

BEZPIECZEŃSTWO INFORMACYJNE W INSTYTUCJACH GOSPODARCZYCH

Zdzisław LUDZIEJEWSKI*

* *Instytut Socjologii Uniwersytet Wrocławski*
e-mail:zdzislaw@ludziejewski.com

Artykuł wpłynął do redakcji 12.11.2012 r., Zweryfikowaną i poprawioną wersję po recenzjach i korekcie otrzymano w listopadzie 2013 r.

Tematem artykułu są zagadnienia związane z bezpieczeństwem informacyjnym w erze społeczeństwa informacyjnego. Artykuł stanowi interdyscyplinarne przedstawienie zagrożeń, jakie niesie ze sobą funkcjonowanie we współczesnym społeczeństwie opartym głównie na zdobywaniu, przetwarzaniu i przepływie informacji.

Słowa kluczowe: *bezpieczeństwo informacyjne, informacje niejawne, kultura informacyjna*

WSTĘP

Współczesne realia funkcjonowania w społeczeństwie i prowadzenia biznesu w erze społeczeństwa informacyjnego przynoszą coraz to nowe zagrożenia bezpieczeństwa. Interdyscyplinarna wiedza z obszaru socjologii, zarządzania i informatyki pozwala na odkrywanie tych zagrożeń oraz wprowadzanie rozwiązań minimalizujących pojawiające się zagrożenia stanu bezpieczeństwa. Aktualnie subdyscyplina socjologii bezpieczeństwa odgrywa istotną rolę w identyfikacji zjawisk społecznych, w tym zagrożeń wpływających na zakres szeroko rozumianego bezpieczeństwa. Zakres znaczeniowy bezpieczeństwa łączony jest również z socjologią organizacji, eksplorującą nowe obszary zagrożeń zgodnie ze specjalizacją tej dyscypliny, z którą funkcjonowanie organizacji jest przedmiotem analiz¹.

Dodatkowo w socjologii organizacji podejmuje się takie wątki tematyczne, jak: problemy władzy i podejmowanie decyzji, artykulacja interesów i formułowanie celów, sprawowanie kontroli, czy wpływ struktur organizacyjnych na efektywność, rekrutację i socjalizację członków czy też relacje między otoczeniem a organizacjami².

Teorie socjologiczne akcentują funkcję społeczeństwa informacyjnego, jako typu społeczeństwa, w którym kluczową rolę pełni informacja. Informacja sensu stricte

¹ H. Sterniczek, M.Z. Żandarowski, *Socjologiczna teoria organizacji*, [w:] *Socjologia organizacji i kierowania*, pod red. Z. Gładziecki, Wyd. PWr, Wrocław 1989, s. 13.

² Ibidem, s. 12.

jest ważniejsza i bardziej cenna niż zasoby materialne. Społeczeństwo informacyjne związane jest z gwałtownym rozwojem technologii telekomunikacyjnej. Informatyzacja przekształciła dotychczasowe systemy pracy, zatrudnienia, sposoby sprawowania władzy, edukacji i oświaty, gospodarowania, wprowadzając nowe wzory kulturowe i cywilizacyjne³.

Co więcej, podstawowym czynnikiem produkcji staje się informacja i wiedza, która wymusza stosowanie nowoczesnych technologii i wpływa na kapitał ludzki oraz społeczny⁴. Oczywiście społeczeństwo informacyjne jest jednym z typów społeczeństw, które następują po sobie w wyniku postępu społecznego.

W przestrzeni społecznej informacja jest zmaterializowanym efektem komunikacji, której z kolei podstawą jest szeroko rozumiana wiedza. Poprzez informacje przekazujemy dane czy wiadomości, będące elementem dalszego procesu działania w społeczeństwie, unikalnego w swoim znaczeniu.

1. INTERPRETACJA POJĘCIA BEZPIECZEŃSTWA, JEGO ATRYBUTY I CHARAKTER

Przyznać należy, iż poczucie bezpieczeństwa stało się, czy też ciągle jest, wartością nadrzędną dla każdego ze społeczeństw. Już niektórzy autorzy proponują zastąpienie słów pokój i wojna pojęciami bezpieczeństwo oraz zagrożenia. Poniekąd zamienność tych terminów uwarunkowana jest także zmianą społeczno-kulturową⁵.

Współczesne teorie socjologiczne interpretują i wyjaśniają procesy społeczne zachodzące w czasie ostatnich kilkudziesięciu lat. Są one oparte na różnych modelach rzeczywistości społecznej, wskazując na niejednakowe czynniki zapewniające bezpieczeństwo lokalne, międzynarodowe czy globalne. Również literatura tego zakresu rozważa bezpieczeństwo jako stan, wartość czy też część tworzonych systemów. Niemniej analizy społeczeństw pierwotnych doprowadzają do wniosku, że stworzenie w świecie przyszłości bezpieczeństwa zbiorowego stanowi istotny warunek przetrwania kultury⁶.

