizatory łączy radiowych,
- urządzenia badawcze łączy,
- systemy analizy nośnej i wiele innych typów oprzyrządowania i oprogramowania.

Nowo pozyskiwane łącza satelitarne lub łącza danych mogą być analizowane z wykorzystaniem. Po przeanalizowaniu podstawowej struktury telekomunikacyjnej, „szerokopasmowy analizator migawkowy" może rejestrować, próbkując dane nawet z systemów o największej przepustowości, co jest wystarczające do szczegółowej analizy łączności. Na początku 1999 roku systemy te umożliwiały odczyt, rejestrację oraz analizę sygnałów do 2,488 Gb/s. Jest to działanie 16 razy szybsze niż w głównych łączach internetowych; większa niż przepustowość telefoniczna dowolnego, współczesnego satelity telekomunikacyjnego; jest to ekwiwalent do 40 tysięcy jednoczesnych rozmów telefonicznych. Może on być wyposażany jeszcze w 40 gigabajtową pamięć, 500 do 1000 razy większą niż stosowaną w standardowych komputerach osobistych, umożliwiając relatywnie długie rejestrowanie łączy danych o dużej szybkości transmisyjnej (2,5 gigabajtowa przepustowość pojedynczego urządzenia przekracza maksymalną bieżącą szybkość transmisji danych w typowej wymianie internetowej). Konstruowane urządzenia posiadają dużą gamę rejestratorów, demulitiplekserów, skanerów i procesorów, dostosowanych do szybkości transmisyjnych rzędu 160 Mb/s. Sygnały mogą być rejestrowane na taśmach szybkich magnetofonów lub na twardych dyskach o dużej pojemności. Przechwytywane sygnały optyczne mogą

być badane przy wykorzystaniu stosownych co do tego analizatorów. Po przeanalizowaniu łącz telekomunikacyjnych następuje przetwarzanie wielokanałowe podczas którego pobiera się i filtruje informacje z żądanych kanałów. W tym zakresie istnieją trzy obszary zainteresowania:

- telefonią zwykłą,
- łączami faksowymi,
- łączami danych.

Są w tych zakresach wykorzystywane wielokanałowe procesory, które rozdzielają informacje foniczne, faksowe i dane na różne „strumienie", w celu ich dalszego przetwarzania i analizy. Wielokanałowy procesor, wykorzystywany w różnych konfiguracjach, może obrabiać jednocześnie 1000 kanałów głosowych oraz automatycznie przetwarzać ruch faksowy, foniczny i danych. „Foniczny demultiplekser kanałowy" może skanować do ponad 56 tysięcy kanałów telekomunikacyjnych, wydzielając ponad 3 tysiące kanałów fonicznych będących w zainteresowaniu. Procesor zapewnia również oprzyrządowanie elektroniczne do przechwytywania sygnałów satelitarnych o niskiej przepustowości wykorzystywanych przez mniejsze instytucje i użytkowników indywidualnych. Umożliwia on również „obróbkę" około 48 kanałów, stosując rozróżnianie pomiędzy fonią, transmisją faksową i danych. Po zidentyfikowaniu kanałów telekomunikacyjnych i wydzieleniu odpowiednich sygnałów, są one poddawane dalszej analizie z wykorzystaniem specjalnego oprogramowania w wyspecjalizowanych stacjach roboczych. Urządzenia te mogą być skrycie instalowane na komputerach typu laptop, które będą wyodrębniały standardowe dane wywiadowcze. Innym sposobem badającym szybką transmisję danych jest technika dostosowana do rejestracji transmisji z szybkością do 2,5 Gb/s. Może ona interpretować i analizować różne rodzaje systemów telekomunikacyjnych. Na przykład informacje faksowe są „Obrabiane" przez interaktywny układ analizy i szybkiego przetwarzania obrazów przechowywanych na dysku. Standardowe oprogramowanie dla komputerów „słownikowych" umożliwia optyczne rozpoznawanie znaków (optical character recognition). Pozwala na przetwarzanie maszynopisu na tekst odczytywany i możliwy do przetwarzania przez komputer. Efektywność tych systemów powoduje, że wywiad elektroniczny oparty na transmisji faksowej staje się ważnym podsystemem zbierania informacji. Jedyną jego wadą jest to, że nie istnieją systemy komputerowe, które mogą niezawodnie rozpoznawać pismo ręczne. Nie wiadomo jak zaprojektować taki system. Wynika z tego że, wiadomości faksowe pisane ręcznie mogą być bezpieczną formą

łączności, która może omijać kryteria nadzoru, zakładając, że informacja związana z sygnałem (numery abonenta wywołującego i wywoływanego) nie zostały rozpoznane jako będące w zakresie zainteresowania i nie zostały skierowane do faksowej stacji roboczej. Tworzone są również urządzenia dostosowane do identyfikacji systemów przywoławczych i wydobywania informacji, które automatycznie przechwytują i przetwarzają dane pochodzące z komercyjnych systemów przywoławczych. Są produkowane procesory, które umożliwiają nagrywanie i odtwarzanie sesji telekonferencyjnych. Są również tworzone systemy do podsłuchiwania sieci komórkowych. Parametry techniczne i dostępność takich systemów wskazuje na to jak wywiad elektroniczny stał się zindustrializowany i przenikający w różne obszary łączności.

Analiza ruchu telekomunikacyjnego jest metodą uzyskiwania informacji związanych z sygnałem. Usługa ta identyfikuje osobę inicjującą połączenie. Analiza ruchu może być wykorzystywana wszędzie tam, gdzie treść wiadomości nie jest dostępna, na przykład wtedy gdy zastosowano szyfrowanie. Z charakteru wywołań, można analizować i badać sieci powiązań personalnych. Jest to główna metoda analizy łączności fonicznej. Zautomatyzowane odczytywanie sprowadza się do rozpoznawania słów kluczowych jest fundamentalne dla komputerów słownikowych. Funkcja słownikowa jest bezpośrednia. Jej działanie jest podobne do przeszukiwarki internetowej. Różnice występują tylko w zawartości i w rozmiarze. Słowniki implementują zadania stacji macierzystej z całej masy zebranych informacji i pozwalają na ich automatyczną dystrybucję. Lawina spływających w ten sposób informacji do ośrodków analitycznych jest poddawana segregacji przez możliwie najsilniejsze komputery. Wyszukają one nie tylko słowa ze „słownika", ale również sprawdzają kontekst wypowiedzi i komputer steruje, która ze skanowanych rozmów bądź e-maili trafi do konkretnego analityka. W tym zakresie zostały stworzone zaawansowane systemy umożliwiające bardzo szybkie sortowanie dużej ilości przechwytywanych informacji. W drugiej połowie lat 80-tych, producenci satelitów, zaprojektowali i wyprodukowali mikrochip dostosowany do szybkie poszukiwania danych. Został on odtajniony w 1972 roku i stał się dostępny do szerokiego wykorzystania komercyjnego. Innym, o mniejszej przepustowości, jest procesor rozpoznawania wzorca. Występuje on w postaci karty do komputera i jest przystosowany do standardowego komputera PC. Może on analizować strumienie danych do 34 Mb/s, dopasowując każdy pojedynczy bit do ponad 1000 poddanych preselekcji wzorów.

Chociaż metody słownikowe i przeszukiwarki słów kluczowych mogą posiadać dużą moc, jednakże one i związane z nimi gigantyczne bazy danych mogą wkrótce stać się przestarzałe. Analiza tematyczna jest silniejszą techniką, i jedną z tych która jest rozwijana z myślą o przyszłych zastosowaniach. Analiza tematyczna umożliwia stawianie zadań typu: „znajdź mi dokumenty dotyczące tematu X". W standardowym teście oceny analizy tematycznej, jednym z zadań jest znalezienie informacji dotyczących słów zastępczych. Tradycyjne podejście wymaga natomiast dostarczenia do komputera wyrażeń kluczowych, Analiza tematyczna pokonuje ten problem i jest lepiej przystosowana do wywiadu osobowego. Główny nacisk badań nad analizą tematyczną jest skupiany na metodzie zwanej analizą N-gram. Analiza ta jest szybką, metodą sortowania i przeszukiwania tekstu czytanego maszynowo, według języka i tematu.. Aby wykorzystać analizę N-gram, operator ignoruje słowa kluczowe i definiuje zadanie poprzez dostarczenie do systemu wybranych dokumentów dotyczących tematu zainteresowania. System określa jaki jest temat z grupy dokumentów, a następnie przelicza prawdopodobieństwo tego, że inne dokumenty pokrywają ten sam temat. Ocenia się, że może on być wykorzystywany przy analizie bardzo dużych zbiorów danych (miliony dokumentów) i stosowany w dowolnym systemie komputerowym.

Systemy rozpoznawania mowy umożliwiają poszukiwanie i identyfikowanie rozmówców w kanałach telefonicznych i są klasyfikowane jako tajne.

2.2.2. Destrukcja transmisyjna (semantyki i relacji)

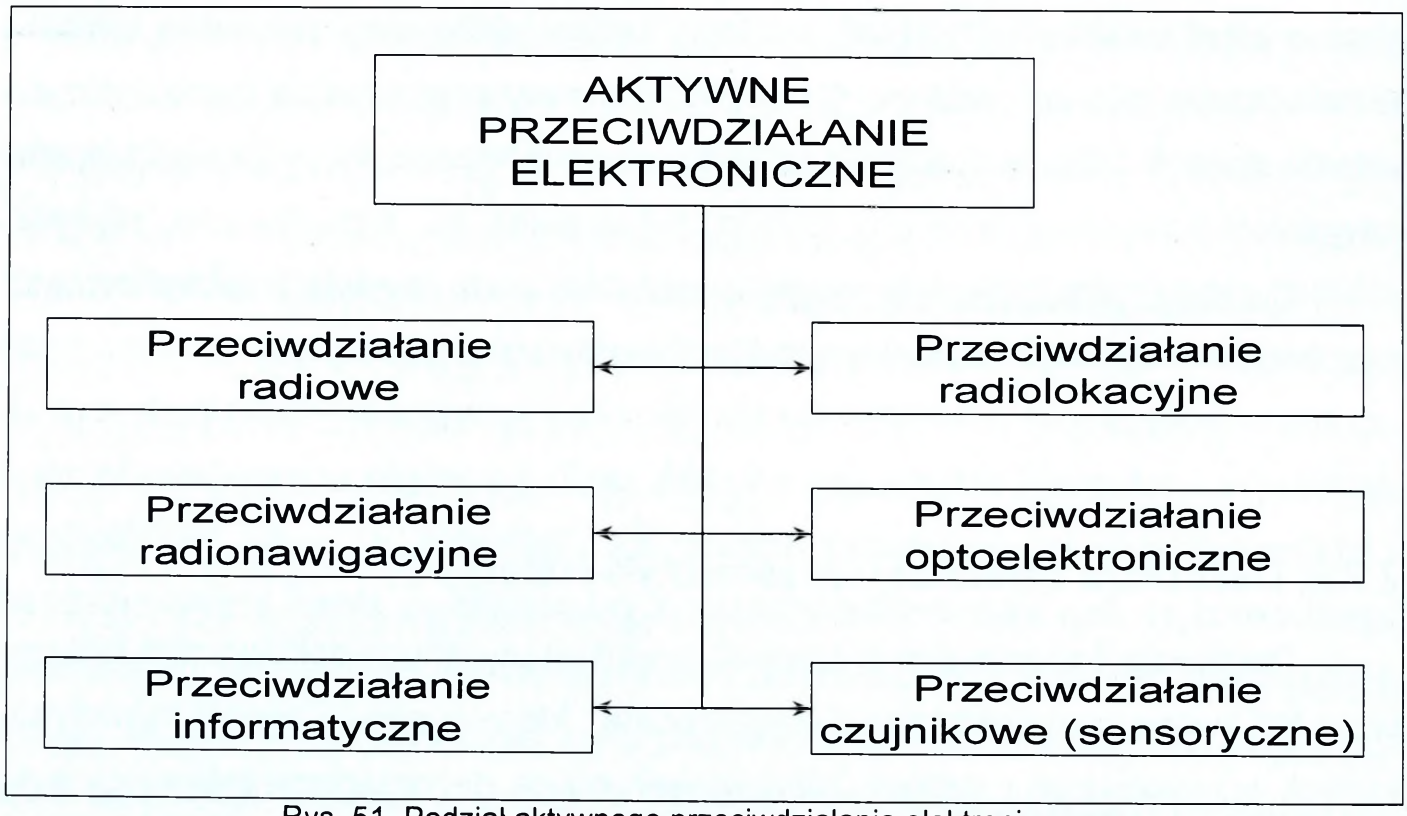
Destrukcja transmisyjną w sieciach teleinformatycznych dokonywana jest poprzez tak zwane „przeciwdziałanie elektroniczne". które obejmuje zespół skoordynowanych przedsięwzięć i działań ukierunkowanych na dezorganizowanie pracy systemów oraz urządzeń elektronicznych przeciwnika, funkcjonujących w środowisku elektromagnetycznym. W ramach tego, ze względu na formę wpływów, wyróżnia się:

- aktywne przeciwdziałanie elektroniczne,
- pasywne przeciwdziałanie elektroniczne.

Aktywne przeciwdziałanie elektroniczne polega na wypromieniowywaniu energii elektromagnetycznej, przez zakłócającej urządzenie nadawcze, ukierunkowanej na elektromagnetyczne nośniki informacji, stosowane w relacjach przeciwnika. W tym

celu mogą być wykorzystywane emisyjne urządzeń stacjonarnych i polowych oraz nadajniki jednorazowego użytku, odznaczające się różnorodnymi parametrami taktyczno-technicznymi, dostosowanymi do konkretnych środków i systemów elektronicznych, na które mają oddziaływać destrukcyjnie.

Aktywne przeciwdziałanie elektroniczne charakteryzuje się różnymi parametrami taktyczno-technicznymi, dostosowywanymi do destrukcji informacyjnych konkretnych środków i systemów elektronicznych przeciwnika. Zakłóceniami aktywnymi oddziałuje się, przede wszystkim, na urządzenia odbiorcze poszczególnych środków elektronicznych. Wytwarzane są na częstotliwościach roboczych, na których dokonywana jest transmisja danych i do których dokładnie dostrajane są nadajniki zakłócające. W skład aktywnych przeciwdziałań elektronicznych, ze względu na rodzaje środków, można wyróżniać: zakłócanie radiowe, zakłócanie radiolokacyjne, zakłócanie radionawigacyjne, zakłócanie optoelektroniczne, zakłócanie informatyczne i zakłócanie czujnikowe (sensoryczne) – rys. 51.



Rys. 51. Podział aktywnego przeciwdziałania elektronicznego

Źródło: Opracowanie autorskie

Pasywne przeciwdziałanie elektroniczne polega na wtórnym promieniowaniu (odpromieniowaniu, odbijaniu i rozpraszaniu) lub obniżeniu mocy energii elektromagnetycznej, w tym jej wchłanianiu przez środki nie będące jej generatorami, w sposób zamierzony, w celu zmylenia, odwrócenia uwagi lub oszukania przeciwnika i jego systemów elektronicznych. Przeciwdziałania pasywne dotyczą najczęściej środków radiolokacyjnych, środków pracujących w podczerwieni oraz urządzeń laserowych.

Wytwarzane są przez sztuczne zmiany właściwości elektromagnetycznych środowiska rozprzestrzeniania się fal elektromagnetycznch Ze względu na sposób oddziaływania na zakłócane urządzenia elektroniczne przeciwnika rozróżnia się przeciwdziałanie: maskujące i imitujące.

Przeciwdziałania maskujące utrudniają lub uniemożliwiają przeciwnikowi wykrywanie i „obróbkę" sygnałów użytecznych. Przy ich zastosowaniu urządzenia rozpoznania elektronicznego przeciwnika rejestrują niepełny i niezgodny z rzeczywistością obraz pracy środków elektronicznych, a prowadzona na jego podstawie analiza może prowadzić do wyciągania fałszywych wniosków. Dla uzyskania efektu zakłóceń maskujących wykorzystywane są:

- dymy metalizowane,
- ekrany maskujące,
- pokrycia przeciw radiacyjne,
- a także zjonizowane środowiska.

Zastosowanie środków wywołujących lokalną jonizację atmosfery powoduje, poprzez zmianę jej właściwości elektromagnetycznych, powstanie barier podobnych do ekranów przeciwradiacyjnych. W przypadku zastosowania tego rodzaju środków, należy wykluczyć możliwość wykorzystywania fal elektromagnetycznych do wszelkiego rodzaju pomiarów i przekazywania danych. Pasywne zakłócenia mogą być też wywołane przez naturalne czynniki, takie jak deszcz, śnieg, gęsta mgła itp.

