BEZPIECZEŃSTWO

INFORMACJI I BIZNESU

Zagadnienia wybrane

BEZPIECZEŃSTWO

INFORMACJI I BIZNESU

Zagadnienia wybrane

pod redakcją
Mirosława Kwiecińskiego

Kraków 2010

Recenzja: prof. dr hab. Leopold Ciborowski

Projekt okładki: Joanna Sroka

Korekta: Izabela Pabisz-Zarębska

ISBN 978-83-7571-104-2

Na zlecenie:

Krakowskiej Akademii
im. Andrzeja Frycza Modrzewskiego
www.ka.edu.pl

Wydawca:
Krakowskie Towarzystwo Edukacyjne sp. z o.o. – Oficyna Wydawnicza AFM,
Kraków 2010

Sprzedaż prowadzi:
Księgarnia „U Frycza"
Kampus Krakowskiej Akademii im. Andrzeja Frycza Modrzewskiego
ul. Gustawa Herlinga-Grudzińskiego 1, 30-705 Kraków
tel./faks: (12) 252 45 93
e-mail: ksiegarnia@kte.pl

Skład: Oleg Aleksejczuk

Druk i oprawa: ESUS

Spis treści

Wstęp

Problematyka bezpieczeństwa obejmuje wiele istotnych dziedzin ludzkiej aktywności. Wzrasta także ogromne zainteresowanie potrzebą badań i kształcenia w dziedzinie wykorzystania wiedzy o zagrożeniach i sposobach ich minimalizowania. Potrzeba ta wynika z zainteresowania tą problematyką praktycznie wszystkich prowadzących aktywną działalność społeczną, gospodarczą czy na rzecz organów państwa. Bezpieczeństwo stało się nie tylko modne, ale głównie niezbędne.

Wśród organizatorów obrad konferencji naukowych, poświęconych tej tak ważnej problematyce, nie mogło zabraknąć także Krakowskiej Akademii im. Andrzeja Frycza Modrzewskiego. Uczelnia posiada w swoim dorobku bogatą ofertę kształcenia w zakresie bezpieczeństwa oraz ochrony informacji. Kształcenie w zakresie bezpieczeństwa realizowane jest na dwóch wydziałach:

- Nauk o Bezpieczeństwie, na których prowadzi się zajęcia na kierunku bezpieczeństwo narodowe, oraz na
- Wydziale Ekonomii i Zarządzania, na którym w ramach kierunku zarządzanie prowadzone są zajęcia na specjalności zarządzanie bezpieczeństwem, oraz na kierunku informatyka i ekonometria na specjalności bezpieczeństwo i kontrola systemów informacyjnych.

Wśród organizatorów konferencji znalazło się także powołane przez uczelnię Międzynarodowe Stowarzyszenie „Edukacja dla Obronności i Bezpieczeństwa". Tym samym obradom konferencji i przekazywaniu jej rezultatów nadano międzynarodowy wymiar.

Prezentowane wydawnictwo stanowi plon obrad międzynarodowej konferencji naukowej zorganizowanej w dniach 12–13 października 2008 roku przez Katedrę Zarządzania Informacją, działającą w ramach Wydziału Ekonomii i Zarządzania, oraz, jak już wspomniano, przez Międzynarodowe Stowarzyszenie „Edukacja dla Obronności i Bezpieczeństwa". Ambicją organizatorów konferencji było włączenie w tok dyskusji licznych przedstawicieli organów administracji państwa i samorządu, praktyki gospodarczej, nauki, mediów oraz studentów, zarówno z kraju, jak i z zagranicy. W odpowiedzi na zaproszenie do udziału w konferencji napłynęło blisko 30 referatów problemowych. Autorami wszystkich przygotowanych tekstów są uznani eksperci w dziedzinie bezpieczeństwa, ochrony informacji, jak również młodzi pracownicy szkół wyższych, a także przedstawiciele praktyki gospodarczej. Patronat medialny objęło pismo o ogólnopolskim zasięgu i uznanej renomie – „Czasopismo Zabezpieczenia".

Całość rozważań autorów podzielona została na kilka części, ściśle ze sobą powiązanych. Odnoszą się one do szerokiej wizji problematyki bezpieczeństwa i zawarte zostały pod następującymi hasłami:

- Bezpieczeństwo informacji,
- Edukacja na rzecz bezpieczeństwa,
- Bezpieczeństwo biznesu, gospodarki i społeczeństwa.

Wypada żywić przekonanie, że każdy wymagający Czytelnik znajdzie dla siebie w przedstawionym materiale tekst, stanowiący dla niego inspirację, czy to badawczą, czy odnoszącą się do praktycznego wymiaru, w tym szczególnie do projektowania systemów i strategii bezpieczeństwa.

Mirosław Kwieciński

Część I
Bezpieczeństwo informacji

Adam Hernas

Bezpieczeństwo informacji, bezpieczeństwo teleinformatyczne i polityka bezpieczeństwa – trzy wymiary ochrony informacji i danych osobowych

Bezpieczeństwo informacji

W dobie istniejącego rozwoju nowych technologii informatycznych i telekomunikacyjnych, wykorzystywanych w coraz większym stopniu do przetwarzania informacji oraz danych osobowych zarówno przez instytucje państwowe, jak i przedsiębiorstwa oraz firmy prywatne, na pierwsze miejsce zdaje się wysuwać zagadnienie prawidłowego zabezpieczenia tego rodzaju aktywów. Współczesne sieci telekomunikacyjne w coraz większym stopniu łączone są w jedną globalną sieć, która nosi nazwę „cyfrowa sieć zintegrowanych usług" (ISDN)[1]. Zadaniem tej sieci jest dostarczenie użytkownikowi szerokiego spektrum usług telekomunikacyjnych, takich jak: przesyłanie głosu, danych, tekstu, a nawet statystycznych i dynamicznych obrazów[2].

Z drugiej strony, nie ma organizacji, która po utracie ważnych i poufnych informacji nie poniosłaby strat. Dowodem na to może być niedawny wyciek danych osobowych z jednego z największych banków w Polsce, kiedy to w wyniku nieprawidłowego zabezpieczenia dostępu do systemu informatycznego, do Internetu dostało się ponad 3 tys. plików zawierających szczegółowe informacje na temat tzw. „wrażliwych danych". Spowodowało to ogólne niezadowolenie i frustrację osób, których życiorysy i listy motywacyjne znalazły się w posiadaniu osób postronnych, nieposiadających prawa dostępu do tego rodzaju informacji. W konsekwencji osłabiło to poczucie bezpieczeństwa interesariuszy banku oraz ich poziom zaufania do tej instytucji.

W tym miejscu należy sobie zadać następujące pytania:

1) Jak w demokratycznym państwie zapobiegać tego rodzaju zdarzeniom, mającym zdecydowanie negatywny wpływ na funkcjonowanie zarówno administracji państwowej, jak i całego sektora prywatnego?
2) Czy wymagania natury prawnej i technicznej stawiane zarówno nowoczesnym systemom informatycznym, jak i ich użytkownikom są na tyle wystarczające, aby zapewnić obywateli, że ich dane nie dostaną się w posiadanie osób do tego nieupoważnionych lub postronnych?

Aby odpowiedzieć na tak zadane pytania, należy przede wszystkim zacząć od wskazania prawnych regulacji dotyczących tematyki ochrony informacji i danych osobowych.

---

[1] Ang. Integrated Services Digital Network.

[2] K. Napierała, *Prawne aspekty ochrony danych osobowych przetwarzanych w systemach teleinformatycznych*, Warszawa 1997, s. 21.

Na pierwszym miejscu można zatem wymienić Konstytucję Rzeczypospolitej Polskiej[3], która w art. 61 ust. 3 mówi, że „ze względu na ochronę wolności i praw innych osób i podmiotów gospodarczych oraz ochronę porządku publicznego, bezpieczeństwa lub ważnego interesu gospodarczego państwa można ograniczyć prawo dostępu do uzyskiwania informacji". Przepis ten ma kluczowe znaczenie dla zrozumienia charakteru prawa dostępu do informacji – choć prawo to ma charakter powszechny, to jednak może podlegać pewnym ograniczeniom.

Z kolei zagadnienia ochrony danych osobowych jako elementu strukturalnego systemu praw i wolności obywatelskich zostały uregulowane w art. 51 tego aktu generalnego, który stanowi m.in., że „nikt nie może być zobowiązany, inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby". Ustawa zasadnicza precyzuje więc fundamenty ochrony danych osobowych w naszym kraju, delegując jednocześnie uprawnienia do tworzenia przepisów rangi niższej[4].

Analizując dalsze rozwiązania prawne z zakresu ochrony informacji i danych osobowych, należy przede wszystkim wyjaśnić, co rozumiemy przez pojęcia: „informacja" oraz „dane osobowe". Otóż zgodnie z art. 6 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[5], za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, tzn. takiej, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Zatem danymi osobowymi nie są określenia ogólne, które nie wskazują konkretnej osoby, np. „Adam, blondyn, prawnik", lecz gdy dodamy: „30 lat, zatrudniony w oddziale X spółki Y w Krakowie na I piętrze", będą to już dane osobowe, gdyż na ich podstawie możemy bez większego problemu zidentyfikować i odnaleźć osobę, której te dane dotyczą.

W każdej chwili mogą być tworzone także nowe formy danych osobowych. Przykładem jest nadanie obywatelowi nowego numeru identyfikacyjnego PESEL czy identyfikacja za pomocą badania struktury kwasu DNA[6].

Informacja stanowi także jeden z najważniejszych aktywów (majątku) współczesnych organizacji. Jest to definicja dość ogólna, która nie zawiera w sobie żadnej klasyfikacji, jednak w kontekście działalności przedsiębiorstw przykładem informacji może być treść wszelkiego rodzaju dokumentów. Ponadto informacja wyrażana i przekazywana jest za pomocą mowy, znaków, obrazu i dźwięku. Może być ona również zapisana, przechowywana i wielokrotnie przetwarzana zarówno na papierze, elektronicznie, jak i na innych nośnikach informacji[7]. Często przybiera ona formę tajemnicy zawodowej lub innych tajemnic prawnie chronionych.

Innym rodzajem informacji jest ta, której nieuprawnione ujawnienie może spowodować istotne zagrożenie dla podstawowych interesów Rzeczypospolitej Polskiej w kwestiach dotyczących porządku publicznego, obronności, bezpieczeństwa, sto-

---

[3] Dz.U. z 1997 r., Nr 78, poz. 483.

[4] R. Szałowski, *Ochrona danych osobowych – komentarz do ustawy*, Zielona Góra 2000, s. 7.

[5] Dz.U. z 2002 r., Nr 101, poz. 926 ze zm.

[6] K. Napierała, *op. cit.*, s. 21.

[7] T. Polaczek, *Audyt bezpieczeństwa informacji w praktyce*, Gliwice 2006, s. 13.

sunków międzynarodowych lub gospodarczych państwa. Ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych[8] nazywa taką informację tajemnicą państwową, wprowadzając jednocześnie definicję tajemnicy służbowej, czyli informacji niejawnej niebędącej tajemnicą państwową, uzyskanej w związku z czynnościami służbowymi albo wykonywaniem prac zleconych, której nieuprawnione ujawnienie mogłoby narazić na szkodę interes państwa, interes publiczny lub prawnie chroniony interes obywateli albo jednostki organizacyjnej[9].

Na kierowniku danej jednostki organizacyjnej spoczywa m.in. obowiązek powołania pełnomocnika ds. ochrony informacji niejawnych (pełnomocnika ochrony), czyli osoby odpowiedzialnej za zapewnienie przestrzegania przepisów zawartych w przedmiotowej ustawie. W przypadku ochrony danych osobowych taką osobą jest administrator danych, który decyduje o celach i środkach przetwarzania danych osobowych. Jednak sama uoin[10] nie definiuje pojęcia „kierownik jednostki organizacyjnej", zatem zastosowanie będą tu miały przepisy określające byt prawny poszczególnych jednostek, np. urzędów państwowych i samorządowych, spółek prawa handlowego, przedsiębiorstw państwowych czy stowarzyszeń[11].

W zakres informacji niejawnych stanowiących tajemnicę państwową wchodzą informacje oznaczone klauzulami „ściśle tajne" i „tajne", zaś w przypadku tajemnicy służbowej – informacje niejawne o klauzulach „poufne" i „zastrzeżone". Ważnym elementem w realizacji ochrony tych informacji jest więc świadomość, przed kim i w jaki sposób mają być one chronione. Przede wszystkim należy chronić je przed ujawnieniem osobom nieuprawnionym, przed niezamierzonym zniszczeniem, kradzieżą lub zagubieniem, przed niewykrytym dostępem osób nieuprawnionych, a także atakami grup terrorystycznych, sabotażowych oraz kryminalnych[12].

Istotne jest także, aby wszystkie czynności przy dokumentach o wysokim stopniu poufności i tajności wykonywane były w strefach kontrolowanego dostępu czy strefach bezpieczeństwa, zabezpieczonych przez strefy administracyjne. Obowiązek ten wynika bezpośrednio z art. 57 uoin, zaś jego realizacja pozwala na prowadzenie wstępnej, tzw. fizycznej selekcji osób, które mogą mieć dostęp do materiałów stanowiących tajemnicę państwową czy służbową. Ustawa wprowadza także wymóg uzyskania przez te osoby poświadczenia bezpieczeństwa, stosownego do rodzaju przetwarzanych informacji niejawnych, z którymi mają one styczność, jak również obowiązek odbycia przez nie stosownego przeszkolenia.