Bezpieczeństwo jest jedną z podstawowych potrzeb człowieka, która jest dla niego bardzo ważna. Poczucie bezpieczeństwa powinno kojarzyć się ze stanem spokoju, brakiem lęku, strachu, obaw. Dyscyplina socjologii bezpieczeństwa w swoistych badaniach zdaje się koncentrować na określaniu stanu: układów, systemów, segmentów i ruchów społecznych służących bezpieczeństwu oraz destrukcyjnych wobec niego⁷. Dla każdego społeczeństwa problematyka bezpieczeństwa to jeden z podstawowych wymiarów jego sposobu myślenia o rzeczywistości społecznej. W ramach funkcjonowania społeczeństwa wyłania się instytucje będące odpowiedzialne za zapewnianie bezpie-

³ A. Giddens, *Socjologia*, Wyd. PWN, Warszawa 2006, s. 382.

⁴ M. Białach, *Rozwój społeczeństwa informacyjnego oraz e-gospodarki w ramach programu operacyjnego kapitał ludzki*, [w:] *Nowoczesność, Ponowoczesność. Społeczeństwo obywatelskie w Europie Środkowej*, pod red. S. Partycki, Wyd. KUL, Lublin 2007, s. 331.

⁵ J. Maciejewski, *Securitologia - uwagi socjologa: bezpieczeństwo w kontekście społeczno-kulturowym*, [w:] *Bezpečnosť a bezpečnostná veda : zborník vedeckých a odborných prác*, pod red. L. Hofreiter, Wyd. Akadémia ozbrojených síl generála Milana Rastislava Štefánika, Liptovský Mikuláš 2009, s. 54.

⁶ B. Malinowski, *Jednostka, społeczność, kultura*, Warszawa 2000, s. 308.

⁷ Z. Zagórski, *Socjologia bezpieczeństwa. O potrzebie nowej subdyscypliny?*, [w:] *Socjologiczne aspekty bezpieczeństwa Narodowego*, pod red. T. Leszczykiewicz, Z. Zagórski, Wyd. WSO im. T. Kościuszki, Wrocław 1999, s. 11.

czeństwa swoim obywatelom. Instytucje te działają w wielu obszarach życia społecznego, stąd też ich ilość jest uzależniona od obszarów wymagających zapewnianie bezpieczeństwa.

Przedstawić można zatem kilka definicji bezpieczeństwa. Jedną z nich podaje, że bezpieczeństwo jest pewnym stanem obiektywnym, polegającym na braku zagrożenia, odczuwanym subiektywnie przez jednostki i grupy. Oznacza to, że bezpieczeństwo składa się z dwóch elementów, obiektywnego i subiektywnego. Pierwszy z nich, mający charakter obiektywny, jest zewnętrzną w stosunku do jednostki, grupy społecznej, zbiorowości. Z kolei drugi ma charakter subiektywny i jest poczuciem bezpieczeństwa⁸. Natomiast w ujęciu potocznym bezpieczeństwo oznacza stan, w którym jednostka ma poczucie pewności, oparcie w drugiej osobie lub w sprawnie działającym systemie prawnym. Przeciwnością bezpieczeństwa jest stan zagrożenia.

Według J. Kukułki bezpieczeństwo rozumiane jest jako: określona pewność istot biologicznych i społecznych, która daje się postrzegać poprzez trzy współzależne wymiary, a mianowicie wymiar podmiotowy jako pewność istnienia i przetrwania, potwierdzający się brakiem poważnych zagrożeń dla interesów związanych z trwaniem fizycznym oraz poprzez wymiar przedmiotowy i procesualny jako pewność niezbędnych warunków rozwoju i aktywności teraz i w przewidywalnej przyszłości⁹.

Bezpieczeństwa nie powinno się traktować jako zmiennej niezależnej, gdyż ma ono następujący charakter:

- dynamiczny i procesualny – ulega ciągłym zmianom pod wpływem złożonych i wieloczynnikowych zjawisk;
- subiektywny i obiektywny – gdyż postawy społeczne wobec bezpieczeństwa tworzą się wskutek wpływu danego zjawiska na jednostkę, grupę społeczną, społeczeństwo;
- uszeregowany, strukturalizowany;
- relatywny – zależny od szeregu czynników¹⁰.

