BEZPIECZEŃSTWO 2009 nr 3–4 TEORIA I PRAKTYKA

Andrzej Żebrowski, Magdalena Mielus

Zagrożenia dla bezpieczeństwa informacji i wiedzy w organizacji

Wprowadzenie

Dostęp do określonych informacji, a także umiejętność ich wykorzystywania umożliwia kontrolowanie nie tylko człowieka, ale i jego środowiska. Informacja powinna zawsze być postrzegana w kategoriach dobra strategicznego – wartego zarówno podboju, jak i destrukcji. Informacja zasila i wspiera wiedzę, która jest wykorzystywana we wszystkich obszarach działania organizacji.

Informacja wywiera istotny wpływ na poziom wiedzy odbiorcy, a w rzeczywistości całej organizacji. Informacje i wiedza dotyczące określonych sfer działalności organizacji były i są przedmiotem zainteresowania nie tylko rzeczywistego przeciwnika. Ich ochrona przed ujawnieniem wobec osób nieuprawnionych stanowi jeden z kluczowych problemów funkcjonowania organizacji rządowych, jak i pozarządowych.

„Możliwość dostępu praktycznie do każdego rodzaju i treści informacji generuje różnorodne zagrożenia. Jedne z najistotniejszych to możliwość przypadkowego ujawnienia bądź celowego pozyskania informacji prawnie chronionych. Zagrożenia dla informacji i wiedzy mają charakter ponadczasowy. Ten obszar zagrożeń zawsze towarzyszył ludzkiemu działaniu. Skala ich natężenia zależna jest od istniejących bądź pojawiających się sprzeczności”[1].

Współczesna ekspansja informacyjna stanowi broń obosieczną, co oznacza, że może zaatakować zarówno przeciwnika, jak i nas samych.

Środowisko narodowe i międzynarodowe organizacji jest coraz bardziej złożone i różnorodne, gdzie w obliczu postępu technologicznego staje się ona podatna na zagrożenia wewnętrzne i zewnętrzne. Uzasadnia to konieczność podejmowania kompleksowych i wzajemnie powiązanych przedsięwzięć natury prawnej i organi-

[1] *Bezpieczeństwo informacyjne III Rzeczypospolitej*, red. A. Żebrowski, Kraków 2000, s. 7.

zacyjnej pozwalających na utrzymanie integralności własnych systemów informacyjnych i systemów informatycznych, ich ochrony przed nieuprawnionym dostępem i destrukcją. Działaniom tego typu muszą towarzyszyć analogiczne czynności ukierunkowane na przeciwnika oraz osiąganie przewagi informacyjnej w procesie zarządzania organizacją.

Informacje i wiedza stanowią zasoby, które decydują o rozwoju każdej organizacji, dlatego wymagają szczególnego zainteresowania ze strony uprawnionych podmiotów zarówno w aspekcie ich budowania, jak i ich bezpieczeństwa.

Celem niniejszego opracowania jest zwrócenie uwagi na problematykę dotyczącą bezpieczeństwa informacji i wiedzy, ze szczególnym wskazaniem na zagrożenia.

Informacja jest użyteczną wiedzą

Każda współczesna organizacja[2] (państwo, korporacja, zespół) funkcjonuje w określonym środowisku wewnętrznym i zewnętrznym, które jest złożone i nieprzewidywalne, przez co ustawicznie narażona jest na ryzyko.

We współczesnym świecie równowaga między państwami uprzemysłowionymi [...] będzie powstawała poprzez stały i rozprzestrzeniony konflikt geoekonomiczny, toczony na poziomie światowym pomiędzy tworzącymi się obecnie biegunami geoekonomicznymi oraz – na poziomie regionalnym – wewnątrz każdego z biegunów, gdzie każde państwo będzie starać się zwiększyć własną konkurencyjność dla uzyskania większego bogactwa, a także zwiększenia dobrobytu własnych obywateli[3]. Zatem w świetle geoekonomii fundamentalnym problemem we współczesnym świecie staje się międzynarodowa konkurencyjność państw albo inaczej międzynarodowa zdolność gospodarki danego państwa do tworzenia bogactwa oraz możliwości zabezpieczenia owego bogactwa przed procesami deprecjacji oraz próbami ekonomicznego zawłaszczenia przez inne nacje[4].

Państwo jako organizacja społeczna charakteryzuje się aktywnością wewnętrzną i zewnętrzną, gdyż „każde państwo realizuje funkcję wewnętrzną i zewnętrzną oraz koncentruje swoją aktywność wokół zarządzania"[5]. Zachodzące w państwie (dotyczy to również innych organizacji) i jego otoczeniu zewnętrznym zmiany wymagają dla skutecznej realizacji swoich funkcji zasilania zarówno materialnego, energetycznego, jak i informacyjnego. Występujące relacje przybierają formę kooperacji pozytywnej (współpracy) i kooperacji negatywnej (walki). W stosunkach z innymi państwami (organizacjami) przedmiotem stymulacji są władze innych państw (organizacji), gdzie

---

[2] Organizacja (w znaczeniu czynnościowym, rzeczowym i atrybutowym – przyp. autora) „to pewien szczególny rodzaj stosunków części do siebie i do złożonej z nich całości; stosunek ten polega na tym, iż części współprzyczyniają się do powodzenia całości. T. Kotarbiński, *Traktat o dobrej robocie*, Wrocław – Warszawa 1958, s. 75 i 109; zob. też J. Zieleniowski, *Organizacja zespołów ludzkich. Wstęp do teorii organizacji i kierowania*, Warszawa 1976, s. 47–64; W. Kieżun, *Sprawne zarządzanie organizacją*, Warszawa 1997, s. 12–13; R.W. Griffin, *Podstawy zarządzania organizacjami*, Warszawa 2004, s. 5.

[3] E.N. Luttwak, *From Gropoltics to Geo-economics. Logic of Conflict, Grammar of Commerce, The National Interest*, 1990, s. 17–23; zob. też C. Jean, *Geopolityka*, Wrocław – Warszawa – Kraków 2003, s. 211.

[4] K. Kłosiński, *Konkurencyjność narodów*, [w:] *Losy świata*, red. K. Kłosiński, Lublin 2003, s. 13.

[5] K.A. Wojtaszczyk, *Kompendium wiedzy o państwie współczesnym*, Warszawa 1998, s. 12 i 22.

występuje informacyjne oddziaływanie na ich percepcję odbiorczą. Mogą one dotyczyć obopólnych (jednostronnych) korzyści, ewentualnych kosztów konfrontacji bądź porażki. Dlatego informacja i wspierana nią wiedza stają się podstawową bronią w walce między państwami, a także jest jedną z podstawowych form wspierania aktywności wewnętrznej państwa. Przekłada się to również na czynności innych organizacji bez względu na charakter prowadzonej działalności.

W tym aspekcie warto mieć świadomość tego, że przełom wieków to wiele zmian, które należy postrzegać w kategoriach rewolucyjnych stanowiących źródło zamieszania intelektualnego w wielu obszarach ludzkiego działania. Dotyczy to również zarządzania informacją i wiedzą w organizacjach.

Postępujące przyspieszenie rozwoju cywilizacyjnego w różnych obszarach działania człowieka to również większa skala i dynamika zmian. „Przeobrażenia, które w przeszłości trwały wieki lub dziesięciolecia, obecnie zachodzą w ciągu pojedynczych lat, a nawet wcześniej”[6]. Przekłada się to na szybkość komunikacji, dostęp do informacji, a w konsekwencji na posiadaną wiedzę.

Znajomość przyczyn zachodzących zmian zarówno pozytywnych, jak i negatywnych, tak w wymiarze wewnętrznym, jak i zewnętrznym wymaga informacji i wiedzy, co pozwala na ich zrozumienie, umiejscowienie w aktualnej rzeczywistości, wykorzystanie w procesie decyzyjnym i praktycznym działaniu.

Wiele podmiotów podejmuje wysiłki mające na celu minimalizowanie obszarów niepewności. Takie możliwości stwarza im informacja i właściwie kształtowana oraz wykorzystywana wiedza.

Wiedza to „płynna kompozycja ukierunkowanego doświadczenia, wartości, użytecznych informacji i fachowego spojrzenia, stwarzająca podstawy do oceny i przyswojenia nowych doświadczeń i informacji. Wiedza rodzi się i wzrasta w ludzkich umysłach. W organizacjach często jest zapisana nie tylko w dokumentach i bazach danych, lecz także w zwyczajach, normach i procedurach”[7].

Wiedza jest przedmiotem gospodarowania wiedzą[8], a proces tworzenia wiedzy w organizacji stanowi ogół specyficznych inicjatyw i działań, które organizacje podejmują w celu zwiększenia ilości wiedzy organizacyjnej[9]. Takie podejście oznacza, że nabywanie wiedzy ma ścisły związek z procesem uczenia się organizacji. Uczenie się to suma wiedzy cząstkowej, którą organizacja nabywa w procesie realizowania swoich zadań w określonym przedziale czasowym poprzez wyznaczenie strategii rozwoju.

Obok człowieka ważnym elementem wiedzy jest informacja, bez której jej systematyczne pomnażanie jest praktycznie niemożliwe.

Dla każdej organizacji ważny jest jej „potencjał informacyjny, przez który należy rozumieć wszelkie zasoby informacyjne (dane, informacje, wiedza), które tworzą infosferę określonego systemu działania (organizacji, instytucji). Ale także systemy informacyjne (informatyczne, telekomunikacyjne) niezbędne do efektywnego prowadzenia określonych, zamierzonych działań”[10].

---

[6] R. Szpyra, *Militarne operacje informacyjne*, Warszawa 2003, s. 8.

[7] Ch. Evans, *Zarządzanie wiedzą*, Warszawa 2005, s. 30.

[8] B. Mikuła, *Elementy nowoczesnego zarządzania. W kierunku organizacji inteligentnych*, Kraków 2001, s. 59.

[9] T. Davenport, L. Prusak, *Working Knowledge: How Organizations Mange What The Know*, Boston 1998.

[10] R. Szpyra, *Militarne operacje...*, *op. cit.*, s. 100.