Miejscem przechowywania, wytwarzania, przetwarzania lub przekazywania dokumentów zawierających informacje niejawne jest kancelaria tajna. Stanowi ją wyodrębniona komórka organizacyjna podległa bezpośrednio pełnomocnikowi i jest ona odpowiedzialna za właściwe rejestrowanie, przechowywanie i obieg oraz wydawanie dokumentów uprawnionym do tego osobom[13]. Kancelaria taka powinna mieścić się w wyodrębnionym pomieszczeniu, zabezpieczonym zgodnie z przepisami i środkami

---

[8] Dz.U. z 1997 r., Nr 78, poz. 483.

[9] T. Szewc, *Ochrona informacji niejawnych – komentarz*, Warszawa 2007, s. 68.

[10] Ustawa o ochronie informacji niejawnych [skrót autora].

[11] M.R. Taradejna, *Tajemnica państwowa i inne tajemnice chroniące interesy państwa i obywateli*, Warszawa 1999, s. 76.

[12] B. Jakubus, M. Ryszkowski, *Ochrona informacji niejawnych*, Warszawa 2001, s. 62.

[13] B. Kurzępa, *Ochrona informacji niejawnych. Zbiór przepisów*, Bielsko-Biała 2000, s. 19.

ochrony fizycznej informacji niejawnych, zawartych w rozporządzeniu Rady Ministrów z dnia 18 października 2005 r. w sprawie organizacji kancelarii tajnych[14] i winna być nadzorowana przez pracowników pionu ochrony (w tym np. służby dyżurne).

Bezpieczeństwo teleinformatyczne

Dokonując klasyfikacji informacji oraz wyjaśniając pojęcie danych osobowych, w następnej kolejności należałoby przeanalizować, jak polski ustawodawca uregulował kwestie wymagań stawianych systemom informatycznym przetwarzającym informacje (w tym niejawne) oraz dane osobowe.

Na podstawie art. 62 ust. 1 uoin zostało wydane rozporządzenie Prezesa Rady Ministrów z dnia 25 sierpnia 2005 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego[15]. W §1 tego aktu prawnego określono główne wymagania bezpieczeństwa teleinformatycznego, jakim winny odpowiadać systemy i sieci teleinformatyczne służące do wytwarzania, przetwarzania, przechowywania lub przekazywania informacji niejawnych, jak również sposób opracowywania dokumentów szczególnych wymagań bezpieczeństwa i procedur bezpiecznej eksploatacji systemów lub sieci teleinformatycznych.

Zgodnie z §3.1 przedmiotowego rozporządzenia, bezpieczeństwo teleinformatyczne zapewnia się, chroniąc informacje przetwarzane w systemach i sieciach teleinformatycznych przed utratą właściwości gwarantujących to bezpieczeństwo, w szczególności przed utratą poufności, dostępności i integralności. Dlatego też zadaniem kierownika danej komórki organizacyjnej, na którym *de facto* bezpośrednio spoczywa obowiązek ochrony informacji niejawnych oraz właściwej organizacji bezpieczeństwa teleinformatycznego, powinno być przede wszystkim zastosowanie takich procedur oraz środków ochrony fizycznej informacji, które zminimalizują możliwość utraty ww. atrybutów bezpieczeństwa systemu. Ogólne zasady realizacji tego obowiązku określono w art. 56–59 uoin. Praktyczna realizacja ww. przepisów będzie zaś polegać m.in. na wydzieleniu stref bezpieczeństwa, stworzeniu systemu przepustek czy stosowaniu urządzeń kryptograficznych, posiadających odpowiednie certyfikaty. Wykonanie tych czynności winno mieć również odzwierciedlenie m.in. w dokumencie o nazwie „Plan ochrony informacji niejawnych".

Bezpieczeństwo infrastruktury teleinformatycznej zależy także od odpowiedniego postępowania pracowników, którzy muszą zdawać sobie sprawę, kiedy ich działanie jest właściwe, a kiedy może być ryzykowne dla całej firmy czy jednostki organizacyjnej. Dlatego ważne jest, aby odbywali oni okresowe szkolenia z zakresu bezpieczeństwa teleinformatycznego oraz uaktualniali wymagane poświadczenia bezpieczeństwa. W warunkach niskiej świadomości zagrożeń wśród osób, które korzystają z systemów i sieci teleinformatycznych procedury postępowania z informacjami niejawnymi przy wykorzystaniu tych systemów i sieci powinny być wyjątkowo rygorystyczne i szczegółowe. Niezbędne jest więc praktyczne analizowanie związanych z tym zagrożeń, w ramach odbywanych z pracownikami szkoleń. Bez tego elementu w ich postępowaniu

[14] Dz.U. z 2005 r., Nr 208, poz. 1741.

[15] Dz.U. z 2005 r., Nr 171, poz. 1433.

będą pojawiały się błędy skutkujące nie pojedynczą, ale stałą utratą informacji podlegających ochronie[16].

Wydaje się, że informacje zawarte w tej części opracowania są odpowiedzią na pierwsze z postawionych pytań.

Polityka bezpieczeństwa

Na podstawie art. 39a uodo[17], zostało wydane rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych[18]. Rozporządzenie to określiło tryb prowadzenia i zakres dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych informacji odpowiednią do zagrożeń oraz kategorii danych objętych tą ochroną. Ponadto zostały w nim zawarte podstawowe warunki techniczne i organizacyjne, jakie powinny spełniać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, jak również wymagania w zakresie odnotowywania udostępniania danych osobowych i bezpieczeństwa przetwarzania danych osobowych. Akt ten nałożył także na kierowników jednostek organizacyjnych podległych MSWiA obowiązek prowadzenia dokumentacji opisującej sposób przetwarzania danych osobowych. Na mocy §3.1 rozporządzenia musiały powstać dwa dokumenty: polityka bezpieczeństwa przetwarzania danych osobowych oraz instrukcja zarządzania systemem informatycznym, w których uregulowano procedury zarządzania oraz zabezpieczenia danych osobowych w administracji publicznej.

Polityka bezpieczeństwa stanowi z kolei dokument zawierający szereg zaleceń oraz jasno sprecyzowanych zadań, których celem jest zabezpieczenie jednostki organizacyjnej lub firmy przed nieuprawnionym udostępnieniem informacji. W dokumencie tym określa się zalecenia dotyczące nie tylko systemów informatycznych i ich zabezpieczenia, ale także kwestie obiegu dokumentów wewnątrz jednostki (firmy), klasyfikacje poziomów dostępu do informacji oraz zasady uzyskiwania fizycznego dostępu do pomieszczeń, w których przechowywane są i przetwarzane chronione informacje[19].

Polityka bezpieczeństwa reguluje zatem następujące procedury:

1) Ochrony danych osobowych;
2) Ochrony dokumentów;
3) Ochrony prawa autorskiego[20].

Uzyskany przez przedsiębiorstwo (firmę) Certyfikat ISO 17799 z zakresu wdrażania polityki bezpieczeństwa stanowi świadectwo, że w przedsiębiorstwie stosuje

---

[16] Zob. M. R. Taradejna, *op. cit.*, s. 81.

[17] Ustawa o ochronie danych osobowych [skrót autora].

[18] Dz.U. z 2004 r., Nr 100, poz. 1024.

[19] T. Polaczek, *op. cit.*, s. 13.

[20] K. Czerwiński, *Audyt wewnętrzny*, Warszawa 2004, s. 190.

się właściwe środki techniczne i organizacyjne, zgodne ze standardem ISO-17799[21] i gwarantujące ochronę poufności, autentyczności i spójności informacji na wszystkich etapach jej przetwarzania[22]. Bardzo ważny z punktu widzenia przestrzegania zaleceń polityki bezpieczeństwa jest art. 23 uodo, który dopuszcza przetwarzanie danych tylko wtedy, gdy:

1) osoba, do której odnoszą się dane, wyrazi na to zgodę, chyba że chodzi o usunięcie tychże danych;
2) zezwalają na to przepisy prawa;
3) jest konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia koniecznych działań przed zawarciem umowy;
4) jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego;
5) jest niezbędne do wypełnienia prawnie usprawiedliwionych celów administratorów danych lub osób trzecich, którym te dane są przekazywane – a przetwarzanie danych nie narusza praw i wolności osoby, której dane dotyczą.

W przypadkach określonych w pkt 3–5 mówi się nie tylko o prawnych przesłankach przetwarzania danych osobowych, ale równocześnie jest to kryterium służące do określania rodzaju danych, jakie mogą być gromadzone[23].

Zarówno w myśl polskiej uodo, jak i regulacji europejskich kategorycznie zabronione jest przetwarzanie tzw. „informacji szczególnie chronionych" (ang. *sensitive data*). Dyrektywa nr 95/46/CE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych ze względu na przetwarzanie danych o charakterze osobowym oraz swobodnego przepływu tych danych[24] zabrania przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność do związków zawodowych, jak również przetwarzanie danych dotyczących zdrowia i życia seksualnego.

Polska uodo w art. 27 ust. 1 poszerza ten katalog o dane osobowe dotyczące: przynależności wyznaniowej lub partyjnej, kodu genetycznego, nałogów, skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym. Jednocześnie w ust. 2 ustawodawca zamieszcza obszerny wykaz sytuacji, w których przetwarzanie informacji objętych zakazem jest jednak dopuszczalne. Przesłanki dopuszczalności przetwarzania danych szczególnie chronionych mają zatem charakter podmiotowy, przedmiotowy bądź sytuacyjno-funkcjonalny[25].

Sytuacje naruszenia ochrony danych osobowych, a zwłaszcza *sensitive data* z punktu widzenia polityki bezpieczeństwa informacji określone są jako sytuacje kryzysowe, związane z incydentami bezpieczeństwa dotyczącymi przetwarzania specyficznej grupy informacji.

---

[21] Odpowiednikiem tego standardu jest obecnie polski standard PN – ISO/IEC 17779: 2007, *Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zarządzania bezpieczeństwem informacji*, http://www.tuv-nord.pl/ (20.07.2008).

[22] http://www.qualityprogress.com.pl/ (16.07.2008).

[23] R. Szałowski, *op. cit.*, s. 85.

[24] Dz. Urz. UE L281 z 23.11.1995.

[25] R. Szałowski, *op. cit.*, s. 103.

Sytuacją kryzysową, według polityki bezpieczeństwa, jest wystąpienie, zagrożenie lub domniemanie kradzieży nieautoryzowanego dostępu, modyfikacji, zatajenia lub utraty (zniszczenia) przetwarzanej w systemie określonej grupy informacji[26].

Naruszenie ochrony danych osobowych może być skutkiem różnych czynników, jak np.:

1) szkodliwego wpływu środowiska na system przetwarzania danych osobowych;
2) zewnętrznych zdarzeń losowych dotyczących systemu przetwarzania danych osobowych;
3) zamierzonych lub niezamierzonych czynności użytkowników dopuszczonych do przetwarzania danych osobowych;
4) nieuprawnionych działań osób nieupoważnionych do dostępu do danych osobowych[27].

Przedmiotowe rozporządzenie Ministerstwa Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. nakłada także na kierowników jednostek organizacyjnych obowiązek opracowania i posiadania formalnej instrukcji zarządzania ochroną danych osobowych. Instrukcja zarządzania określa sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem procedur nadawania uprawnień, metod i środków uwierzytelniania użytkowników, sposobu zabezpieczenia systemu teleinformatycznego oraz nośników zawierających dane osobowe. Zawarte w niej procedury i wytyczne są obowiązujące dla wszystkich użytkowników systemów, stosownie do przydzielonych uprawnień, zakresu obowiązków i odpowiedzialności.

Do obsługi systemu informatycznego oraz wchodzących w jego skład urządzeń służących do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie wydane przez administratora danych, który obowiązany jest zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane, zwłaszcza gdy przekazuje się je za pomocą urządzeń teletransmisji danych. Prowadzi on także ewidencję osób zatrudnionych przy ich przetwarzaniu. Osoby te są zobowiązane do zachowania tego rodzaju danych w tajemnicy, tzn. nie mogą ich ujawniać podmiotom i osobom nieuprawnionym, przy czym obowiązek ten trwa również po ustaniu zatrudnienia[28].

W rozporządzeniu wprowadzono dodatkowo trzy poziomy zabezpieczeń systemów informatycznych, które uwzględniają kategorie modyfikowanych danych oraz zagrożenia wynikające z ich przetwarzania:

1) Podstawowy, który stosuje się, gdy w systemie informatycznym nie są przetwarzane dane ujawniające pochodzenie rasowe lub etniczne oraz jeżeli żadne z urządzeń systemu informatycznego służącego do przetwarzania danych osobowych nie jest połączone z siecią publiczną;
2) Podwyższony, jeżeli w systemie informatycznym przetwarzane są dane ujawniające pochodzenie rasowe lub etniczne oraz jeżeli żadne z urządzeń systemu informatycznego służącego do przetwarzania danych osobowych nie jest połączone z siecią publiczną;

---

[26] M. Byczkowski, *Polityka Bezpieczeństwa Informacji a ochrona danych osobowych. Część III*, „Ochrona Danych Osobowych" 2000, nr 8.

[27] http://www.qualityprogress.com.pl/ (16.07.2008).

[28] R. Szałowski, *op. cit.*, s. 146.

3) Wysoki, gdy przynajmniej jedno urządzenie systemu informatycznego służącego do przetwarzania danych osobowych połączone jest z siecią publiczną[29].

Ochrona danych osobowych w SIS oraz VIS

Bardzo ważnym i interesującym, choć w polskiej rzeczywistości stosunkowo nowym tematem jest ochrona danych osobowych w Systemie Informacyjnym Schengen (ang. *Schengen Information System* – SIS)[30] oraz Systemie Informacji Wizowej (ang. *Visa Information System* – VIS)[31]. System SIS został ustanowiony jako narzędzie rekompensujące zniesienie kontroli na granicach pomiędzy państwami Obszaru Schengen. Jego celem jest utrzymanie porządku oraz bezpieczeństwa publicznego, łącznie z bezpieczeństwem narodowym, na terytoriach państw członkowskich oraz stosowanie postanowień Konwencji dotyczących przepływu osób na tych terytoriach, z wykorzystaniem informacji znajdujących się w SIS. Dlatego też Polska w momencie przystąpienia do układu z Schengen w dniu 21 grudnia 2007 r. zobligowana została do stosowania regulacji prawa europejskiego odnośnie do przetwarzania danych osobowych oraz innych informacji w systemach SIS oraz VIS.