Wpływ na bezpieczeństwo mają wszystkie interakcje społeczne, a także zachodzące w gospodarce czy polityce. Kultura bezpieczeństwa danego społeczeństwa wskazuje na obowiązujący system znaczeń, poprzez który określona grupa ludzi rozumie zagrożenia na świecie. System ten zwiera również wyjaśnienia związane z wypadkami – dlaczego i jak powstają. Kultura bezpieczeństwa jest zatem wyrazem tego, jaki jest stosunek danej społeczności do ryzyka, zagrożeń i bezpieczeństwa oraz jakie wartości w tym zakresie uważane są za istotne. Wysoka kultura bezpieczeństwa jest związana z wysoką wartością nadawaną zdrowiu i życiu ludzkiemu oraz utrzymywaniem granicy między niezbędnym ryzykiem, które jest nieodłącznym elementem życia i rozwoju a zapewnieniem bezpieczeństwa i ochrony przed zagrożeniami¹¹. Dlatego też problema-

⁸ H. Korzeniowska, *Edukacja dla bezpieczeństwa w systemie oświatowym Europy na przykładzie Polski i Słowacji*, EAS, Kraków 2004, s. 9-11.

⁹ J. Kukułka, *Narodziny nowych koncepcji bezpieczeństwa*, [w:] *Bezpieczeństwo międzynarodowe w Europie środkowej po zimnej wojnie*, pod red. J. Kukułki, Warszawa 1994, s. 41.

¹⁰ J. Szmyd, *Bezpieczeństwo jako wartość. Refleksja aksjologiczna i etyczna* [w:] *Zarządzanie bezpieczeństwem*; pod red. P. Tyrała, Wyd. Profesjonalnej Szkoły Biznesu, Kraków 2000, s.166.

¹¹ J. Maciejewski, op. Cit., s. 55.

tyka bezpieczeństwa we współczesnych realiach społecznych jest bardzo ważnym obiektem badań.

2. KULTURA INFORMACYJNA

Ocena socjologii jako dziedziny naukowej zajmuje się również problematyką komunikacji międzyludzkiej. Jeśli uznaje się, że: zadaniem socjologii jest badanie życia ludzkiego we wszystkich jego różnorodnych przejawach¹², to komunikacja właśnie tym procesom podlega. Kreowana współcześnie kultura informacyjna w swoich korzeniach oparta jest na procesach komunikacji i przekazywania informacji. Stąd też zasadne jest traktowanie komunikacji (we wszystkich jej przejawach) jako faktu społecznego, mającego miejsce w zmienianiu rzeczywistości społecznej.

Powszechnie wykorzystywane symbole i znaki komunikacji stanowią o jakości informacji w przestrzeni społecznej. Na aspekty komunikacji powołuje się A. Giddens, określając ją jako: przepływ informacji od jednej jednostki lub grupy do innej jednostki bądź grupy. Komunikacja jest niezbędna dla interakcji społecznej¹³.

Kulturowe pochodzenie procesu komunikacji, a co za tym idzie przekazywanie informacji, będących efektem kumulowanej w przestrzeni społecznej wiedzy jest oczywista. Czynności społeczne tworzenia i przekazywania informacji są aktualnym doświadczeniem jednostek. W procesach socjalizacji człowiek uczy się zasad pełnienia ról społecznych i zawodowych, a co za tym idzie jego działania są zgodne z przyjętym systemem norm i wartości społecznych.

Kiedy ludzie podzielają te same wartości, zwykle zachowują się zgodnie z tym, jakiego zachowania oczekują od siebie nawzajem. Co więcej, często uważają taką zgodność za coś bardzo dobrego - nawet jeśli wydaje się ona sprzeczna z ich bezpośrednim interesem. Fakt, że te wspólne wartości są nabywane przez uczenie się, nie zaś dziedziczne, nie umniejsza ich wagi dla ludzkiego zachowania. Przeciwnie stają się one częścią osobowości jako takiej. W ten sposób spajają one społeczeństwo, ponieważ to, co społecznie oczekiwane staje się zarazem potrzebą indywidualną¹⁴. Stąd też zasadne jest łączenie bezpieczeństwa z wymiarem kulturowym człowieka.

O systemie społecznym można mówić wtedy, gdy mamy do czynienia ze zróżnicowaniem ról i pozycji społecznych a także społeczną akceptacją wynikających z tego zróżnicowania praw i obowiązków, oraz istnieniem wspólnych norm i wartości¹⁵. Bezpieczeństwo w systemie społecznym jest wartością nadrzędną i oczywistą. Owa kultura rozwija się we wszystkich płaszczyznach życia społecznego, w tym także w przestrzeni organizacji gospodarczych. Kultura informacyjna pozwala na zrozumienie zjawisk, jakimi są informacja i komunikacja, a w konsekwencji na ich wykorzystanie w organizacji gospodarczej. Można nawet przyjąć, że kultura informacyjna to jeden z istotniejszych elementów jej potencjału, co jest bardzo bliskie pojęciu kultury kierowania¹⁶. Oba elementy działania zorientowanego na przekaz informacyjny, jak

¹² A. Duszak, N. Fairclough, *Krytyczna analiza dyskursu. Interdyscyplinarne podejście do komunikacji społecznej*, Wyd. Universitas, Kraków 2008, s. 48.

¹³ A. Giddens, op.cit. s.723.

¹⁴ C.W. Mills, *Wyobraźnia socjologiczna*, Wyd. PWN, Warszawa, 2007, s. 85.