„Bardzo często informacja kojarzona jest też z wiedzą. Na przykład w informatyce wiedzę traktuje się jako informację pozwalającą na wnioskowanie na podstawie konkretnej sytuacji lub konkretnych danych. Przy tym wiedza znacznie wykracza poza informacje, ponieważ implikuje zdolność do rozwiązywania problemów, rozumnego zachowania i działania. Wiedza umożliwia również ciągłe lub wybiórcze rozumowanie, a także wyciąganie, na podstawie zasobów informacyjnych, odpowiednich wniosków. Najczęściej tak pojmowaną wiedzę utożsamia się ze zbiorem reguł lub z tak zwaną bazą wiedzy, podczas gdy np. informacje utożsamia się z bazą danych lub z tak zwaną bazą faktów"[11].

Warto wskazać na ścisły związek informacji i człowieka „tak jak foton nie może istnieć bez pędu, tak informacja nie może istnieć bez umysłu ludzkiego. Tylko ten organ natury ludzkiej dostosowany jest do nieskończonego przetwarzania transformowanych doznań recepcyjnych w wyobrażenia informacyjne. [...] każda informacja jest szczególną formą sygnału, która oprócz wspólnych cech wyróżnialności, właściwych dla sygnału i informacji, posiada jeszcze tę właściwość, że inspiruje umysł ludzki do tworzenia pewnej wyobraźni"[12].

Charakterystyczne cechy odróżniające wiedzę od informacji wynikają m.in.:

a) z potrzeby człowieka (zarządzających państwem, korporacją, itp.), jaką jest „wiedzieć o czymś",
b) wiedzę tworzy się w teraźniejszości, patrząc jednocześnie w przyszłość,
c) dotychczasowa wiedza stanowi podstawę dla jej rozwoju (dla wiedzy nowej),
d) wiedza to wynik myślenia i doświadczenia,
e) wiedza należy do ludzi,
f) wiedza krąży w społeczeństwie wieloma kanałami.

Ponadto wiedza jest dynamiczna i zmienia się w czasie, jest dostępna i niejawna, szybko się dezaktualizuje, niekiedy trudno ją uchwycić, a przy braku umiejętności także wykorzystać.

Współcześnie wszystkie organizacje w trakcie realizowania swoich funkcji zarówno w otoczeniu wewnętrznym, jak i zewnętrznym mogą wykorzystywać posiadaną wiedzę, ponieważ[13]:

- sama wiedza może być produktem,
- umiejętność gromadzenia i wykorzystania wiedzy to podstawowa kompetencja organizacji,
- wiedza może strukturalizować się dzięki procesowi kodyfikacji, przykładowo w technologiach, kompetencjach pracowników, bazach danych, procedurach, dokumentacji organizacyjnej,
- wiedza może się zmaterializować w konkretne decyzje przekładane na działania,
- wiedza pozwala też na obniżanie poziomu niepewności w trakcie realizacji przedsięwzięć związanych z ryzykiem.

Wiedza traktowana jest również jako ogół wiadomości jednostki. Ponadto przyjmuje się, że wzrost wiedzy u jednostki to nie tylko ilościowy przyrost informacji, ale

[11] S. Antczak, *Zarządzanie zasobami informacyjnymi w siłach powietrznych*, „Myśl Wojskowa" 2002, nr 1, s. 46.

[12] L. Ciborowski, *Walka informacyjna*, Toruń 1999, s. 50.

[13] B. Mikuła, *Elementy nowoczesnego zarządzania*, *op. cit.*, s. 61–62.

podstawowa przyczyna reorganizacji wszystkich danych, jakimi ona dysponuje[14]. Wiedza to również wynik procesu myślenia związanego z dostępem do użytecznych informacji i posiadanych doświadczeń, którymi dysponuje człowiek.

Każdy człowiek nabywa wiedzę praktycznie przez całe życie, nie tylko w procesie indywidualnego kształcenia, ale przede wszystkim w procesie współdziałania z innymi. Oznacza to, że działalność organizacji ma ścisły związek z uczeniem się i stanowi nierozerwalną całość wszelkich zmian, jakie w niej występują.

Takie podejście pozwala postawić tezę, że wiedza zmienia się w sposób dynamiczny, a przy właściwym jej wykorzystywaniu pozwala zarządzającym organizacją na dostosowanie się do zmian, jakie występują w jej otoczeniu. Wiedza ma ścisły związek z informacją, bez której nie może się rozwijać. Dlatego należy ją w pierwszej kolejności wskazać i zidentyfikować, następnie pozyskać i przetworzyć tak, aby można było z niej korzystać.

Wiedza będzie stanowiła źródło przewagi nad przeciwnikiem tylko wówczas, gdy będzie systematycznie rozwijana, służyła nie tylko konkretnej organizacji, ale i społeczeństwu:

- z pomysłów rodzą się kolejne pomysły, a dzieląc się wiedzą, nie tracimy jej, wzbogacamy natomiast innych[15],
- pomysły to instrukcje, jak łączyć ze sobą ograniczone zasoby materialne w kombinację o coraz większej wartości[16],
- pomnażanie wiedzy oznacza tchnięcie nowego ducha w firmę (lub człowieka). Pomaga wyróżnić się z tłumu konkurentów[17].

Informacje, jakie znajdują się w bazach danych, pozwalają na analizowanie, ocenę i prognozowanie rozwoju sytuacji decyzyjnej w organizacji.

Zgromadzona w organizacji wiedza pozwala na zbudowanie uporządkowanych zbiorów dotyczących rzeczywistych i potencjalnych zagrożeń. Wynik poznawczy procesów informacyjnych w walce niezbrojnej (zbrojnej) w informacjach zwrotnych i wewnętrznych należy określić mianem obszaru wiedzy.

Dążenie do uzyskania przewagi informacyjnej zawsze towarzyszyło ludzkiemu działaniu. Przewaga informacyjna ma miejsce wówczas, gdy organizacja jest zdolna do gromadzenia, przechowywania, przetwarzania i przesyłania informacji w sposób ciągły, kodowania i dekodowania oraz posiada możliwości zakłócania analogicznych działań przeciwnika. W tym procesie ważne jest również bezpieczeństwo zasobów informacyjnych i wiedzy. Przewaga informacyjna, precyzyjne dane o obiektach oddziaływania są kluczem do odniesienia sukcesu w działalności organizacji. Dominacja nad konkurencją (przeciwnikiem – przyp. autora) we wszystkich stanach funkcjonowania organizacji, a także pokazanie swojej mocy to również jeden z przejawów przewagi informacyjnej[18].

Wartość zasobów informacyjnych (w tym i wiedzy) dla gracza jest funkcją następujących elementów:

---

[14] Szerzej: N. Sillami, *Słownik psychologiczny*, Katowice 1994, s. 321.

[15] T. Davenport, L. Prusak, *Working Knowledge: How Organizations Mange What The Know*, Boston 1998.

[16] *Ibidem*.

[17] A. Bird, *Careers as Repositories of Knowledge: A New Perspective on Boundaryless Careers*, „Journal of Organizational Behaviour" 1994, nr 15, s. 328.

[18] G. Nowacki, *Informacja w walce zbrojnej*, Warszawa 2002, s. 135.

- po pierwsze, czy dane zasoby są istotne dla zainteresowań i zobowiązań danego gracza,
- po drugie, możliwości danego gracza, tzn. wiedza, umiejętności i narzędzia pozwalające na skuteczne wykorzystanie posiadanych zasobów,
- po trzecie, dostępność danych zasobów dla danego gracza,
- po czwarte, dostępność dla innych graczy,
- po piąte, integralność zasobów,
- po szóste, czas, który oznacza to, że zasoby informacji wraz z jego upływem mogą nabierać wartości lub ją tracić.

Ta swoista walka o informacje jest prowadzona praktycznie w każdej dziedzinie, co szczególnie jest widoczne w sferze politycznej, gospodarczej, społecznej, naukowo-technicznej, religijnej i militarnej. Jej podstawowym celem jest zdobycie takich informacji, których nie posiada przeciwnik, wprowadzenie go w błąd, uzyskanie zaskoczenia, a w konsekwencji odniesienie sukcesu.

Należy mieć świadomość tego, że celem zdobywania informacji nie jest to, aby wiedzieć wszystko, lecz to, aby wiedzieć dostatecznie dużo, a zwłaszcza wiedzieć więcej niż przeciwnik, i to w określonym czasie.

Walka o informacje i wiedzę

Warunkiem skutecznego działania organizacji jest posiadanie efektywnego systemu zarządzania, odpowiedzialnego m.in. za efektywne zarządzanie zasobami organizacji. Chodzi zarówno o zasoby osobowe, jak również kapitałowe, materiałowe, energetyczne, techniczne i informacyjne, co w sumie przekłada się na zarządzanie wiedzą organizacji.

„W rezultacie pojawiają się rozmaite rodzaje walki: handlowa, finansowa, terrorystyczna, psychologiczna, przemytnicza (prowadząca do zachwiania rynku i ekonomicznego porządku), medialna (manipulowanie tym, co ludzie wiedzą i słyszą, dla kierowania nimi), narkotykowa (uzyskiwanie szybkich i znacznych nielegalnych profitów z rozprzestrzeniania katastrofy w innych krajach), informacyjna (w sieciach informacyjnych), technologiczna (tworzenie monopolu przez niezależne ustanawianie standardów), surowcowa (grabież zasobów i dóbr innych), fałszywa pomoc ekonomiczna (jawne obdarowywanie kogoś przy skrytym zdobywaniu nad nim kontroli), kulturowa (kreowanie i narzucanie trendów kulturowych w celu asymilowania tych, którzy reprezentują inny punkt widzenia), poprzez prawo międzynarodowe i inne, temu podobne”[19].

Podkreślić należy, że różnorodność form niemilitarnej, jak i militarnej wojny jest tak duża, że jest trudna do pełnego zidentyfikowania. Ma to szczególne znaczenie współcześnie, gdzie postęp technologiczny zwiększa sposoby prowadzenia walki. Ponadto istnieją możliwości stosowania mieszanych form walki, co wpływa na jej skuteczność.

„Pierwszym nowym obszarem intensywnie wyłaniającym się jest sfera informacyjna. We współczesnych warunkach rozwoju, wykorzystując tę sferę, podmiot bez żadnego przygotowania może zagrażać bezpieczeństwu organizacji. [...] Obecnie jednym

[19] R. Szpyra, *Militarne operacje...*, *op. cit.*, s. 11.

z nietradycyjnych obszarów walki jest nowa jakość wykorzystania sfery informacyjnej. Nowość ta polega głównie na tym, że informacja wykorzystywana była głównie do zasilania procesów decyzyjnych, teraz staje się dodatkowo środkiem walki, czyli bronią. W wyniku gwałtownego rozwoju technologicznego, szczególnie w obszarze elektroniki, pojawiło się głębokie uzależnienie od informacji, a w węższym znaczeniu – także od sieci komputerowych. W rezultacie zarówno w sferze praktyki, jak i w teorii pojawiła się walka informacyjna"[20].