Polskie regulacje prawne dotyczące przedmiotowych zagadnień pojawiły się w drugiej połowie 2007 r., kiedy to w dniu 24 sierpnia została uchwalona ustawa o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej[32]. W akcie tym określone zostały zarówno zasady i tryb udziału poszczególnych organów administracyjnych w SIS oraz VIS, jak i obowiązki organów dokonujących wpisów oraz organów posiadających prawo dostępu do danych w zakresie wykorzystywania informacji zawartych w SIS i VIS poprzez Krajowy System Informatyczny (KSIS).

W myśl regulacji prawa europejskiego, każde z państw członkowskich wyznacza organ nadzorczy odpowiedzialny, zgodnie z prawem krajowym, za przeprowadzanie niezależnego nadzoru nad danymi krajowego modułu informacyjnego SIS oraz za monitorowanie czy przetwarzanie i wykorzystywanie danych wprowadzonych do tego systemu nie narusza praw osób, których dane te dotyczą[33]. W świetle polskiej ustawy kompetencje nadzorcze nad funkcjonowaniem komponentów krajowych posiada Minister Spraw Wewnętrznych i Administracji, zaś w zakresie przetwarzania danych osobowych – Generalny Inspektor Ochrony Danych Osobowych (GIODO).

Ponadto Polska, jako jedna ze stron porozumienia, została w świetle Konwencji zobligowana do wyznaczenia organu odpowiedzialnego za jej krajowy moduł Systemu Informacyjnego Schengen (KSIS), za którego pośrednictwem wprowadza swoje wpisy do tego systemu. W Polsce organem odpowiedzialnym za sprawne działanie i bezpieczeństwo SIS został Komendant Główny Policji, który dodatkowo podejmuje

[29] §6 Rozporządzenia.

[30] Ustanowiony na mocy postanowień Konwencji Wykonawczej do układu z Schengen z dnia 14 czerwca 1985 r. (Dz.Urz. UE L239 z 22.09.2000).

[31] Powstały na mocy Decyzji Rady 2004/512.WE z 8 czerwca 2004 r. w sprawie ustanowienia Wizowego Systemu Informacyjnego (VIS), Dz.Urz. UE L213 z 15.06.2004.

[32] Dz.U z 2007 r., Nr 165, poz. 1170.

[33] Art. 114 Konwencji Wykonawczej.

niezbędne środki w celu zapewnienia zgodności funkcjonowania KSIS z postanowieniami Konwencji[34].

Wykorzystywanie danych może następować bez wiedzy i zgody osób, których dane dotyczą oraz bez obowiązku ujawniania faktycznego celu zbierania danych[35]. Jednak osobie, której została wyrządzona szkoda przez niezgodne z prawem działanie lub zaniechanie związane z wykorzystywaniem danych SIS, przysługuje w tej sprawie wystąpienie z wnioskiem o naprawienie szkody do Skarbu Państwa poprzez Prokuratorię Generalną Skarbu Państwa[36].

W myśl art. 118 Konwencji Wykonawczej, Polska zobowiązała się także, w odniesieniu do swojego krajowego modułu Systemu Informacyjnego Schengen, przyjąć niezbędne środki w celu:

1) odmowy nieupoważnionym osobom dostępu do sprzętu służącego przetwarzaniu danych osobowych (kontrola dostępu do sprzętu);
2) zapobiegania nieupoważnionemu czytaniu, kopiowaniu, modyfikacji lub usuwaniu nośników danych (kontrola nośników danych);
3) zapobiegania nieupoważnionemu wprowadzaniu danych oraz nieupoważnionym inspekcjom, modyfikacjom lub usuwaniu przechowywanych danych osobowych (kontrola gromadzenia danych);
4) zapobiegania wykorzystywania zautomatyzowanych systemów przetwarzania danych przez nieupoważnione osoby z wykorzystaniem sprzętu do przekazywania danych (kontrola użytkownika);
5) zapewnienia, aby osoby upoważnione do wykorzystywania zautomatyzowanych systemów przetwarzania danych miały jedynie dostęp do danych objętych ich upoważnieniem (kontrola dostępu do danych);
6) zapewnienia możliwości weryfikacji i stwierdzania, do których organów dane osobowe mogą być przekazywane z wykorzystaniem sprzętu do przekazywania danych (kontrola transmisji danych);
7) zapewnienia możliwości weryfikacji i stwierdzenia, które dane osobowe zostały wprowadzone do zautomatyzowanych systemów przetwarzania danych oraz kiedy i przez kogo dane zostały wprowadzone (kontrola dostarczania danych);
8) zapobiegania nieupoważnionemu czytaniu, kopiowaniu, modyfikacji lub usuwaniu danych osobowych podczas przekazywania danych osobowych lub podczas przenoszenia nośników danych (kontrola dostarczania danych).

Katalog organów odpowiedzialnych za przestrzeganie powyższych zaleceń zawiera rozdział 2 ustawy o udziale Rzeczypospolitej Polskiej w SIS oraz VIS.

Podsumowanie

Ochrona informacji niejawnych oraz danych osobowych to zagadnienia bardzo istotne dla prawidłowego funkcjonowania bezpiecznego państwa. Dlatego też powinny być one poważnie traktowane zarówno przez osoby mające do nich dostęp oraz zaj-

[34] *Ibidem*, Art.108.

[35] Art. 11 ustawy o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej.

[36] *Ibidem*, Art. 12.

mujące się szeroko rozumianym ich przetwarzaniem, jak i przez osoby fizyczne (lub prawne), które z uzasadnionych przyczyn chcą uzyskać tego typu informacje. Jednocześnie osoby zajmujące się zawodowo tego typu problematyką muszą posiadać nie tylko szeroką wiedzę teoretyczną, popartą posiadaniem odpowiednich dokumentów, ale i wiedzę praktyczną, polegającą na znajomości procedur i przepisów związanych z tego rodzaju zagadnieniami.

W demokratycznym państwie prawa, jakim jest Rzeczpospolita Polska, poszanowanie godności człowieka stanowi źródło jego wolności i praw obywatelskich. Godność ta jest naczelną wartością państwa, jest ona nienaruszalna i stanowi podstawę do ochrony danych osobowych[37]. Dlatego też każde bezprawne ujawnienie danych ścigane jest z urzędu i zagrożone sankcjami finansowymi oraz karnymi, łącznie z karą pozbawienia wolności. Ustanowienie administratora danych osobowych jako osoby odpowiedzialnej za ochronę tych danych w określonej firmie czy jednostce organizacyjnej nakłada na niego obowiązek zastosowania wszelkich dostępnych środków technicznych i organizacyjnych w celu ich należytego zabezpieczenia. Do jego podstawowych obowiązków należy ponadto wdrażanie zasad bezpieczeństwa określonych w Polityce bezpieczeństwa i Instrukcji zarządzania. To administrator danych przeprowadza szkolenia oraz kształtuje świadomość pracowników odnośnie do ważności i aktualności tematyki ochrony danych osobowych.

Przedstawione w niniejszym opracowaniu przepisy w pierwszym rzędzie służą realizacji dwóch podstawowych funkcji:

1) są instrumentem niezbędnym dla poszanowania podstawowych, uznanych powszechnie praw i wolności obywateli danego państwa, zwłaszcza prawa do prywatności;
2) ich zadaniem jest ochrona interesów użytkowników najnowszej technologii informatycznej oraz zapewnienie niezbędnego dla prowadzonych przez nich działań zaufania i bezpieczeństwa.

   Jest to zarazem odpowiedź na drugie z wyżej postawionych pytań.

Bibliografia

Byczkowski M., *Polityka Bezpieczeństwa Informacji a ochrona danych osobowych. Część III*, „Ochrona Danych Osobowych" 2000, nr 8.

Czerwiński K., *Audyt wewnętrzny*, Centrum Doradztwa i Informacji Difin, Warszawa 2004.

Jakubus B., Ryszkowski M., *Ochrona informacji niejawnych*, Wydawnictwo Projekt, Warszawa 2001.

Kurzępa B., *Ochrona informacji niejawnych. Zbiór przepisów*, Studio Sto, Bielsko-Biała 2000.

Napierała K., *Prawne aspekty ochrony danych osobowych przetwarzanych w systemach teleinformatycznych*, Dom Wydawniczy ABC, Warszawa 1997.

Polaczek T., *Audyt bezpieczeństwa informacji w praktyce*, Helion, Gliwice 2006.

[37] http://www.giodo.gov.pl/ (18.07.2008).

Szałowski R., *Ochrona danych osobowych – komentarz do ustawy*, Zachodnie Centrum Organizacji, Zielona Góra 2000.
Szewc T., *Ochrona informacji niejawnych – komentarz*, Wydawnictwo C.H. Beck, Warszawa 2007.
Taradejna M.R., *Tajemnica państwowa i inne tajemnice chroniące interesy państwa i obywateli*, Wydawnictwo Mini Press, Warszawa 1999.

Akty normatywne:

Konstytucja Rzeczypospolitej Polskiej z dnia 4 kwietnia 1997 r. (Dz.U. z 1997r., Nr 78, poz. 483).
Konwencja wykonawcza do układu z Schengen z dnia 14 czerwca 1985 r. (Dz.Urz. UE L239 z 22.09.2000).
Dyrektywa nr 95/46/CE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych ze względu na przetwarzanie danych o charakterze osobowym oraz swobodnego przepływu tych danych (Dz.Urz. UE L 281 z 23 listopada 1995).
Ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz.U. z 1997 r., Nr 78, poz. 483).
Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r., Nr 101, poz. 926 ze zm.).
Decyzja Rady 2004/512.WE z 8 czerwca 2004 r. w sprawie ustanowienia Wizowego Systemu Informacyjnego (VIS) (Dz.Urz. UE L213 z 15.06.2004).
Ustawa z dnia 24 sierpnia 2007 r. o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Systemie Informacji Wizowej (Dz.U. z 2007 r., Nr 165, poz. 1170).
Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004 r., Nr 100, poz. 1024).
Rozporządzenie Prezesa Rady Ministrów z dnia 25 sierpnia 2005 r. w sprawie podstawowych wymogów bezpieczeństwa teleinformatycznego (Dz.U. z 2005 r., Nr 171, poz. 1433).

Strony internetowe:

http://www.qualityprogress.com.pl/ (16.07.2008).
http://www.giodo.gov.pl/ (18.07.2008).
http://www.tuv-nord.pl/ (20.07.2008).

Marek Jabłoński
Magdalena Mielus

Zagrożenia bezpieczeństwa informacji w organizacji gospodarczej

Wprowadzenie

Współczesne organizacje gospodarcze zmuszone do prowadzenia działalności w warunkach niepewności i chaosu, coraz częściej poddają modyfikacjom swoje podejście do bezpieczeństwa. W obliczu różnorodnych zagrożeń, organizacje te stoją przed koniecznością brania pod uwagę zarówno zdarzeń lokalnych, jak i globalnych, które mogą wpływać na ich działalność.

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

Celem niniejszego artykułu jest przedstawienie zagrożeń związanych z bezpieczeństwem informacji w organizacji gospodarczej. Na tak sformułowany cel opracowania złożyło się zaprezentowanie definicji bezpieczeństwa informacji występujących na gruncie literatury przedmiotu oraz zagrożeń informacyjnych. Podjęto także próbę ramowego ujęcia zagadnienia kształtowania zachowań pracowniczych w małej organizacji umożliwiających zabezpieczanie informacji.

Bezpieczeństwo informacji

W kontekście postrzegania i poszukiwania poczucia bezpieczeństwa warto uwzględnić model zaprezentowany przez D. Freia, który uwzględnia cztery elementy:

1) stan braku bezpieczeństwa – w którym występuje rzeczywiste i istotne zagrożenie zewnętrzne, którego postrzeganie jest adekwatne,
2) stan obsesji – w którym niewielkie zagrożenie postrzega się jako duże,
3) stan fałszywego bezpieczeństwa – w którym istotne zagrożenie postrzegane jest jako niewielkie,
4) stan bezpieczeństwa – w którym zagrożenie zewnętrzne jest niewielkie, a jego postrzeganie prawidłowe[1].

Pojęcie bezpieczeństwa ujmowane jest na różne sposoby, w których jednak można doszukać się wątków wspólnych. Oto kilka przykładów definiowania bezpieczeństwa (tab. 1).

[1] K. Liedel, *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Toruń 2006, s. 9.