¹⁵ J. Szacki, *Historia myśli socjologicznej*, Wyd. PWN, Warszawa, 2002, s. 820.

¹⁶ A. Żebrowski, *Zakłócenie informacyjne elementem rozwoju organizacji gospodarczej*, [w:] *Wywiad*

i elementy kierowania zasobami organizacji (materialnymi i niematerialnymi) budują obszar bezpieczeństwa tejże organizacji.

Informacja buduje zasoby wiedzy organizacji, zasoby, które wykorzystywane są przez ludzi w procesach pracy. Jednakowoż pracownicy, jak i kierownicy tworzą system informacyjny w zamiarze realizacji ustanowionych celów organizacyjnych. Informacja, a raczej jej treść, jakość, czas przekazu czy istotność przesądzą o sukcesie organizacji gospodarczych.

3. BEZPIECZEŃSTWO INFORMACJI

Cudze tajemnice wzbudzają ciekawość tak ogromną, że poświęca się dla ich zdobycia duże pieniądze, a nawet życie. Podobnie ochrona własnych tajemnic bywa warta majątku, a także życia, najczęściej cudzego. To gra o najwyższą stawkę – bezpieczeństwo – które stało się wartością docenianą codziennie przez przezornego biznesmena, każdego człowieka, całe społeczeństwo. Zagrożenia braku informacji lub niebezpieczeństwo utraty tajemnicy zawsze towarzyszyły człowiekowi, ale obecnie nie tylko utrudniają życie i rozwój, ale wręcz stają się przyczyną destrukcji i upadku. Albo też szansą na niespodziewany sukces i fortunę¹⁷.

Powodem takiej sytuacji jest taki rozwój gospodarczy, polityczny i militarny świata, którego podstawowym elementem jest rywalizacja. Wpływ na to ma również globalizacja, powodująca istotne zmiany w podejściu do źródeł surowców naturalnych, niezbędnych do produkcji, a także nowych i otwierających się rynków zbytu. Czynniki te spowodowały przewartościowanie podejścia do bezpieczeństwa. Zarówno w życiu poszczególnych jednostek, jak i instytucji gospodarczych, czy nawet organizmów państwowych. Rozwój nowoczesnych technologii informacyjnych, na niespotykaną dotychczas skalę, spowodował rozwój wymiany informacji i wzrost jej znaczenia szczególnie informacji o działaniach potencjalnego konkurenta czy też przeciwnika. Cały ten stan rzeczy możemy nazwać postępującą wojną informacyjną. Szczególnie, że informacja wypiera tradycyjne dobra i staje się podstawową i pożądaną wartością, czy też zasobem.

Poczucie bezpieczeństwa jest jedną z podstawowych potrzeb człowieka – jest wartością nadrzędną. Bezpieczeństwo wyraża bowiem zintegrowany wskaźnik wszystkich cząstkowych wartości, które są dla człowieka najcenniejsze. W związku z tym, zaliczając bezpieczeństwo do dóbr podstawowych, należy podkreślić, iż powinno ono stanowić przedmiot najwyższej uwagi w zarządzaniu każdą organizacją gospodarczą¹⁸.

Warto wspomnieć o modelu D. Freia, który jest pomocny w kontekście postrzegania bezpieczeństwa. Uwzględniono w nim cztery elementy:

- stan braku bezpieczeństwa – w którym występuje rzeczywiste i istotne zagrożenie zewnętrzne, którego przedstawienie jest adekwatne;
- stan obsesji – w którym niewielkie zagrożenia postrzega się jako duże;

i kontrwywiad gospodarczy wobec wyzwań bezpieczeństwa biznesu, pod red. J. Kaczmarek, M. Kwieciński, Wyd. Dom Organizatora, Toruń 2010, s. 17.

¹⁷ L. Korzeniowski, A. Peplowski *Wywiad gospodarczy Historia i współczesność*, Wyd. EAS, Kraków 2005, s. 5.

¹⁸ M. Jabłoński, M. Mielus, *Zagrożenia bezpieczeństwa informacji w organizacji gospodarczej*, [w:] *Bezpieczeństwo informacji i biznesu Zagadnienia wybrane*, pod red. M. Kwieciński, Oficyna Wydawnicza AFM, Kraków 2010, s. 25.

- stan fałszywego bezpieczeństwa – w którym istotne zagrożenie postrzegane jest jako niewielkie;
- stan bezpieczeństwa – w którym zagrożenie wewnętrzne jest niewielkie, a jego postrzeganie prawidłowe¹⁹.

Gdy przejdziemy do pojęcia bezpieczeństwa informacyjnego, zauważymy różnice w definiowaniu tego zjawiska przez poszczególnych autorów. Bezpieczeństwem informacji możemy nazwać, według L. Ciborowskiego obronę informacyjną, która polega na uniemożliwieniu i utrudnieniu zdobywania danych o fizycznej naturze aktualnego oraz planowanego stanu rzeczy i zjawisk we własnej przestrzeni funkcjonowania, a także utrudnianiu wnoszenia entropii informacyjnej do komunikatów i destrukcji fizycznej do nośników danych²⁰.