Dla ludzkości, w tym dla kierujących organizacjami, cyberprzestrzeń jest nowym środowiskiem, które z jednej strony przyczynia się do naszego rozwoju, natomiast z drugiej stanowi poważne wyzwanie. Wyobraźmy sobie świat, gdzie informacja jest medium wymiany, a gotówka używana jest jedynie do zakupów podręcznych – świat, gdzie informacja, a nie język angielski, niemiecki, japoński czy rosyjski jest wspólnym językiem; świat, gdzie potęga wiedzy i informacji może uzurpować sobie siłę równą militarnej; świat całkowicie uzależniony od nowych narzędzi wysokiej techniki, która czyni informację dostępną permanentnie komukolwiek, gdziekolwiek, w każdym czasie; świat, gdzie ten, kto kontroluje informację, kontroluje ludzi; świat, gdzie elektroniczna prywatność już nie istnieje[21].

Idąc tym tokiem rozumowania, należy podkreślić, że w procesie rozwoju społeczeństw i ich politechnizacji codziennego życia, coraz większego znaczenia nabiera dysponowanie informacją, ale nie każdą, lecz ściśle wyselekcjonowaną. Z uwagi na to, że informacja jest dobrem, które pozwala na lepszy i bezpieczniejszy rozwój, dużą wagę przywiązuje się do jej zdobywania, przechowywania, przetwarzania, bezpieczeństwa (o czym wspominano) i dystrybucji dla uprawnionych podmiotów cywilnych i wojskowych.

Współczesne środowisko człowieka (organizacji) charakteryzuje się ogromnym wzrostem znaczenia technologii cyfrowych i komputerów, które są czynnikami łączącymi niemal wszystkie obszary działalności człowieka. Ośrodki przetwarzania informacji i łączności oparte na technologii cyfrowej pozwalają skrócić czas niezbędny do podjęcia decyzji, a następnie właściwych działań. Taki stan można osiągnąć, wykorzystując technikę teleinformatyczną na drodze sensor – centrum decyzyjne. Sensorem będą wszelkie źródła informacji o przeciwniku, natomiast centrum decyzyjne stanowią stanowiska, gdzie podejmowane są decyzje. Wykorzystywanie techniki teleinformatycznej pozwala na skrócenie czasu przepływu informacji (wewnętrznej drogi) między uprawnionymi podmiotami.

Według opinii niektórych teoretyków zajmujących się badaniem rozwoju cywilizacji, informacja jest tym czynnikiem, który stymuluje procesy związane z rozwojem i postępem. Informacja odgrywa również podstawową rolę w sposobie rozgrywania konfliktów zbrojnych i niezbrojnych w obszarze informacji, gdzie ma miejsce wspieranie wiedzy konkurencyjnej organizacji.

Istotą obecnej rewolucji technicznej dotykającej wszystkich obszarów działania człowieka jest koncepcja osiągnięcia zwycięstwa przez wykorzystanie instrumentów walki informacyjnej. Przyjmuje się, że technika informacyjna stanowi najważniejszą broń XXI w., której skuteczność oddziaływania porównuje się z bronią masowego ra-

[20] *Ibidem*, s. 11–12.

[21] R. Szpyra, *Militarne operacje...*, *op. cit.*, s. 89.

żenia. Należy zaznaczyć, że walka informacyjna traktowana jako broń informacyjna nie jest już zastrzeżona wyłącznie dla rządów, korporacji, służb specjalnych czy służb policyjnych. „Komputerowe i informacyjne bronie są dostępne z katalogów i sklepów. Te arsenały mogą być budowane przez hobbystów w domu. Oczywiście, siły zbrojne rozwijają swoje arsenały broni, którymi prowadzi się walkę informacyjną"[22].

Na wojnę informacyjną składają się działania, których celem jest ochrona, wykorzystanie, uszkodzenie, zniszczenie informacji lub zasobów informacji albo też zaprzeczenie informacjom po to, aby osiągnąć znaczne korzyści, jakiś cel lub zwycięstwo nad przeciwnikiem[23]. W innym ujęciu walka informacyjna to kooperacja negatywna wzajemna, przynajmniej dwupodmiotowa, realizowana w sferach: zdobywania informacji, zakłócania informacyjnego i obrony informacyjnej, gdzie każdemu działaniu jednej strony przyporządkowane jest działanie antagonistyczne strony drugiej[24].

W odniesieniu do walki zbrojnej „walka informacyjna składa się z działań podejmowanych dla zachowania integralności własnych systemów informacyjnych i ich ochrony przed eksploatacją, degradacją lub destrukcją, przy jednoczesnym eksploatowaniu, degradowaniu i destrukcji systemów informacyjnych przeciwnika oraz osiąganie przewagi informacyjnej w procesie użycia sił zbrojnych"[25].

Walka informacyjna może być również umieszczana między zimną wojną, obejmującą wojnę ekonomiczną, a wojną gorącą z wykorzystaniem broni konwencjonalnej (masowego rażenia). Podkreślić należy, że w porównaniu z wojną ekonomiczną, obliczoną na długotrwałe działania, wojna informacyjna może spowodować nie tylko naruszenie, ale i zniszczenie infrastruktury informacyjnej przeciwnika. Generalnie przyjmuje się, że wojna informacyjna to działania typu „sukces – porażka".

Walka informacyjna składa się z następujących przedsięwzięć:

- ataku informacyjnego, polegającego na zdobywaniu, przetwarzaniu i dystrybucji informacji o przeciwniku. W ramach tego procesu informacje muszą być wiarygodne, pełne, a ich transmisja powinna być selektywna i spełniać warunki aktualności,
- zakłócania percepcji odbiorczej przeciwnika,
- obrony informacyjnej przed atakiem informacyjnym przeciwnika.

Powyższe przedsięwzięcia wywierają zarówno bezpośredni, jak i pośredni wpływ na wiedzę organizacji (własnej i przeciwnika).

Celem nadrzędnym walki informacyjnej jest uzyskanie panowania nad przeciwnikiem w sferze informacyjnej. Oznacza to dążenie do stworzenia takiej sytuacji, gdzie zasoby informacyjne podmiotów zarządzających są aktualne, dokładne, pełne i wiarygodne, co zapewnia przewagę informacyjną nad przeciwnikiem i umożliwi realizowanie przyjętych zadań. Tak idealny stan jest praktycznie nie do osiągnięcia, jednak należy podejmować działania pozwalające na zrealizowanie przyjętych celów.

W tym miejscu warto zwrócić uwagę na naturę walki informacyjnej, która ma związek m.in. z: brakiem geograficznych, przestrzennych i politycznych granic; brakiem doraźnych granic; wielością obiektów ataku; anonimowością strony atakującej; powszechnym dostępem do technologii teleinformatycznych; niejasną odpowiedzial-

[22] *Ibidem*, s. 89.

[23] W. Schwartau, *Information Warfare*, Thunder s Mout Press, 1996, s. 12.

[24] L. Ciborowski, *Walka...*, *op. cit.*, s. 187.

[25] R. Szpyra, *Militarne operacje...*, *op. cit.*, s. 87.

nością; brakiem szybkich i skutecznych rozwiązań; niejasnymi regulacjami prawnymi; aktami kryminalnymi i wojnami.

W wojnie informacyjnej biorą udział nie tylko komputery i sieci komputerowe. Obejmuje ona informacje we wszelkiej postaci i przesyłane wszystkimi środkami, począwszy od ludzi i ich fizycznego środowiska do druków, telefonów, radia i telewizji, do komputerów i sieci komputerowych[26].

Wojna informacyjna to operacje skierowane przeciw treści informacji i operacje przeciw związanym z nimi systemom, włącznie z oprzyrządowaniem, oprogramowaniem i pracą człowieka[27].

„Przedmiotem bezpośredniej walki informacyjnej będzie zawsze człowiek traktowany jako element dowolnego systemu informacyjno-sterującego. W związku z powyższym przestrzeń bezpośredniej walki informacyjnej tworzy człowiek i wszelkie narzędzia, których użycie zespolone zostało z przedmiotem zainteresowania, warunkiem działania postrzeganego bezpośrednimi zmysłami tego podmiotu"[28]. Dlatego człowiek stanowi poważne zagrożenie dla systemu informacyjnego organizacji, jej wiedzy, a w konsekwencji realizacji celów przyjętych przez organizację.

Walka informacyjna dotyczy władzy. Ten, kto kontroluje informacje, ten kontroluje ludzi i ich środowisko.

Walka informacyjna dotyczy także polityki. Kiedy Irak czy Korea Północna rozwijają narodowe potencjały nuklearne, stanowi to sygnał dla społeczności międzynarodowej, że przyszły konflikt nie będzie tym, czym był kiedyś. Dotyczy to również współcześnie prowadzonych działań asymetrycznych.

Walka informacyjna dotyczy również pieniędzy, strachu i przeżycia. Ten, kto posiada dostęp do informacji, ma możliwość manipulowania rynkiem finansowym (np. giełdą papierów wartościowych), przekłada się to także na strach inwestorów.

Walka informacyjna dotyczy wyzwań. Brak skutecznych rozwiązań, mało czytelne regulacje prawne i ich niestosowanie, a nawet zaniechanie stanowią poważne zagrożenie dla systemów i sieci teleinformatycznych.

Walka dotyczy także kontroli informacji. W cyberprzestrzeni ma miejsce elektroniczna anarchia, która rozprzestrzenia się bardzo szybko i nie poddaje się żadnej kontroli np. ze strony państwa. Postęp naukowo-techniczny i powszechny dostęp do sprzętu teleinformatycznego przyczynia się m.in. do wspomnianej anarchii.

Trudno oszacować straty spowodowane prowadzeniem walki informacyjnej. Koszty ekonomiczne tej walki są trudne do określenia, tym bardziej że globalna sieć informacyjna, Internet, pozbawiona jest jakiejkolwiek kontroli narodowej. Straty dotyczą nie tylko finansów, ale przede wszystkim ludzi.