Przeciwdziałania imitujące wprowadzają do zakłócanego systemu fałszywe dane. Za ich pomocą można wytworzyć na ekranie wskaźnika stacji radiolokacyjnej zobrazowanie w azymucie i odległości nieistniejących celów. Zakłócenia te dezorientują przeciwnika i utrudniają mu podjęcie właściwej decyzji. Imitujące zakłócenia pasywne wytwarzają:

- odbijacze kątowe[47],
- odbijacze dipolowe[48],

---

[47] *Odbijacze kątowe* dzięki zwiększonemu odbijaniu energii elektromagnetycznej są używane do pozorowania obiektów rzeczywistych w otaczającym je tle. Wielkość odbijanej energii zależy od kształtu i rozmiarów odbijaczy. Specjalna konstrukcja odbijaczy kątowych powoduje znaczne odbicia energii przy stosunkowo niewielkich wymiarach.

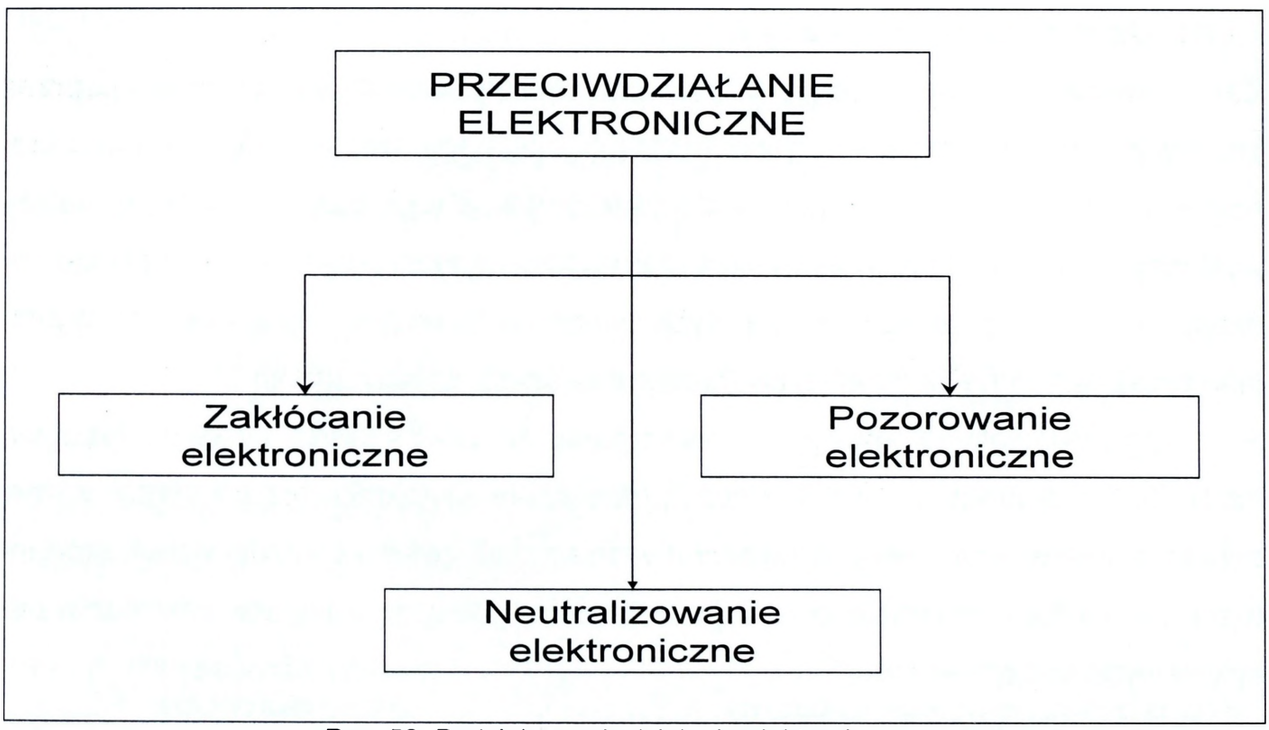
[48] *Odbijacze dipolowe,* to najczęściej metalizowane włókna szklane i poliamidowe, włókna węglowe lub metalizowana, odpowiednio cięta folia. Długość tych elementów z reguły odpowiada długości 1/2 λ. Środki dipolowe są przeznaczone do zakłócania stacji radiolokacyjnych, pozorowania obiektów i maskowania rzeczywistych obiektów. Dipole można wyrzucać w określonych odstępach czasowych, na dużych przestrzeniach. Sygnał odbity od chmury można obserwować na ekranie wskaźnika jako plamkę o dużej jaskrawości, plamka ta sugeruje istnienie określonego obiektu. Jeśli zostanie wyrzucona duża liczba środków dipolowych w określonym obszarze

- oraz wszelkiego rodzaju pułapki i fałszywe cele radiolokacyjne.

Największą efektywność przeciwdziałani elektronicznego osiąga się w następstwie zmasowanego, niespodziewanego i kompleksowo stosowanego różnego rodzaju oddziaływań elektronicznych w stosunku do najważniejszych środków i obiektów elektronicznych przeciwnika – szczególnie na głównych kierunkach i w decydujących etapach działań. Mając na uwadze potrzeby walki, należy wydzielać większość sił i środków przeciwdziałania elektronicznego na główny kierunek działania wojsk. Jest to niezbędne do wyeliminowania ważnych środków elektronicznych przeciwnika i stworzenia dogodnych warunków do działania wojsk własnych.

Przeciwdziałanie elektroniczne dzieli się na (rys. 52):

- zakłócanie elektroniczne,
- pozorowanie elektroniczne,
- neutralizowanie elektroniczną.



Rys. 52. Podział przeciwdziałania elektronicznego

Źródło: Opracowanie autorskie

Neutralizacja elektroniczna polega na celowym użyciu energii elektromagnetycznej o dużej gęstości[49], powodującym uszkodzenie lub zniszczenie podzespołów elektronicznych sprzętu bojowego, wykorzystywanego głównie w procesie dowodzenia i łączności, kierowania uzbrojeniem, nawigacji i rozpoznania. Klasyczne środki

na ekranie wskaźnika powstaje zobrazowanie w postaci jasnego pasma o znacznej długości (często także szerokości), to z kolei powoduje zakłócenia w pracy stacji oraz maskowanie obiektów będących w tym sektorze.

[49] Ta forma oddziaływania była dotychczas rozpatrywana jedynie w sytuacji użycia broni jądrowej, gdzie część energii wybuchu zamieniała się w impuls EM.

generacji silnych impulsów elektromagnetycznych , charakteryzują się wielkimi mocami promieniowania – nawet ponad tysiąc razy większymi niż generują klasyczne środki tego rodzaju. Impuls elektromagnetyczny powoduje krótkotrwałe wzbudzenie silnych napięć i prądów w aparaturze elektronicznej, powodując uszkodzenia (przegrzewanie) wrażliwych elementów tej aparatury – układów scalonych, cewek itp. Środki te mogą porazić aparaturę elektroniczną znajdującą się na znacznym obszarze, w tym także wykonaną w technologii „stealth". Można je wykorzystywać do niszczenia środków elektronicznych, szczególnie czułych na to zjawisko systemów termowizyjnych i czujników laserowych. Do środków fizycznego niszczenia, z użyciem energii o dużej gęstości, może być zaliczona także:

- broń częstotliwości radiowych,
- broń laserowa,
- broń cząstek elementarnych,
- a także urządzenia mikrofalowe i laserowe o określonej mocy.

Środki mikrofalowe i laserowe zalicza się do broni selektywnego działania, a zakres ich wykorzystania może się zwiększyć w miarę polepszenia parametrów taktyczno-technicznych.

Pozorowanie elektroniczne to kompleks przedsięwzięć organizacyjnych i technicznych mających na celu wprowadzanie w błąd urządzeń elektronicznych przeciwnika (głównie środków rozpoznania elektronicznego). Działania te mogą przyjąć formę aktywną lub pasywną. Polegają na sztucznym tworzeniu „obrazu" (obiektu, czynności itp.) zbliżonego do rzeczywistego poprzez promieniowanie, odbijanie lub tłumienie energii elektromagnetycznej. Przekazywane sygnały wraz z treściami informacyjnymi wytworzają u przeciwnika przekonanie realności o sytuacji nieistniejącej w rzeczywistości. Odbierający nie powinien zorientować się, że sygnały są spreparowane lub zmodyfikowane i przekazaną treść przyjąć jako prawdziwą. W tym przypadku ukrycie rzeczywistych zamiarów wojsk własnych osiąga się drogą emisji fałszywych informacji i sygnałów elektromagnetycznych maskujących sygnały użyteczne oraz na odpowiednim odbijaniu lub tłumieniu sygnałów wejściowych, w sposób mający na celu zmylenie przeciwnika w zakresie wykorzystania informacji pozyskanej przez jego systemy elektroniczne. W pozorowaniu elektronicznym wykorzystuje się w szerokim zakresie pasywne zakłócenia elektroniczne.

Pozorowanie elektroniczne osiąga się przez:

- tworzenie obiektów dezinformujących (pozornych),
- stosowanie manewru pozornego środkami lub energią elektromagnetyczną oraz pozornych przedsięwzięć organizacyjnych,
- deformowanie obiektów rzeczywistych dla rozpoznawczych urządzeń elektronicznych przeciwnika.

Pozorowanie elektroniczne można realizować poprzez: manipulację, symulację i imitację.

Manipulacja[50] polega na zmianie profili elektronicznych rozmieszczanych środków elektronicznych w celu uniemożliwienia przeciwnikowi rozpoznania ich sygnałów, np. poprzez emisję fałszywych informacji we własnych relacjach łączności oraz tworzenie pozornych relacji łączności. Możliwe są również fałszywe poziomy energii promieniowania ścieżek ruchu wojsk własnych, a także zmiany parametrów obiektów oraz kontrolowane zerwania i naruszenia zasad wymiany radiowej (wyłomy, przekroczenia, naruszenia, wyciek spreparowanych informacji związanych z działaniami bojowymi lub etapami walki).

Symulacja polega na elektronicznej reprezentacji (pozorowaniu) własnych sił (całych lub części systemów elektronicznych) w innych miejscach niż znajdują się one rzeczywiście (w trakcie trwania tzw. „ciszy radiowej"). Jej celem jest przeciwdziałanie rozpoznaniu elektronicznemu przeciwnika w określaniu ugrupowania wojsk własnych, ich rozmieszczenia, potencjalnych możliwości oraz zamiarów.

Imitowanie[51] polega na upodobnieniu sygnałów zakłócających do sygnałów użytecznych emitowanych przez przeciwnika. W odniesieniu do systemów łączności należy prowadzić je poprzez włączanie się do relacji radiowych przeciwnika i przesyłania kłamliwych informacji. Stosowane w radiolokacji, powodują na wskaźnikach powstawanie fałszywych zobrazowań znaków celów, analogicznych do znaków celów realnych. W ten sposób można wytworzyć na ekranie wskaźnika stacji radiolokacyjnej zobrazowanie celu w takim azymucie i odległości, gdzie nie ma celów rzeczywistych. Zastosowanie tych zakłóceń dezorientuje użytkownika oraz utrudnia podjęcie właściwych decyzji.

Pozorowanie elektroniczne stanowi część ogólnego planu wprowadzania przeciwnika w błąd. Działania pozorujące wymagają zwykle scentralizowanej koor-

[50] Manipulacja utożsamiana bywa z dezinformacją radiową.
[51] Imitowanie w odniesieniu do środków łączności i radionawigacji utożsamiane bywa z dywersją radioelektroniczną.

dynacji i kierowania. Dlatego wojska wykonują działania pozorujące w ograniczonej skali, w wybranych i kluczowych okresach walki (operacji).

Zakłócanie elektroniczne jest jednym z ważniejszych elementów walki elektronicznej. Przedsięwzięcia zakłócania elektronicznego zapobiegają lub ograniczają możliwości efektywnego wykorzystania przestrzeni elektromagnetycznej przez przeciwnika i w ten sposób wykluczają lub ograniczają jego możliwości dowodzenia i wykorzystania środków walki. Zakłócanie elektroniczne polega na celowym (rozmyślnym) promieniowaniu energii elektromagnetycznej w celu osłabienia efektywności odbiorczych urządzeń (systemów) elektronicznych wykorzystywanych przez przeciwnika i jest aktywną formą przeciwdziałania elektronicznego. Zakłócanie to wnosi do relacji informacyjnych przeciwnika dodatkowe wartości energetyczne, które powodują dezorganizację ich pracy. W zależności od potrzeb i uwarunkowań sytuacyjnych Może przyjmować formę „rażenia" lub „uderzenia elektronicznego" wyrażających zmasowane i kompleksowe użycie, w określonym czasie i miejscu, aktywnych środków walki elektronicznej, w ścisłym powiązaniu z rażeniem ogniowym. Zasadniczymi obiektami zakłócania elektronicznego mogą być:

- w systemach łączności – urządzenia łączności radiowej KF i UKF;
- w systemach radionawigacyjnych – pokładowe i naziemne urządzenia odbiorczo-wskaźnikowe i odbiorcze urządzenia nawigacyjnych;
- w systemach radiolokacyjnych – naziemne stacje radiolokacyjne rozpoznania pola walki, stacje naprowadzania rakiet i kierowania ogniem oraz pokładowe stacje radiolokacyjne lotnictwa i sił morskich;
- w systemach samonaprowadzania – urządzenia elektroniczne głowic samonaprowadzających się bomb, pocisków, rakiet, itp.;
- w systemach radiotelesterowania – różnego typu środki i urządzenia zapewniające zdalne sterowanie uzbrojeniem wojsk, samolotami bezpilotowymi oraz pociskami rakietowymi (przeciwpancernymi, przeciwlotniczymi itp.);
- w systemach optoelektronicznych – urządzenia elektroniczne prowadzące rozpoznanie w ultrafiolecie, w zakresie promieniowania widzialnego oraz bliskiej, średniej i dalekiej podczerwieni;
- w systemach informatycznych – sieci informatyczne rozległe i lokalne oraz zautomatyzowane miejsca pracy na stanowiskach dowodzenia przeciwnika.

Z uwagi na charakter powstawania wyróżnia się, zakłócenia: przypadkowe[52] oraz celowe. Zakłócenia celowe są wytwarzane przez specjalne nadajniki zakłócające lub pasywne retranslatory energii elektromagnetycznej. Wyróżnia się zakłócenia celowe: aktywne, pasywne i kombinowane (w przypadku jednoczesnego stosowania zakłóceń aktywnych i pasywnych).

Zakłócenie elektroniczne może być realizowane jest przez stosowanie nadajników emitujących aktywne sygnały o strukturze zbliżonej do sygnałów użytecznych przeciwnika. Specjalne stacjonarne lub mobilne nadajniki wykonywane są jako stacje: przewoźne, powietrzne (samolotowe, śmigłowcowe) i okrętowe0. Wyróżnia się również nadajniki zakłócające jednorazowego użycia: które mogą być przenoszone jako specjalna amunicja artyleryjska lub urządzenia zrzucane z samolotu lub śmigłowca bądź rozmieszczane przez grupy dywersyjno-rozpoznawcze.

Ze względu na szerokość zakłócającego pasma można wyróżniać:

- zakłócenia selektywne,
- zakłócenia szerokopasmowe (zaporowe),
- zakłócenia wielopunktowe,
- zakłócenia „pływające".

Zakłócenia selektywne (wąskopasmowe, punktowe) odznaczają się dużą dokładnością dostrojenia urządzeń stacji zakłócającej do częstotliwości roboczej zakłócanego środka elektronicznego. Przy stosowaniu tych zakłóceń nadajnik promieniuje sygnał zakłócający o szerokości pasma optymalnej do zakłócanego urządzenia. Zasadniczym zaś warunkiem, pozwalającym na realizację zakłóceń wąskopasmowych, jest dokładna znajomość częstotliwości roboczych poszczególnych środków elektronicznych przeciwnika. Do podstawowych zalet zakłóceń wąskopasmowych można zaliczyć: maksymalny zasięg zakłóceń (cała moc zakłóceń przypada na częstotliwość zakłócaną); minimalny wpływ na pracę własnych stacji. Spośród wad można wyróżnić: łatwość uniknięcia zakłóceń selektywnych; wymagana znajomości zakłócanej częstotliwości; mało efektywne wykorzystanie własnych środków zakłócających.