Kolejna definicja bezpieczeństwa informacyjnego, opisana przez M. Jabłońskiego i M. Mielus, została skonstruowana poprzez przedsięwzięcia, jakie należy zastosować, aby uzyskać stan bezpieczeństwa i składają się na nie: zapobieganie (działanie prewencyjne), odstraszenie, wskazywanie i ostrzeżenie, wykrywanie, przygotowanie na sytuację awaryjną oraz reakcja na ewentualny atak²¹.

Wraz z rozwojem społeczeństwa informacyjnego, a tym samym zwiększenia znaczenia informacji w życiu gospodarczym poprzez informatyzację, poziom ochrony informacji wydaje się rzeczą priorytetową. Bardzo trafną definicję obszaru bezpieczeństwa informacji podali M. Kaliski, A. Kierkowska oraz G. Tomaszewski.

Bezpieczeństwo informacji to nie tylko zabezpieczenia fizyczne i techniczne zasobów informatycznych. Bezpieczeństwo informacji to przede wszystkim dążenie do zapewnienia i utrzymania poufności, integralności, dostępności, rozliczalności, autentyczności, niezaprzeczalności i niezawodności informacji i systemów, w których są one przetwarzane. To także odpowiednio przeszkolony i świadomy zagrożeń personel, to odpowiednio zdefiniowane umowy z dostawcami, to również sformalizowane plany ciągłego działania i procedury postępowania. Bezpieczeństwo to proces – i jak każdy proces – wymaga ciągłego doskonalenia²².

Ostatnią definicją, jaką przedstawię, jest najszersza definicja bezpieczeństwa informacyjnego zaproponowana przez P. Bączka. Jest ona bardzo podobna do potocznego rozumienia tego zjawiska, obejmująca ochronę tajemnicy służbowej i państwowej. Bezpieczeństwo informacyjne – w szerokim ujęciu – rozumiane jest jako stan wolny od zagrożeń, które pojmowane są głównie jako:

- przekazywanie informacji nieuprawnionym podmiotom;
- szpiegostwo;

¹⁹ K. Lidel, *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Wydawnictwo Adam Marszałek, Toruń 2006, s. 9.

²⁰ L. Ciborowski, *Walka informacyjna*, Wyd. Adam Marszałek, Toruń 1999, s. 186.

²¹ M. Jabłoński, M. Mielus. op.cit., s. 25.

²² M. Kaliski, A. Kierkowska, G. Tomaszewski, *Ochrona informacji i zasobów relacyjnych przedsiębiorstwa*, [w:] *Wywiad i kontrwywiad gospodarczy wobec wyzwań bezpieczeństwa biznesu*, pod red. J. Kaczmarek, M. Kwieciński, Wyd. Dom Organizatora, Toruń 2010, s. 34.

– działalność sabotażowa i dywersyjna²³.

Bezpieczeństwem informacyjnym jest również każde działanie, system lub metoda, które zmierzają do zabezpieczenia zasobów informacyjnych gromadzonych, przetwarzanych, przekazywanych, przechowywanych w pamięci komputerów oraz sieci teleinformatycznych²⁴.

Z prezentowanych powyżej definicji bezpieczeństwa informacyjnego, możemy wywnioskować, że składa się na nie nie tylko zabezpieczenie przed niepowołanym dostępem, kradzież danych czy ich zniszczenie. Należy je rozumieć znacznie szerzej.

Bezpieczeństwo informacyjne należy rozumieć jako składową bezpieczeństwa fizycznego, osobowo-organizacyjnego oraz teleinformatycznego organizacji gospodarczej²⁵.

Jest bezsprzecznym faktem, że zasoby informacyjne są najcenniejszym dobrem każdego przedsiębiorstwa. Docenienie tej informacji spowodowało uświadomienie sobie przez osoby zarządzające przedsiębiorstwem, że skuteczność ich działania i konkurencyjność na rynku zależna jest od pozyskania informacji. Spowodowało to wzrost znaczenia, a także rozwój wywiadu gospodarczego. Przedmiotem szczególnego zainteresowania konkurencyjnych firm są wyniki badań i plany konstrukcyjne, a także listy dostawców i klientów, planowane kampanie marketingowe, oraz polityka cenowa wobec klientów.

Zdobywanie informacji o konkurencji ma długą historię w gospodarce, jednak termin wywiad gospodarczy na zorganizowane zbieranie danych pojawił się stosunkowo niedawno. Możemy przyjąć za początek lata osiemdziesiąte XX w. Wtedy to w amerykańskich collegach zaczęto nauczać przedmiotu o zdobywaniu informacji o konkurencji.