Współczesny wymiar to ścisły związek między postępem cywilizacyjnym a informacją, o którą należy walczyć. To również źródło nowych konfliktów i form ich rozwiązywania w środowisku zdominowanym przez technikę teleinformatyczną. Takim przykładem jest Internet, który spowodował, że informacja jest powszechnie dostępna. Łatwy dostęp do informacji, co wyraźnie należy podkreślić, stanowi źródło wielu zagrożeń zarówno dla samej informacji, jak i wiedzy.

---

[26] D.E. Denning, *Wojna informacyjna i bezpieczeństwo informacji*, Warszawa 2002, s. 14.

[27] *Ibidem*.

[28] Szerzej: G. Nowacki, *Informacja w walce zbrojnej*, Warszawa 2002, s. 57.

Zagrożenia

Zagrożenie z jednej strony to pewien stan psychiczny lub świadomościowy wywołany postrzeganiem zjawisk (zdarzeń – przyp. autora), które subiektywnie ocenia się jako niekorzystne lub niebezpieczne, a z drugiej czynniki obiektywne powodujące stany niepewności i obaw[29].

Generalnie można powiedzieć, że zagrożenia to wszelkie możliwe działania dotyczące jakiegoś zasobu lub procesu, które mogą spowodować straty.

„Zagrożenia to pośrednie lub bezpośrednie destrukcyjne oddziaływania na podmiot. Rozróżnia się zagrożenia potencjalne i realne; subiektywne i obiektywne; zewnętrzne i wewnętrzne, militarne i niemilitarne (polityczne, ekonomiczne, społeczne, informacyjne, ekologiczne, przyrodnicze itp.), kryzysowe i wojenne, intencjonalne i przypadkowe (losowe). W opisie zagrożeń intencjonalnych wyróżnić można cztery elementy: aktora, jego intencje, możliwości oraz czas na reakcję"[30]. Ponadto zagrożenia zaliczane są do szerokiej grupy traktowanej jako wyzwania. Z kolei wyzwania pod warunkiem właściwego zidentyfikowania i rozpoznania stanowią dla organizacji szanse, natomiast te, które zostały zlekceważone, niepodejmowane lub też podejmowane, ale z opóźnieniem mogą przekształcić się w określonych warunkach w zagrożenia.

Zagrożenia możemy usystematyzować w następujących grupach:

- strategiczne (mające wpływ na długoterminowe cele organizacji),
- operacyjne (mające wpływ na codzienne funkcjonowanie organizacji),
- finansowe (związane z działaniami finansowymi i kapitałem organizacji),
- zgodności (wpływające na utrzymywanie zgodności z aktualnie obowiązującymi regulacjami prawnymi).

Jeżeli przyjmiemy za punkt rozważań związek zagrożeń z konkretną organizacją, to wyróżnia się[31]:

1) zagrożenia niewymagające specyficznej wiedzy dziedzinowej związanej z konkretną organizacją:
   - zagrożenia naturalne (ulewy, powódź, trzęsienia ziemi, erupcje wulkanów, pożary itp.),
   - zagrożenia typu zatrzymanie działalności,
2) zagrożenia wymagające specyficznej wiedzy z danej dziedziny (tj. związane z konkretną organizacją), np.:
   - utrata kluczowych pracowników (wiąże się z utratą wiedzy organizacji – przyp. autor),
   - utrata kluczowego partnera (np. politycznego, gospodarczego, wojskowego),
   - utrata reputacji,
   - awaria systemów IT.

Zagrożenia mające wpływ na systemy informacyjne i teleinformatyczne organizacji, które bezpośrednio przekładają się na zagrożenia jej wiedzy można sklasyfikować w sposób następujący[32]:

---

[29] S. Korecki, *System bezpieczeństwa Polski*, Warszawa 1994, s. 54.

[30] S. Koziej, *Między piekłem a rajem. Szare bezpieczeństwo na progu XXI wieku*, Toruń 2006, s. 11.

[31] K. Liderman, *Analiza ryzyka i ochrona informacji w systemach komputerowych*, Warszawa 2008, s. 42.

[32] *Ibidem*.

1) siły wyższe (zmiany prawa, katastrofy finansowe, duża fluktuacja pracowników, klęski żywiołowe itp.). Negatywne skutki to: zniszczenie zasobów informacji, utrata dostępności, obniżenie stanu ochrony, utrata wiedzy organizacji;
2) nieuprawnione i przestępcze działania ludzi:
   - zagrożenia związane z kradzieżami fizycznymi i zagubieniami sprzętu, oprogramowania i dokumentów – możliwe skutki: głównie utrata dostępności i poufności informacji,
   - zagrożenia związane z podsłuchami różnego typu (w tym wykorzystanie klasycznych technik szpiegowskich) sprzętu i oprogramowania – możliwe skutki: utrata poufności informacji,
   - nieuprawnione działania personelu – możliwe skutki: utrata dostępności, integralności i poufności informacji, obniżenie poziomu ochrony,
   - nieuprawnione działania osób postronnych – możliwe skutki: utrata dostępności, integralności i poufności informacji, obniżenie poziomu ochrony;
3) błędy personelu obsługującego system komputerowy – możliwe skutki: utrata dostępności, integralności i poufności informacji, obniżenie poziomu ochrony;
4) skutki złej organizacji pracy, w tym zagrożenia związane z błędami w ochronie fizycznej i technicznej – możliwości utraty dostępności, integralności i poufności;
5) awarie i uszkodzenia sprzętu oraz wady oprogramowania – możliwe skutki: głównie utrata dostępności informacji oraz obniżanie poziomu ochrony.

Poziom zagrożenia zależy od poziomu wrogości przeciwnika, jego możliwości i minimalizowania czasu na reakcję.

Szeroka gama zagrożeń naturalnych i celowych sprawia, że poważnym problemem dla każdej organizacji jest system ochrony informacji, a w konsekwencji i wiedzy.

Zagrożenia związane z prowadzeniem „wojny informacyjnej to: zakłócanie pracy komputerów, szpiedzy, satelity szpiegowskie, podsłuch, kamery obserwujące, fizyczne niszczenie urządzeń komunikacyjnych, fałszowanie dokumentów, manipulowanie percepcją, operacje psychologiczne i wprowadzanie wirusów komputerowych. Są jeszcze inne formy wojny informacyjnej, takie jak wykradanie tajemnic, wkraczanie w sfery prywatności, fałszowanie poczty elektronicznej. Niektóre z tych działań są w pewnych okolicznościach przestępstwem, inne mogą być wprawdzie nieetyczne, ale są legalne, jeszcze inne traktuje się jako przyjęty sposób postępowania rządów i różnych instytucji. Niektóre operacje są związane z konfliktami militarnymi, inne z konfliktami na poziomie indywidualnym lub społecznym oraz na poziomie firm. Wszystkie te działania mają wspólną cechę – ich celem jest zdobycie lub wykorzystanie zasobów informacyjnych na korzyść sprawcy i na niekorzyść strony drugiej”[33].

Aktualnie każde państwo musi się liczyć z możliwościami ataku informacyjnego na narodową infrastrukturę informacyjną, od której uzależnione jest jego sprawne funkcjonowanie. „Celami mogą się stać główne dziedziny gospodarki narodowej, w tym system bankowy i finansowy, sieci zasilania w energię elektryczną, sieci rurociągów gazowych i naftowych, system telekomunikacji oraz ogólnonarodowy i lokalne systemy komunikacji lądowej, powietrznej i morskiej. Wszystkie te dziedziny strategicznej infrastruktury narodowej przechodzą gwałtowne przemiany, często o charak-

[33] D.E. Denning, *Wojna informacyjna...*, *op. cit.*, s. 11.

terze rewolucyjnym, w warunkach presji prywatyzacyjnej, globalizacyjnej i napływu różnorodnej techniki informacyjnej"[34].

Atak na systemy informacyjne i systemy teleinformatyczne to celowe działania ludzi, których zadaniem jest naruszenie tajności, integralności lub dostępności do informacji znajdujących się w zasobach organizacji. W ramach ataku informatycznego mogą być stosowane następujące formy:

- atak informatyczny w obszarze przetwarzania danych cyfrowych,
- atak elektroniczny,
- działania psychologiczne,
- dezinformacja (mylenie),
- atak ogniowy.

Zjawiskiem zasługującym na podkreślenie jest atak socjotechniczny, przez który należy rozumieć „wywieranie wpływu na ludzi i stosowanie perswazji w celu oszukania ich tak, aby uwierzyli, że socjotechnik jest osobą o sugerowanej przez siebie, a stworzonej na potrzeby manipulacji, tożsamości. Dzięki temu socjotechnik jest w stanie wykorzystać swoich rozmówców przy dodatkowym (lub nie) użyciu środków technologicznych, do zdobycia poszukiwanych informacji"[35]. Jak twierdzi K. Mitnick: „tęsknota za poczuciem absolutnego bezpieczeństwa jest naturalna, ale prowadzi wielu ludzi do fałszywego poczucia braku zagrożenia. [...] Bezpieczeństwo staje się zbyt często iluzją. Jeżeli do tego dodamy łatwowierność, naiwność i ignorancję, sytuacja dodatkowo się pogarsza"[36].

* * *

Jednym z podstawowych zagrożeń jest niekontrolowany ulot niejawnych informacji. Kolejne bardziej niebezpieczne zagrożenie powstaje w wyniku wpływania jednostek i organizacji na innych poprzez wysyłanie informacji fałszywych, czyli tzw. dezinformacja. Znaczenie dezinformacji w przebiegu konfliktów zarówno zbrojnych, jak i niezbrojnych doceniane jest zawsze: „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 dezorganizację i bierz go; przyjąwszy pokorny wygląd, wzbudź niepewność siebie; napadaj przeciwnika, kiedy nie jest przygotowany; pojawiaj się tam, gdzie on ciebie nie oczekuje"[37]. Działania tego charakteru mają poważny wpływ na wiedzę praktycznie każdej organizacji.