Zakłócenia zaporowe (szerokopasmowe) są stosowane do obezwładniania jednocześnie wielu środków elektronicznych. „Zagłuszaniu" podlegają całe pasma

[52] Zakłócenia przypadkowe powstają w wyniku oddziaływania zjawisk przyrodniczych oraz urządzeń technicznych na środki elektroniczne. Zjawiska przyrodnicze dotyczą najczęściej: wyładowań atmosferycznych, zorzy polarnej, wybuchów słonecznych i opadów. Urządzenia techniczne obejmują spawarki, źle zabezpieczone silniki elektryczne itp.

częstotliwości wykorzystywane przez przeciwnika. Prowadzi je kilka nadajników lub nadajniki zakłócające jednorazowego użycia. Zakłócenia takie stosuje się w przypadku słabego rozpoznania spektrum elektromagnetycznego przeciwnika. Celem zakłóceń zaporowych jest uniemożliwienie przeciwnikowi korzystania z częstotliwości roboczych w określonym paśmie (podzakresie). Podstawowymi zaletami zakłóceń zaporowych są: efektywne oddziaływanie przeciwko szerokopasmowym źródłom emisji; wymagają minimalnego sterowania; mogą być wykorzystane do zakłócania wielu sygnałów; zmuszają do rekonfigurowania rozbudowanych sieci łączności. Spośród wad można wyróżnić: małą efektywność (wykorzystana moc nadajników rozkłada się proporcjonalnie na wszystkie częstotliwości zakłócanego pasma), duże prawdopodobieństwo zakłócenia pracy własnych stacji.

Zakłócenia wielopunktowe to zakłócanie pojedynczych częstotliwości. Ich główną zaletą jest zwiększona efektywność zakłócania w porównaniu z zakłócaniem selektywnym (punktowym).

Zakłócenia „pływające" polegają na punktowo-zaporowym przemieszczaniu energii zakłócającej po zakłócanych częstotliwościach. Podstawowymi zaletami zakłóceń pływających są: efektywne użycie zakłóceń przeciwko sieciom wieloczęstotliwościowym; cała moc sygnału zakłócającego jest skupiona w danej chwili na jednej częstotliwości; duży zasięg zakłóceń; możliwość sterowania własnymi stacjami w celu uniknięcia zakłóceń wzajemnych. Spośród wad można wyróżnić: skomplikowane technicznie urządzenia.

Ze względu na strukturę sygnału zakłócającego można wyróżniać:

- zakłócenia modulowane (szumowe),
- zakłócenia manipulowane,
- zakłócenia impulsowe,
- zakłócenia kombinowane.

Zakłócenia modulowane (szumowe) realizują sygnały odpowiednich częstotliwości modulowane amplitudowo, częstotliwościowo lub fazowo. Zwykle są to zakłócenia szumowe, charakteryzujące się przypadkowymi parametrami. Zakłócenia szumowe mogą zakłócać wiele rodzajów pracy radiostacji, a przede wszystkim pracę foniczną.

Zakłócenia manipulowane realizują sygnały odpowiednich częstotliwości manipulowane ręcznie lub automatycznie amplitudowo, częstotliwościowo lub fazowo.

Stosowane są najczęściej do zakłócania wąskopasmowych emisji telegraficznych z manipulacją amplitudy, częstotliwości lub fazy.

Zakłócenia impulsowe realizują ciągi krótkotrwałych impulsów, w których modulowany jest czas trwania, amplituda, częstotliwość, faza lub kilka parametrów jednocześnie. Zakłócenia te charakteryzują się bardzo krótkim czasem promieniowania energii, wytworzone są przez nadajnik na częstotliwościach zakłócanych środków radioelektronicznych. Jeśli częstotliwość powtarzania zakłóceń pokrywa się z częstotliwością powtarzania zakłócanej stacji, mamy do czynienia z zakłóceniami synchronicznymi. Jeżeli natomiast te częstotliwości się nie pokrywają, mówimy o zakłóceniach impulsowych nie synchronicznych. Zakłócenia te mogą być odzewowe (jednokrotne albo wielokrotne) lub niezależne. Zakłócenia impulsowe są wykorzystywane do zakłócania środków pracujących impulsowo, np. stacji radiolokacyjnych, stacji radioliniowych, urządzeń telesterowania itp.

Zakłócenia kombinowane realizują sygnały odpowiednich częstotliwości modulowane i manipulowane równocześnie na kilka sposobów, na przykład manipulacja impulsowa w połączeniu z modulacją szumową. Tego rodzaju zakłócenia stosowane są głównie do naruszania pracy środków radioliniowych oraz radiotelegrafii z przesuwem częstotliwości.

Ze względu na zasięg działania urządzeń zakłócających można wyróżniać:

- zakłócenia bliskiego zasięgu,
- zakłócenia dalekie zasięgu.

Zakłócenia bliskiego zasięgu zapewniają skuteczne zagłuszanie i dezorganizację pracy środków elektronicznych przeciwnika na odległość do 10 km od miejsca pracy nadajnika lub stacji zakłócającej. Stosowane są przez nadajniki zakłócające jednorazowego użytku i autonomiczne środki zakłócające.

Zakłócenia dalekiego zasięgu zapewniają skuteczne zagłuszanie i dezorganizację pracy środków elektronicznych przeciwnika z odległości powyżej 10 km (nawet do kilkuset kilometrów).

Ze względu na czas trwania działań można wyróżzniać:

- zakłócenia krótkotrwałe,
- zakłócenia długotrwałe.

Zakłócenia krótkotrwałe prowadzone są w czasie równym a nawet krótszym od czasu nadawania jednego lub kilku sygnałów przeciwnika.

Zakłócenia długotrwałe polegają na zakłócaniu pracy środków elektronicznych w czasie od kilkunastu minut do kilku godzin. Stosowane są m.in. przy wykorzystaniu nadajników jednorazowego użytku.

Ze względu na sposób promieniowania (koncentrowania energii) można wyróżniać:

- zakłócanie dookolne,
- zakłócanie kierunkowe.

Zakłócenia dookólne występują wówczas, gdy promieniowanie anteny odbywa się we wszystkich kierunkach z jednakową mocą. Stosuje się je, wówczas gdy nie są znane miejsca rozmieszczenia zakłócanych środków, w nadajnikach zakłócających jednorazowego użytku i często w stacjach pracujących w ruchu. Ujemną cechą zakłóceń dookólnych jest stosunkowo niski stopień efektywności wykorzystania energii, wynikający ze znacznego jej rozproszenia.

Zakłócenia kierunkowe występują wtedy, gdy energia elektromagnetyczna jest promieniowana przez antenę stacji zakłócającej w kierunku zakłócanego środka elektronicznego przeciwnika. Uzyskuje się to przez stosowanie anten o charakterystyce kierunkowej. Umożliwia to uzyskiwanie, w punkcie odbioru, większego natężenia pola energii zakłócającej. Zakłócenia kierunkowe zwiększają efektywność wykorzystania mocy nadajnika. Stosowanie takich zakłóceń jest konieczne w przypadku zagłuszania urządzeń o dużej kierunkowości anten oraz skomplikowanych strukturach sygnału.

Pod koniec lat siedemdziesiątych i na początku osiemdziesiątych wojska zajmujące się zakłócaniem przeszły z samodzielnego działania stacji rozpoznania i zakłócania do działań polegających na łączeniu ich we wspólne systemy, z centralnym zespołem obróbki informacji otrzymywanej od wielu stacji rozpoznania, co pozwoliło znacznie zwiększyć efektywność działań bojowych[53].

Efektywność zakłócania stacji radioelektronicznych określa się miarą zniszczenia informacji wchodzącej na wejście wykrytej stacji, drogą tworzenia sumy energetycznej sygnału pożądanego i zakłóceń. Dobranie parametrów sygnału zakłócającego jest skomplikowane, ale oczywiście istnieje wariant optymalny, który uwzględnia minimum nakładów na osiągnięcie założonej efektywności. Niezbędnym jest dokonanie oceny środków zakłócających wg kryterium „efektywność/koszty". Liczbo-

[53] Perunow Ju.M., Fomiczew K.I., Judin L.M., *Radioelektronnoe podawlenie informacjonnych kanałow sistem uprewlenia orurziem.*, Radiotechnika 2003, Moskwa.

wym wskaźnikiem efektywności zniszczenia pożądanej informacji jest współczynnik zakłóceń, równy stosunkowi zakłócenie/sygnał na wejściu zakłócanego odbiornika. Jeżeli znamy wartość współczynnika zakłócenia to możemy określić nieodzowną wielkość potencjału energetycznego który zakłóci pożądaną stację.

Jakość zakłóceń ocenia współczynnik prawidłowego działania, określający wykorzystanie mocy zakłóceń potrzebnych do zniszczenia pożytecznej informacji, przy wykorzystaniu przez zakłócaną stację radiolokacyjną różnorodnych sposobów i systemów ochrony przed zakłóceniem. Dla białego szumu Gaussa współczynnik jakości równy jest jeden, dla wszystkich innych zakłóceń, różniących się od szumu białego jest on mniejszy od jedności, dla quasi-nieprzerywanego prostoszumowego zakłócenia współczynnik jakości zbliżony jest do białego szumu Gaussa.

Jednostki wojskowe zajmujące się zakłóceniami, zorganizowane są zwykle w system batalionów zakłóceń (wyposażonych w zautomatyzowane systemy kierowania), w skład których wchodzą najczęściej po trzy kompanie zakłóceń. Każda kompania posiada na wyposażeniu również zautomatyzowany systemy kierowania, a także mobilne stacje rozpoznania i stacje zakłóceń. Wchodzące w skład batalionu trzy kompanie mogą pracować tak razem jak i oddzielnie. Stacje rozpoznania radiolokacyjnego mają za zadanie lokalizować rozmieszczone na samolotach: pokładowe stacje radiolokacyjne oraz systemy łączności i kierowania bronią. Stacje te rozwijane są na stanowiskach dowodzenia batalionu i kompanii zakłóceń.

Nowoczesne stacje rozpoznania radiolokacyjnego pracują najczęściej w zakresie częstotliwości 0,02-18 GHz, z sektorem pracy wynoszącym od 18° do 30°, wykrywają bardzo słabe sygnały radarów pokładowych, powstające z tzw. „listków bocznych" charakterystyki promieniowania, z odległości 100-150 km (czułość – 88 dB, nie uwzględniając parametrów anteny). Stacje określają dokładne współrzędne celów i potrafią identyfikować do 60 celów.

W każdej kompanii zakłóceń znajduje się zwykle po 9 stacji zakłóceń, pracujących przeciwko wykrytym, nieprzyjacielskim samolotom. Wykorzystywane stacje pracują w zakresie częstotliwości (8 – 10) i (13,3 – 17,5) GHz, w sektorach o szerokości 45°, można je tak usytuować, aby zabezpieczały pełną dookólność. Moc promieniowania dochodzi do 1 kW, a czułość od– 57 do– 60 dB/W. Radary samolotów rozpoznają na odległości 120 - 150 km, po włączeniu zakłóceń zasięg skutecznego rozpoznania spada do 50 - 60 km. Batalion zakłóceń może posiadać 27 stacji zakłóceń, co

umożliwia mu pokrycie zakłóceniami obszaru o wymiarach 100x100 km, a nawet 200x200 km.

Stacje zakłóceń są w pełni cyfrowe, wyposażone w nowoczesne układy analizy sygnałów (pasmo analizy do 1 GHz), wzmacniacze na ciele stałym i anteny z szykiem fazowym. Umożliwia to prowadzenie zakłócania pokładowych stacji radiolokacyjnych o złożonych sygnałach.

Zakłócanie systemów łączności krótkofalowej i ultrakrótkofalowej realizują zespoły środków składających się z trzech podzespołów zakłócających: łączność krótkofalową, łączność ultrakrótkofalową oraz łączność lotniczą w zakresie fal ultrakrótkich. Każdy z podzespołów jest sterowany przez mobilny zestaw kierowania. Stacje posiadają odbiorniki cyfrowe z procesorami, które umożliwiają wykrywanie wielu celów i lokalizowanie ich współrzędnych, a także automatyczną współpracę z jednostkami artylerii. Istnieją rozwiązania, które umożliwiają zakłócanie komunikacji radiowej. Mogą być łączone z urządzeniami określającym kierunek, co zwiększa ich efektywność w środowisku o dużej liczbie emisji. Techniki te są przewidywane do wykorzystywania z pokładów śmigłowców i lekkich samolotów wielozadaniowych. Mogą być także montowane na środkach bezpilotowych. Istnieją także bataliony silnych zakłóceń, wyposażone w stacje zakłóceń szumowych dysponujących bardzo wysokimi mocami. Tworzone są również systemy zakłóceń funkcjonujące z wykorzystywaniem szeregu pojedynczych, przenośnych urządzeń odbiorczo-nadawczych, posiadających własne zasilanie. Urządzenia te przewidywane są do rozmieszczania na prawdopodobnych kierunkach działań wojsk nieprzyjacielskich. Ich istota funkcjonalna sprowadza się do tego, że przechwycony sygnał radiolokacyjnych odbierany jest przez antenę odbiorczą urządzenia, które automatycznie wysyła sygnał zakłócający. Urządzenia tego typu rozmieszczane są w dość dużym rozproszeniu (do kilku kilometrów jedno od drugiego). Ma to na względzie, że po zniszczeniu jednego urządzenia zakłócającego pracę przejmuje automatycznie urządzenie następne i tym samym system taki jest trudny do neutralizowania.

Nowoczesne procedury zakłócania są w pełni automatyzowane[54]. Komputery pokładowe zapewniają kompatybilną współpracę wszystkich elementów wpływających na dostrajanie, wybór emisji i jej generowanie sygnału. Urządzenia są lokowa-

[54] Multimedialna biblioteka systemów walki elektronicznej WSOSP Dęblin, http://www.kaiss.wsosp.deblin.pl/biblioteka_systemow/inf_og.htm

ne na różnych nośnikach. Są bardzo często instalowane na samolotach i śmigłowcach. Zapewniają pokrycie zakresu szerokiego pasma częstotliwości.

Nadajniki zakłóceń aktywnych urządzeń radiolokacyjnych dzielą się na:

- nadajniki szumowe,
- nadajniki mylące.

Nadajniki szumowe mogą generować trzy rodzaje sygnałów:

- zaporowe – wytwarzające szumy, których energia zakłóceń jest rozłożona w szerokim paśmie częstotliwości,

wąskopasmowe – zakłócenia szumowe generuje się w szerokości widma odpowiadającego szerokości pasma przepuszczania liniowej części odbiornika zakłócanego.

Nadajniki zakłóceń mylących są uruchamiane w odpowiedzi na sygnały odbierane od źródła promieniowania elektromagnetycznego. Nadajniki te emitują sygnały, które nie są rozpoznawane jako zakłócenia. Do zalet tej metody zakłócania można zaliczyć stosunkowo niską moc nadajników, większą odporność na działanie pocisków samonaprowadzających się na źródło zakłóceń oraz dokładne dopasowanie widma sygnałów zakłócających do pasma przepuszczania liniowej części odbiornika stacji zakłócanej. Podstawową wadą jest konieczność posiadania aktualnych i bardzo dokładnych parametrów stacji zakłócanej. Istnieje zatem wiele metod wytwarzania zakłóceń mylących, w wyniku których, np. na wskaźniku radaru śledzenia wytworzy się fałszywy cel znajdujący się na innym kierunku lub w impulsowych radarach śledzenia celu nastąpi zmylenie w odległości – w obu przypadkach wytwarzany jest fałszywy impuls symulujący echo odbite od celu. Istnieją również zakłócające urządzenia destrukcyjne, służące do niszczenia celów emitujących energię elektromagnetyczną, a przede wszystkim stacji radiolokacyjnych. Funkcję tę mogą spełniać pociski rakietowe wyposażone w bierne układy kierowania, które umożliwiają dokładne naprowadzenie na źródło promieniowania. Innym sposobem może być niszczenie energią skierowaną w postaci promieniowania laserowego lub mikrofalowego o wielkiej mocy.

Zakłócanie systemów radionawigacyjnych obejmuje działania organizacyjne i techniczne, które uniemożliwią lub utrudnią obiektom ruchomym przeciwnika określanie swojego miejsca położenia w przestrzeni. Współczesne systemy radionawigacyjne[55] można podzielić na dwie grupy:

---

[55] System radionawigacyjny to:

- autonomiczne, których środki radioelektroniczne są tylko wewnątrz poruszających się obiektów i umożliwiają określenie położenia niezależnie od urządzeń zewnętrznych (naziemnych lub kosmicznych),
- nieautonomiczne – wykorzystujące odbiorcze lub odbiorczo-zapytujące urządzenia współpracujące z naziemnymi lub satelitarnymi źródłami sygnałów nawigacyjnych.