Zdefiniowania pojęcia wywiad gospodarczy podjęli się w swojej encyklopedii autorzy N. Polmar i T.B. Allen, którzy piszą: wywiad gospodarczy to gromadzenie i ocena informacji o charakterze ekonomicznym, w przeważającej mierze pochodzących ze źródeł jawnych²⁶. Z kolei według M. Hermana wywiad wiąże się ze zbieraniem informacji, stawianiem pytań, opisem, przygotowaniem odpowiednich hipotez i przedstawieniem dowodów, tak aby prowadzić jak najbardziej efektywną politykę²⁷.

Powyższe definicje wywiadu nie wspominają o legalnych metodach pozyskiwania informacji i jawnych źródłach. Wywiad w znaczeniu potocznym to zdobywanie informacji od respondenta za pośrednictwem bezpośredniego kontaktu. Oczywiście w dobie nowoczesnych rozwiązań kontakt bezpośredni nie zawsze oznacza osobisty. Charakterystyczne jest rozróżnienie pojęcia wywiad, jako czegoś pozytywnego, od pojęcia szpiegostwo, które najczęściej na negatywną konotację.

²³ P. Bączek, *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Wyd. Adam Marszałek, Toruń 2006, s. 71.

²⁴ Ibidem.

²⁵ J. Łuczak, *Zarządzanie bezpieczeństwem informacji*, Wyd. U. E., Poznań, s. 80.

²⁶ N. Polmar, T.B. Allen, *Księga szpiegów Encyklopedia*, Wyd. Magnum, Warszawa, s. 636.

²⁷ M. Herman, *Potęga wywiadu*, Warszawa 2002, s. 11.

Na to rozróżnienie zwraca uwagę również L. Korzeniowski. Zasadnicza różnica pomiędzy wywiadem a szpiegostwem, dotyczy metod i źródeł informacji. Wywiad gospodarczy korzysta głównie z legalnych metod i jawnych źródeł informacji, natomiast szpiegostwo gospodarcze wykorzystuje metody zabronione prawem i niejawne, objęte tajemnicą lub zastrzeżone źródła informacji. Granica pomiędzy tak rozumianym wywiadem gospodarczym a szpiegostwem przemysłowym jest płynna i często to, co jedno państwo traktuje jako wywiad gospodarczy, przez inne może być traktowane jako szpiegostwo przemysłowe wymierzone w jego interesy²⁸.

Sam proces gromadzenia cennych informacji, czy to poprzez wyspecjalizowane działy firmy, czy też firmy zewnętrzne specjalizujące się w tym, jest schematyczny i można go przedstawić w następujący sposób:

- planowanie – określenie celu operacji wywiadowczej, sposobów zdobywania informacji oraz kontroli efektywności jednostek zajmujących się jej gromadzeniem;
- gromadzenie – proces zdobywania informacji i przekazywania ich do dalszej obróbki;
- przetwarzanie – proces przekształcania informacji przetworzonej w gotowe dane wywiadu, obejmujące analizę i interpretację;
- przekazywanie – dystrybucja danych wywiadowczych między odbiorców²⁹.

Nie istnieje jeden schemat organizowania pracy osób zajmujących się zdobywaniem informacji gospodarczych. W wielu krajach najpopularniejsza jest forma zinstytucjonalizowana, tworzone są firmy, najczęściej nazywane wywiadowniami gospodarczymi, pracownicy których posiadają odpowiednią wiedzę i umiejętności do pozyskiwania informacji. Oferują oni swoje usługi na wolnym rynku, pozostałym przedsiębiorstwom. Część firm jednak organizuje takie działy wewnątrz swojej struktury organizacyjnej, sporym mankamentem takiego rozwiązania jest odpowiedni dobór i szkolenie pracowników, a także personelu odpowiedzialnego za koordynację ich działań. Problemem może być również zapewnienie odpowiedniego zaplecza technicznego i informacyjnego.

Niezależnie czy proces zbierania informacji powierzymy firmie zewnętrznej czy też pracownikom naszego przedsiębiorstwa, niezwykle ważne jest, aby ich działania mieściły się w ramach prawa, a informację pozyskiwane były legalnymi metodami. W Polsce przepisami regulującymi w przestrzeni gospodarczej bezpieczeństwo informacji są akty prawne i przepisy, wśród których, wymienić można: Ustawę o ochronie danych osobowych³⁰, Ustawę o ochronie informacji niejawnych³¹, Ustawę o ochronie osób i mienia³², Ustawę o zwalczaniu nieuczciwej konkurencji³³, Kodeks Pracy³⁴ oraz

²⁸ L. Korzeniowski, A. Peplowski, *Wywiad gospodarczy Historia i współczesność*, Wydawnictwo EAS, Kraków 2005, s. 85.

²⁹ N. Polmar, T.B. Allen, op. cit., s. 137.

³⁰ Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz. U. 2002 r. Nr 101 poz. 926).