Na początku XXI w. komputery stały się powszechnie dostępne. „Są one tanie, często niewielkie, często połączone między sobą, wbudowane we wszystko, od kuchni mikrofalowej po precyzyjne pociski sterowane. Komputery uczestniczą we wszystkich rodzajach procesów, włącznie z procesami biznesowymi, bankowością i finansami, transportem, nawigacją, dystrybucją energii elektrycznej i wody, edukacją, rozrywką, administracją rządową, opieką zdrowotną, pogotowiem, działaniami militarnymi. Umożliwiają one handel elektroniczny, telemedycynę, telekonferencje i te-

[34] P. Gawliczek, J. Pawłowski, *Zagrożenia asymetryczne*, Warszawa 2003, s. 103.

[35] K. Mitnick, W. Simon, *Sztuka podstępu*, Gliwice 2003, s. 4.

[36] *Ibidem*, s. 20.

[37] Sun Tsu, *Sztuka wojny*, Warszawa 1994.

lekomunikację. W konsekwencji informacje wrażliwe, kiedyś ograniczone do rozmów i dokumentów trzymanych w biurach, zostały teraz skomputeryzowane i są przesyłane publicznymi sieciami. Przez to są potencjalnie podatne na kradzież, wykorzystanie i sabotaż przez osoby lub instytucje znajdujące się w znacznej odległości"[38].

„Za symptomatyczne należy uznać stwierdzenie, że: [...] ponad 100 milionów komputerów łączy nas wzajemnie poprzez niesłychanie złożony system układów komunikacyjnych, zarówno naziemnych, jak i satelitarnych. [...] rządowe i komercyjne systemy komputerowe są tak słabo dziś chronione, że można je praktycznie uznać za bezbronne. Czeka nas zatem elektroniczne Pearl Harbor"[39].

Nową pod względem jakościowym płaszczyznę działań terrorystycznych stanowi ich postępujące uzależnienie od elektronicznego przekazu informacji. Tak zwany infoterroryzm (terroryzm informatyczny, terroryzm sieciowy, cyberterroryzm) stanowi realne zagrożenie, co jest dostrzegalne w wielu organizacjach.

„Nawet zdobyta i właściwie przetworzona wiedza (czyt. informacja) staje się bezużyteczna, gdy trafia w niewłaściwe ręce albo też wówczas, gdy przyswajają ją niewłaściwe umysły w niewłaściwym czasie. Stąd bierze się potrzeba, by dystrybuować ją różnie, lecz w należyty sposób"[40].

„Bardzo często występują tendencje do tego, aby wiedzieć możliwie dużo lub w ogóle wszystko wiedzieć. W związku z tym w systemach wymiany danych i komunikatów często w obiegu występuje znacznie więcej ich postaci, niż jest to potrzebne. W praktyce należy taką tendencję ograniczać, ponieważ może doprowadzić do wywołania takiego napływu danych, iż zostanie zablokowany proces decyzyjny – istota tego zagrożenia wynika z reguł teorii masowej obsługi.

Najczęściej występuje brak tych danych, które są w określonej chwili potrzebne. Aby się tego ustrzec, w planie zdobywania informacji należy uwzględniać nie tylko siły i środki, lecz również obszar, potrzeby czasowe oraz wydajność systemów dystrybucji informacji.

W systemie informacyjnym znajduje się nadmiar danych, których jednak w pewnej chwili nie można wykorzystać. Z reguły wynika to z braku czasu na ich opracowanie i przekazanie.

Wiele posiadanych danych dezaktualizuje się, zanim zostaną przez kogokolwiek wykorzystane"[41].

Bazy danych wykorzystywane w procesach decyzyjnych wymagają zarówno rozwiązań technicznych, jak i organizacyjnych, które pozwalają na generowanie strumieni informacyjnych o odpowiedniej intensywności w celu utrzymania aktualności danych w stosunku do odwzorowywanej rzeczywistości. Podkreślić należy, że „w większości baz danych nie rozważa się problemu informacji niedokładnych, zmieniających się w czasie, niepełnych i niespójnych. Informacje takie nazywa się informacjami niepewnymi"[42]. W trakcie budowania i eksploatacji baz danych stosuje się następującą metodykę: informacje uznaje się za pewne i wprowadza do baz danych lub uznaje

[38] D.E. Denning, *Wojna informacyjna...*, *op. cit.*, s. 17.

[39] A. Toffler, H. Toffler, *Wojna i antywojna*, Warszawa 1997, s. 218.

[40] *Ibidem*.

[41] G. Nowacki, *Informacja...*, *op. cit.*, s. 25.

[42] J. Januszewicz, M. Koselski, *Dynamiczne uwarunkowania wojskowych baz danych*, „Myśl Wojskowa" 2002, nr 1, s. 156–157.

się je za niepewne i wówczas nie są wprowadzane do baz danych. „Praktyka wykazuje, że w większości systemów zarządzania wykorzystuje się informacje niepewne, przy czym jest to oparte na dużym indywidualnym doświadczeniu w danej dziedzinie. [...] Z konieczności wykorzystywania informacji niepewnych wynika konieczność stworzenia mechanizmów, które umożliwiłyby przechowywanie takiej informacji w bazie danych z uwzględnieniem i zasygnalizowaniem ich mniejszej wartości. Nie jest to sprawa prosta ani oczywista, ponieważ po umieszczeniu informacji niepewnych w bazie danych mogą być one traktowane tak samo jak informacje wiarygodne, jeśli nie będzie mechanizmów odróżniających je od informacji pewnych"[43]. Stanowi to poważny problem dla poziomu wiedzy każdej organizacji, z czym zarządzający powinni się liczyć.

* * *

Dynamika zmian występujących w środowisku działania organizacji sprawia, że zarządzanie organizacjami jest coraz trudniejsze. Oznacza to, że osoby funkcyjne powinny posiadać wszechstronną wiedzę z zakresu problematyki związanej z wykonywanym zawodem, struktur organizacyjnych, stanu zasobów organizacji, możliwości własnych i przeciwnika, a także nowoczesnych metod szybkiej i efektywnej obróbki informacji. Ilość i różnorodność informacji zwiększa odpowiedzialność zarządzających za podjęte decyzje i wyniki działań. W tych złożonych warunkach do cech charakterystycznych zarządzania zalicza się:

- krótki czas na wypracowanie decyzji,
- brak dostępnych informacji o możliwościach własnych i przeciwnika,
- wzrost odpowiedzialności zarządzających za skutki podjętych decyzji.

Wskazane uwarunkowania są źródłem stresu, który ma negatywny wpływ na podejmowane decyzje, niekiedy błędne, co stwarza sytuacje zagrażające realizacji przyjętych celów. Również przekonanie zarządzających o swojej nieomylności czy lekceważenie informacji przekładanych przez uprawnione podmioty mają negatywny wpływ na stan wiedzy decydenta, a tym samym proces decyzyjny. Dlatego tak istotny jest właściwy dobór osób funkcyjnych, który wyeliminuje realne źródła niekompetencji zakłócające proces zarządzania.

Podkreślić należy, że racjonalne wypracowanie decyzji jest uwarunkowane sprawnym procesem myślenia, szczególnie myśleniem problemowym, gdzie właściwa informacja stanowi o jego skuteczności. W trakcie tego złożonego procesu mogą pojawiać się różnorodne zaburzenia, na przykład ograniczona zdolność rozumienia i logicznego myślenia, kojarzenia oraz skłonność do powtórzeń. Cechą charakterystyczną sytuacji trudnych jest to, że zakłócają normalny przebieg czynności kierowania, zmieniając tym samym prawdopodobieństwo osiągnięcia jego celu. Spośród sytuacji trudnych można wyróżnić: derywacje, przeciążenia, utrudnienia, konflikty i zagrożenia.

Do innych zagrożeń zalicza się czynniki tłumiące aktywność twórczą w organizacji, które zależą od stylu kierowania: utajony lęk i brak zaufania, ograniczony przepływ informacji, narzucanie celów, nadmierna kontrola zachowania[44].

---

[43] *Ibidem*, s. 157.

[44] Szerzej: Z. Pietrasiński, *Twórcze kierownictwo*, Warszawa 1975, s. 91.

Zagrożenie dla zasobów informacyjnych (wiedzy) organizacji stanowią ich słabe punkty. Takie słabe punkty mogą się pojawić w elementach urządzeń i programów, a także w działaniach człowieka. Można je wprowadzać podczas wytwarzania produktu, dostarczania go, instalowania, konfigurowania, stosowania, modyfikowania i konfigurowania[45].

Warto mieć świadomość tego, że zagrożenie wystąpi wówczas, gdy pojawi się jakiś uczestnik gry, który ma zamiar przeprowadzić atak, ma możliwości i warunki do jego przeprowadzenia. Mogą to być ludzie z wewnątrz organizacji, hakerzy, korporacje, rządy, przestępcy i terroryści.

* * *

Każdy zarządzający powinien mieć świadomość tego, że podstawowym zagrożeniem informacyjnym jest brak informacji. Ponadto bez aktualnej, rzetelnej i sprawdzonej (bardzo często stan trudny do osiągnięcia) informacji trudno jest mówić o wiedzy organizacji, a tym bardziej o możliwościach podejmowania właściwych decyzji.

Przeciwieństwem braku informacji jest jej nadmiar, czyli tzw. chaos informacyjny. Ma miejsce wówczas, kiedy odbiorca otrzymuje za dużo informacji, gdzie wiele z nich nie nadaje się do wykorzystania z uwagi na znikomą wartość. Chaos może być zarówno wynikiem braku właściwego zarządzania, bałaganu, nieładu, jak również konsekwencją świadomego działania ludzi zmierzających do zatajenia określonych ludzi. „Poczucie chaosu w pewnych dziedzinach życia publicznego, np. w polityce, gospodarce, prawodawstwie, w wiedzy o własnym społeczeństwie bywa również następstwem działań manipulacyjnych. Prowadzi do tego wyczerpujące bombardowanie psychiki człowieka wielością niezrozumiałych bodźców, a także przekazywanie sprzecznych ze sobą i nakładających się na siebie informacji. Do poczucia chaosu prowadzą też sugestywne hasła, odnoszące się do hierarchii wartości”[46].

„Ważną rolę odgrywa w tym momencie właściwa informacja (co przekłada się na wiedzę – przyp. autora). Jeśli kiedyś mogliśmy odczuwać niedosyt informacji, to dzisiaj nierzadko uciążliwy może być jej nadmiar. Czy możemy mieć o to pretensje do rzeczywistości? Przecież, jeśli jeszcze nie tak dawno zaledwie brodziliśmy w strumykach reglamentowanej informacji, to dzisiaj mamy duże trudności, żeby utrzymać się na powierzchni tego wzburzonego morza informacji trzeciej fali, jednocześnie starając się dotrzeć do wyznaczonego celu”[47].