Zakłócania systemów autonomicznych, opartych o pokładowe stacje radiolokacyjne, są identyczne jak w przypadku zakłócania systemów radiolokacyjnych.

Nieautonomiczne systemy radionawigacyjne można podzielić na systemy bliskiej i dalekiej nawigacji. W każdym z nich występują inne czynniki, które determinują możliwości i skuteczność zakłócania. Generalnie technika zakłócania polega na wprowadzeniu w kanały odbiorcze systemów radionawigacyjnych, sygnałów uniemożliwiających określanie współrzędnych.

Na funkcjonowanie systemów radionawigacyjnych negatywny wpływ mogą wywierać nie tylko zakłócenia celowe (zamierzone), ale również i zakłócenia przypadkowe (niezamierzone).

Zakłócenia niezamierzone to przede wszystkim częstotliwości harmoniczne, listki boczne charakterystyk atenowych, efekty intermodulacji oraz te, których nie udaje się ustalić przy pomocy tradycyjnych metod kontroli częstotliwości. Są one groźne nie tylko dla strefowych (lokalnych) systemów radionawigacyjnych, ale także i dla systemu globalnego radionawigacji satelitarnej. Wynika to z faktu, że nawet nadajniki małych mocy mogą zakłócać odbiorniki tego systemu w promieniu do 10 km. Pracę odbiorników mogą zakłócać nawet telefony komórkowe.

Zakłócenia zamierzone (celowe) globalnego systemu radionawigacyjnego Mogą być realizowane z masowym wykorzystywaniem przenośnych nadajników zakłócających jednorazowego użycia. Są to urządzenia o bardzo małych rozmiarach, których koszt jednostkowy, często nie przekracza 100 dolarów. Zawsze jednak nale-

---

1) zespół urządzeń radionawigacyjnych rozmieszczonych na ziemi i na obiektach ruchomych, przeznaczony do realizacji prawidłowego prowadzenia tych obiektów po wyznaczonej trasie, naprowadzania samolotów na miejsce lądowania - bez widoczności, kontroli i regulacji itp.;

2) sposób określania pozycji ruchomego obiektu za pomocą pokładowych urządzeń radionawigacyjnych współpracujących z naziemnymi pomocniczymi urządzeniami radionawigacyjnymi. System radionawigacyjny służy więc ogólnie do określania miejsca położenia obiektów ruchomych (zarówno cywilnych jak i wojskowych) w przestrzeni trójwymiarowej za pomocą urządzeń umieszczonych na tych obiektach i wykorzystaniu urządzeń bazowych o ustalonym w danym momencie czasowym położeniu.

ży brać pod uwagę fakt, że zakłócanie obszarowe spowoduje również zakłócenie również środków własnych.

Zakłócanie czujnikowe (sensoryczne) polegają na obezwładnianiu poszczególnych detektorów lub uniemożliwianiu ich pracy drogą dostarczania energii zakłócającej odpowiadającej parametrami sygnałom bodźcowym, charakterystycznym dla danego środowiska: akustycznego (fale sprężyste[56] - infradźwięki, ultradźwięki), magnetycznego, elektrycznego, chemicznego oraz wszelkiego rodzaju uboczne efekty towarzyszące działaniom bojowym, na przykład: termiczne, sejsmiczne, naciskowe, zapachowe. Przedsięwzięcia wykonywane w ramach zakłócania czujnikowego Można podzielić na organizacyjne i techniczne. Winny one być ze sobą ściśle powiązane i wzajemnie się uzupełniać. Celem ich jest zawsze dezorganizacja rozpoznania w wyniku ograniczenia pracy i eliminowania tych źródeł, które emitują sygnały bodźcowe sensorów: akustycznych, magnetycznych, elektrycznych i chemicznych. Analiza współczesnych konfliktów zbrojnych sugeruje, że generatory infradźwięków mogą być również wykorzystane na polu walki do obezwładniania siły żywej. Obrona przed nimi powinna opierać się na budowaniu tzw. miękkich zasłon, które absorbują energię tych fal oraz na tworzeniu tzw. pól aktywnego hałasu. Istota działania tych pól, polega na wytworzeniu fali dźwiękowej o tych samych parametrach, lecz odwróconej w fazie o 180°.

Zakłócanie optoelektroniczne ma na celu utrudnianie bądź uniemożliwianie przeciwnikowi zdobywanie oraz przetwarzanie tych danych, których nośnikami są fale elektromagnetyczne pasma optycznego. Przeciwdziałania optoelektroniczne dotyczą środków rozpoznania i sterowania pracujących w podczerwieni, termolokatorów, urządzeń telewizyjnych oraz urządzeń laserowych.

W zakłócaniu telewizyjnym szczególną uwaga jest skupiana na zakłócaniu obrazów ruchomych z towarzyszącymi im dźwiękami. Zakłóceniami są objmowane wszystkie środki radiowe, radioliniowe i radiosatelitarne wykorzystywane do transmisji przekazu telewizyjnego.

Zakłócanie noktowizyjne obejmuje oddziaływania, które umożliwiają widzenie w całym zakresie promieniowania podczerwonego. Zakłócanie to jest powiązane z innymi rodzajami zakłócania optoelektronicznego. Krótkotrwałe zakłócenie rozpoznania optoelektronicznego, mogą realizować specjalne generatory dymotwórcze,

[56] Fale sprężyste - zaburzenia rozchodzące się w ośrodku sprężystym. Polegają na drganiu cząsteczek wokół punktu równowagi. Ilustrowana encyklopedia dla wszystkich. Fizyka, wyd. WNT, Warszawa 1991, s. 77.

które wytwarzają zasłony dymne oraz dymy o znacznie podwyższonej lub obniżonej temperaturze. Obniżają one znacznie efektywność środków rozpoznania optoelektronicznego, znacznie utrudniają przeciwnikowi prowadzenie nie tylko obserwacji optycznej, ale także termowizyjnej i laserowej. Realizacja przedsięwzięć technicznych zakłócania rozpoznania optoelektronicznego jest realizowana za pomocą etatowych oraz podręcznych środków i materiałów. Środki etatowe pozwalają na znaczne skrócenie czasu przygotowania ich do użycia oraz zapewnią lepsze rezultaty. Wprowadzone na wyposażenie wojsk poliamidowe siatki maskujące charakteryzują się zaledwie dostatecznymi zdolnościami zakłócania rozpoznania optycznego (maskowania), w zakresie widma widzialnego oraz w bliskiej podczerwieni.

Doświadczenia ostatnich wojen i konfliktów lokalnych wskazują, że skutecznym środkiem zakłócania w omawianym widmie (optoelektronicznym), jest malowanie maskujące[57], spełniające funkcje:

- ochronne (ukrywające);
- pozorujące;
- deformujące.

W malowaniu ochronnym są wykorzystywane specjalne farby, które powodują zlewanie się widma obserwowanego celu z widmem tła. Farby takie, nazywane metamorficznymi, powodują zmianę koloru pod wpływem warunków zewnętrznych m.in. temperatury i natężenia oświetlenia. Malowaniem pozorującym są pokrywane obiekty imitujące, których kształt, kolorystyka i charakterystyki spektralne, nie odbiegają od obiektów rzeczywistych. Takie cechy obiektów rzeczywistych mają m.in. obiekty pozorne wytwarzane za pomocą zestawu DECEPTION - szwedzkiej firmy Barracuda. Są to obiekty w większości wykonane w skali 1:1, pozorujące sprzęt bojowy taki jak: czołgi, transportery, zestawy artyleryjskie, systemy rakietowe, a nawet mosty, bazy lotnicze itp. Ich koszty produkcji nie przekraczają 0,5% wartości pozorowanego obiektu. Rozproszenie wysiłku rozpoznawczego przeciwnika na obiektach pozornych, zwiększa szansę na przetrwanie elementów rzeczywistych ugrupowania operacyjnego (bojowego), bowiem przy zastosowaniu właściwego sposobu pozorowania, prawdopodobieństwo przeprowadzenia ataku na cel pozorny jest bardzo wysokie.

Rosja produkuje szeroką gamę różnorodnych środków zabezpieczających[58] przed rozpoznaniem optycznym, są to komplety maskujące, które zabezpieczają po-

[57] W naszych wojskach nie ma etatowych zestawów do malowania maskującego, a przygotowanie stanów osobowych do jego wykonania nie jest wystarczające.

wierzchnię o wymiarach od kilkunastu do kilkuset metrów kwadratowych, mogą być wykorzystywane w temperaturach od – 40° do + 40° C, a kamuflaż umożliwia stosowanie ich w letnim roślinno-zadrzewionym terenie lub w terenie pustynno-stepowym.

Podobne komplety maskujące zabezpieczają obiekty przed rozpoznaniem optycznym i radiolokacyjnym. W celu zabezpieczenia się przed rozpoznaniem obiektów promieniujących ciepło, stosuje się komplety odbijające ciepło, mogą one być stosowane łącznie z kompletami zabezpieczającymi przed rozpoznaniem optycznym i radiolokacyjnym. Kolejne obiekty pozorne podobne do tych wytwarzanych przez firmę Barracuda, nazywane są makietami sprzętu bojowego. Makiety te wykorzystuje się do imitowania jednostek wojskowych, pododdziałów usytuowanych w rejonach rozmieszczenia i na pozycjach bojowych. Rozpoznanie optyczne, radiolokacyjne, pracujące w podczerwieni oraz systemy naprowadzania broni - identyfikują te makiety jako autentyczny sprzęt bojowy. Efekt imitacji w zakresie fal radiowych zapewnią powłoki odbijające fale. Makiety te są wykonywane z dużą dbałością o parametry techniczne np. wymiary z dokładnością do kilku cm, praktycznie nie do odróżnienia w rozpoznaniu satelitarnym.

Na szczególną uwagę zasługuje również malowanie deformujące, nazywane kamuflażowym. Do malowania wykorzystuje się różnego rodzaju farby nitrocelulozowe, olejne, kazeinowe oraz farby nowej generacji oparte na dyspersji koloidowej, poliuretanowe i wodne.

Zakłócanie systemów laserowych ma na celu utrudnić bądź uniemożliwić przeciwnikowi korzystanie z tych urządzeń. Obejmuj między innymi laserowe urządzenia lotnicze stosowane w:

- nawigacji lotniczej - do pomiaru wysokości i prędkości lotu, oświetlania identyfikowanego terenu, określania współrzędnych kątowych, określania warunków atmosferycznych;
- rozpoznaniu lotniczym - do oświetlania terenu przy wykonywaniu zdjęć lotniczych w nocy i trudnych warunkach atmosferycznych, ukośnego fotografowania dużych obszarów, prowadzenia rozpoznania o wysokiej jakości zobrazowania przy lotach na niskim pułapie, uzyskiwania trójwymiarowych zobrazowań (trzeci wymiar uzyskiwany za pomocą dalmierza laserowego).

[58] Zgodnie z ofertą eksportową rosyjskiej firmy Rosoboronexport.

W działaniach bojowych lotnictwa - do wybierania i oświetlania wiązką lasera celów punktowych, przewidzianych do ataku bombami i pociskami rakietowymi samonaprowadzającymi się na laserowo oświetlone cele, w zbliżeniowych zapalnikach laserowych oraz kierowania ogniem lufowej broni pokładowej samolotów i śmigłowców. W wojskach lądowych, zakłócenia są ukierunkowywane na laserowe urządzenia celownicze. Eliminując subiektywne przyczyny niecelności, urządzenia te pozwalają na prowadzenie znacznie bardziej precyzyjnego ognia, zarówno przy strzelaniu z broni lufowej, jak i używaniu przeciwpancernych pocisków rakietowych naprowadzanych na cel wiązką lasera. Lasery mogą być również szeroko wykorzystywane do monitorowania pola walki, oświetlania obiektów ugrupowania operacyjnego i naziemnej infrastruktury, określania warunków atmosferycznych, lądowej nawigacji, a nawet oślepiania siły żywej, chociaż zabraniają tego konwencje genewskie.

Zakłócanie systemów informatycznych może być prowadzone przeciwko systemom (sieciom) informatycznym, najczęściej w postaci złośliwego oprogramowania, które powoduje blokowanie dostępu do zbiorów danych, wymazanie w krótkim czasie ich dużej liczby, spowalnianie pracy programów użytkowych itp. Oprogramowanie to może być wprowadzane poprzez kanały radiowe i linie łączności światłowodowej łączące centralną jednostkę systemu z terminalami użytkowników. Wielu specjalistów uważa, że przyszła wojna będzie polegała na blokowaniu dostępu do prawdziwych danych i wprowadzaniu w błąd przeciwnika przez udostępnianie danych fałszywych. Celem tej walki będzie rozpoznanie a następnie obezwładnienie systemów komputerowych przeciwnika, tak aby nie był on zdolny do podejmowania jakichkolwiek racjonalnych działań.

Elektronika, informatyka oraz optoelektronika w systemach dowodzenia, kierowania, łączności i rozpoznania (Command, Control, Communication and Intelligence), zarówno podczas przygotowania jak i prowadzenia operacji na współczesnym polu walki, znacznie zwiększyły szybkość i skuteczność działań sił zbrojnych. Funkcjonujące, różnorodne systemy C^{3}I promieniują energię elektromagnetyczną w wolnej, dostępnej dla wszystkich przestrzeni, coraz szerzej wykorzystują technikę komputerową. Spowodowało to pojawienie się nowego typu komputerowej walki elektronicznej[59]. Opracowywane i rozwijane są metody wprowadzania programów wiruso-

59 Należy rozróżniać pojęcia komputerowej walki elektronicznej i cyberterroryzmu. W ekspertyzach NATO [Por. E. Vernon Jr., Information War and International Security, Report for Committee General NATO, 285 STC (99) 81, 1999; M. Mates, Technology and Terrorism, Draft inter Report for Sub-Committee on Proliferation of

wych do wojskowych systemów radioelektronicznych. Wirusy zakłócają pracę systemów komputerowych, uszkadzają programy robocze, powodują, że wyniki ich działania mogą zawierać fałszywą informację, albo też doprowadzają do uszkodzenia posiadanych danych. Wydarzenia ostatnich lat udowodniły, że wykorzystywanie wirusów komputerowych jest zagrożeniem nie tylko teoretycznym, ale może ono doprowadzić do rzeczywistego, całkowitego uszkodzenia systemów i obiektów[60]. Przykładem może być operacja „Pustynna burza" w Iraku, gdzie wykorzystując technologię wirusów komputerowych udało się unieszkodliwić systemy OPLot. „Zarażone" wirusem systemy zostały zablokowane, co pozwoliło lotnictwu amerykańskiemu praktycznie bez strat własnych przeniknąć w przestrzeń powietrzną Iraku i z powodzeniem wykonywać zaplanowane wcześniej operacje wojskowe[61]. W związku z tymi pozytywnymi doświadczeniami, Armia USA zaplanowała wykonanie szeregu testów sprawdzających możliwości wykorzystania wirusów komputerowych w charakterze środków walki elektronicznej, a także przeprowadzenie badań metod zdalnej implementacji wirusów za pomocą środków taktycznej łączności radiowej[62].

Jednym z celów działania wirusów może być zakłócenie pracy systemu. Wywoływane zakłócenia polegają na: niszczeniu lub zmianie zawartości plików, blokowaniu pracy systemu, obciążaniu procesora dodatkową pracą, generowaniu dźwięku, obrazu lub tekstu. Inne możliwe działania wirusów to np.:

- umożliwienie nieautoryzowanego dostępu do systemu;
- wykonywanie akcji ujawniających informacje o systemie/danych, np. wysłanie atakującemu interesujących go informacji/danych – kradzież danych;
- ataki „dla sportu", pozostawianie nieszkodliwych znaków typu „tu byłem", mogą mieć pozytywny efekt – ujawnienie słabości systemu;
- niszczenie sprzętu;
- umożliwienie przejęcia kontroli nad systemem (również bezśladowej kontroli)

Military Technology, 2001], pojawiają się wartościowe definicje i rozróżnienia. Cyberterroryzmem określone zostały: akty terroryzmu z zastosowaniem informacji albo systemów informacyjnych, jako narzędzi ataku bądź obrony. Zastrzeżono przy tym, że między cyberprzestępstwem a cyberterroryzmem istnieje różnica, co do motywów i celów, zatem nie każdy rodzaj cyberataku uznany będzie za cyberterrorystyczny. Celem działań cyberterorystycznych będzie wywołanie strachu, paniki wśród ludności cywilnej albo zakłócenie systemów obronności państwa. Komputerowa walka elektroniczna, uwzględniając jej motywy i cele jest pewnego rodzaju cyberatakiem.