³¹ Ustawa o ochronie informacji niejawnych z dnia 5 sierpnia 2010 r. (Dz. U. Nr 182, poz. 1228).

³² Ustawa o ochronie osób i mienia z dnia 22 sierpnia 1997 r. (Dz.U. Nr 114, poz. 740). Tekst jednolity z dnia 26 lipca 2005 r. (Dz.U. Nr 145, poz. 1221).

³³ Ustawa o zwalczaniu nieuczciwej konkurencji (Dz.U. 1993 Nr 47 poz. 211).

Ustawę o prawie autorskim³⁵. Przytoczone uwarunkowania prawne wskazują, że bezpieczeństwo informacji nie jest jednorazowym aktem, lecz procesem jego ciągłego zapewniania.

PODSUMOWANIE

Rozwój techniki, jaki nastąpił po drugiej wojnie światowej, a w szczególności systemów telekomunikacyjnych i elektroniki, spowodował niezwykle szybki wzrost możliwości komunikacji. Nastąpiła era informacji, bowiem stała się ona najważniejszym i najbardziej pożądanym ze wszystkich zasobów. Większość ze składników sukcesu czy to przedsiębiorstwa, wojska czy państwa jako całości opiera się na przesyłaniu, zdobywaniu i kontrolowaniu informacji.

Systemy informatyczne we współczesnej przestrzeni gospodarczej, ze względu na szeroką skalę wykorzystywania narzędzi cyfrowych, stanowią z jednej strony bezcenne źródło skondensowanej wiedzy o stanie podmiotów gospodarczych i nie tylko, a z drugiej strony są celem dla nieuprawnionych w zdobywaniu tychże informacji, do bezwzględnej walki w konkurencyjnych obszarach działalności.

Dlatego też coraz bardziej zdajemy sobie sprawę z wagi, jaką ma dla naszego życia i funkcjonowania wiedza, jaką udało nam się zdobyć. Powoduje to naturalny stan, kiedy chronimy coraz lepiej informację, traktując ją jako nasze dobro. Jednocześnie nasi konkurenci chcą pozyskać posiadaną przez nas wiedzę jak najniższym kosztem. W wyniku sprzeczności interesów, a także wrogich działań stosuje się coraz bardziej skuteczne metody pozyskiwania informacji i ochrony przed nimi. Charakter tych działań obecnie prawie całkowicie został przeniesiony z gruntu społecznego czy też częściowo militarnego (choć zdobywanie informacji od zawsze jest integralną częścią działań militarnych) na płaszczyznę gospodarczą i zdobywanie wiedzy o konkurencyjnych firmach. Upowszechnienie tego zjawiska jest zależne w dużej mierze od poziomu informatyzacji, uprzemysłowienia i wielkości państwa, w jakim funkcjonuje przedsiębiorstwo.

Celem ochrony informacji jest zatem zapewnienie bezpieczeństwa dla cennych zasobów organizacji, takich jak informacje zarządcze, informacje o sprzęcie czy informacje o stosowanym oprogramowaniu. Poprzez dobór odpowiednich środków bezpieczeństwa wspomaga się skuteczniejsze osiągnięcie celów biznesowych, chroniąc tym samym cele firmy, jej misję, fizyczne i finansowe zasoby, reputację, pozycję prawną czy pracowników. Dlatego niezwykle istotne jest poznanie zagrożeń związanych z bezpieczeństwem informacji oraz sposobów przeciwdziałania tym zagrożeniom. Jest to o tyle istotne, że ze względu na bardzo dynamiczne zmiany, jakie zachodzą w związku z rozwojem technik informatycznych, pojawiają się nowe zagrożenia, nieznanne wcześniej. Szczególnym polem do manewru jest rozwój informatyki, co umożliwia zdobywanie informacji zdalnie, bez fizycznej obecności w miejscu jej przechowywania. Stanowi to wyzwanie nie tylko dla przedsiębiorców, dbających o swoje interesy, ale i dla państwa, które tak powinno skonstruować system prawny, aby zapewnić ochronę przed takimi działaniami, a w końcu nas samych, wszyscy jesteśmy przecież pracownikami i użytkownikami komputerów.

³⁴ Kodeks pracy, stan prawny na dzień 12 stycznia 2011 r.

³⁵ Ustawa o prawie autorskim i prawach pokrewnych z dnia 4 lutego 1994 r. (Dz.U. 1994 nr 24 poz. 83).