Gwałtowny, a niekiedy zaskakujący przebieg zjawisk i zdarzeń sprawia, że wiele zdobytych informacji szybko się dezaktualizuje, co oznacza, że ulegają starzeniu się. Na ten proces ma wpływ przede wszystkim czas, jaki upłynął od momentu pozyskania informacji, do momentu jej przekazania dla podmiotów decyzyjnych. Ta sytuacja przekłada się na aktualność wiedzy w organizacji.

Należy stwierdzić, że obecnie zarządzający organizacjami bywają źle poinformowani nie ze względu na niedostatek informacji, ale ich nadmiar. „Dlatego w odniesieniu do każdego stanowiska kierowniczego często nieodzowne jest stosowanie zasady selekcji informacji, określanej również mianem zasada 20–80. Okazuje się bo-

[45] D.E. Denning, *Wojna informacyjna...*, *op. cit.*, s. 14.

[46] A. Lepa, *Świat manipulacji*, Częstochowa 1995, s. 157.

[47] M. Cieślarczyk, *Kultura informacyjno-organizacyjna jako element potencjału bojowego sił zbrojnych – sił powietrznych*, „Myśl Wojskowa” 2002, nr 1, s. 48.

wiem, że tylko 20% informacji docierających do kierownictwa dotyczy spraw kluczowych i te 20% w 80% przesądza o wynikach działalności"[48].

Zagrożenie dla wiedzy w organizacji stanowią również luki informacyjne, które w trakcie podejmowania decyzji skutkują tym, że informacje niepełne traktowane są jako wystarczające lub stanowią uzupełnienie już istniejącej luki informacyjnej, które zarządzający uznaje za właściwe. Zalicza się do nich m.in. informacje niesprawdzone, subiektywne szacunki prowadzone na wątpliwych podstawach. W praktyce okazuje się, że są to jedne z najczęściej występujących przesłanek o negatywnym charakterze. „Procedury decyzyjne bywają zwykle dostosowywane do informacji, którą ma decydent, znajduje się on jak gdyby w klatce informacyjnej. W wypadku działań rutynowych mamy do czynienia z samoograniczającym się oddziaływaniem dostępnych zbiorów informacji i procedur decyzyjnych. Nowe informacje nie są wykorzystywane, bo rutyna decyzyjna ich nie wymaga, i odwrotnie – nie zmienia się procedur decyzyjnych, bo brakuje informacji. Przełamanie syndromu klatki informacyjnej przez decydentów systemów informacyjnych jest niekiedy trudnym zadaniem"[49].

Kolejna niezmiernie istotna kwestia związana jest z przezwyciężaniem trudności w zakresie określenia tzw. puli informacji o kluczowym znaczeniu dla procesu decyzyjnego. W dzisiejszych czasach krytycznym zadaniem nie jest [...] generowanie, przechowywanie lub przekazywanie informacji, lecz jej filtrowanie[50]. Te uwarunkowania stanowią zagrożenie dla wiedzy organizacji, tym bardziej że „wszystkie decyzje łączy jedna prawidłowość. W każdej decyzji ważne jest zarówno sformułowanie właściwego pytania, jak i właściwej odpowiedzi. Nawet najlepsza odpowiedź na źle sformułowane pytanie jest bezwartościowa"[51].

„W badaniach na temat wykorzystywania informacji w działalności organizacji około 92% respondentów podało, że pracują w organizacjach, gdzie intensywnie korzysta się z wiedzy [...] zawartej w informacjach. Jednak tylko 6% uważa, że efektywnie wykorzystuje informacje, podczas gdy 31% przyznaje się do nieefektywnego gospodarowania nimi. Jako główną przyczynę tego podaje się, iż członkowie organizacji nie potrafili zinterpretować lub wykorzystać dostępnej informacji, a zdarza się również, że takie same pomyłki są popełniane kilka razy. Prawie każdy z badanych zwracał uwagę na to, że wąskie gardła w dostępie do wiedzy w ich organizacjach są przyczyną kosztownych pomyłek lub nieefektywnych operacji, zaś 87% stwierdziło, że pomimo wielkich nakładów na szkolenia pracowników i rozwój techniki informatycznej kosztowne błędy były popełniane z tego powodu, iż wiedza nie była osiągalna we właściwym miejscu lub czasie albo dostępna w niewłaściwym formacie"[52].

* * *

W ostatnim okresie jesteśmy świadkami postępu w sferze technik transferu wiedzy, który de facto zależy od koncepcji materializacji wiedzy. „Jest ona transformacją

[48] Relacje 20–80 należy traktować jako umowną. W rzeczywistości mogą występować dość znaczne odchylenia od tej proporcji, lecz główna idea zasady pozostaje zazwyczaj niezmieniona; G. Nowacki, *Informacja w walce zbrojnej*, Warszawa 2002, s. 86.

[49] J. Kozioł, *Zarządzanie zasobami informacyjnymi*, „Myśl Wojskowa" 2002, nr 1, s. 75.

[50] H.A. Simon, *Podejmowanie decyzji kierowniczych. Nowe nurty*, Warszawa 1982, s. 158.

[51] G. Nowacki, *Informacja...*, *op. cit.*, s. 87.

[52] J. Kozioł, *Zarządzanie zasobami...*, *op. cit.*, s. 60.

wiedzy w formę, dzięki której wiedzą można manipulować, można wiedzę przechowywać, transmitować, wyszukiwać i wykorzystywać bez ciągłego odwoływania się do osoby, od której ona pochodzi"[53]. Czynnikiem, który sprzyja utracie wiedzy w organizacji, jest m.in. znaczna rotacja kadry. Kiedy specjaliści w określonej dziedzinie opuszczają organizację w wyniku niewłaściwej polityki kadrowej czy restrukturyzacji organizacji – traci ona bezpowrotnie część swojej wiedzy. Wydaje się, że działania te mogą prowadzić do poważnych zakłóceń w procesie transferu wiedzy, który ma miejsce pomiędzy odchodzącymi a przychodzącymi pracownikami.

Zakłócenia te mogą skutkować obniżeniem poziomu wiedzy stanu osobowego, a szczególnie kadry kierowniczej organizacji. Jest to szczególnie niebezpieczne dla tych organizacji, gdzie występuje wysokie nasycenie nowoczesną techniką.

Ludzie są tym aktywem organizacji, który jest zdolny do inicjowania działań, mogących poprawić jej pozycję w środowisku narodowym i międzynarodowym. Pracownicy związani z organizacją przyczyniają się do pomnażania jej wiedzy i mogą wpływać na jej efektywność. Natomiast wraz z ich odejściem organizacja traci część wiedzy, co oznacza, że wiedza przepada wraz z pracownikiem. Jest to bardzo poważny problem, którego skala zależy od zarządzających.

Warto mieć na uwadze to, że głównym przedmiotem działań pozytywnych, jak i negatywnych w relacji między organizacjami jest w istocie władza, a władza to informacja. Bezpośrednim przedmiotem oddziaływania w środowisku ich działania są inne organizacje, gdzie ma zastosowanie stymulacja pożądanych działań. W procesie tym kierujący organizacjami doświadczają przede wszystkim oddziaływania informacyjnego, co obok wykształcenia i doświadczenia ma wpływać na ich wiedzę. Jeżeli kierujący organizacją stwierdzi, że przeciwnik ma sprzeczne cele, to wówczas podejmował on będzie działania zróżnicowane co do formy.

Systemy informacyjne wspomagające procesy decyzyjne w organizacji przy niewłaściwym zabezpieczeniu lub jego braku podatne są na stymulowanie percepcji odbiorczej konkurencji nie tylko informacjami prawdziwymi, ale i fałszywymi. Stymulowanie informacjami może również sprowadzać się do sterowania emocjami w celu ograniczenia racjonalnego podejmowania decyzji. Postęp naukowo-techniczny sprawia, że informacja stopniowo staje się podstawowym narzędziem stymulacji w konkurencyjnej walce między organizacjami.

Celem każdego ataku na zbiory danych organizacji jest przejęcie kontroli nad zasobami chronionego systemu informacyjnego, a następnie ukrycie tego faktu możliwie długo bądź fizyczne zniszczenie dowodów ingerencji[54].

Atak informatyczny jest prowadzony w obszarze przetwarzania danych cyfrowych i sprowadza się do niejawnego wprowadzenia przez atakującego złośliwego kodu komputerowego do ściśle określonego systemu lub sieci komputerowej dla realizacji założonych celów. Złośliwe kody mogą przybierać formę: wirusów, bomb logicznych i programowanych czasowo, tylnych drzwi, koni trojańskich, robaków lub ich kombinacji właściwych co do realizowanych funkcji.

Atakującym może być każda organizacja lub pojedyncza osoba posiadająca odpowiednią wiedzę i wyposażenie pozwalające na zainstalowanie takiego kodu.

---

[53] *Ibidem*, s. 78.

[54] Szerzej: A. Żebrowski, W. Kwiatkowski, *Bezpieczeństwo informacji III Rzeczypospolitej*, Kraków 2000, s. 63.

Zagrożenie spowodowania nieodwracalnych szkód w zasobach informacyjnych organizacji stanowi istotny element odstraszania w procesie ich konfrontacji. Ważnym zadaniem ataku informacyjnego jest możliwość sterowania procesami decyzyjnymi przeciwnika przez wprowadzenie do obiegu określonej informacji lub dezinformacji. Do form ataku informacyjnego zalicza się m.in.:

- zrywanie procedur wymiany informacji,
- manipulowanie informacjami (dezinformacja, zatajenie, zniekształcenie),
- korzystanie z nieautoryzowanego dostępu do zasobów informacyjnych oraz nielegalne zbieranie i używanie informacji,
- nielegalne kopiowanie danych zawartych w systemach informatycznych, w tym bazach i bankach danych,
- masowe niszczenie oprogramowania.

Należy przyjąć, że każdy użytkownik systemu informacyjnego bez względu na posiadany stopień dostępu do informacji może przypadkowo naruszyć istniejący system bezpieczeństwa. Znacznie większe straty mogą być spowodowane przez personel posiadający bezpośredni dostęp do takiego systemu. Wynika to przede wszystkim z istnienia naturalnych możliwości, co pozwala m.in. na: pozyskiwanie informacji w sposób skryty, na ich manipulowanie, transmisję, usunięcie, wydruk czy też przekazanie osobie do tego nieuprawnionej.