[60] Gramar M.L., Pratt S.R., *Computer virus countermeasures – a new type of EW*, - Defence Electronices, 1990, v. 22, Oct.

[61] Morzys O.W., *Wirtualnyj terrorizm – realnoct naszego wremeni. – Zaszczita informatii.* „Konfident", Janwar-aprel 1999, s. 66-69; Informacja TASS – gazeta „Prawda" z 13 stycznia 1992 r.

[62] *Army to award contract for studying potential of computer viruses as electronic countermeasures.* – Aviation Week and Space Technology,1990, v.132, N 20, p.38;

osobie niepowołanej;

Wirus komputerowy to program, który dostaje się do systemu bez zgody użytkownika, potrafi się rozmnażać, doczepiać oraz ukrywać wewnątrz plików zawierających kod wykonywalny, lub wewnątrz systemowych sektorów na dyskach. Wirusy plików uaktywniają się w momencie uruchomiania zainfekowanego programu i wykonują zazwyczaj niepożądane czynności. Wirusy sektorów systemowych uaktywniają się przy starcie systemu i zarażają dostępne dyski logiczne. Wirusy nie są oddzielnymi programami - nie potrafią działać samodzielnie, w celu aktywizacji potrzebują uruchomienia jakiegoś programu bazowego, którego są częścią. Istnieją również makrowirusy (wirusy skryptowe), które składają się z instrukcji w języku wysokopoziomowym, wykonywanych przez interpreter. Są to programy zapisywane jako makra i rozpowszechniane najczęściej z plikami pakietów biurowych.

Wirusy komputerowe należą do najczęściej występujących zagrożeń programowych systemów i sieci teleinformatycznych. Istnieje kilka typów takich programów różniących się między sobą sposobem zachowania, sposobem uruchamiania i rozprzestrzeniania się. Należą do nich: wirusy (viruses); bakterie (bacteris); robaki (worms); tylne drzwi (back doors); bomby logiczne (logic bombs); konie trojańskie (trojan horses).

Działanie robaków i bakterii jest podobne, z tą różnicą, że dla bakterii polem działania jest pojedynczy system, a dla robaków – sieć informacyjna. Bakteria to program rozmnażający się (samokopiujący się). Bakterie reprodukują się wykładniczo, zabierając ostatecznie całą moc obliczeniową procesora, pamięć lub wolny obszar pamięci dyskowej, powodując blokadę systemu. Robak stanowi program samo powielający się, który działa samodzielnie i przenosi się z urządzenia na urządzenie dzięki połączeniom sieciowym. Może on dzielić się na części działające na wielu różnych urządzeniach. Program ten może również uaktywnić się i powielać oraz zainicjować niepożądaną akcję w danym systemie, zmniejszając wydajność serwerów aż do całkowitej ich blokady. Nie zmienia on innych programów, chociaż może być nosicielem innego, umożliwiającego to kodu, jakim jest np. wirus.

Wirus komputerowy infekuje określony element systemu i rozprzestrzenia się we wspólnym systemie informacyjnym na obiekty wykorzystywane przez ten system, co pozwala na oddziaływanie w sposób pośredni na inne interesujące obiekty, które są łatwiej dostępne i mniej chronione. Program wirusowy może być zorientowany na poszukiwanie konkretnych aplikacji, w których może on znajdować się w stanie pa-

sywnym, aż do czasu wprowadzenia go do akcji. Działanie wirusa może przejawiać się w różnych formach: niezauważalnej zmianie funkcji zainfekowanego systemu, zniszczeniu systemu lub zniszczeniu plików danych i programów.

Programy wirusowe charakteryzują następujące podstawowe cechy:

- zespolenie – umożliwia programom wirusowym rozprzestrzenianie się na inne programy i utrudnia ich wykrycie;
- uniwersalność – polega na tym, że są one gotowe do działania z różnymi dowolnymi programami, zwykle nie potrzeba nawet żadnej informacji o zakażanym programie;
- zdolność do rozprzestrzeniania się – jest nieodzowną cechą programów wirusowych; zawirusowany program może rozprzestrzeniać się na inne programy i pliki, tworzące system informacyjny i w tym sensie wirus komputerowy zachowuje się podobnie jak wirus biologiczny;
- efektywność programów wirusowych – w wielu przypadkach jest bardzo wysoka; w wyniku ich ataku może nastąpić pełna utrata informacji, uszkodzenie programu, a czasami całego systemu operacyjnego;
- wielofunkcyjność – przejawia się w różnorodności funkcjonalnej wirusów; niektóre wirusy komputerowe zarażają wskazane wcześniej programy, omijając pliki z danymi i aplikacje systemu operacyjnego; inne mają powodować uszkodzenia i niszczenie plików; efektywność programów wirusowych zwiększa się, ponieważ mogą one pozostawać nieujawnione do określonego momentu czasowego (początku działania operacyjnego); pozwala to wirusowi na powielanie się do czasu, aż użytkownik zarażonego systemu wykryje go;
- stałość programu wirusowego – zawiera się w tym, że nawet po jego wykryciu, usunięcie go jest skomplikowanym problemem, ponieważ posiada on zdolność ponownego rozprzestrzeniania się od jednej z powstałych wcześniej kopii.

Podstawowa różnica pomiędzy tradycyjną walką elektroniczną a komputerową walką elektroniczną wykorzystującą wirusy komputerowe, polega na tym, że środki tradycyjnej walki elektronicznej oddziaływają na elementy odbiornika atakowanego systemu, natomiast wirusy oddziaływają na procesory zakłócanego systemu. Specyfika komputerowej walki elektronicznej pozwala na wykorzystywanie jej do dezorganizacji operacji. Posiada właściwość przedłużenia działania zakłóceń w zaatakowanym systemie, także po zaimplementowaniu wirusa. Tworząc określone typy wiru-

sów, można zaprojektować mechanizmy ich oddziaływania na atakowane obiekty wcześniej, a tym samym uwzględniać ten fakt przy tworzeniu planów operacyjnych. Realizacja komputerowej walki elektronicznej może być tajna. Wirusy mogą rozprzestrzeniać się i niszczyć system niezauważalnie dla użytkowników. Nie wiedząc o ich działaniu, obiekt zaatakowany nie może się bronić, tzn. wprowadzać zmian w programie roboczym albo podejmować przeciwdziałania.

Efektywność komputerowej walki elektronicznej wymaga, aby była ona pewna i ukierunkowana. Posiadając informacje apriori o obiekcie, który ma zostać zaatakowany, można dużo wcześniej przygotować i wprowadzić odpowiedni wirus. Stanie się on aktywnym dopiero po otrzymaniu polecenia do działania, wcześniej nie oddziałuje on na procesory i nie rozprzestrzenia się. Ważną jest informacja potwierdzająca, że wirus osiągnął zaplanowane miejsce i jest gotowy do działania. Taką informację można uzyskać na podstawie obserwacji pracy linii nadawczych, albo po otrzymaniu sygnału, wcześniej zaprogramowanego w kodzie wirusa.

Realizację komputerowej walki elektronicznej może ułatwiać tendencja do rozwijania systemów radioelektronicznych, polegająca na zwiększonym wykorzystywaniu:

- rozdzielania cyfrowej obróbki sygnałów i danych,
- wbudowanych komputerów z modyfikowalnym oprogramowaniem,
- sieciowych systemów łączności,
- standardowych komputerów,
- standardowego oprogramowania zabezpieczającego,
- standardowych linii przekazu danych i formatów informacji.

Powyższe przedsięwzięcia powodują: obniżenie kosztów i uproszczenie obsługi technicznej złożonych systemów, podwyższenie ich szybkości działania oraz informatywności. Z drugiej zaś strony powodują wzrost zagrożenia wykorzystania komputerowej walki elektronicznej, doprowadzają do upraszczania metod wprowadzania wirusów programowych.

Efektywność komputerowej walki elektronicznej zależy od zdolności wirusa do rozprzestrzeniania się i infekowania systemu. W większości współczesnych wojskowych systemów dowodzenia, łączności i rozpoznania, zaimplementowane są środki obrony przed ingerencją przeciwnika. Jednakże specyfika zakłóceń komputerowych pozwala w wielu przypadkach obejść te zabezpieczenia.

Istnieją cztery sposoby wprowadzenia wirusa do zaatakowanego systemu informatycznego[63]:

- Bezpośredni – polega na wykorzystaniu środowiska, w którym funkcjonuje atakowany system. Przykładowo, jeśli atakowanym obiektem jest radiostacja, to do wprowadzenia wirusa wykorzystuje się sygnały radiowe idące bezpośrednio do jej anteny i urządzenia odbiorczego. W systemach kierowania walką, łączności i rozpoznania wirus wprowadza się bezpośrednio do urządzenia odbiorczego po linii kierowania i przesyłania danych z nadzieją, że odbiornik odbierze i odpowiednio zaimplementuje go. W wyniku rozprzestrzenienia, wirus będzie infiltrował wszystkie obiekty związane z zainfekowanym systemem. Przy czym wystarczy tylko raz pokonać obronę systemu przed zakłóceniami, aby później w dowolnym momencie czasowym on zadziałał, niezależnie od dokonywanych zmian rodzajów pracy zwiększających ochronę przed zakłóceniami. Jak wiadomo, przy realizacji tradycyjnych zakłóceń elektronicznych, są one efektywne tylko w chwili przełamania zabezpieczeń chroniących pracę odbiornika przed zakłóceniami. Uwzględniając całą złożoność komputerowej walki elektronicznej, należy ukierunkowywać jej atak na najsłabiej bronione ogniwo w systemie przeciwdziałania zakłóceniom atakowanego obiektu.
- Przez pośrednika – zakłada się wykorzystanie innego środowiska, niż to, które określa jego przeznaczenie. Przykładowo, do wprowadzenia wirusa mogą być wykorzystywane systemy zasilania, stabilizacji, termoregulacji, silniki bezpośrednio lub pośrednio połączone elektrycznie z obiektem – celem ataku.
- Prosty – przewiduje bezpośrednie oddziaływanie na interesujący procesor. Może być to wykonane np. drogą ciągłego przekazu wirusa w czasie odbioru normalnej korespondencji przez atakowany obiekt. W tym przypadku skutecznym zabezpieczeniem może być ochrona antywirusowa atakowanego obiektu.
- Nieprosty – może okazać się bardzo skutecznym sposobem. Został obliczony na bezwładność wirusa, przewiduje on wykorzystanie do wprowadzenia programu wirusowego najsłabszego (najmniej chronionego) obiektu systemu, od którego wirus powinien się rozprzestrzeniać w kierunku obiektu, który jest zasadniczym celem ataku. W tym celu można wykorzystać oprzyrządowanie obsługi materiałowo-technicznej i diagnostyki stanu interesującego systemu. Infekując wirusem wska-

[63] Perunow Ju.M., Fomiczew K.I., Judin L.M., Radioelektronnoe podawlenie informacjonnych kanałow sistem uprewlenia orurziem., Radiotechnika 2003, Moskwa

zany procesor, można zainfekować i inne procesory, wchodzące w skład danego systemu, a tym samym osiągnąć zamierzony cel. Metoda ta wyróżnia się dużą prostotą i wysoką efektywnością, ponieważ jest bardzo trudno opracować mechanizmy, które przewidywałyby drogę rozprzestrzeniania się infekującego wirusa.

Istnieją również różne warianty i sposoby prowadzenia komputerowej walki elektronicznej, wśród których można wyróżnić:

- Typu „konia trojańskiego" – przewiduje wprowadzenie wirusa do atakowanego systemu i pozostawienie go w stanie pasywnym do czasu wystąpienia założonego zdarzenia lub momentu czasowego. Jego zaletą jest to, że wirus pozostaje w uśpieniu przez określony czas, nie powodując żadnych podejrzeń.
- Typu „wymuszonej kwarantanny" – zakłada jawne wprowadzenie wirusa do systemu. W rezultacie zakażony węzeł (obiekt) stwarza niebezpieczeństwo rozprzestrzenienia zainfekowania na inne węzły, co prowadzi do obniżenia efektywności pracy zaatakowanego systemu.
- Typu „przeładowania" – wielokrotne powielanie wirusa ma na celu zmniejszenie przelotowości i szybkości działania systemu;
- Typu „strefowania" – przewiduje wprowadzenie wirusa komputerowego do sieci w celu uszkodzenia określonego pliku, obiektu albo innego systemu. W tym przypadku wirus sam się rozprzestrzenia i sam się niszczy we wszystkich punktach, dopóki nie znajdzie obiektu – celu. Po uszkodzeniu ostatniego lub docelowego obiektu, wirus ostatecznie ulega samolikwidacji, nie zostawiając żadnych śladów.

Zakłócanie systemów informatycznych obejmuje penetrację bierną, stanowiąc zagrożenie dla zachowania tajemnicy oraz penetrację aktywną, zagrażającą autentyczności danych.

Zakłócanie penetracji biernej dotyczy dostępu przeciwnika do danych, a w sieciach komputerowych do monitorowania ich przepływu lub ustalenia struktury sieci. Penetracja bierna może być prowadzona w formie: przeglądania, przenikania i wnioskowania.

Przeglądanie polega na przeszukiwaniu sieci komputerowej w celu pozyskania danych. Jest to proces podobny do śledzenia w kanałach łączności, przy czym istnieją tu dwie istotne różnice. Po pierwsze w sieciach komputerowych dane są przechowywane znacznie dłużej i dlatego są zdecydowanie bardziej narażone na przeglądanie niż kanały łączności na śledzenie. Po drugie, kanały łączności są narażone na

śledzenie wtedy, kiedy przeciwnik ma dostęp energetyczny do sygnałów. Natomiast przeglądanie jest możliwe wówczas, gdy przeciwnik „złamie" zabezpieczenia i kody dostępu do sieci lub wybranych obszarów pamięci systemów komputerowych.

Przenikanie zwane też przeciekaniem informatycznym, dotyczy przepływu danych do nieuprawnionych użytkowników podczas procesów realizowanych przez legalnych użytkowników systemu.

Wnioskowanie dotyczy procesów ustalenia danych niejawnych, na podstawie ogólnie dostępnych lub jawnych informacji. Na przykład: przechwycenie przez przeciwnika danych z logistyki dotyczących np. ilości zamawianego pieczywa umożliwia określenie ilości żołnierzy danej jednostki.

Zakłócanie penetracji aktywnej dotyczy ochrony własnych zbiorów lub strumieni danych, przed rozmyślnym ich modyfikowaniem przez przeciwnika. Celem takiego działania może być pozyskiwanie danych połączone z ich zastępowaniem innymi zbiorami. W jej ramach, przeciwnik może przykładowo wprowadzić do sieci błędne komunikaty i polecenia dotyczące wykonywanych zadań czy obiektów ataku. Jeżeli dane będą zmieniane w umiejętny sposób lub w minimalnym zakresie, to takie zniekształcanie będzie bardzo trudne do wykrycia.

Przy zakłócaniu penetracji aktywnej uwzględnia się: zniekształcanie, podszywanie i niszczenie danych.

Zniekształcanie (modyfikacja) danych w sieciach komputerowych jest odpowiednikiem aktywnego zakłócania w kanałach łączności. Zniekształcanie może być użyte do wykonywania określonych zmian w bazach danych, zamazywanie dotychczasowych danych przez zapisywanie bezużytecznych informacji lub usuwanie całych plików.

Podszywanie się jest odpowiednikiem dywersyjnych działań dezinformacyjnych w kanałach łączności. Dotyczy sytuacji, w której przeciwnik podszywa się pod uprawnionego użytkownika sieci i w ten sposób uzyskuje dostęp do plików i zbiorów. Odmianą takiego działania jest przypadek, gdy przeciwnikowi uda się wprowadzić program stymulujący funkcje systemu, dzięki czemu uzyskuje dostęp do najbardziej zastrzeżonych informacji.

Niszczenie danych dotyczy zamierzonego zamazania lub usunięcia części lub całych plików lub programów. Niszczenie danych może być również niezamierzone, spowodowane wadliwym oprogramowaniem lub usterką sprzętu, a także pomyłką użytkownika.