Tabela 1. Wybrane definicje bezpieczeństwa według różnych autorów

A. Maslow	Bezpieczeństwo „obejmuje zaspokojenie takich potrzeb jak: istnienie, przetrwanie, całość, tożsamość (identyczność), niezależność, spokój, posiadanie i pewność rozwoju. Brak bezpieczeństwa powoduje niepokój i poczucie zagrożenia. Biorąc pod uwagę poczucie tego zagrożenia, w nauce wyróżnia się bezpieczeństwo wewnętrzne i bezpieczeństwo zewnętrzne. Bezpieczeństwo wewnętrzne oznacza stabilność i harmonijność danego organizmu lub podmiotu, natomiast bezpieczeństwo zewnętrzne brak zagrożenia ze strony innych podmiotów lub czynników zewnętrznych"[2].
Słownik języka polskiego	Bezpieczeństwo to stan niezagrożenia, spokoju, pewności. Bezpieczeństwo związane jest z niezakłóconym funkcjonowaniem jakiegoś obiektu odnoszącego się do wszelkiej działalności człowieka[3].
Słownik terminów z zakresu psychologii dowodzenia i zarządzania	„Bezpieczeństwo – stan, daje poczucie pewności i gwarancję jego zachowania oraz szansę na doskonalenie. Jedna z podstawowych potrzeb człowieka to sytuacja odznaczająca się brakiem ryzyka utraty czegoś, co człowiek szczególnie ceni, na przykład zdrowia, pracy, szacunku, uczuć, dóbr materialnych. Wyróżnia się m.in. bezpieczeństwo globalne, regionalne, narodowe; bezpieczeństwo militarne, polityczne, społeczne; bezpieczeństwo fizyczne, psychiczne, socjalne; bezpieczeństwo strukturalne i personalne"[4].
W. Šmid	„Bezpieczeństwo (ang. *safety*) – jest to sytuacja odznaczająca się brakiem ryzyka (np. w inwestowaniu, planach strategicznych produktu itp.) albo zasobów (materialnych, ludzkich)"[5].

Źródło: opracowanie własne.

Przytoczone w tabeli 1 definicje charakteryzuje różny poziom ogólności i odmienność spojrzenia na problem bezpieczeństwa z racji reprezentowania przez autorów różnych dyscyplin naukowych, takich jak np.: lingwistyka, politologia, psychologia, wojskowość i zarządzanie. Powyższe definicje pozwalają wyprowadzić wniosek, iż podstawowym zadaniem organizacji gospodarczych jest tworzenie i doskonalenie systemów bezpieczeństwa, stwarzając przy tym poczucie bezpieczeństwa dla uczestników tych organizacji i ich otoczenia. Najszersze rozumienie bezpieczeństwa wyraża się w stwierdzeniu, iż „pewien podmiot jest bezpieczny, jeśli jest zdolny do osiągania swoich celów"[6].

Bezpieczeństwo informacji to nic innego jak „obrona informacyjna, która polega na uniemożliwieniu i utrudnieniu zdobywania danych o fizycznej naturze aktualnego oraz planowanego stanu rzeczy i zjawisk we własnej przestrzeni funkcjonowania,

[2] K. Liedel, *Bezpieczeństwo informacyjne...*, *op. cit.*, s. 7.

[3] *Słownik języka polskiego*, red. M. Szymczak, t. 1, Warszawa 1988, s. 147.

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

[5] W. Šmid, *Metamarketing*, Kraków 2000, s. 50.

[6] J. Konieczny, *O metodzie rozumowań w etyce bezpieczeństwa*, „Bezpieczeństwo. Teoria i praktyka. Moralne problemy bezpieczeństwa" 2008, numer specjalny, s. 97.

a także utrudnianiu wnoszenia entropii informacyjnej do komunikatów i destrukcji fizycznej do nośników danych"[7].

Obrona informacyjna obejmuje takie przedsięwzięcia jak: a) zapobieganie (działania prewencyjne), b) odstraszanie, c) wskazywanie i ostrzeganie, d) wykrywanie, e) przygotowanie się na sytuację awaryjną, oraz f) reakcję na ewentualny atak.

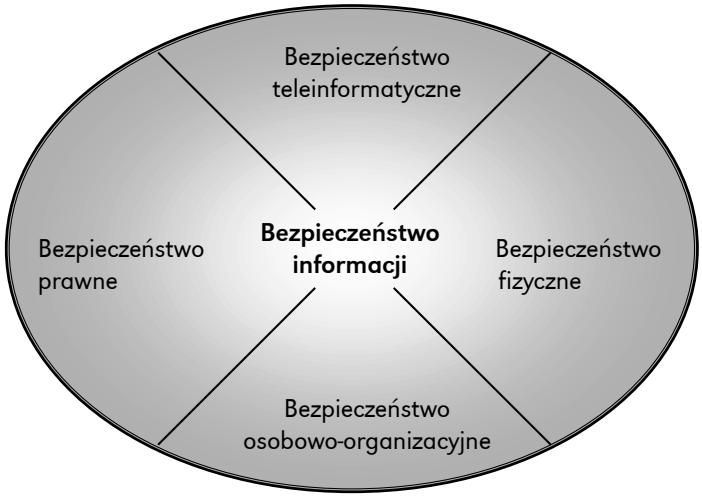
Na każdym poziomie zarządzania bezpieczeństwem informacji zasadniczym celem jest niedopuszczenie do ich ujawnienia. Należy podkreślić, że zbyt szerokie rozumienie bezpieczeństwa może utrudniać przepływ informacji w państwie czy organizacji gospodarczej niezbędnych do ich sprawnego i skutecznego funkcjonowania.

Istnieje także zróżnicowane podejście do definiowania pojęcia bezpieczeństwa informacyjnego. W potocznym rozumieniu bezpieczeństwo informacyjne obejmuje jedynie ochronę informacji stanowiących tajemnicę państwową i służbową. Bezpieczeństwo informacyjne – w szerokim ujęciu – rozumiane jest jako stan wolny od zagrożeń, które pojmowane są głównie jako:

- przekazywanie informacji nieuprawnionym podmiotom;
- szpiegostwo;
- działalność dywersyjna lub sabotażowa[8].

Bezpieczeństwem informacyjnym jest również każde działanie, system bądź metoda, które zmierzają do zabezpieczenia zasobów informacyjnych gromadzonych, przetwarzanych, przekazywanych, przechowywanych w pamięci komputerów oraz sieci teleinformatycznych[9]. Bezpieczeństwo informacyjne należy rozumieć jako składową bezpieczeństwa fizycznego, prawnego, osobowo-organizacyjnego oraz teleinformatycznego organizacji gospodarczej[10] (rys. 1).

Rysunek 1. Składowe bezpieczeństwa informacji



Źródło: *Zarządzanie bezpieczeństwem informacji*, red. J. Łuczak, Poznań 2004, s. 80.

[7] L. Ciborowski, *Walka informacyjna*, Toruń 1999, s. 186.

[8] P. Bączek, *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Toruń 2006, s. 71.

[9] *Ibidem*.

[10] *Zarządzanie bezpieczeństwem informacji*, red. J. Łuczak, Poznań 2004, s. 80.

Ponadto, bezpieczeństwo informacyjne jest stanem wewnętrznym i zewnętrznym pozwalającym na zmniejszenie zagrożeń, jakie towarzyszą pracy z informacjami. To władze danej jednostki gospodarczej podejmują decyzje dotyczące problematyki wewnętrznej i zewnętrznej w oparciu o prawdziwe i wiarygodne informacje, zaś organizacja ich przekazywania powinna być jak najbardziej bezpieczna. Bezpieczeństwo informacyjne jest bowiem ważnym elementem pozwalającym zapewnić równowagę na każdym etapie działalności i ciągłość działań każdej organizacji.

Bezpieczeństwo jest procesem ciągłym, w ramach którego organizacje gospodarcze starają się udoskonalać różnorodne mechanizmy zapewniające im poczucie bezpieczeństwa. Odzwierciedleniem swoistego rozumienia i traktowania bezpieczeństwa jako kluczowego obszaru zainteresowań organizacji gospodarczych są ich działania mające na celu zapewnienie pożądanego bezpieczeństwa. Świadomość tego, jakie posiada ono znaczenie pojawia się najczęściej dopiero wtedy, gdy stajemy w obliczu zagrożenia. Zapewnienie bezpieczeństwa informacji jest ponadto zadaniem trudnym i kosztownym, co w wielu przypadkach może stanowić przyczynę zaniechania działań zmierzających do rozwiązania pojawiających się w tym zakresie problemów.

Klasyfikacja zagrożeń bezpieczeństwa informacji

Właściwe zdefiniowanie zagrożeń stanowi podstawę zapewnienia bezpieczeństwa informacji w organizacji. Zagrożenie to sytuacja lub stan, które komuś zagrażają lub w których ktoś czuje się zagrożony. Źródłem zagrożenia może być również osoba stanowiąca zagrożenie lub wzbudzająca poczucie zagrożenia[11].

„W definicjach politologicznych, zwłaszcza odnoszących się do kwestii bezpieczeństwa, zagrożenia mieszczą się w szerszej grupie określanej jako wyzwania. Wyzwania, które są właściwie rozpoznawane i podejmowane stanowią szanse, zaś wyzwania niepodejmowane lub podejmowane za późno mogą przekształcić się w zagrożenia"[12]. Podobnie traktuje się zagrożenia również w innych naukach jak na przykład w zarządzaniu czy socjologii.

Organizacje gospodarcze, których działania skupiają się na rozwoju i podążaniu w kierunku nowych rozwiązań, stają przed niespotykanymi dotąd wyzwaniami i zagrożeniami, których katalog nieustannie się powiększa. Listę wybranych zagrożeń informacyjnych dla organizacji gospodarczej przedstawiono na rysunku 2.

Prowadzenie działalności gospodarczej niesie ze sobą ryzyko, które pojawia się w postaci określonego zagrożenia. Ryzyko to przybiera różne formy i może ulegać zmianom w czasie.

„W refleksji nad niepewnością i ryzykiem w globalnym społeczeństwie informacyjnym należy ryzyko łączyć z zagrożeniami, a raczej kumulacją ryzyk wywodzących się z licznych źródeł zagrożeń"[13]. Wyróżniamy wiele źródeł zagrożeń/ryzyka: a) ryzyko egzystencjalne, b) ryzyko kulturowe, c) ryzyko informacyjne, d) ryzyko technologiczne, e) ryzyko ekonomiczne, f) ryzyko ekologiczne, g) ryzyko polityczne i inne[14].

---

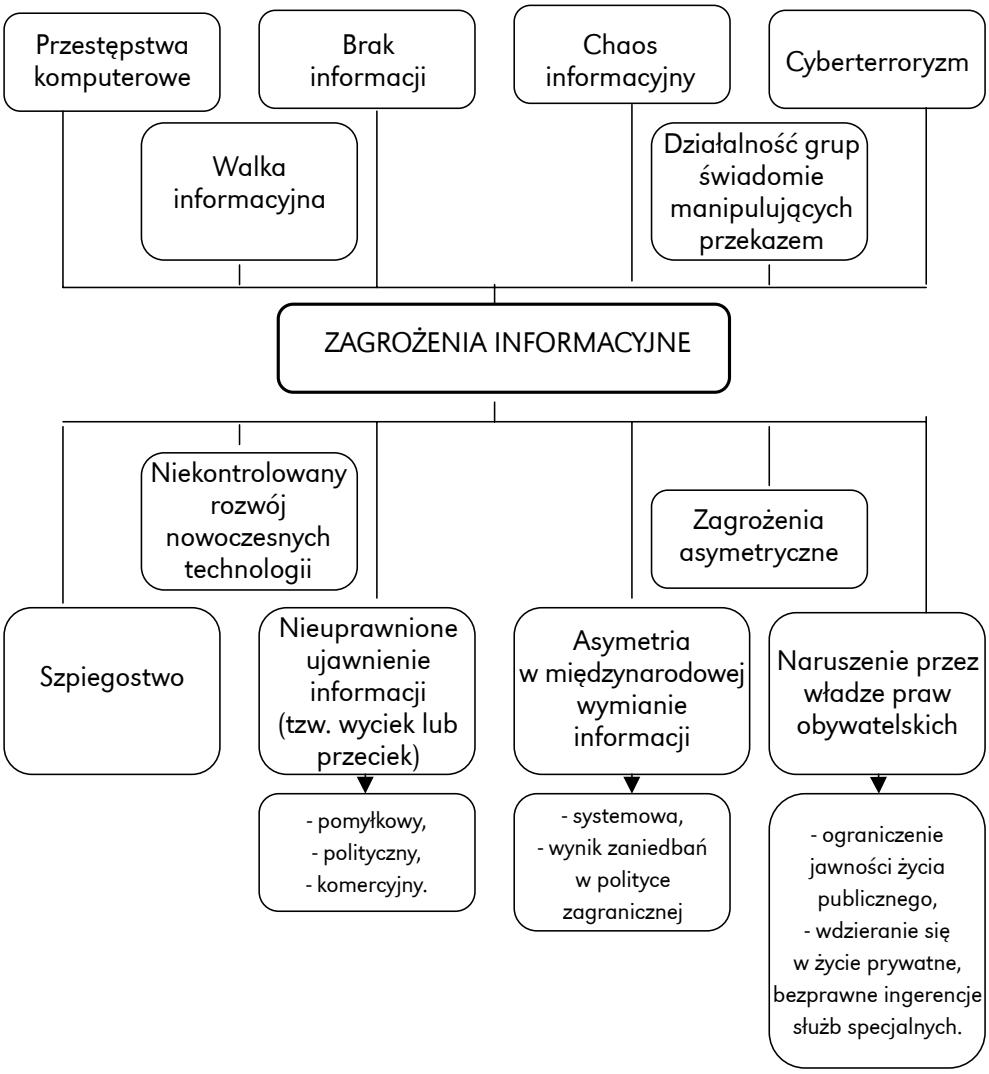
[11] http://sjp.pwn.pl/lista.php?co=zagro%BFenie (18.07.2008).

[12] P. Bączek, *op. cit.*, s. 30.

[13] P. Sienkiewicz, *Społeczeństwo informacyjne jako społeczeństwo ryzyka*, [w:] *Społeczeństwo informacyjne. Aspekty funkcjonalne i dysfunkcjonalne*, red. L.W. Haber, M. Niezgoda, Kraków 2006, s. 64.

[14] *Ibidem*.

Rysunek 2. Podział zagrożeń informacyjnych



Źródło: P. Bączek, *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, *op. cit.*, s. 30.