Celowe zagrożenie jest wynikiem połączenia trzech elementów, takich jak motyw, środek realizacji (realizacji włamania do systemu informacyjnego) i okazja, czyli posiadanie naturalnego dostępu.

Obiektem ataku może być również pracownik organizacji z uwagi na zajmowane stanowisko, pełnioną funkcję, co bezpośrednio wiąże się z dostępem do informacji będących przedmiotem zainteresowania konkurencji.

Można założyć, że wiele organizacji nie zdaje sobie sprawy ze skali wartości wiedzy, jaką dysponują, a także strat, jakie ponoszą w wyniku nierozsądnych decyzji w procesie jej zarządzania. Ograniczanie wydatków i redukcja personelu stanowi przesłankę do zmniejszenia skuteczności ochrony informacji, a w konsekwencji i wiedzy. W warunkach globalnego zawirowania finansowego wobec groźby utraty pracy rośnie liczba pracowników, którzy decydują się na kradzież istotnych informacji znajdujących się w zasobach organizacji, co bezpośrednio uderza w jej wiedzę. Celem takiego postępowania jest zwiększenie swojej atrakcyjności dla przyszłego pracodawcy bądź odegranie się na poprzedniku. Takie postępowanie jest widoczne zarówno u pracowników młodych, jak i z dużym stażem.

W związku z tym pracodawcy w celu realizacji przyjętych strategii muszą zwracać uwagę na potencjał decydujący o możliwościach organizacji, gdzie zasoby osobowe i informacyjne kształtują wiedzę, a przy właściwym jej wykorzystaniu utrzymanie lub umocnienie swojej pozycji na rynku wewnętrznym lub międzynarodowym.

Bezpieczeństwo informacji i wiedzy

„Bezpieczeństwo jest stanem, który daje poczucie pewności, i gwarancje jego zachowania oraz szanse na doskonalenie. Jedna z podstawowych potrzeb człowieka to sy-

tuacja odznaczająca się brakiem ryzyka utraty czegoś, co człowiek szczególnie ceni, na przykład zdrowia, pracy, szacunku, uczuć, dóbr materialnych"[55].

Bezpieczeństwo należy zawsze postrzegać z punktu widzenia zagrożeń i wyzwań, a także szans sprostania im przy minimalnych kosztach, co ma swój wymiar zarówno obiektywny, jak i subiektywny:

- obiektywny wymiar posiada cechy funkcjonujące niezależnie od naszej świadomości, do których zalicza się: zagrożenia, wyzwania i szanse,
- subiektywny wymiar to cechy związane z naszą percepcją widzenia otaczającego środowiska, świadomością zagrożeń i budowania koncepcji bezpieczeństwa.

Warto bowiem wiedzieć, które zagrożenia są realne, jakie przy tym jest prawdopodobieństwo jego wystąpienia i jakie będą straty.

W tym aspekcie istotnym czynnikiem dla rozwoju państwa i innych organizacji jest ich bezpieczeństwo: narodowe, polityczne, społeczne, socjalne, strukturalne i personalne, etniczne, wyznaniowe, psychologiczne, kulturowe, ekonomiczne, informacyjne, zasobów naturalnych, żywnościowe, ekologiczne, wojskowe i inne.

W określonych przypadkach wymienione aspekty bezpieczeństwa mogą dominować w dowolnej kolejności, to jednak czynnik informacyjny obok politycznego będzie zawsze jego decydującym wyznacznikiem. Ponadto nie w każdej organizacji będą występowały wszystkie wymienione kategorie bezpieczeństwa. Tym bardziej że bezpieczeństwo jest kategorią uniwersalną i stopniowo przesuwa się w kierunku bezpieczeństwa pozamilitarnego.

Przykładowo ekonomiczne bezpieczeństwo jest postrzegane przez trójelementową strukturę: ekonomiczną niezależność, stabilność oraz zrównoważenie, zdolność do rozwoju oraz postępu[56]. W związku z tym można powiedzieć, że ekonomiczne bezpieczeństwo to całokształt czynników oraz uwarunkowań zabezpieczających niezależność gospodarki narodowej, stabilność oraz zrównoważenie, a także gwarantowanych zdolności do nieustannej i odnowy i samodoskonalenia[57].

Tworzenie koncepcji bezpieczeństwa ekonomicznego państwa i innych organizacji wymaga kompleksowych i wzajemnie powiązanych przedsięwzięć wspieranych przez państwo, przy jednoczesnym określeniu przyszłości społeczno-gospodarczej w okresie trwającej transformacji. Proces budowania bezpieczeństwa ekonomicznego państwa (dotyczy to również bezpieczeństwa innych organizacji) wymaga niezbędnej wiedzy ze strony uprawnionych podmiotów, dzięki której można stworzyć system monitoringu otoczenia i występujących tam wskaźników, pozwalających na sygnalizowanie zagrożeń dla gospodarki i na podjęcie decyzji przeciwdziałających.

Przykładowo takimi wskaźnikami mogą być[58]:

- w aspekcie wewnętrznym: stopa bezrobocia, poziom inflacji, różnice w dochodach,
- w aspekcie zewnętrznym: saldo obrotów bieżących, poziom zadłużenia międzynarodowego państwa, zależności państwa od importu surowców, wyrobów, technologii.

---

[55] *Słownik terminów z zakresu psychologii dowodzenia i zarządzania*, Warszawa 2000, s. 17.

[56] L. Abatkin, *Rossija. Poisk samoopredelenija*, Moskwa 2002, s. 86.

[57] *Bezpieczeństwo ekonomiczne państwa*, red. T. Guz, K.A. Kłosiński, P. Marzec, Lublin – Tomaszów Lubelski 2006, s. 41.

[58] *Ibidem*, s. 42.

Budowanie bezpieczeństwa we wszystkich obszarach działania każdej organizacji wymaga ochrony jej zasobów informacyjnych i wiedzy, które współcześnie jest niezmiernie trudne.

Bezpieczeństwo informacji oznacza uzasadnione zaufanie (np. analizę ryzyka i przyjęcie metod postępowania z ryzykiem), że potencjalne straty wynikające z niepożądanego (przypadkowego lub świadomego) ujawnienia, modyfikacji, zniszczenia lub uniemożliwienia przetwarzania informacji nie zostaną poniesione[59]. Obejmuje ona zapobieganie rozpoznaniu i niedopuszczenie do informacyjnego ataku lub uzyskania pożądanej efektywności tego ataku przez przeciwnika.

Zadaniem rozpoznania prowadzonego przez strony konfliktu jest dążenie do uzyskania informacji znajdujących się w posiadaniu każdego z jej uczestników. W aktywności tej występują dwa podstawowe elementy: przedmiot zainteresowania – informacja i element rozpoznania dążący do wejścia w jej posiadanie. Z kolei zapobieganie może przybierać formę przeciwdziałania aktywności rozpoznawczej przeciwnika i ochrony własnych informacji przed nieuprawnionym dostępem. Przeciwdziałanie aktywności rozpoznawczej przeciwnika sprowadza się do odstraszania lub obezwładniania. Natomiast ochrona informacji jest realizowana przez wiele przedsięwzięć natury kontrwywiadowczej, ochrony psychologicznej, ochrony elektronicznej, ochrony informatycznej, inżynieryjną rozbudowę i kontrdezinformację. Zaznaczyć przy tym należy, że przedsięwzięcia związane z obszarem ochrony informacji (wiedzy) mają ścisły związek z bezpieczeństwem działań i maskowaniem.

Warunkiem budowania systemu bezpieczeństwa informacyjnego (wiedzy) w organizacji świadomość zarządzających co do jego zasadności. Znajomość zagrożeń, skutków ataku na zasoby informacyjne i zasoby wiedzy, a także procedur pozwalających na niedopuszczenie lub minimalizowanie negatywnych skutków ataku, stanowi podstawę do wypracowania i wdrożenia polityki bezpieczeństwa informacji (wiedzy) organizacji.

Na zabezpieczenie informacji (wiedzy) składają się elementy: prawne, organizacyjne, osobowe, techniczne i programowe wykorzystywane w procesach ochronnych do działań, których celem jest zapewnienie właściwego poziomu ochrony logicznej i fizycznej informacji (wiedzy), a także elementów systemów i sieci teleinformatycznych.

Sposoby zabezpieczenia informacji (wiedzy) można zaliczyć do następujących grup:

1) fizycznej i technicznej ochrony przed nieuprawnionym dostępem ognia i wody, fizycznym dostępem obejmującym nie tylko ludzi, ale również systemy alarmowania o monitoringu, włamaniach i ppoż., środki mechaniczne (sejfy, zamki, przegrody budowlane itp.),
2) sprzętowej i programowej, do których zalicza się:
   - ochronę dostępu,
   - kryptograficzną ochronę tajności i integralności informacji,
   - monitorowanie przepływu pakietów w sieci i działań użytkowników,
   - zapewnienie odpowiedniego poziomu dostępności do informacji,
   - właściwe niszczenie informacji zapisanej na komputerowych nośnikach i na wydrukach z systemów komputerowych,

[59] K. Liderman, *Analiza ryzyka i ochrona informacji...*, *op. cit.*, s. 204.

3) organizacyjnej i personalnej, który obejmuje:
   - właściwe udokumentowanie systemu ochrony informacji,
   - klasyfikowanie informacji i przyznawanie uprawnień związanych z dostępem,
   - szkolenia i treningi,
   - określanie i przydzielanie zakresów odpowiedzialności za ochronę informacji,
   - nadzór i kontrolę w zakresie ochrony informacji,
   - zasady reagowania na naruszanie bezpieczeństwa systemu informacyjnego i systemu teleinformatycznego.

„Cechą poprawnego pod względem inżynierskim systemu bezpieczeństwa informacyjnego i teleinformatycznego jest skuteczność. Jej podstawową przesłankę stanowi kompleksowość takiego systemu, która jest rozumiana w sposób następujący:
- zastosowane zabezpieczenia powinny uwzględniać każdą z uprzednio wymienionych grup tzw. dywersyfikacja zabezpieczeń,
- zabezpieczenia powinny być zorganizowane tak, żeby zapewnić wykrycie naruszenia bezpieczeństwa i prób takich działań oraz skuteczną ochronę mimo przełamania części zabezpieczeń"[60].