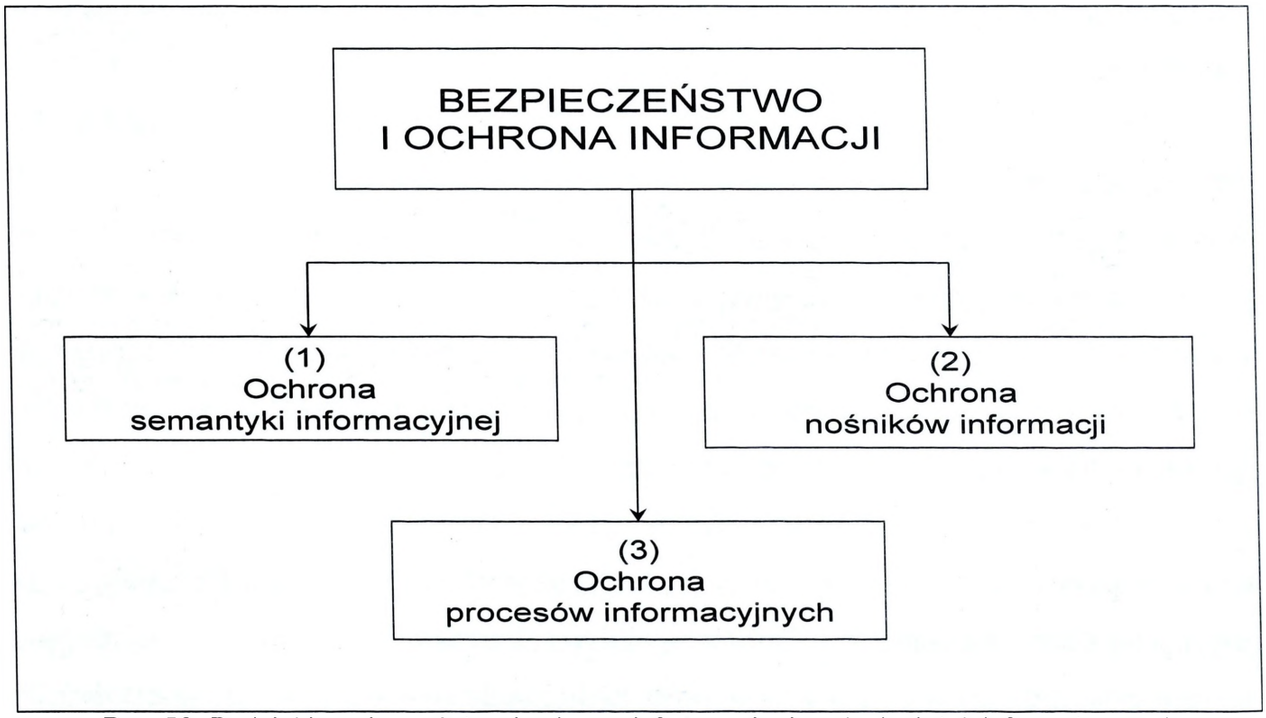
Zakłócanie elektroniczne stanowi bardzo skuteczny sposób dezorganizacji pracy i działania różnorakich środków i systemów elektronicznych wykorzystywanych w dowodzeniu wojskami i kierowaniu środkami walki przeciwnika. Ogranicza ono zakres i możliwości wykorzystania ww. systemów przez poszczególne dowództwa i sztaby a ponadto w wielu sytuacjach jest przyczyną powstających u przeciwnika znacznych strat w sile żywej i sprzęcie bojowym.

W rezultacie zakłócania elektronicznego środków i systemów elektronicznych przeciwnika następują zmiany w ilości danych przesyłanych do poszczególnych dowództw i sztabów oraz do wojsk wykonujących określone zadania bojowe. Często, mimo sprawności technicznej środków elektronicznych w wielu ogniwach dowodzenia wystąpić może całkowita lub częściowa utrata danych albo opóźnienie w przekazywaniu wiadomości bojowych. Poza tym przekazywane dane mogą być w znacznym stopniu zniekształcone, zamazywane i deformowane. Występować może zmniejszenie ich ilości lub też zwiększenie w drodze imitowania. Do dowództw i sztabów (na stanowiska dowodzenia), do wojsk i środków walki docierać będą dane niepełne, wątpliwe, odznaczające się niskim stopniem wiarygodności. Przekaz danych może być też na pewien okres czasu całkowicie przerwany. Brak danych lub niski stopień ich wiarygodności uniemożliwia lub utrudnia realizację terminowego, skoordynowanego i operatywnego dowodzenia wojskami i kierowania środkami walki. Obniża to sprawność bojową wojsk, ich siłę uderzeniową i skuteczność działań, uniemożliwia terminowe wykonanie zadań bojowych oraz bardzo często prowadzi do znacznych strat w sile żywej i sprzęcie bojowym. Należy jednak mieć na uwadze, że efekty zakłócania elektronicznego wzrastają w przypadku ścisłej koordynacji działań elektronicznych z oddziaływaniem ogniowym na wybrane obiekty elektroniczne. Czas zakłócania elektronicznego powinien być podporządkowany potrzebom wykonania zadań ogniowych i manewrowych. Szczególnie jest to widoczne w walce z systemami obrony powietrznej i systemami dowodzenia wojsk lądowych.

ZAKOŃCZENIE – PODSUMOWANIE WNIKÓW BADAŃ

Z przeprowadzonych dociekań poznawczych, zawartych w rozdziale pierwszym i drugim, wynika, że bezpieczeństwo i ochrona informacji w sieciach teleinformatycznych w ogóle, a tym samym i organizowanych na potrzeby wojsk lądowych winna się koncentrować na następujących przedsięwzięciach (rys. 53):

- ochronie semantyki informacyjnej,
- ochronie nośników informacji,
- ochronie procesów informacyjnych.



Rys. 53. Podział bezpieczeństwa i ochrony informacyjnej w sieciach teleinformatycznych

Źródło: Opracowanie autorskie

Problematyka ta winna być uwzględniana we wszelkich działaniach i na wszystkich poziomach władzy organizacyjnej, jako zbiór odpowiednio usystematyzowanych i skoordynowanych przedsięwzięć organizacyjno-technicznych i eksploatacyjnych, zapewniających stabilną pracę środkom i systemom elektronicznym funkcjonującym

w warunkach kooperacji negatywnej wzajemnie. Właściwe zorganizowana i prowadzona może znacznie komplikować i utrudniać przeciwnikowi zdobywanie danych o charakterystykach środków elektronicznych, ich właściwościach pracy, strukturze organizacyjnej, o zasadach działania i ugrupowaniu wojsk, ich wyposażeniu w sprzęt bojowy oraz możliwościach i gotowości bojowej. Ponadto może też uniemożliwiać lub utrudniać ustalenie rzeczywistego rozmieszczenia środków elektronicznych ich zasad pracy oraz uodporniać je niszczące zakłócenia. Przedsięwzięcia ochronne winny być ukierunkowywane przeciwko:

- rozpoznaniu elektronicznemu,
- zakłócaniu elektronicznemu,
- niszczeniu ogniowemu środkami naprowadzanymi na źródła promieniowania elektromagnetycznego,
- oddziaływaniu kierunkową energią elektromagnetyczną.

Winna także uwzględniać przedsięwzięcia eliminujące wzajemne zakłócanie się systemów dowodzenia, kierowania i łączności, wynikające z wykorzystywania spektrum elektromagnetycznego przez własne środki radioelektroniczne, w tym samym czasie i przestrzeni.

(1) Ochrona semantyki informacyjnej winna obejmować odpowiednie przedsięwzięcia i działania przeciwrozpoznawcze uniemożliwiające i utrudniające zdobywanie danych o własnych systemach elektronicznych. Szczególnie, winna się koncentrować na ukrywaniu pracy nadawczych środków elektronicznych i wykorzystywanych nośników informacji. Przeciwdziałanie rozpoznaniu powinno być uwzględniane nie tylko podczas eksploatacji urządzeń elektronicznych, ale także w okresie planowania działań. W systemach dowodzenia i kierowania wojsk funkcjonuje wiele różnorodnych i odrębnych elementów, które – wypełniając różne funkcje – wymagają korzystania również i z różnych środków techniki (radiowej, radiolokacyjnej, radionawigacyjnej, optoelektronicznej, kablowej, informatycznej itp.). Środki te wymagają odpowiednio zróżnicowanej ochrony, gdyż funkcjonują w warunkach dostępności dla systemów rozpoznania elektronicznego przeciwnika. Uwzględniać przy tym należy, że:

- „Dostępność elektromagnetyczną" środków radiowych jest uzależniona od warunków energetycznych, tzn. wymaganego stosunku poziomu sygnału do szumu na wejściu urządzenia odbiorczego. Środki radiowe są dostępne elektromagnetycz-

nie w określonym obszarze, który nazywa się „strefą dostępności elektromagnetycznej". Głębokość tej strefy zależy przede wszystkim od: mocy w łączu radiowym tworzonym przez nadajnik i urządzenie rozpoznawcze lub odbiornik przeciwnika, rodzaju modulacji, anteny nadawczej i odbiorczej urządzenia rozpoznawczego, a także od długości fali nośnej, jej polaryzacji oraz właściwości elektrycznych gruntu na trasie między źródłem emisji i środkiem rozpoznawczym.

- Dostępność czasowa środków radiowych warunkowana jest czasami trwania seansów radiowych oraz intensywnością wymiany korespondencji radiowej. Jest ona wprost proporcjonalna do wielkości tych składowych.
- Dostępność „oznakowa" i „strukturalna" warunkowana jest istnieniem cech demaskujących pracę środków i systemów elektronicznych. Cechy te umożliwiają organom rozpoznania elektronicznego identyfikowanie sygnałów emitowanych przez te środki, a poprzez to ich lokalizację oraz określenie składu sieci (linii) radiowych i węzłów łączności oraz ich przynależności do szczebla dowodzenia.
- Dostępność semantyczna uwarunkowana jest stopniem utajnienia wiadomości przekazywanych w systemach elektronicznych.

Uogólniając powyższe można stwierdzić, że obronę systemów elektronicznych przed rozpoznaniem należy ukierunkowywać na ograniczanie do niezbędnego minimum dostępności elektromagnetycznej, czasowej, oznakowej, strukturalnej i semantycznej bezprzewodowych środków i urządzeń teletransmisyjnych w strefach i sektorach niepożądanych. Istota działań w tym zakresie polega na ochronie urządzeń nadawczych promieniujących energię elektromagnetyczną oraz na ochronie treści znaczeniowej (informacji) zawartej w tej energii. Do obiektów elektronicznych szczególnie wrażliwych i najmniej odpornych na rozpoznanie, a następnie zakłócanie. należą systemy: radiowe krótkofalowe, radiolokacyjne i radionawigacyjne. Większą odporność posiadają systemy radiowe ultrakrótkofalowe malej mocy i systemy radioliniowe. Najwyższą odporność posiadają natomiast systemy kablowe (przewodowe, światłowodowe) i informatyczne.

Zakres i sposób realizacji zadań ochronnych jest zróżnicowana. Należy ją inaczej postrzegać w okresie przygotowywania walki i inaczej w toku prowadzenia.

W okresie przygotowania walki ochrona semantyki informacyjnej, przed rozpoznaniem i zakłócaniem elektronicznym przeciwnika. winna być organizowana poprzez:

- opracowanie odpowiednich dokumentów dla poszczególnych systemów i środków elektronicznych;
- wypracowanie odpowiedniej koncepcji prowadzenia działań ochronnych uwzględniających:
  - przydział stosownych częstotliwości roboczych, zabronionych i zastrzeżonych,
  - czas pracy środków elektronicznych,
  - sposoby i zmiany rodzajów pracy,
  - sposobów i okoliczności wykorzystywania rezerwowych środków i kanałów łączności;
- tworzenie elementów pozornej sytuacji elektronicznej w rejonie walki, ściśle skoordynowanej z ogólnym planem maskowania;
- określenie sygnałów ostrzegania i przedsięwzięć do natychmiastowego wykonania.

W toku prowadzenia walki ochrona przed rozpoznaniem i zakłócaniem elektronicznym winna polegać na wykonywaniu przedsięwzięć zawartych w uprzednio opracowanych planach.

Ochrona semantyki informacyjnej w relacjach radiowych winna się głównie koncentrować na:

- ograniczaniu cech demaskujących urządzeń nadawczych,
- ograniczeniu pracy środków radiowych do niezbędnego minimum,
- przestrzeganiu reżimów pracy i przepisów korespondencji radiowej,
- utajnianiu danych przekazywanych w sieciach i kierunkach radiowych.

Analizując cechy demaskujące pracę systemów elektronicznych, należy również zwracać uwagę na ich parametry techniczne. Bardzo skutecznym i coraz częściej wykorzystywanym sposobem przeciwdziałania wykryciu środków radiowych jest stosowanie, podczas pracy i wymiany informacji, sygnałów z rozproszonym widmem. Wynika to z faktu, że systemy szerokopasmowe posiadają następujące zalety:

- dostosowanie do selektywnego adresowania informacji,
- możliwość realizacji wielodostępu,
- małą widmową gęstość mocy utrudniającą wykrycie sygnału,
- możliwość maskowania informacji przed przechwyceniem,
- dużą odporność na zakłócenia interferencyjne,

- większą odporność na zaniki, co wynika z faktu, że sygnał zajmuje szerokie pasmo co przy zanikach selektywnych powoduje tylko utratę małej jego część.

Rozpraszanie widma sygnału w szerokim paśmie częstotliwości powoduje, że dzięki małej widmowej gęstości energii nadawanego sygnału są one trudne do wykrycia i przechwycenia. Łącząc to jeszcze ze złożonymi technikami modulacji i detekcji realizujących rozpraszanie widma i wykorzystujących pseudolosowe skoki częstotliwości nośnej, tworzą odmienne ciągi dla każdego użytkownika i tym samym umożliwiło nie tylko zwiększanie odporności na zakłócenia i efekty zaników w kanale, ale także umożliwiło wykorzystanie tego samego pasma częstotliwości przez wielu użytkowników jednocześnie. Wynika to prawa Clouda E. Shannona, o przepływności w kanale telekomunikacyjnym, że wraz ze zwiększaniem pasma sygnału zwiększa się jednocześnie przepływność w kanale, przy tym samym stosunku sygnału do szumu:

$$C = B\log\left(1+\frac{P}{N_0 B}\right)\ [bit/sekundę],$$

gdzie:

C – szybkość transmisji danych,

B – szerokość wykorzystywanego pasma,

P – średnia moc sygnału,

N_0 – moc widmowa szumu w torze transmisyjnym.

Zakłócenie pracy systemu, w którym informacja jest przesyłana za pomocą skokowo zmieniających się częstotliwości, nastąpi wtedy, gdy zostanie zakłócona każdą z tych częstotliwości, z mocą co najmniej równą mocy sygnału użytecznego przesyłanego na tej częstotliwości. W praktyce, bez dodatkowych usprawnień, system może pracować poprawnie nawet wtedy gdy zakłóconych zostanie mniej prawie połowa kanałów. Do technik tych należą urządzenia pracujące:

- W systemach DS (Direct Sequence), w których wykorzystywane jest zjawisko kluczowania fazy sygnału nośnego ciągiem pseudolosowym, różnym dla każdego z użytkowników.
- W systemach TH (Time Hopping), w których czas transmisji jest sterowany przez sekwencję kodową – tzn. sekwencja kodowa steruje włączaniem i wyłączaniem nadajnika. Dzięki temu możliwe jest uzyskanie zwielokrotnienia czasowego TDMA (Time Division Multiple Access). Taka postać sygnału, jako modulacji szerokopasmowej, znajduje zastosowanie głównie w powiązaniu z FH. Zasadniczą różnicą

między FH a T-FH, w kwestii rozdzielenia czasu trwania częstotliwości i zmian częstotliwości, jest to, że w systemach FH transmitowana częstotliwość zmienia się wraz z każdym kolejnym czasem trwania bitu kodu, podczas gdy w systemach T-FH częstotliwość może zmienić się tylko przy przejściu z zera na jeden w sekwencji kodowej.

- W systemach hybrydowych, które są uzupełnieniem wyżej wymienionych modulacji szerokopasmowych i oferują dodatkowe korzyści użytkowe dla technik DS i FH. Najbardziej użytecznymi formami systemów hybrydowych są połączenia modulacji FH i DS, TH i FH oraz TH i DS. Korzyścią z połączenia dwóch metod modulacji szerokopasmowych jest zazwyczaj to, że mogą być tworzone charakterystyki, które nie są możliwe do uzyskania w pojedynczych metodach modulacji.