W organizacjach o charakterze gospodarczym spotykamy się z coraz większą skalą przestępstw i patologii gospodarczych. Poniżej przedstawiono zagrożenia w biznesie w zakresie przestępstw gospodarczych, komputerowych i działalności wywiadów (tab. 2).

Tabela 2. Przestępstwa w biznesie

Przestępstwa w biznesie		
Gospodarcze i bankowe	**Komputerowe**	**Działalność wywiadów**
• Fałszerstwa dokumentów publicznych (np. tożsamości, sprawozdań finansowych) • Oszustwa: – kredytowe, – prywatyzacyjne, – podatkowe, – celne, – ubezpieczeniowe, – upadłościowe, – wyłudzenie towarów, – „pranie pieniędzy", – inne.	– niszczenie informacji, – fałszerstwa danych, – podsłuch, – sabotaż, – piractwo, – wandalizm, – hakerstwo, – kraking.	– gospodarczego (technologiczny, handlowy, konkurencyjny, finansowy, strategiczny), – wojskowego, – naukowego.

Źródło: M. Kuta, *Polityka bezpieczeństwa informacji w przedsiębiorstwie – aspekty praktyczne*, [w:] R. Borowiecki, M. Kwieciński, *Monitorowanie otoczenia, przepływ i bezpieczeństwo informacji. W stronę integralności przedsiębiorstwa*, Zakamycze, Kraków 2003, s. 267.

Poza kategoriami przestępstw wymienionymi w powyższej tabeli istnieją również przestępstwa kryminalne, takie jak: kradzieże, napady rozbójnicze oraz akty terroru.

Przestępstwa występujące w biznesie tworzą specyficzną grupę, ponieważ zagrażają przedsiębiorstwom oraz instytucjom, stanowią zagrożenie dla zasobów organizacji, np. dla posiadanych baz informacji, środków pieniężnych, wartościom firmy takim jak reputacja, wyrobione stosunki bądź przywileje handlowe danego przedsiębiorstwa[15].

Pojęcie bezpieczeństwa informacyjnego można przybliżyć poprzez identyfikację następujących obszarów zagrożeń, wśród których wymienia się:

- zagrożenia losowe – to wszelkiego rodzaju klęski żywiołowe, katastrofy, wypadki np. pożar budynku, w którym przechowywane są nośniki informacji, wpływające na stan bezpieczeństwa informacyjnego organizacji;
- tradycyjne zagrożenia informacyjne – szpiegostwo, działalność dywersyjna lub sabotażowa ukierunkowana na zdobycie informacji, ofensywną dezinformację prowadzoną przez inne osoby, podmioty lub organizacje;
- zagrożenia technologiczne – zagrożenia związane z gromadzeniem, przechowywaniem, przetwarzaniem, przekazywaniem informacji w sieciach teleinformatycznych. Do takich zagrożeń zaliczamy: przestępstwa komputerowe, cyberterroryzm, walkę informacyjną;

[15] M. Kuta, *Polityka bezpieczeństwa informacji w przedsiębiorstwie – aspekty praktyczne*, [w:] R. Borowiecki, M. Kwieciński, *Monitorowanie otoczenia, przepływ i bezpieczeństwo informacji. W stronę integralności przedsiębiorstwa*, Zakamycze, Kraków 2003, s. 268.

– zagrożenia wynikające z niedostatecznych rozwiązań organizacyjnych i strukturalnych[16].

Ze względu na lokalizację, źródła zagrożeń dzieli się na:

1. wewnętrzne – powstające wewnątrz organizacji, które obejmują:
   – zagrożenie utratą, uszkodzeniem danych lub brakiem możliwości obsługi z powodu błędu lub przypadku,
   – zagrożenie utratą lub uszkodzeniem poprzez celowe działania nieuczciwych użytkowników;
2. zewnętrzne – powstające poza organizacją, obejmują zagrożenie utratą, uszkodzeniem danych lub pozbawieniem możliwości obsługi przez celowe lub przypadkowe działanie ze strony osób trzecich w stosunku do sieci lub systemu;
3. fizyczne, w których utrata, uszkodzenie danych lub brak możliwości obsługi następuje przez wypadek, awarię, katastrofę lub inne nieprzewidziane zdarzenie wpływające na system informacyjny bądź urządzenie sieciowe[17].

Jednym z najistotniejszych potencjalnych źródeł zagrożeń dla bezpieczeństwa organizacji gospodarczej jest naruszanie przepisów ochraniających te organizacje przez osoby posiadające dostęp do informacji. Napotyka się również trudności związane z wdrażaniem w życie Ustawy o ochronie informacji niejawnych.

Rozwój teleinformatyki i globalnego rynku automatyzuje procesy produkcyjne oraz finansowo-księgowe, umożliwia globalną i szybką komunikację, a nawet pozwala na zdalne zawieranie umów między kontrahentami. Jednak nie należy zapominać, że prowadzenie działalności gospodarczej w oparciu o teleinformatyzację, oprócz korzyści niesie ze sobą różne zagrożenia. Systemy informatyczne mają na celu gromadzenie, przetwarzanie i szybkie udostępnianie danych. „Wielkość ich i jakość, a zwłaszcza źródło pochodzenia stanowią przedmiot zainteresowania nie tylko służb specjalnych i innych instytucji będących potencjalnym przeciwnikiem, ale także organizacji o charakterze terrorystycznym oraz pojedynczych osób”[18]. Systemy informatyczne mogą być zagrożone ze strony każdego, kto posiada dostateczny zasób wiedzy i umiejętności.

Bezpieczeństwo systemów i sieci teleinformatycznych „to taki zakres przedsięwzięć, który ma na celu uniemożliwienie niepowołanym osobom dostępu do wartościowej informacji, do której można dotrzeć przez przechwyt emisji radiowych i analizę ruchu w sieciach radiowych lub wprowadzenie w błąd tych, którzy takową analizę mogą prowadzić. Bezpieczeństwo systemów łączności obejmuje systemy transmisji, bezpieczeństwo środków utrudniających oraz środków mających na celu fizyczną ochronę systemów łączności, materiałów niejawnych i informacji związanych z systemami łączności”[19].

Ataki na zbiory danych stanowiących tajemnicę państwową lub służbową mają na celu przejęcie kontroli nad chronionymi systemami. Ataki na systemy komputerowe występują wówczas, gdy działania zmierzające do naruszania jego bezpieczeństwa są celowe. Wyróżnia się dwie grupy ataków:

---

[16] P. Bączek, *op. cit.*, s. 72.

[17] A. Żebrowski, M. Kwiatkowski, *Bezpieczeństwo informacji III Rzeczypospolitej*, Kraków 2000, s. 65.

[18] *Ibidem*, s. 63.

[19] M. Herman, *Potęga wywiadu*, Warszawa 2002, s. 170.

- ataki aktywne – to bezpośrednie lub pośrednie aktywne oddziaływanie na system, polegające na modyfikowaniu strumienia danych lub tworzeniu danych fałszywych,
- ataki pasywne – to brak aktywnego oddziaływania na system. Do działań tych należy szeroko rozumiany podsłuch lub podgląd, analiza ruchu w sieci w celu zlokalizowania takich elementów jak serwer czy stanowiska pracy[20].

Zagrożenie atakiem występuje wtedy, gdy dostępne są takie możliwości jak:

- nieuprawniony dostęp do przechowywanych, przetwarzanych i przesyłanych informacji niejawnych bez oddziaływania na system;
- nieuprawnione oddziaływanie na system, którego wykorzystanie może spowodować:
  - zmiany funkcjonowania sieci teleinformatycznej, dostęp do przesyłanych, przetwarzanych i przechowywanych informacji,
  - dezinformację,
  - zniszczenie informacji i innych zasobów systemu,
  - sfałszowanie lub nieuprawnioną modyfikację informacji[21].

W roku 2007 najczęściej pojawiającym się rodzajem ataku były oszustwa komputerowe, drugim – obraźliwe i nielegalne treści, na trzeciej pozycji uplasowało się natomiast gromadzenie informacji. W ciągu pięciu lat zmniejszyła się liczba tych ostatnich o 57 punktów procentowych.

Ponad połowa atakujących to firmy komercyjne (58,8%). Z roku na rok CERT Polska (Computer Emergency Response Team Polska) notuje coraz więcej takich przypadków. 18,5% atakujących pozostało nieznanych, w związku z czym, przed organizacjami zajmującymi się szeroko pojętą ochroną stają coraz to nowe wyzwania. CERT często nie jest w stanie zidentyfikować prawdziwego źródła ataku, gdyż atakujący ukrywa się za serwerem Proxy, botnetem czy przejętą maszyną nieświadomej ofiary. Pojawiły się również i upowszechniły działające na granicy prawa firmy udostępniające łącza, serwery fizyczne i wirtualne, na których umieszczane są nielegalne treści, a firmy te chronią swoich klientów, zapewniając im anonimowość[22].

Najstarszą techniką mającą na celu wyprowadzenie danych z przedsiębiorstwa jest technika zbierania przez konkurencję informacji poprzez przeszukiwanie śmieci inwigilowanej jednostki. Technika ta znajduje się na pograniczu zewnętrznego i wewnętrznego zagrożenia. Stanowi ona realne zagrożenie dla organizacji takich jak banki, instytucje finansowe, ubezpieczeniowe, przedsiębiorstwa opracowujące i wdrażające nowe technologie, dla których poufność kontaktów z klientem jest podstawą zdobywania udziału w rynku. „O popularności tej techniki decyduje nie tylko łatwość, z jaką dane takie można zdobyć, lecz również – w przypadku zatrzymania – bezkarność"[23].

Informacje związane z działalnością ekonomiczną i finansową, a także dane osobowe również winny podlegać daleko idącej ochronie. Przykładem luki w systemie ochrony danych osobowych może być fakt wykradzenia list z nazwiskami, adresami i zastrzeżonymi numerami telefonów ok. 200 tys. abonentów z baz danych piotrkowskiego oddziału TP SA (dane na płytach CD można było kupić na bazarze za 10 zł)[24].

---

[20] A. Żebrowski, M. Kwiatkowski, *op. cit.*, s. 63.

[21] A. Barczyk, T. Sydoruk, *Bezpieczeństwo systemów informatycznych zarządzania*, Warszawa 2003, s. 70.

[22] http://www.cert.pl/PDF/Raport_CP_2007.pdf (14.07.2008).

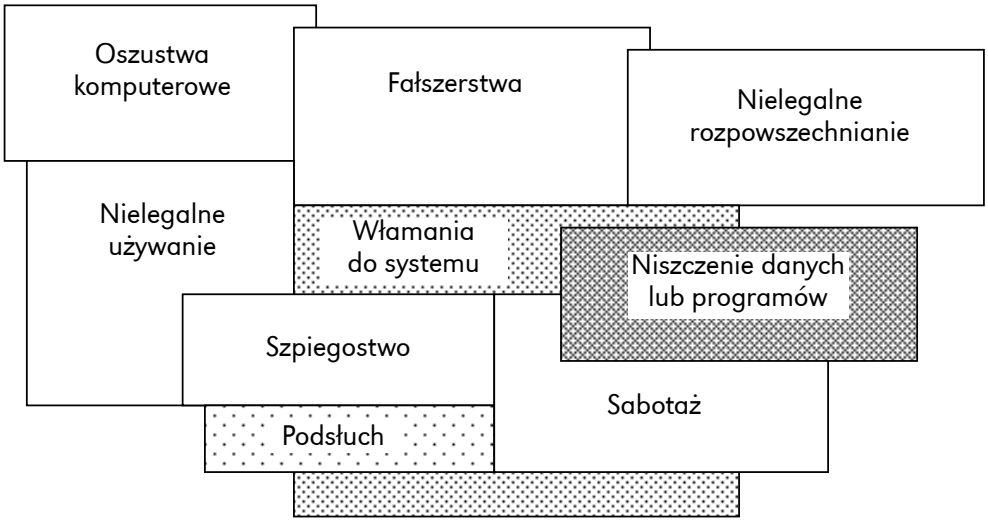
[23] *Zarządzenie bezpieczeństwem informacji*, *op. cit.*, s. 45.

[24] www.wiadmosci.tvp.pl (wiadomość z dnia 20 kwietnia 2003).

Rozwój technologii informacyjnych stwarza dogodne warunki dla prowadzenia działalności przestępczej. Pojawiające się nowe rozwiązania z jednej strony wspomagają procesy podejmowania decyzji na różnych szczeblach zarządzania organizacją, natomiast z drugiej przynoszą ze sobą jakościowo nowe niebezpieczeństwa. Zagrożenia te mogą naruszać zasoby: osobowe, materialne, finansowe, informacyjne[25].

Poniższy rysunek przedstawia formy działań charakterystycznych dla przestępstw informatycznych (rys. 3).

Rysunek 3. Rozkład i nakładanie się przestępstw komputerowych



Źródło: B. Fischer, *Przestępstwa komputerowe i ochrona informacji*, Zakamycze, Kraków 2000, s. 33.

W tab. 3 przedstawiono z kolei zagrożenia w podziale na: losowe wewnętrzne, losowe zewnętrzne, celowe wewnętrzne, celowe zewnętrzne.

Zagrożenia wewnętrzne uznawane są za groźniejsze niż zewnętrzne – konsekwencje ich wystąpienia prowadzą do znacznie większych strat i komplikacji. Największe niebezpieczeństwo zagraża systemom informatycznym organizacji gospodarczych ze strony ich własnych pracowników. To oni w sposób świadomy bądź nieświadomy niszczą, modyfikują lub przekazują osobom niepowołanym najcenniejsze informacje. Dopuszczalność takich działań wynika ze stosowania zabezpieczeń ukierunkowanych zazwyczaj na odpieranie ataków pochodzących z zewnątrz, zapominając przy tym o wysokim prawdopodobieństwie ataku wewnętrznego.