Warto mieć na uwadze to, że system bezpieczeństwa informacyjnego i system bezpieczeństwa teleinformatycznego powinien być skuteczny, co oznacza, że:
- przełamanie nawet części środków ochrony nie powinno prowadzić do naruszenia tajności, integralności lub dostępności chronionej informacji,
- każda próba penetracji systemu powinna być rozpoznana i sygnalizowana. Jeżeli chodzi o kwestię wykrycia i rozpoznania penetracji, to przy umiejętnym prowadzeniu walki informacyjnej ten fakt jest niezmiernie trudny do wykrycia i zidentyfikowania.

Bezpieczeństwo informacji i wiedzy jest również traktowane jako działania defensywne prowadzone w ramach walki informacyjnej, a jej celem jest obrona zasobów informacyjnych (wiedzy) przed następującymi atakami: zwiększeniem dostępności dla strony atakującej, zmniejszeniem dostępności dla strony defensywnej lub zmniejszeniem integralności. „Jej celem jest efektywna kosztowo obrona. Oznacza to, ze koszt środków ochronnych powinien być mniejszy niż straty, które pojawiłyby się, gdyby tych środków nie było"[61].

Należy zaznaczyć, że w praktyce nie można zapewnić efektywnej kosztowo ani w ogóle wystarczającej obrony, która by zapobiegała wszystkim ofensywnym operacjom i tym samym pozwoliła uniknąć wszelkich strat[62].

W walce informacyjnej można wskazać następujące obszary obrony informacyjnej:
- wskazanie i ostrzeganie (ma na celu rozpoznanie możliwości ataku zanim on nastąpi lub tez jego wczesnej fazy),
- wykrycie (pozwala na stwierdzenie momentu ataku),
- zapobieganie (przeciwdziałanie atakowi poprzez odmowę dostępu stronie atakującej do zasobów znajdujących się w jego zainteresowaniu),

[60] K. Liderman, *Analiza ryzyka i ochrona informacji...*, *op. cit.*, s. 15.

[61] D.E. Denning, *Wojna informacyjna...*, *op. cit.*, s. 41.

[62] Szerzej: *ibidem*.

- odstraszanie (niekoniecznie musi zapobiegać atakowi, ale powinno skutkować tym, że atak jest nieopłacalny),
- przygotowanie na sytuacje awaryjne (oznacza zdolność do przywrócenia stanu przed atakiem i na odparcie ataku po jego nastąpieniu),
- odpowiedź na atak (polega na minimalizowaniu strat, przywrócenie stanu poprzedzającego atak i wzmocnienie obrony).

W procesie budowania systemu bezpieczeństwa informacji i wiedzy w organizacji należy dążyć do stworzenia takich procedur, które stanowią zaporę dla nieuprawnionego dostępu w sposób tani i niejawny dla otoczenia.

Przyjęcie i wdrażanie procedur związanych z bezpieczeństwem informacji i wiedzy pozwala na realizację przyjętej misji przez organizację, co jednak wymaga modyfikacji poprzez dostosowywanie do pojawiających się zagrożeń.

Podsumowanie

Powyższe zagrożenia (a także te, których jeszcze nie znamy) dla systemów informacyjnych i informatycznych przekładają się bezpośrednio na wiedzę organizacji, a w konsekwencji na wykonywanie założonych celów.

Warto mieć świadomość tego, że zagrożenia dla informacji i wiedzy ulegają ciągłej ewolucji, gdzie dominują zmiany w postępie naukowo – technicznym i technologicznym. Nadal jednak najsłabszym ogniwem w systemie bezpieczeństwa informacji i wiedzy jest człowiek.

Formy występowania zagrożeń są coraz bardziej wyrafinowane, a tym samym trudne do wykrycia. Mimo podejmowanych przedsięwzięć prawnych i organizacyjnych, to jednak w wielu przypadkach przy lekceważeniu obowiązujących procedur ma miejsce zarówno kontrolowany, jak i niekontrolowany ulot informacji. Uzasadnia to konieczność wypracowania i praktycznego wdrażania procedur pozwalających na minimalizowanie ewentualnych skutków ataku na zasoby informacyjne i zasoby wiedzy. Istotne jest również systematyczne monitorowanie otoczenia zarówno wewnętrznego, jak i zewnętrznego organizacji ze szczególnym wskazaniem na źródła rzeczywistych i potencjalnych zagrożeń – to zadanie na dziś i jutro.

Aby informacje i wiedza były skutecznie chronione, należy stosować rozwiązania systemowe podlegające ciągłemu usprawnianiu. Powinna obowiązywać zasada, że każdy system ochrony informacji i wiedzy musi być dostosowany do przedmiotów ochrony i zasad obowiązujących w danej organizacji. Jednym z proponowanych rozwiązań strukturalnych w kontekście, którego można rozpatrywać ochronę informacji i wiedzy, jest układ organizacyjny, odnoszący się do funkcji sprawowanych przez: kierownictwo, użytkowników (personel), służbę bezpieczeństwa informacji.

W praktyce sposób zorganizowania bezpieczeństwa informacji i wiedzy w organizacji sprowadzić możemy do:

- określenia zakresu obowiązków osób funkcyjnych,
- określenia obowiązków dla użytkowników,
- określenie celów, obowiązków i uprawnień dla służby bezpieczeństwa informacji,
- opracowanie planu pracy i planu kontroli,

- określenie zasad prowadzenia kontroli bieżących w odniesieniu do kierownictwa i samokontroli w odniesieniu do użytkowników,
- ujęcie w planie szkolenia ważniejszych zamierzeń w sferze ochrony informacji wiedzy przez kierownictwo i służbę bezpieczeństwa informacji oraz przyjęcie wniosków,
- stawianie zadań wynikających z zaleceń zawartych w protokołach z przeprowadzonych kontroli,
- zabezpieczenia technicznego wykonawstwa zadań przez organizację wynikających z obowiązujących przepisów dotyczących ochrony informacji prawnie chronionych, co bezpośrednio przekłada się na ochronę wiedzy.

„Pamiętajmy! Informacje trzeba chronić, gdyż, jeśli dostaną się w niepowołane ręce, mogą przysporzyć wielu strat i kłopotów każdemu z nas"[63]. Dlatego każdy kierujący organizacją w procesie zarządzania powinien uwzględniać funkcjonowanie komórki, której podstawowym celem powinno być monitorowanie jej otoczenia wewnętrznego i zewnętrznego, wskazywanie rzeczywistych i potencjalnych zagrożeń i podejmowanie działań uniemożliwiających (lub ograniczających) przeprowadzenie ataku na zasoby informacyjne i wiedzy organizacji.

Bibliografia

Abatkin L., *Rossıja. Poisk samoopredelenıja*, Moskwa 2002.

Antczak S., *Zarządzanie zasobami informacyjnymi w siłach powietrznych*, „Myśl Wojskowa" 2002, nr 1.

Bezpieczeństwo ekonomiczne państwa, red. T. Guz, K.A. Kłosiński, P. Marzec, Lublin – Tomaszów Lubelski 2006.

Bezpieczeństwo informacji III Rzeczypospolitej, red. A. Żebrowski, Kraków 2000.

Bird A., *Careers as Repositories of Knowledge: A New Perspective on Boundaryless Careers*, „Journal of Organizational Behaviour" 1994, nr 15.

Ciborowski L., *Walka informacyjna*, Toruń 1999.

Cieślarczyk M., *Kultura informacyjno-organizacyjna jako element potencjału bojowego sił zbrojnych – sił powietrznych*, „Myśl Wojskowa" 2002, nr 1.

Davenport T., Prusak L., *Working Knowledge: How Organizations Mange What The Know*, Boston 1998.

Denning D.E., *Wojna informacyjna i bezpieczeństwo informacji*, Warszawa 2002.

Evans Ch., *Zarządzanie wiedzą*, Warszawa 2005.

Gawliczek P., Pawłowski J., *Zagrożenia asymetryczne*, Warszawa 2003.

Januszewicz J., Koselski M., *Dynamiczne uwarunkowania wojskowych baz danych*, „Myśl Wojskowa" 2002, nr 1.

Jean C., *Geopolityka*, Wrocław–Warszawa–Kraków 2003.

Kłosiński K., *Konkurencyjność narodów*, [w:] *Losy świata*, red. K. Kłosiński, Lublin 2003.

[63] J. Niezgódka, *Jak bronić się przed hackerami*, Warszawa 1998, s. 158.

Korecki S., *System bezpieczeństwa Polski*, Warszawa 1994.

Kotarbiński T., *Traktat o dobrej robocie*, Wrocław–Warszawa 1958.

Koziej S., *Między piekłem a rajem. Szare bezpieczeństwo na progu XXI wieku*, Toruń 2006.

Kozioł J., *Zarządzanie zasobami informacyjnymi*, „Myśl Wojskowa" 2002, nr 1.

Lepa A., *Świat manipulacji*, Częstochowa 1995.

Liderman K., *Analiza ryzyka i ochrona informacji w systemach komputerowych*, Warszawa 2008.

Luttwak E.N., *From Gropoltics to Geo-economics. Logic of Conflict, Grammar of Commerce*, The National Interest, 1990.

Mikuła B., *Elementy nowoczesnego zarządzania. W kierunku organizacji inteligentnych*, Kraków 2001.

Mitnick K., Simon W., *Sztuka podstępu*, Gliwice 2003.

Niezgódka J., *Jak bronić się przed hackerami*, Warszawa 1998.

Nowacki G., *Informacja w walce zbrojnej*, Warszawa 2002.

Pietrasiński Z., *Twórcze kierownictwo*, Warszawa 1975.

Schwartau W., *Information Warfare*, Thunder s Mout Press, 1996.

Sillami N., *Słownik psychologiczny*, Katowice 1994.

Simon H.A., *Podejmowanie decyzji kierowniczych. Nowe nurty*, Warszawa 1982.

Słownik terminów z zakresu psychologii dowodzenia i zarządzania, Warszawa 2000.

Sun Tsu, *Sztuka wojny*, Warszawa 1994.

Szpyra R., *Militarne operacje informacyjne*, Warszawa 2003.

Toffler A., Toffler H., *Wojna i antywojna*, Warszawa 1997.

Wojtaszczyk K.A., *Kompendium wiedzy o państwie współczesnym*, Warszawa 1998.