Systemy szerokopasmowe powinny być wykorzystywane w systemach łączności i walki elektronicznej, ponieważ zmniejszają zagrożenie dla własnych środków i są trudne do wykrycia i przechwycenia zawartych w nich informacji.

Ochrona semantyki informacyjnej przed rozpoznaniem winna być jednym z podstawowych zadań ochrony systemów elektronicznych przed oddziaływaniem przeciwnika. Wszystkie systemy i środki elektroniczne wykorzystywane w czasie walki wymagają odpowiedniej, specyficznej osłony, w celu wyeliminowania lub ograniczenia dostępności sił i środków rozpoznania elektronicznego przeciwnika. Dzięki kontroli elektronicznej i stosowaniu szerokopasmowych systemów łączności powinno się wykrywać i usuwać wszystkie cechy demaskujące pracę środków elektronicznych.

Ochrona radiolokacyjna powinna polegać na osłonie własnych środków radiolokacyjnych przed rozpoznaniem i zakłócaniem przeciwnika. Urządzenia ostrzegające o opromieniowaniu radiolokacyjnym, umożliwiają:

- wykrywanie promieniowania w paśmie częstotliwości odpowiadających częstotliwości pracy pokładowych stacji radiolokacyjnych, radarów systemów rakietowych ziemia - powietrze i woda – powietrze,
- określanie typu radaru,
- określanie kierunku opromieniowania,
- określanie rodzaju pracy radaru,
- określanie przybliżonej odległości,
- rejestrowanie raportów z lotów operacyjnych, których analiza pozwala uzyskać informacje dotyczące parametrów odbieranych sygnałów radiolokacyjnych, dzięki

czemu istnieje możliwość aktualizacji biblioteki źródeł oprogramowania służącej do identyfikacji zagrożeń,

- ustalania częstotliwości nośne impulsów.
- ustalanie częstotliwość powtarzania impulsów
- ustalanie czasu trwania impulsów,
- ustalanie średniej mocy promieniowania,
- ustalanie kształtu impulsu,
- ustalanie rodzaju anteny,
- ustalanie sposobu przemieszczania wiązki.

Wszystkie te cechy sygnałów oraz dane samego radaru umożliwiają, poprzez porównanie z uprzednio wprowadzonymi do pamięci danymi, określenie jaki typ radaru opromieniował statek powietrzny. Nowoczesne radary mogą pracować w kilku różnych trybach, co powoduje znaczne utrudnienia w procesie ich identyfikacji. Ma to kluczowe znaczenie, w momencie, gdy radar przeciwnika przechodzi z trybu „poszukiwanie" w tryb „śledzenie" (odpowiednio zaprogramowany odbiornik jest w stanie poinformować o tym fakcie). Nowoczesne radary mogą też pracować jednocześnie w obu tych trybach, co może uniemożliwić ostrzeżenie pilota o fakcie „zablokowania" jego samolotu jako celu.

Urządzenia ostrzegające o odpaleniu pocisku rakietowego działają też w zakresie podczerwieni i ultrafioletu. Są to odbiorniki wykrywające specyficzne promieniowanie emitowane w tych pasmach przez silniki pocisków rakietowych na paliwo stałe (wyjątek stanowią niektóre pociski rakietowe „ziemia-powietrze"). Detektory podczerwieni wykrywają docierające do nich promieniowanie, które następnie jest analizowane w odbiorniku. Jeżeli wyniki tej analizy potwierdzają zgodność jego cech z promieniowaniem emitowanym przez silniki rakietowe na paliwo stałe, to odbiornik uruchamia sygnalizację świetlną i dźwiękową w kabinie samolotu. Może również przesyłać sygnały do urządzeń przeciwdziałania aktywnego i pasywnego, powodując ich zadziałanie.

Urządzenia ostrzegające o zbliżaniu się pocisku rakietowego działają również na zasadzie wykorzystania radaru dopplerowskiego. Impulsy wypromieniowane przez ten radar, po odbiciu się od zbliżającego się pocisku rakietowego, są odbierane przez odbiornik. Na podstawie zmiany częstotliwości sygnału odbitego w stosunku do sygnału wysłanego (efekt Dopplera). Odbiornik określa prędkość lotu wykrytego pocisku. Pozwala ona na odróżnienie wystrzelonego pocisku rakietowego od innych

obiektów latających. Inne dane uzyskane za pomocą radaru, takie jak: odległość wystrzelonej rakiety oraz jej azymut, są przesyłane z odbiornika na wskaźnik w kabinie pilota, umożliwiając podjęcie działań mających na celu uniknięcie trafienia samolotu. Poza sygnalizacją świetlną, informującą o odpaleniu pocisku rakietowego, załoga jest również informowana sygnałem dźwiękowym. Dodatkowo odbiornik może również sterować pracą środków pasywnego i aktywnego przeciwdziałania.

Funkcje ochronne mogą też spełniać laserowe odbiorniki ostrzegawcze znajdują się na wyposażeniu głównie śmigłowców bojowych. Ostrzegają one o opromieniowaniu przez odległościomierz laserowy, lub laserowe urządzenie wskazywania celu. Detektory tych urządzeń muszą jednak spełniać określone wymagania, które decydują o ich możliwościach wykorzystania bojowego. Powinny być zatem dostosowane parametrycznie do:

- odbierania bardzo słabych sygnałów w szerokim zakresie warunków oświetlenia zewnętrznego, z prawdopodobieństwem większym niż 0,95,
- odbierania i identyfikowania zarówno promieniowania w postaci fali ciągłej jak i impulsowego,
- odróżniania promieniowania laserowego od optycznej interferencji (szczególnie promieni słonecznych) w celu uniknięcia fałszywych alarmów,
- odbioru promieniowania w zakresie minimum 0,42.-.1,06) μm,
- rozdzielczości 3° w polu widzenia 90°.

W celach ochronnych mogą być też wykorzystywane tak zwane „elektroniczne zintegrowane tarcze ochronne (Elecronic Integrated Protestion Shield).

Ochrona optoelektroniczna winna się skupiać na stosowaniu osłon i filtrów szerokopasmowych.

Ochrona sensoryczna (czujnikowa) winna się koncentrować na ukrywaniu przed rozpoznaniem i zakłócaniem własnych detektorów, które wykorzystują energię odpowiadającą parametrami sygnałom bodźcowym, charakterystycznym dla środowiska akustycznego, magnetycznego, elektrycznego, chemicznego itp.

Niezmiernie ważną funkcję w ochronie semantyki informacyjnej spełnia maskowanie techniczne, realizowane w szerokim spektrum widma elektromagnetycznego. W tym zakresie winno się stosować:

- siatki maskujące,
- farby do malowania deformującego (farby na dyspersji alkidowej, poliuretanowej, farby rozpuszczalne w wodzie),

- zestawy do maskowania sprzętu bojowego,
- środki maskowania przeciwradiolokacyjnego,
- środki maskowania termalnego,
- piany maskujące,
- środki maskowania aktywnego (urządzenia ostrzegające o opromieniowaniu obiektu wiązką laserową lub radiolokacyjną, wyrzutnie środków dymnych, wyrzutnie substancji i ładunków emitujących energię cieplną, cele radiolokacyjne).

(2) Ochrona nośników informacji winna obejmować wszelkie przedsięwzięcia związane z osłanianiem emisji elektromagnetycznych przed destrukcyjnymi oddziaływaniami energetycznymi. Szczególnie trudnym przedsięwzięciem, wymagającym rozwiązań zarówno organizacyjnych jak i technicznych, jest neutralizowanie pracy nadajników zakłóceń jednorazowego użycia. W tym celu zespoły węzłów łączności powinny umieć je wykrywać, niszczyć lub neutralizować, bądź też wychodzić poza strefy ich skutecznego oddziaływania. Neutralizowanie nadajników może polega na ekranowaniu ich za pomocą, np. lekkich metalizowanych siatek, cienkich arkuszy folii aluminiowej lub kilku odpowiednio wysokich prętów metalowych wbitych w ziemię wokół poszczególnych nadajników, powoduje to natychmiastowe i skuteczne ograniczanie rozprzestrzeniania się energii elektromagnetycznej emitowanej przez te nadajniki. Czynność ta jest mniej czasochłonna niż ich niszczenie, gdyż nie wymaga angażowania wyspecjalizowanych sił i środków. Natychmiastowe i precyzyjne lokalizowanie nowo pojawiających się źródeł energii elektromagnetycznej w rejonie węzłów łączności winny zabezpieczać zautomatyzowane systemy pelengacyjne, które powinny rozróżniać sygnały pochodzące z nadajników zakłóceń jednorazowego użycia od sygnałów emitowanych przez własne nadajniki. Do eliminacji większych źródeł zakłócających winno się używać fizycznych środków niszczenia, znajdujących się w dyspozycji wojsk. Przedsięwzięcia ochronne winny też uwzględniać zabezpieczanie przed niekompatybilnością elektromagnetyczną pracy własnych systemów i środków elektronicznych, chroniąc je w ten sposób przed wewnętrznymi i zewnętrznymi zakłóceniami interferencyjnymi. Istotne znaczenie dla zapewniania kompatybilności elektromagnetycznej ma wybór miejsc pracy dla środków elektronicznych. Winno się przy tym uwzględniać właściwości terenu (ukształtowania, pokrycia i infrastruktury) z zamysłem zmniejszenia ewentualnych zakłóceń. Warunki te mogą wpływać na zmniejszenie gęstości mocy energii elektromagnetycznej w rejonie rozwijania środków elektro-

nicznych, w przypadku gdy znajdują się tam przeszkody typu: las, zabudowa, konstrukcje metalowe itp. Umiejętne wykorzystanie terenu pozwala obniżyć poziom wzajemnych zakłóceń lub całkowicie je wyeliminować. Zasadniczy wpływ na ich ograniczenie posiada rygorystyczne przestrzeganie normatywów odległości między środkami elektronicznymi, a zwłaszcza pomiędzy radiostacjami średniej mocy i stacjami radioliniowymi rozwijanymi w obrębie tego samego węzła łączności lub w sąsiednich rejonach.

(3) Ochrona procesów informacyjnych dotyczy głównie sieci informatycznych. Swym zasięgiem winna obejmować ochronę przed „wirusami", „koniami trojańskimi", „bombami logicznymi", „robakami" i „bakteriami". Podejmowane w tym zakresie przedsięwzięcia winny się koncentrować na:

- ciągłym kontrolowaniu dostępu, włączając w to szereg przedsięwzięć uniemożliwiających wniknie wirusów do systemu,
- wykrywaniu wirusów,
- lokalizowaniu wirusów i zapobieganiu rozprzestrzenianiu się ich,
- niszczeniu (usuwaniu) wirusów,
- odbudowywaniu plików z danymi, jeśli wirusowi udało się je znacznie uszkodzić,
- stosowaniu „rezerw operacyjnych", uwzględniających warianty operacji z pominięciem uszkodzonego systemu.

Realizacja przedsięwzięć ochronnych wymaga przyjęcia właściwej ostrożności odnoszącej się do hardwaru i softwaru, a także ścisłego przestrzegania zasad eksploatacyjnych. W ramach tego winno się uwzględniać:

- ścisłą kontrolę dostępu do urządzeń z centralnymi procesorami i programami.
- śledzenie pracujących programów,
- ograniczenia w łączeniu systemów operacyjnych,
- wykorzystywanie programów antywirusowych do likwidacji wirusów w zainfekowanych programach,
- przeładowywanie programów zabezpieczających, w celu ich „dezynfekcji",
- zapewniania ścisłego przestrzegania zasad maskowania radiowego,
- obserwowanie poprawności pracy systemu,
- przeciwdziałania zapobiegające rozprzestrzenianiu się wirusów,
- poddawanie zainfekowanych obiektów kwarantannie,
- opracowywania rezerwowych planów eksploatacji..

Sieci informatyczne, bez odpowiednich zabezpieczeń i mechanizmów ochronnych, narażone są na penetrację i dostęp do ich baz danych, a zgromadzone w nich zasoby danych, stają się obiektami rozpoznania, modyfikacji lub zniszczenia. Włączanie się do nich nieupoważnionych użytkowników jest stosunkowo łatwe i dalece prawdopodobne.

Fizyczną ochronę sieci i systemów teleinformatycznych należy zapewniać poprzez:

- umieszczanie urządzeń w odpowiednich strefach bezpieczeństwa uwzględniając przy tym: klauzulę tajności, ilości informacji niejawnych oraz zagrożenia w zakresie ujawnienia, utraty i modyfikacji przez osoby nieuprawnione,
- instalację środków zabezpieczających pomieszczenia przed nieuprawnionym dostępem, podglądem i podsłuchem.

Elektromagnetyczną ochronę sieci i systemów teleinformatycznych winno się stosować w celu uniemożliwienia przejęcia informacji zawartej w ubocznym promieniowaniu elektromagnetycznym urządzeń wytwarzających, przetwarzających, przechowujących i przesyłających informacje niejawne. Osiąganie tego winno się zapewniać poprzez:

- umieszczanie urządzeń, połączeń transmisyjnych, linii zasilających i sygnałowych w strefach bezpieczeństwa, gwarantujących spełnianie wymagań zabezpieczenia elektromagnetycznego,
- stosowanie urządzeń, połączeń transmisyjnych, linii zasilających i sygnałowych o obniżonym poziomie emisji,
- ekranowanie urządzeń oraz filtrowanie zewnętrznych linii zasilających i sygnałowych.

Wytwarzanie i przekazanie informacji niejawnych winno się odbywać za pośrednictwem systemów i sieci teleinformatycznych, które składają się z certyfikowanych urządzeń i narzędzi kryptograficznych. Ochrona ta winna uwzględniać:

- szyfrowanie informacji,
- stosowanie mechanizmów kryptograficznych gwarantujących integralność i zabezpieczenie przed nieuprawnionym ujawnieniem informacji,
- uwierzytelnianie podmiotów;
- uwierzytelnianie informacji,

- precyzyjną i ciągłą kontrolę uzasadnionego dostępu do systemu i sieci teleinformatycznej wytwarzających, przetwarzających, przechowujących i przekazujących informacje niejawne,
- kompleksową i spójną organizację wszelkich zabezpieczeń, adekwatną do wartości zasobów informacyjnych i możliwych zagrożeń.

Przedsięwzięcia organizacyjne, nazywane również administracyjnymi, powinny zawierać określone reguły postępowania, a w szczególności:

- regulacje prawne w zakresie ochrony kryptograficznej,
- przepisy dotyczące organizacji i funkcjonowania służb ochrony systemów,
- normy w zakresie bezpieczeństwa systemów teleinformatycznych,
- zasady dostępu osób korzystających z zasobów sieci komputerowych,
- zbiory procedur i algorytmów postępowania w celu odtworzenia systemów po awariach i dekonspiracji.

Działania na informacjach niejawnych powinny się odbywać tylko w miejscach do tego przystosowanych, zabezpieczonych przed fizycznym dostępem dla osób nieuprawnionych. Praktycznie w każdej jednostce i sztabie, gdzie wykonuje się działania na informacjach niejawnych, powinny być zorganizowane odpowiednio wyposażone stanowiska pracy. Takie stanowiska powinny być wyposażone w sprzęt komputerowy spełniający wymogi norm krajowych[1], lub sprzęt wykonany w technologii zgodnej ze stosownymi wymoganimi. Dla takiego stanowiska należy m.in. zorganizować:

- strefy ochronne oraz nadzór pomieszczeń i sprzętu (karty magnetyczne, telewizja przemysłowa, rejestracja ruchu osób),
- ochronę przed dostępem do informacji (selektywny dostęp do informacji dla poszczególnych użytkowników przez wprowadzenie zakresu uprawnień i haseł dostępu).

Ważną rolę powinno też odgrywać zabezpieczenie personalne obejmujące:

- odpowiedni dobór kadr,
- certyfikaty bezpieczeństwa,
- okresowe sprawdzanie umiejętności fachowych.

W ramach przedsięwzięć technicznych ważną rolę powinna odgrywać programowa ochrona danych. Systemy zabezpieczeń powinny być budowane w oparciu o

[1] Norma Polska PN-92 T-20001/02 pt. ,Współdziałanie systemów otwartych (OSI). Podstawowy model odniesienia. Architektura zabezpieczeń".

komputerowe programy ochronne, będące z zasady integralnym elementem systemu operacyjnego. Powinny chronić przed nieuprawnionym dostępem do sieci i ich fragmentów.