LITERATURA

1. Bączek P., *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Wyd. Adam Marszałek, Toruń 2006.
2. Białach M., *Rozwój społeczeństwa informacyjnego oraz e-gospodarki w ramach programu operacyjnego kapitał ludzki*, [w:] *Nowoczesność, Ponowoczesność. Społeczeństwo obywatelskie w Europie Środkowej*, pod red. Partynicki S., Wyd. KUL, Lublin 2007.
3. Ciborowski L., *Walka informacyjna*, Wyd. Adam Marszałek, Toruń 1999.
4. Duszak A., Fairclough N., *Krytyczna analiza dyskursu. Interdyscyplinarne podejście do komunikacji społecznej*, Wyd. Universitas, Kraków 2008.
5. Giddens A., *Socjologia*, Wyd. PWN, Warszawa 2006.
6. Herman M., *Potęga wywiadu*, Wyd. Bellona, Warszawa 2002.
7. Jabłoński M., Mielus M., *Zagrożenia bezpieczeństwa informacji w organizacji gospodarczej*, [w:] *Bezpieczeństwo informacji i biznesu Zagadnienia wybrane*, pod red. Kwieciński M., Oficyna Wydawnicza AFM, Kraków 2010.
8. Kaliski M., Kierkowska A., Tomaszewski G., *Ochrona informacji i zasobów relacyjnych przedsiębiorstwa* [w:] *Wywiad i kontrwywiad gospodarczy wobec wyzwań bezpieczeństwa biznesu*, pod red. Kaczmarek J., Kwieciński M., Wyd. Dom Organizatora, Toruń 2010.
9. Korzeniowska H., *Edukacja dla bezpieczeństwa w systemie oświatowym Europy na przykładzie Polski i Słowacji*, Wyd. EAS, Kraków 2004.
10. Korzeniowski L., Peplowski A., *Wywiad gospodarczy Historia i współczesność*, Wyd. EAS, Kraków 2005.
11. Kukułka J., *Narodziny nowych koncepcji bezpieczeństwa*, [w:] *Bezpieczeństwo międzynarodowe w Europie środkowej po zimnej wojnie*, pod red. Kukułka J., Warszawa 1994.
12. Lidel K., *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Wydawnictwo Adam Marszałek, Toruń 2006.
13. Łuczak J., *Zarządzanie bezpieczeństwem informacji*, Wyd. U. E., Poznań 2001.
14. Maciejewski J., *Securitologia – uwagi socjologa: bezpieczeństwo w kontekście społeczno-kulturowym*, [w:] *Bezpečnosť a bezpečnostná veda : zborník vedeckých a odborných prác*, pod red. Hofreiter L., Wyd. Akadémia ozbrojených síl generála Milana Rastislava Štefánika, Liptovský Mikuláš 2009.
15. Malinowski B., *Jednostka, społeczność, kultura*, PWN, Warszawa 2000.
16. Mills C.W., *Wyobrażenia socjologiczne*, Wyd. PWN, Warszawa 2007.
17. Polmar N., Allen T.B., *Księga szpiegów Encyklopedia*, Wyd. Magnum, Warszawa 2000.
18. Sterniczek H., Żandarowski M.Z., *Socjologiczna teoria organizacji*, [w:] *Socjologia organizacji i kierowania*, pod red. Gładziecki Z., Wyd. PWr, Wrocław 1989.

19. Szacki J., *Historia myśli socjologicznej*, Wyd. PWN, Warszawa 2002.
20. Szmyd J., *Bezpieczeństwo jako wartość. Refleksja aksjologiczna i etyczna* [w:] *Zarządzanie bezpieczeństwem*, pod red. Tyrała P., Wyd. Profesjonalnej Szkoły Biznesu, Kraków 2000.
21. Zagórski Z., *Socjologia bezpieczeństwa. O potrzebie nowej subdyscypliny?*, [w:] *Socjologiczne aspekty bezpieczeństwa narodowego*, pod red. Leszczykiewicz T., Zagórski Z., Wyd. WSO im. T. Kościuszki, Wrocław 1999.
22. Żebrowski A., *Zakłócenie informacyjne elementem rozwoju organizacji gospodarczej*, [w:] *Wywiad i kontrwywiad gospodarczy wobec wyzwań bezpieczeństwa biznesu*, pod red. Kaczmarek J., Kwieciński M., Wyd. Dom Organizatora, Toruń 2010.

INFORMATION SECURITY CONSIDERATIONS IN FINANCIAL INSTITUTIONS

Summary

The theme of the article is the issues related to conducting business in the era of information society. The article is an interdisciplinary presentation of the risks posed by the operation of modern enterprises. Today information has a greater value than material resources. The article will present major threats and the methods of counteracting them.

Keywords: *information security, secret information, information culture*

NOTA BIOGRAFICZNA

mgr Zdzisław LUDZIEJEWSKI – doktorant Instytutu Socjologii Uniwersytetu Wrocławskiego, uczestnik 12 Międzynarodowych Konferencji Naukowych w kraju i zagranicą (m.in. w Akademii Obrony Narodowej im gen. Stefanika w Liptowskim Mikulaszu na Słowacji), autor 12 publikacji, członek Polskiego Towarzystwa Socjologicznego, członek Konwentu Wydziału Nauk Społecznych Uniwersytetu Wrocławskiego.