Zagrożenia wewnętrzne stanowią największe niebezpieczeństwo i to właśnie z nimi mamy najczęściej do czynienia. Niezamierzone błędy ludzi, zaniedbania użytkowników, defekty sprzętu i oprogramowania lub celowe działania nieuczciwych użytkowników są działaniami tworzącymi zagrożenie. Jako szczególny rodzaj zagrożenia wewnętrznego można zaliczyć proces rekrutacji pracownika, który w przyszłości będzie miał dostęp do poufnych danych organizacji, która go zatrudni. „Zdarza się bowiem,

[25] A. Żebrowski, M. Kwiatkowski, *op. cit.*, s. 70.

że konkurencja przysyła pod pozorem znalezienia pracy człowieka, którego głównym celem jest uzyskanie poufnych danych. Człowiek taki z reguły posiada wysokie kompetencje, niekiedy legitymuje się również zwolnieniem go z konkurencyjnej firmy w celu uwiarygodnienia"[26].

Zagrożenia zewnętrzne obejmują celowe lub przypadkowe działania ze strony osób trzecich powodujące niebezpieczeństwo utraty lub uszkodzenia danych, pozbawienia obsługi, systemu lub sieci oraz szpiegostwo, wandalizm i terroryzm. Do zagrożeń zewnętrznych można zaliczyć rozprzestrzeniające się w sieciach lokalnych i rozległych wirusy komputerowe, które niszczą dane, uszkadzają zawartość plików bądź zniekształcają zapis danych na dysku. Szkody powodowane przez wirusy mogą prowadzić do uszczerbku na wizerunku organizacji gospodarczej, a także generować wydatki finansowe na przywrócenie działania uszkodzonego systemu.

Każda organizacja gospodarcza musi postrzegać zagrożenia związane z włamaniami na serwery w celu kradzieży lub usunięcia danych jako realne i przeciwdziałać im najlepiej, jak potrafi. Brak pokory w tym względzie wynikający z przekonania – i dzielenia się tym przekonaniem w otoczeniu – o posiadaniu najlepszego systemu zabezpieczającego może sprowadzić niebezpieczeństwo wcześniej, niż miałoby to miejsce w warunkach normalnych. Przez pojęcie „warunki normalne" rozumie się system o optymalnym zabezpieczeniu, bez dzielenia się informacją na temat stopnia zabezpieczenia ochranianego systemu. Szerzenie opinii, że dana organizacja posiada najlepsze rozwiązania ochrony informacji, stanowi wyzwanie dla osób czerpiących satysfakcję z włamywania się do obcych systemów.

Tabela 3. Podział zagrożeń wg kryterium pochodzenia i losowości

	LOSOWE	CELOWE
WEWNĘTRZNE	– niezamierzone błędy operatorów i użytkowników, – wady sprzętu, – wady oprogramowania	– działania własnych pracowników wynikające z chciwości, chęci rewanżu itp., – działania użytkowników wykraczające poza ich obowiązki, nadgorliwość itp., – szpiegostwo, – wandalizm, chuligaństwo, – terroryzm
ZEWNĘTRZNE	– zbyt wysoka temperatura lub wilgotność (pożar, zalanie), – zanieczyszczenie powietrza, kurz, pył, – zakłócenie w zasilaniu, – zakłócenie w procesach komunikacji, – wyładowania atmosferyczne, klęski żywiołowe itp.	– działania przestępców komputerowych podejmowane z chęci zysku, – działania przedstawicieli prasy i innych mediów, szukających dostępu do informacji, – szpiegostwo, – wandalizm, chuligaństwo, – terroryzm

Źródło: A. Barczyk, T. Sydoruk, *Bezpieczeństwo systemów informatycznych zarządzania*, *op. cit.*, s. 77.

[26] *Zarządzenie bezpieczeństwem informacji*, *op. cit.*, s. 45.

Kształtowanie zachowań zabezpieczających informacje w małej firmie

Zaprezentowane dotąd zagadnienia bezpieczeństwa informacji organizacji związane są przede wszystkim z jej otoczeniem, które postrzegane jest jako wrogo nastawione do organizacji i realizowanych procesów organizacyjnych. Takie podejście umożliwia projektowanie zestawu instrumentów gwarantujących tworzenie zapór informacyjnych tak, aby istotne z perspektywy zamierzeń strategicznych zasoby informacji znajdowały się poza bezpośrednim i pośrednim wpływem zewnętrznych uczestników gry rynkowej. Instrumenty i różnego rodzaju zabiegi przeciwdziałające wyciekom informacji na zewnątrz organizacji już na etapie ich projektowania spełniają istotną funkcję zapobiegawczą, bowiem kierunkują członków organizacji na przejawianie zachowań utrudniających pozyskiwanie przez otoczenie informacji organizacji. Z kolei ich internalizacja, będąca pochodną uczenia się, może gwarantować, iż podsystem społeczny przedsiębiorstwa będzie reprezentował strategie czuwania, a przez to stanowić będzie najszczelniejszą barierę przeciwdziałającą utracie istotnych informacji danego przedsiębiorstwa. Ważne jest, aby niniejsze podejście nie stało się przyczyną odizolowania podmiotu gospodarczego od otoczenia.

Taka perspektywa wydaje się szczególnie istotna w odniesieniu do małych organizacji, które nie potrzebują skomplikowanych i kapitałochłonnych rozwiązań techniczno-organizacyjnych, ale bardziej zainteresowane są prostymi metodami i technikami, które spełnią oczekiwania decydentów. Prostota ta związana jest być może nie tyle ze strukturą i zakresem pewnych rozwiązań, ile z tym, iż zarządzanie małymi podmiotami rynkowymi jest przede wszystkim intuicyjne. Dokonuje się w głowie właściciela – menedżera. W rezultacie menedżer organizacji może oddziaływać na ochronę cennych informacji poprzez dawanie przykładu swoją osobą, wskazywanie, jakimi informacjami członkowie organizacji mogą i powinni dzielić się z otoczeniem, które ze zbiorów informacji powinni zabezpieczać przed wydostaniem się na zewnątrz organizacji. W takim znaczeniu kluczową sprawą jest wykształcenie w organizacji właściwych zachowań organizacyjnych, które w przypadku małych podmiotów gospodarczych odgrywają istotniejszą rolę w bezpieczeństwie informacji, aniżeli jakiekolwiek środki organizacyjno-techniczne. Właściwe zachowania organizacyjne:

- wzmacniają postawy pracownicze gwarantujące ochronę cennych informacji i udostępnianie odpowiednich treści do otoczenia,
- wzmacniają samokontrolę członków organizacji w sterowaniu przepływami informacji między organizacją a otoczeniem,
- identyfikują działania pracownicze ukierunkowane na poszukiwanie cennych informacji w otoczeniu nie tylko w ramach pełnionych obowiązków, ale także w czasie poza pracą,
- umożliwiają dyfuzję najlepszych praktyk między pracownikami celem dostosowania ich aktualnych potrzeb związanych z ochroną informacji,
- dostosowują działania i praktyki członków organizacji do zmian w otoczeniu, tj. realizowanych zleceń, zawieranych transakcji, kontrahentów.

Poza wymienionymi funkcjami zachowań pracowniczych w obszarze zabezpieczania informacji, mają one za zadanie promowanie w organizacji i jej otoczeniu

praktyk będących pochodną procesów uczenia się na poziomie indywidualnym, grupowym, organizacyjnym i międzyorganizacyjnym (zob. tab. 4). W projektowaniu i upowszechnianiu właściwych zachowań zasadniczą rolę odgrywa właściciel/menedżer organizacji – jego postawa oddziałuje na podległych pracowników, od niego także rozpoczyna się proces organizacyjnego uczenia się na wszystkich poziomach. Jego postawa warunkuje przebieg procesu uczenia się, ale może także ten proces zahamować. Niestety, nie zostaną tu poruszone zagadnienia związane z rolą menedżera w procesie organizacyjnego uczenia się służącą zabezpieczeniu informacji organizacji, bowiem wymagałoby to uwzględnienia obszarów problemowych znacznie wykraczających poza tematykę niniejszego opracowania, w szczególności: przywództwa, zaufania, lojalności, kultury organizacyjnej, stylów kierowania.

Odniesieniem uczenia się pracowników jest bezpieczeństwo informacji, może ono przebiegać w różnej konfiguracji, w znaczeniu poziomu organizacyjnego uczenia się inicjującego działania i praktyki umożliwiające zabezpieczanie informacji na pozostałych poziomach tego procesu. Przyjmując jednak, iż zagadnienie ochrony informacji odnosi się do małej organizacji, w której decyzje i działania pracowników nie były bezpośrednio związane z ochroną informacji, można przyjąć, iż proces ten inicjowany jest przez właściciela/menedżera. W pierwszej kolejności zachodzi on na poziomie indywidualnym, sprowadza się więc do tworzenia, upowszechniania i rozwijania doświadczeń oraz wyobrażeń członków organizacji, których rezultatem będą metafory identyfikowane przez poszczególnych członków organizacji. Ze zbioru czynników kształtowania zachowań najważniejsze jest promowanie zaangażowania, perspektywiczności myślenia oraz zarządzanie „od dołu". W stosowaniu tych stymulatorów zasadniczą rolę odgrywa właściciel/menedżer – bez jego udziału i bezpośredniego zaangażowania nikłe są szanse na zainicjowanie i skuteczność procesu organizacyjnego uczenia się ukierunkowanego na ochronę informacji.

Zdefiniowanie metafor na poziomie indywidualnym umożliwia zachodzenie procesu interpretacji, w którym wzajemne zrozumienie kwestii dotyczących bezpieczeństwa cennych dla organizacji informacji, a także podejmowanych praktyk w tym zakresie warunkuje nawiązywanie dialogu i konwersacji. Inicjowana w ten sposób komunikacja członków organizacji może zapewnić dyfuzję najlepszych praktyk, uczenie się członków organizacji oraz pobudzanie ich do wzajemnej interakcji celem promowania zrozumienia (*sense making*). Jednak na tym poziomie zasadnicze są: perswazja i jednolite nazewnictwo. Przy czym należy pamiętać, że celem procesu interpretacji jest internalizacja wśród członków organizacji istotności kwestii związanych z bezpieczeństwem informacji.

Nawiązywany dialog i konwersacje pomiędzy członkami organizacji stanowi gwarant kształtowania zachowań pracowników na poziomie grupowym, rozpoczynając proces integracji członków organizacji wokół zagadnień związanych z bezpieczeństwem informacji. Rezultatem tego jest wypracowanie systemu interaktywnego, który stanowi regulator zachowań organizacyjnych. W przebiegu uczenia się zachowań na poziomie grupowym kluczową rolę w odniesieniu do małych firm odgrywa: promowanie poczucia zaufania i przynależności grupowej oraz eliminowanie atmosfery współzawodnictwa.

Tabela 4. Proces organizacyjnego uczenia się wraz z przykładowymi czynnikami kształtującymi pożądane zachowania pracownicze

Poziom organizacyjnego uczenia się	**Proces**	**Nakład**	**Stymulatory procesu uczenia się i czynniki kształtowania zachowań**	**Efekt**
Indywidualny	Intuicyjny	Doświadczenia, wyobrażenia	Rozwijanie ciekawości intelektualnej Opowiadania (*storytelling*) Traktować problemy jak wyzwania Perspektywiczność myślenia Zaangażowanie Zarządzanie „od dołu”	Metafory
	Interpretacyjny	Wzajemne zrozumienie	Kult wartości Zachęcanie do podejmowania ryzyka i nauki Dostarczanie jednolitego nazewnictwa Perswazja	Konwersacja, dialog
Grupowy	Integracyjny	Wzajemne zrozumienie i dostosowania	Eliminowanie barier funkcjonalnych Eliminowanie atmosfery współzawodnictwa Promowanie poczucia zaufania i przynależności grupowej Przyznawanie nagród pracownikom, którzy najsprawniej dzielą się wiedzą Egalitaryzm	Systemy interaktywne
Organizacyjny	Instytucjonalizowania	Standardy, Systemy diagnostyczne Skodyfikowane doznania i doświadczenia	Swoboda organizacyjna Samoorganizacja Fluktuacja kadry między różnymi projektami Bazy danych najlepszych pomysłów Wirtualne grupy zadaniowe	Zasady i procedury
Międzyorganizacyjny				

Źródło: opracowanie własne.

Wskazane powyżej poziomy procesu organizacyjnego uczenia się są istotniejsze aniżeli uczenie się na poziomie organizacyjnym i międzyorganizacyjnym, zwłaszcza na etapie początkowym, którego zasadniczym celem jest zwrócenie uwagi członków organizacji na kwestie bezpieczeństwa. W świetle powyższego należy także nadmienić, iż realizacja działań zmierzających do kształtowania wspólnego zrozumienia kwestii dotyczących bezpieczeństwa informacji oraz przejawiania właściwych zachowań w przypadku małych firm odbywać się powinna w ramach grup nieformalnych. Związane jest to przede wszystkim z niewystarczającymi zasobami finansowymi małych podmiotów gospodarczych, aby działania te realizować w ramach specjalnie wyznaczonych w tym celu spotkań. Z jednej strony presja czasu i bieżące prowadzenie działalności uniemożliwiają prowadzenie tego rodzaju aktywności, z drugiej zaś, przekazanie informacji przez właściciela/menedżera, względnie któregoś z pracowników innym członkom organizacji może odbywać się przy okazji przerw w pracy czy wspólnego dyskutowania zagadnień związanych z realizacją zadań w organizacji.