SKOROWIDZ NOWEJ TERMNOLOGII

Czysta postać informacji	Semantyka nieoznaczona bytująca w ludzkim umyśle bez przypisanego jej identyfikującego znaku językowego – synonim informacji potencjalnej.....	43
Dane	Elementarne treści znaczeniowe (fizyczne i semantyczne), przyjmowane za podstawę w szerszych zestawieniach procesowych i semantycznych.....	58
Decyzja (jako rzecz)	Postanowienie lub rozstrzygnięcie, zawierające zbiór dezyderatów i ustaleń zmierzających do osiągnięcia owego postanowienia lub rozstrzygnięcia.....	73
Dezinformacja bezpośrednia (recepcyjna)	Celowo zniekształcona struktura sytuacyjna, znajdująca się w zasięgu bezpośredniej dostępności recepcyjnej dla obserwatora.....	133
Dezinformacja pośrednia (sensoryczna)	Celowo zniekształcona struktura sytuacyjna, znajdująca się poza zasięgiem bezpośredniej dostępności recepcyjnej dla obserwatora.....	134
Engram semantyczny	Ślad pamięciowy treści wyobrażeniowej spowodowany zewnętrznym lub wewnętrznym doznaniem człowieka.....	43
Informacja	Nazwa treści doznań zmysłowych i umysłowych człowieka.....	47
Informacje decyzyjne	Treści semantyczne wyrażone znakami językowymi, odzwierciedlające wolę decydenta w określonej sprawie.....	86
Informacyjny	Człon kontekstowy nazwy, oznaczający rzeczy, stany, procesy i zjawiska związane z informacją i informowaniem.....	67
Informować	Przekazywać treści znaczeniowe, za pomocą etnicznych znaków językowych.....	41
Komunikacyjna postać semantyki	Engram semantyczny z przypisanym znakiem językowym identyfikującym jego postać – synonim semantyki oznaczonej.....	45
Quasi-informacja	Informatyczny znak językowy, dostosowany do przetwarzania w maszynach cybernetycznych.....	65
Relacja asocjacyjna	Związek pojęciowy występujący pomiędzy obrazem percepcyjnym i znakiem językowym symbolizującym ten obraz.....	40

Relacja informacyjna	Związek asocjacyjny występujący pomiędzy znakiem językowym i jego semantycznym interpretatorem.....	39
Relacja percepcyjna	Proces mózgowy transformujący doznania recepcyjne w obrazy percepcyjne.....	40
Relacja recepcyjna	Związek fizyczny występujący pomiędzy receptorem i przedmiotem poznania.....	40
Relacja rozpoznawcza	Związek refleksyjny występujący pomiędzy człowiekiem i dostrzeganym przez niego przedmiotem poznania.....	39
Relacyjna postać semantyki	Engram semantyczny zespolony ze znakiem językowym i nośnikiem materialnym znaku językowego.....	46
Semantyka nieoznaczona	Engram semantyczny bez przypisanego mu znaku językowego (tylko osobnicze wyobrażenie) – synonim informacji potencjalnej.....	43
Semantyka oznaczona	Engram semantyczny z przypisanym znakiem językowym identyfikującym jego postać – synonim komunikacyjnej postaci semantyki.....	45
Tresura naturalna	Gatunkowe naśladownictwo w świecie zwierząt, powodowane warunkami istnienia w określonych środowiskach.....	68
Tresura sztuczna	Ludzkie działanie, świadomie ukierunkowane na przyzwyczajanie zwierząt do wykonywania określonych czynności.....	68
Treści informacyjne	Treści semantyczne, występujące w relacjach informacyjnych.....	83
Treści rozpoznawcze	Treści recepcyjne i semantyczne, występujące w relacjach rozpoznawczych.....	83
Zasoby intelektualne	Zbiór osobniczych predyspozycji umysłowych, dostosowanych do poznawania istoty bytu.....	88
Zasoby ludzkie	Bogactwo człowieka, objawiające się przez wszystko co wypełnia jego wnętrze umysłowe, fizjologiczne i fizyczne.....	87
Zasoby mentalnościowe	Zbiór swoistych sposobów osobniczego myślenia i ustosunkowywania się do rzeczywistości.....	88
Zasoby pojęciowe	Zbiór myślowych odzwierciedleń, całościowych ujęć istotnych cech przedmiotów, rzeczy i zjawisk.....	87

Zasoby sprawnościowe	Zbiór predyspozycji osobniczych do wykonywania określonych czynności fizycznych i umysłowych.....	88
Zasoby umiejętnościowe	Zbiór predyspozycji osobniczych do transformowania wiedzy w praktyczne zastosowania.....	88
Źródło informacji	Człowiek przekazujący treści znaczeniowe, za pomocą etnicznych znaków językowych.....	53

WYKAZ RYSUNKÓW I TABEL

Rysunki

1. Zasadniczy związek przyczynowo-skutkowy występujący w procesie powstawania środowiska informacyjnego i środowiska wiedzy..... 10
2. Procedura postępowania przy nadawaniu nazw wyodrębnionym pojęciom..... 14
3. Obraz konotacyjny zasadniczych elementów oddziaływania..... 15
4. Zobrazowanie pojęciowej interpretacji terminu „kierowanie" wg T. Pszczołowskiego..... 16
5. Zobrazowanie pojęciowej interpretacji terminu „kierowanie" wg L. Pasiecznego i innych..... 18
6. Związek funkcjonalny kierowania z zarządzaniem..... 19
7. Zobrazowanie pojęciowej interpretacji terminu „kierowanie" wg J. Kurnala..... 19
8. Uogólniona struktura kierowania..... 21
9. Ogólny podział wpływów (oddziaływań) kierowniczych..... 23
10. Ogólny podział fizycznych wpływów (oddziaływań) kierowniczych..... 24
11. Ogólny podział niefizycznych wpływów (oddziaływań) kierowniczych..... 25
12. Ogólny podział sterowniczych wpływów (oddziaływań) kierowniczych..... 26
13. Sterowanie pracą zestawu komputerowego..... 27
14. Ogólna kategoryzacja czynników sprawczych kierowania..... 28
15. Dendryt kierowania..... 30
16. Szkic sytuacyjny obrazujący powstawanie informacji..... 35
17. Szkic sytuacyjny obrazujący powstawanie informacji i proces informowania..... 36
18. Schemat powstawania informacji i informowania..... 38
19. Klasyczny model definicji realnej..... 39
20. Szkic obrazujący powstawanie engramów semantycznych (semantyki nieoznaczonej)..... 42

21. Szkic obrazujący przetwarzanie indukcyjno-dedukcyjne..... 44

22. Komunikacyjna postać semantyki..... 44

23. Relacyjna postać semantyki..... 46

24. Trójkąt semantyczny..... 51

25. Diagramy obrazujące tworzenie informacji i informowanie..... 53

26. Układy oryginałów i ich modeli w relacjach rozpoznawczych i informacyjnych..... 57

26. Szkic obrazujący funkcje logiczne bramek w przetwarzaniu danych binarnych..... 59

27. Cyfrowy obraz kodu wektorowego w układzie ósemkowym i szesnastkowym..... 60

28. Prądowy obraz kodu wektorowego odwzorowywanego w „maszynie cybernetycznej..... 60

29. Usytuowanie informacji w stosunku do „maszyny cybernetycznej..... 62

30. Model funkcjonalny komputera..... 63

31. Szkic obrazujący reakcje człowieka i zwierzęcia na oddziaływanie bodźca wzroku..... 66

32. Podstawowe nazewnictwo i zasadniczy podział definicji (wg terminologii stosowanej w logice)..... 73

33. Struktura przedmiotowa (rzeczowa) decyzji „realnej wyraźnie”..... 74

34. Zobrazowanie zmienności stanu otoczenia decyzyjnego S w czasie Δt 76

35. Zobrazowanie amplitudy odchyleń operacyjnych i taktycznych od strategicznej linii celu..... 77

36. Lokalizacja człowieka (jako obiektu kierującego) w prakseologicznym modelu (układzie) działania celowego..... 81

37. Model strukturalno-funkcjonalny potrzeb decyzyjnych..... 83

38. Hierarchia potrzeb ludzkich wg Abrahama Maslowa..... 86

39. Relacyjne powiązania zasobów ludzkich..... 91

40. Kształtowanie ufności informacyjnej podczas realizacji postanowień decyzyjnych..... 95

41. Algorytm kształtowania przekonań mentalnościowych w procesie realizacji postanowień decyzyjnych ... 97

42. Graficzna interpretacja prawdopodobieństwa warunkowego ... 102

43. Zagrożenia informacyjne ... 109

44. Diagram obrazujący dezinformację recepcyjną (bezpośrednią) ... 133

45. Diagram obrazujący dezinformację sensoryczną (pośrednią) ... 134

46. Podział walki elektronicznej ... 136

47. Podział rozpoznania elektronicznego ze względu na dostosowanie techniczne ... 142

48. Widma sygnałów, z klasycznymi modulacjami 2FSK ... 146

49. Widma sygnałów z klasycznymi modulacjami 2PSK ... 147

50. Przelot czterech kanałów informacyjnych w jeden strumień informacyjny ... 147

51. Podział aktywnego przeciwdziałania elektronicznego ... 176

52. Podział przeciwdziałania elektronicznego ... 178

53. Podział bezpieczeństwa i ochrony informacyjnej w sieciach teleinformatycznych ... 203

T a b e l e

1. Wybrane przykłady pojęciowych interpretacji terminu „informacja" ... 11

2. Pojęciowa interpretacja terminu „informacja" ... 47

3. Model wyboru wariantu decyzyjnego ... 101

4. Zestawienie kalkulacyjne dotyczące wyboru decyzji bez korzystania z dodatkowych informacji o stanach otoczenia zewnętrzne ... 104

5. Aprioryczna identyfikacja stanów otoczenia decyzyjnego ... 105

6. Aprioryczna i aposterioryczna identyfikacja stanów otoczenia zewnętrznego ... 106

7. Zestawienie umożliwiające szacowanie korzyści wynikających z posiadania dodatkowych informacji o stanach otoczenia zewnętrznego występujących podczas realizacji postanowień decyzyjnych ... 107

BIBLIOGRAFIA

Ajdukiewicz K.,
„Zarys logiki", PZWS, Warszawa 1959

Bertalanffy L.,
„Ogólna teoria systemów (podstawy, rozwój, zastosowania)", PWN, Warszawa 1984.

Chomsky N. A.,
„Syntactic Structures", The Hague/Paris, Mouton 1957.

Ciborowski L.,
„Walka informacyjna", Europejskie Centrum Edukacyjne", Toruń 1999.

Ciborowski L.,
„A wszystko rozpoczęło się od świecącej rurki i wyobrażeń Rzymian..." (manuskrypt monografii), Warszawa 2009.

Fayol H.,
„Administracja przemysłowa i ogólna", Poznań 1947.

Couffignal L.,
„La Cybernetique", Pressem Universitaires de France, Paris 1963.

Couffignal L.,
„Les machines a penser", Les Editions de Minuit, Paris 1964.

Duncan C.
„IPTV Ltd. – Edinburgh, Part 2/5:The state of the art in communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband ultilanguage leased or common carrier systems, and its applicability to COMINT targetting and selection, including speech recognition, STOA Programme", European Parliament, EP/IV/B/STOA/98/1401.

Epstein E. J.,
,,Postęp", SCRIPTAMENENT, 1993.

Festinger L.,
„Teoria dysonansu poznawczego (A Theory of Cognitive Dissonance, wyd. 1957)", PWN, Warszawa 2007.

Flechtner H. J.,
„Grundbegriffe der Kybernetik", Wissenschaftliche Verlagsgesellschaft M.B.H., Stuttgart 1967.

Gramar M.L., Pratt S.R.,
„Computer virus countermeasures – a new type of EW", Defence Electronices 1990.

Greniewski H.,
„Elementy cybernetyki sposobem niematematycznym wyłożone", PWN, Warszawa 1959.

Greniewski H.,
„Sprawy wszystkie i jeszcze inne (o logice i cybernetyce)", KiW, Warszawa 1970.

Grzybowski M.,
„Posterunek radiolokacyjny, podstawowy komponent bojowy Wojsk Radiotechnicznych WLOP", Przegląd WLOP, sierpień 2003.

Hume D.,
„Badania dotyczące rozumu ludzkiego", De Agostini Polska Sp. z o.o., Warszawa 2001, [Printed in Spain przekładu: J. Łukasiewicza i K. Twardowskiego, „An enquiry concerning Human Understanding", Wydawnictwa Polskiego Towarzystwa Filozoficznego (wydanie 2), Lwów 1919].

Kempisty M. (redakcja),
„Mały słownik cybernetyczny", WP, Warszawa 1973.

Kietliński R., „Aspekty problemu podejmowania decyzji personalnych", art. w Zeszycie Naukowym Uniwersytetu Łódzkiego nr 61, s. 55, UŁ, Łódź 1969.

Kopaliński W.,
„Słownik wyrazów obcych i zwrotów obcojęzycznych (wydanie dziewiąte)", WP, Warszawa 1975.

Kotarbiński T.,
„Traktat o dobrej robocie (wdanie siódme)", Ossolineum, Wrocław·Warszawa·Kraków·Gdańsk·Łódź, 1982.

Kozaczuk W.,
„Wojna w eterze", Wydawnictwo Radia i Telewizji, Warszawa 1977.

Kurnal J.,
„Zarys teorii organizacji i zarządzania", PWE, Warszawa 1970.

Kwiatkowski T.,
„Wykłady i szkice z logiki ogólnej", UMCS, Lublin 2002.

Marciszewski W. (redakcja), Kotarbiński T. (konsultacja),
„Mała encyklopedia logiki", Zakład Narodowy im. Ossolińskich, Wrocław – Warszawa – Kraków 1970.

Maslow A.,
„Motywacja i osobowość", PWN, Warszawa 2006.

Mates M.,
„Technology and Terrorism", Draft inter Report for Sub-Committee on Proliferation of Military Technology, 2001.

Mazur M.
„Jakościowa teoria informacji", WNT, Warszawa 1970.

Morton A.,
„Przewodnik po teorii poznania", Spacja, Warszawa 2002.

Morzys O.W.,
„Wirtualnyj terrorizm – realnoct naszego wremeni – Zaszczita informatii", Konfident, Janwar-aprel 1999.

Ogden C.K., Richards I.A.,
„The Meaning of Meaning: A Study of the Influence of Languaage upon Thought and of the Science of Symbolism", Harcout, Brace & World, New York 1946.

Omyła M.,
„Zarys logiki", Wydawnictwa Szkolne i Pedagogiczne, Warszawa 1995.

Pasiecznego L. (redakcja),
„Encyklopedia organizacji i zarządzania", PWE, Warszawa 1982.

Perunow J.M., Fomiczew K.I., Juin L.M.,
„Radioelektronnoje podawlenie informacjonnych kanałow sistem uprewlenia orurziem", Radiotiechnika, Moskwa 2003

Pieniak. J.,
„Określenie kryterium wiarygodności rozpoznania radiowego" (projekt publikacji do Zeszytu Naukowego AON}, Warszawa 2005.

Pieniak J.,
„Prowadzenie rozpoznania elektronicznego w ramach walki informacyjnej", Sesja Naukowa 100. rocznicy urodzin Mariana Rajewskiego, Warszawa 2005.

Pszczołowski T.,
„Mała encyklopedia prakseologii i teorii organizacji", Zakład Narodowy imienia Ossolińskich, Wrocław – Warszawa – Kraków – Gdańsk 1978.

Rybarczyk M.,
„Ślepe ucho Pentagonu", Przekrój z 29.12.2005.

Sadowski W.,
„Decyzje i prognozy", PWE, Warszawa 1977.

Scheffs W.,
„Rozpoznanie informatyczne nową płaszczyzną prowadzenia walki elektronicznej", Automatyzacja Dowodzenia, Warszawa 2003.

Sokołowski S. J.,
„Logika w dowodzeniu i kierowaniu", Wydawnictwo MON, Warszawa 1972.

Supernat J.,
„Techniki decyzyjne i organizatorskie (wydanie 2)", Limited, Kolonia 2003.

Sun Zi,
„Sztuka wojny (przekład K.A.M.)", Przedświt, Warszawa 1994.

Toffler Alvin i Heidi,
„Trzecia fala", PIW, Warszawa 1997.

Wiener N.,
„Cybernetyka, czyli sterowanie i komunikacja w zwierzęciu i maszynie", PWN, Warszawa 1971.

Wiener N.,
„Cybernetyka i społeczeństwo", K i W, Warszawa 1960.

Vernon E., „Information War and International Security", Report for Committee General NATO, 285 STC (99) 81, 1999.

Zieleniewski J.,
„Organizacja i zarządzanie (wydanie III)", PWN, Warszawa 1969.