Osobną kwestią związaną z bezpieczeństwem informacji szczególnie w małych podmiotach rynkowych jest rozstrzygnięcie, w jakim stopniu posiadane informacje narażone są na utratę i, co ważniejsze, wykorzystanie przez potencjalnych konkurentów. W szczególności chodzi o to, jaki rodzaj informacji należy chronić w tego typu podmiotach. Kwestia ta wydaje się tym istotniejsza, że funkcjonowanie małych podmiotów w przestrzeni społeczno-gospodarczej uzależnione jest od wymiany informacji pomiędzy podobnymi podmiotami gospodarczymi. Ograniczając się w tym względzie do małych zakładów wytwórczych czy usługowych dostarczających finalnemu konsumentowi produktu czy usługi, można przyjąć, iż dyfuzja informacji sprzyja ich konkurencyjności. Umożliwia wymianę praktyk, sposobów nawiązywania relacji z innymi uczestnikami rynkowymi. W wielu przypadkach wzajemna wymiana informacji jest kluczowym sposobem uczenia się takich przedsiębiorstw. Z kolei przyjęcie wzorca ochrony informacji powoduje, iż organizacje zamykają się na rozwój, a ich odizolowanie może znacznie utrudnić ich funkcjonowanie.

W takim znaczeniu, o ile kształtowanie zachowań na poziomie indywidualnym i grupowym ma za zadanie wskazywanie pracownikom rangi zabezpieczenia informacji przed wydostaniem się na zewnątrz, tak na poziomie organizacyjnym i międzyorganizacyjnym proces organizacyjnego uczenia się powinien być ukierunkowany odwrotnie. Ma za zadanie kształtować postawy i zachowania pracowników zmierzające do dyfuzji informacji w otoczeniu. Tym samym należy wśród członków organizacji promować odmienną postawę wobec otoczenia, nie wrogiego, lecz przyjaznego. Oczywiście nie chodzi tutaj o sprzeczne formułowanie przekazów, ale o to, by działania podejmowane w organizacji sprzyjały nawiązywaniu relacji z otoczeniem. Uzasadnieniem takiego podejścia jest przypuszczenie, iż wykształcenie na poziomie indywidualnym i grupowym świadomości pracowników spowoduje, iż przekazywać oni będą jedynie te informacje, które nie zagrażają pozycji przedsiębiorstwa na rynku. Zasadniczo chodzi tu o symetrię przepływu informacji między otoczeniem a organizacją. Relacje z otoczeniem w znaczeniu transakcji polegają na wzajemnej wymianie, z jednej strony przepływie strumieni materialnych, z drugiej zaś niematerialnych. Trudno oczekiwać od partnerów, nawet potencjalnych, postaw i zachowań altruistycznych. Chcąc uzyskać informacje od innych uczestników gry rynkowej, niezbędne jest przekazanie czegoś w zamian, z reguły także informacji. Trudno w tym miejscu rozstrzygnąć, które z in-

formacji nadają się do wymiany i udostępniania, brak jest bowiem w tym względzie badań naukowych, które identyfikowałyby zbiory informacji szczególnie ważnych dla małej firmy i których udostępnienie innym podmiotom rynkowym mogłoby zagrozić jej pozycji rynkowej. Tym samym, wnioskiem o charakterze normatywnym kierowanym pod kątem właścicieli/menedżerów małych podmiotów jest potrzeba zidentyfikowania elementu wyróżniającego ją w otoczeniu. Przy czym bardziej chodzi tu o element behawioralny, związany z miękkimi obszarami zarządzania, tj. łatwość nawiązywania kontaktów, lojalność pracowników, doświadczenia w branży i wprawa w działaniu. Szczególnie w odniesieniu do małych podmiotów rynkowych mniej istotne jest wyposażenie techniczne, maszyny i aparatura, bowiem dostęp do nich jest podobny dla wszystkich, barierą w ich pozyskaniu jest natomiast stopa zwrotu inwestycji i związane z tym ryzyko. Przegląd małych przedsiębiorstw funkcjonujących w poszczególnych sektorach wskazuje, iż funkcjonują one, dysponując podobnym wyposażeniem i konkurują przede wszystkim w oparciu o miękkie obszary zarządzania. Osobną kwestią jest to, czy element wyróżniający małą organizację w otoczeniu, a mieszczący się w sferze niematerialnej możliwy jest do skopiowania przez innych uczestników rynkowych. Jednak kwestia ta znajduje się poza bezpośrednim zasięgiem tematu niniejszego opracowania.

Podsumowanie

Bezpieczeństwo należy do nadrzędnych wartości: było i jest sytuowane jako milcząca przesłanka jednego z najwyżej cenionych i uważnie chronionych dóbr. Znaczenie bezpieczeństwa, w tym bezpieczeństwa informacji, sukcesywnie wzrasta szczególnie w obszarze praktyki. Praktyczne znaczenie bezpieczeństwa informacji pozwala bowiem uwydatniać i zaktualizować problemy związane z omawianą wartością, jaką jest bezpieczeństwo.

Spośród wielu istniejących podejść i rozwiązań zmierzających do zapewnienia bezpieczeństwa informacji organizacji gospodarczej niniejszy artykuł prezentuje podstawy teoretyczne wraz z rozważaniami na temat kształtowania zachowań pracowników małej firmy zabezpieczających informacje.

Bibliografia

Barczyk A., Sydoruk T., *Bezpieczeństwo systemów informatycznych zarządzania*, Bellona, Warszawa 2003.

Bączek P., *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Wydawnictwo Adam Marszałek, Toruń 2006.

Konieczny J., *O metodzie rozumowań w etyce bezpieczeństwa*, „Bezpieczeństwo. Teoria i praktyka. Moralne problemy bezpieczeństwa" 2008, numer specjalny.

Borowiecki R., Kwieciński M., *Monitorowanie otoczenia, przepływ i bezpieczeństwo informacji. W stronę integralności przedsiębiorstwa*, Kantor Wydawniczy Zakamycze, Kraków 2003.

Ciborowski L., *Walka informacyjna*, Wydawnictwo Adam Marszałek, Toruń 1999.
Fischer B., *Przestępstwa komputerowe i ochrona informacji*, Kantor Wydawniczy Zakamycze, Kraków 2000.
Herman M., *Potęga wywiadu*, Bellona, Warszawa 2002.
Kuta M., *Polityka bezpieczeństwa informacji w przedsiębiorstwie – aspekty praktyczne*, [w:] R. Borowiecki, M. Kwieciński, *Monitorowanie otoczenia, przepływ i bezpieczeństwo informacji. W stronę integralności przedsiębiorstwa*, Kantor Wydawniczy Zakamycze, Kraków 2003.
Liedel K., *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Wydawnictwo Adam Marszałek, Toruń 2006.
Sienkiewicz P., *Społeczeństwo informacyjne jako społeczeństwo ryzyka*, [w:] *Społeczeństwo informacyjne. Aspekty funkcjonalne i dysfunkcjonalne*, red. L.W. Haber, M. Niezgoda, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2006.
Słownik języka polskiego, red. M. Szymczak, t. 1, Wydawnictwo Naukowe PWN, Warszawa 1988.
Słownik terminów z zakresu psychologii dowodzenia i zarządzania, Akademia Obrony Narodowej, Warszawa 2000.
Šmid W., *Metamarketing*, Wydawnictwo Profesjonalnej Szkoły Biznesu, Kraków 2000.
Zarządzenie bezpieczeństwem informacji, red. J. Łuczaka, Oficyna Współczesna, Poznań 2004.
Żebrowski A., Kwiatkowski M., *Bezpieczeństwo informacji III Rzeczypospolitej*, Oficyna Wydawnicza Abrys, Kraków 2000.

Strony internetowe:
http://sjp.pwn.pl/lista.php?co=zagro%BFenie (18.07.2008).
http://www.cert.pl/PDF/Raport_CP_2007.pdf (14.07.2008).
www.wiadmosci.tvp.pl (wiadomość z dnia 20 kwietnia 2003).

Franciszek Danielewski

Specyficzność informacji w działaniach wojennych

Wprowadzenie

Wojna stanowi integralny element historii ludzkości, w różny sposób wpływający na rozwój, albo też – alternatywnie – regresję cywilizacji. Ta dwuznaczność przyczyniła się do wykształcenia pewnych postaw, w dużym zakresie kontrolnych, co do jej intensywności i częstotliwości. Mamy bowiem do czynienia nie tylko z sytuacjami współdziałania państw, ale również z sytuacjami konfliktowymi. Państwo, będąc suwerennym podmiotem, może posługiwać się odpowiednimi środkami, w tym siłą zbrojną. Odwołuje się do tego specyficznego środka w przypadku realizacji wyznaczonych celów względem innego państwa. W przypadku przeciwstawienia się zbrojnego drugiej strony, mamy wówczas do czynienia ze stanem wojny[1]. W świetle danych historycznych dotyczących zdarzeń konfliktowych uwidacznia się stałe dążenie do regulacji postępowania stron biorących udział w działaniach wojennych. Można wyszczególnić dwie zasadnicze płaszczyzny rozważań: a) ustalenie zbioru regulacji podejmowania działań wojennych; b) ustalenie zbioru struktur, co do których uczestnicy działań wojennych powinni się odwoływać, ażeby walki zbrojne były prowadzone w sposób sprawiedliwy. Te dwa wymiary są przedmiotami szczegółowych ustaleń etycznych i prawnych.

W niniejszym artykule podjęto rozważania nad znaczeniem i rolą informacji w działaniach zbrojnych, ewentualnymi reperkusjami w konceptualizacji i terminologii oraz perspektywami ich rozwoju.

Wojna: pojęcia i definicje

Przegląd literatury ukazuje szeroki zakres odniesień: wojna ograniczona i totalna, wojna zimna i gorąca, wojna światowa i lokalna, wojna kontrolowana i niekontrolowana, wojna przypadkowa i zaplanowana, wojna konwencjonalna i nuklearna, wojna wypowiedziana i niewypowiedziana, wojna agresywna/ofensywna i obronna, wojna ogólna i graniczna, wojna międzynarodowa i domowa, wojna plemienna i cywilizowana, wojna prewencyjna i odwetowa, a także: wojna absolutna, wojna wyzwoleńcza, wojna zaborcza, wojna handlowa, wojna grabieżcza, wojna rewolucyjna, wojna polityczna, wojna ekonomiczna, wojna imperialistyczna, wojna partyzancka, wojna psychologiczna, wojna strategiczna, wojna dynastyczna, wojna obyczajowa, wojna święta, wojna ludobójcza. Złożoność ta wynika z faktu, iż określenia wskazują na różne

[1] T. Ślipko, *Zarys etyki szczegółowej*, t. 2, Kraków 2005, s. 320 i n.

aspekty i perspektywy wojny, tj. przyczyny, techniki wojenne, motywy lub cele wojny czy zachowania uczestników działań wojennych[2]. Jednak w każdym powyższym przypadku występuje aspekt przemocy, wyrażający się w sposób: kolektywny, wprost, wyraźny, osobowy, intencjonalny, zorganizowany, zinstytucjonalizowany, instrumentalny, usankcjonowany, a także: zrytualizowany i uregulowany. Wymiary te nie są wyczerpujące, albowiem wojna/stan wrogości jest specyficzną kategorią przemocy[3]. Ponadto nie odnoszą się one tylko do postaw, zachowań, ale zakładają istnienie określonych przyczyn wojny. W tym ujęciu wojna imperialistyczna, przykładowo, może być rozpatrywana jako zestaw postaw, które stanowią źródła wojny, a także jako specyficzny rodzaj odpowiedzialności, którą ponosi państwo ją wywołujące. Istota wojny nie wyraża się w prowadzonych działaniach zbrojnych, ale we wrogości i postawach charakteryzujących politykę zagraniczną określonego państwa.

Psychologiczny aspekt wojny został podniesiony przez Hobbesa w dziele *Lewiatan*, w którym zmienności stanu wojny i pokoju porównuje do stanów pogody: „As the nature of foul weather lieth not in a shower or two of rain, but in an inclination thereto of many days together; so the nature of war consisteth not in actual fighting, but in the known disposition thereto during all the time there is no assurance to the contrary"[4]. Wypowiedź ta może stanowić szersze odniesienie do dyskusji nad stanem pokoju: czy można go definiować jako stan bez wojny (w rozumieniu aktualnych działań zbrojnych)?[5]

Formalne i materialne aspekty pokoju i wojny

W świetle badań stan pokoju różni się od stanu wojny bardziej formalnie niż materialnie, albowiem w grę wchodzą jakości: *locus* i implementacja, a nie określone przejawy zachowania człowieka. Pokój stanowić więc może pewien zespół stałych, rozproszonych, niezorganizowanych, wewnętrznych konfliktów (*vide* państwa), natomiast wojna jest konfliktem ostrym, zorganizowanym, skoncentrowanym na obszarach peryferyjnych środowiska społeczno-politycznego. W tym kontekście, wojna i pokój różnią się między sobą jedynie stosowanymi środkami służącymi do osiągnięcia jednych i tych samych celów[6]. Dostrzega to francuski myśliciel R. Aron, który formułę C. von Clausewitza: „wojna jest kontynuacją polityki [...]", zamienia w jej przeciwstawienie: „polityka jest kontynuacją wojny [...]"[7]. Obie formuły, jego zdaniem, są równoważne, gdyż wyrażają kontynuację rywalizacji oraz stosowania środków przemocy lub humanitarnych, aby osiągnąć dokładnie te same cele. Takie stanowisko znajduje wyraz także u innych myślicieli. U H. Ecclesa bowiem czytamy: „natura wojny ulega zmianie, w szczególności w tym zakresie, iż coraz bardziej zamazuje się linia demarkacyjna

---

[2] F. Grieves, *Conflict and order: an introduction to international relations*, Boston 1977.

[3] J. van der Dennen, *On War: Concepts, Definitions, Research Data – A Short Literature Review and Bibliography*, [w:] UNESCO Yearbook on Peace and Conflict Studies 1980, Greenwood Press, Westport CT, 1981, p. 128 n.

[4] Q. Wright, *A study of war*, Chicago 1965.

[5] F. Grieves, *op. cit.*

[6] H. Barbera, *Rich nations and poor in peace and war*, Lexington 1973.

[7] R. Aron, *Peace and war: a theory of international relations*, New York 1966.

między stanem pokoju a stanem wojny"[8]; H. Barbera z kolei stwierdza: „Za obu zjawiskami, pokoju i wojny, mieści się to samo zjawisko władzy"[9].

Zwolennicy realizmu politycznego opowiadają się za istnieniem wspólnej bazy kategorii wojny i pokoju, a mianowicie – dążenia do władzy. To sprawia, że stanowią one dwie strony tej samej aktywności społeczno-politycznej. Przyczyny stanu wojny i przyczyny stanu pokoju w jakiś sposób są równoważne. Wojna i pokój nie muszą zatem być traktowane jako rozdzielne stany zachowań ludzkich, albowiem pokój zależny jest od zagrożeń i siły, a w niektórych przypadkach stanowi krystalizację uprzednio stosowanej przemocy. We współczesnych systemach politycznych nie ma istotnej różnicy między stanem wojny a stanem pokoju. Stąd takie zjawisko jak: pokojowe działania sił zbrojnych. Wojna jest więc pewnym zestawem środków służących osiąganiu określonych celów, a narzędzia militarne mogą być stosowane w celach służebnych społecznie lub też im przeczącym. Cele, na rzecz których prowadzone są działania wojenne, mogą być akceptowalne przez szersze grupy społeczne jako godziwe, co oznaczałoby, że instytucja wojny spełnia funkcje istotne w życiu społeczeństwa. Wojna służy bowiem zażegnywaniu konfliktów, przywracaniu należnych praw ludzkich, przeciwdziałaniu wszelkim patologiom w szerszej skali. Stąd też działania o charakterze innym niż militarny[10]. Tego typu sformułowania stanowią wyraźne reminiscencje literackie, jak np.: „pokój jest wojną" z dzieła Orwella *Rok 1984*. Interesujące jest również stanowisko zajmowane przez D. Wellsa: nie ma żadnego stanu pośredniego (czyśćca) między wojną a pokojem[11].

Oprócz powyższych definicyjnych rozważań, istnieją również inne stanowiska, w których omawiane kategorie ujmowane są jako graniczne pewnego *continuum*. Między nimi istnieje zatem określone pole demarkacyjne. R. Brodie stwierdza, że stosowana przez ludzi przemoc znajduje swój skondensowany, najwyższy poziom w działaniach wojennych, aczkolwiek nie są one zwykłymi jej przejawami. Wojna jest czymś więcej, zawiera w sobie, zdaniem uczonego, własną konfigurację przemocy, w której mieszczą się różne zjawiska, jak: po pierwsze – wojna od czasów antycznych posiada wyraźnie dający się wyszczególnić moment początkowy, oraz, co nie mniej ważne, moment końcowy; po drugie, wojna stanowi konfigurację różnych ceremonii (w tym religijnych)[12].

Społeczno-polityczne ujęcie wojny

Wojna, zgodnie z prawem międzynarodowym, z zasady może zachodzić między dwoma suwerennymi politycznymi bytami – państwami. W takim ujęciu wojna jest narzędziem stosowanym do rozwiązywania zaistniałych różnic między jednostkami przynależnymi do politycznego porządku świata. Tym samym zachodzi istotna różnica między stanem konfliktowym wewnątrz określonego państwa, do którego rozwiązania

[8] H. Eccles, *Military concepts and philosophy*, New Brunswick 1965.

[9] H. Barbera, *op. cit.*

[10] C. Eagleton, *International government*, New York 1948.

[11] D. Wells, *The war myth*, New York 1967.

[12] B. Brodie, *War and politics*, London 1973.

służą pokojowe mechanizmy i środki, a konfliktem w skali międzynarodowej. Wojna powoduje użycie wprost instytucji państwowych: polityki zagranicznej oraz sił zbrojnych. Wojnę należy więc rozpatrywać w kontekście międzynarodowym[13]. Tego rodzaju sformułowanie na temat wojny jako zjawiska międzynarodowego podzielają przedstawiciele różnych dyscyplin naukowych, w szczególności analitycy wojskowi. W ramach realizmu politycznego dostrzega się, że państwo może realizować swoje cele narodowe jedynie w drodze okazywania woli walki albo też gotowości prowadzenia wojny o różnej skali intensywności jako instrumentu własnej polityki zmierzającej do osiągnięcia zamierzonych celów[14]. To odpowiada stanowisku K. von Clausewitza, iż wojna jest aktem przemocy skierowanym przeciwko oponentom, ażeby zmusić ich do postępowania zgodnie z określoną wolą decydenta. W innym miejscu myśliciel ten wskazuje, iż przemoc jest również wykorzystywana jako narzędzie polityczne. Takie ujęcie wojny krytykowane jest z powodu jej ogólności. Zdaniem G. Sorela[15] wojna jest aktem politycznym, który podejmują państwa w sytuacji wyczerpania innych sposobów rozwiązania spraw spornych, zabezpieczenia własnych interesów, aby w drodze użycia sił zbrojnych ustalić przewagę, a przez to móc wywrzeć wpływ na innych. H. Kallen, krytykując definicję K. von Clausewitza, twierdzi, iż wojnę można definiować jako zbrojne starcie między dwoma lub więcej suwerennymi instytucjami, które używają sił zbrojnych, aby osiągnąć zamierzony cel. Istotnym terminem w tym sformułowaniu jest organizacja, która rozciąga się poza siły zbrojne i obejmuje cywilne obszary działalności, takie jak przemysł czy handel, a także wpływa na zachowania poszczególnych jednostek ludzkich.

Interesująca z punktu socjologicznego jest propozycja A. Johnsona[16], który wojnę traktuje jako rodzaj konfliktu zbrojnego między dwiema określonymi populacjami, jak: plemię, szczep, państwo lub mniejsza grupa społeczna, religijna czy polityczna. Zwolennicy tej definicji podkreślają szerokie ujęcie zbrojnego konfliktu, aczkolwiek jej mankamentem jest brak wskazania na czas jego trwania, jak też wielkości zaangażowanych jednostek. Z kolei B. Russell[17] definiuje wojnę jako konflikt między dwoma grupami społecznymi, a każda z nich próbuje unicestwić przeciwnika, aby osiągnąć pożądany cel. Angielski filozof stwierdza, iż pożądane przez walczące strony są władza i bogactwo.

M. Wallace z kolei traktuje wojnę jako rodzaj usankcjonowanego sposobu stosowania wobec siebie broni przez określonych członków różnych grup społecznych. Uczestnicy zmagania zbrojnego są odpowiednio wyszkoleni oraz funkcjonują w grupach, które kierowane są przez inne zespoły o charakterze politycznym, a wspierane, w różny sposób, przez całą populację cywilną[18]. A. Ashworth[19] dodaje, że wojna totalna stanowi typ konfliktu zbrojnego między dwoma mocarstwami, w których zasoby ludzkie i materiale organizowane są w sposób racjonalny w celu osiągnięcia zwycięstwa. Ludność mobilizowana jest zarówno w zakresie jej aktywności, jak też w sferze

[13] R. Aron, *op. cit*.

[14] J. Lider, *On the nature of war*, Westmead 1977.

[15] G. Sorel, *Réflections sur la violence*, Paris 1912.

[16] A. Johnson, *War*, New York 1935.

[17] B. Russell, *Why men fight*, New York 1916.

[18] M. Wallace, *War and rank among nations*, Lexington 1973.

[19] A. Ashworth, *The sociology of trench warfare 1914–1918*, British Journal of Sociology XIX, 4, 1968, pp. 406–423.

psychologicznej. W grę wchodzi powszechny pobór, jak również prowadzenie propagandy ukierunkowanej przeciwko wrogowi.

W latach siedemdziesiątych XX wieku zwrócono uwagę na inne aspekty wojny. Podkreślano, iż dotyczy ona przemocy zorganizowanej na dużą skalę, ukierunkowanej przez państwo (czy też rząd) przeciwko innemu państwu lub innej organizacji politycznej. Wysuwane propozycje w przeważającej większości wskazywały na polityczny charakter wojny. Ważna jest także argumentacja, iż wojna nie może już odnosić się do konfliktów zbrojnych między państwami. R. Barringer[20] rozważa wojnę jako jeden z możliwych sposobów polityki zmierzającej do rozwiązania zaistniałego konfliktu lub zabezpieczenia interesów. W tym sensie wojna jest jednym z wielu możliwych proceduralnych sposobów rozwiązywania konfliktów, jak: negocjacje, doradztwo, mediacje czy arbitraż. Wojna stanowi zatem pewien podsystem szerokiej gamy procedur rozwiązywania konfliktów. Rozpoznana sytuacja pozwala na systematyczną ocenę wielkości zaangażowanych sił zbrojnych. W tym ujęciu termin „wojna" posiada już określone implikacje prawne, co powoduje, że nie ma ryzyka wzrostu wrogości. Z kolei A. Bozeman[21] zwraca uwagę, że termin „wojna międzynarodowa" nie musi odnosić się do stanu konfliktu zbrojnego między państwami, albowiem mamy coraz szersze spektrum stron zaangażowanych militarnie wewnątrz bytu państwowego, co powoduje trudności w ustaleniu linii między stroną legalną a nielegalną. Często w takie konfliktowe sytuacje zaangażowane są czynniki zewnętrzne, co jeszcze bardziej utrudnia określenie podstaw pokoju i wojny. W niektórych więc przypadkach instytucje państwowe nie mogą ustalić typu prowadzonych działań militarnych, a przez to ustalić warunków pokojowych. Następuje erozja bytu państwowego jako fundamentu normatywnego w politycznej organizacji światowej. Pojawia się koegzystencja państwa z antypaństwowymi organizacjami jako aktywnymi aktorami na światowej scenie politycznej. W tak naświetlonym kontekście większą uwagę zwraca się ku kategorii cywilizacji jako właściwszego punktu odniesienia w rozważaniach nad fenomenem wojny.

Powyższe, wybrane tylko sformułowania wskazują, że w zakresie złożonych form wojny i pokoju, a przede wszystkim przemocy, zachodni model państwa coraz bardziej przestaje pełnić użyteczną funkcję identyfikacyjną takiego zjawiska jak: wojna międzynarodowa czy wojna domowa. W problematyce stosunków międzynarodowych rysuje się więc, zdaniem A. Bozemana, erozja pojęcia państwa narodowego jako realnego centrum normotwórczego, kontroli oraz integracji. W toczących się działaniach militarnych daje się zaobserwować narastające zjawisko funkcjonowania niezależnych, współdziałających ze sobą bytów pozapaństwowych, co podważa słuszność stosowania terminu „międzynarodowy porządek". W grę wchodzi organizacja tzw. alternatywnego społeczeństwa. W tym kontekście duże znaczenie przywiązuje się do pojęcia cywilizacji, albowiem jest ona zjawiskiem pojemniejszym niż pojęcie państwa. Cywilizacja obejmuje szeroki wachlarz politycznych, zbrojnych formacji, ruchów wyzwoleńczych oraz imperiów; mieszczą się w niej anarchiści i despoci, fundamentaliści religijni i wszelkiego rodzaju transregionalne porozumienia o charakterze finansowym. W przeciwieństwie do bytu państwowego, cywilizacja jest o wiele trwalsza w czasie, pomimo niezbyt wyraźnej określoności przestrzennej. Co ważniejsze, cywili-

[20] R. Barringer, *War: patterns of conflict*, Cambridge 1972.

[21] A. Bozeman, *War and the clash of ideas*, Orbis, 20, 1, Spring 1976, pp. 61–102.

zacja jest czymś neutralnym, nie ma określonych konotacji normatywnych czy aksjologicznych[22].

W częściowym podsumowaniu tych rozważań warto podkreślić, że istnieje bogata literatura, w której podnoszone są inne niż wyżej przedstawione aspekty wojny. W grę wchodzą rozważania natury filozoficznej, etycznej, jak też prawnej. Klasycznym przykładem tych ostatnich jest fundamentalne dzieło Q. Wrigtha *A Study of War*. Przedstawienie tych rozważań wymaga jednak szczegółowych badań porównawczych.

Stanowisko filozoficzno-etyczne wobec wojny

Dla dalszych rozważań konieczne są pewne odniesienia filozoficzne i etyczne. W dobie rozwoju technologii informatycznych inaczej traktowane są bowiem podstawowe pojęcia, pojawiły się też nowe formy konfliktu, co, jak się wydaje, wymusza rewizję dotychczasowego rozumienia wojny sprawiedliwej. Zwrócenie uwagi na etyczną stronę omawianego zagadnienia poniekąd znajduje uzasadnienie w fakcie, iż obszerna literatura w zakresie tzw. wojny informatycznej nie podejmuje jej etycznego wymiaru. W jakimś sensie wyjaśnieniem tego stanu rzeczy jest to, iż wojna informatyczna posiada wielowymiarowy charakter[23]. Wojna technologiczno-informatyczna to pojęcie obejmujące swym zakresem wykorzystanie cyberprzestrzeni do przeprowadzenia ataku na centra komunikacyjne oraz infrastrukturę, w której w użyciu są media informatyczne. Tak zarysowany charakter tej formy wojny stwarza określone problemy w zakresie konstrukcji etycznych warunków jej inicjowania i prowadzenia. Przedmiot ten posiada swoją wagę w rzeczywistości państw wysokorozwiniętych. Zagrożenia są tym większe, iż coraz bardziej uświadamiany jest jej niszczący charakter zarówno w obszarze ściśle militarnym (C2), jak też w obszarach cywilnych. Etyczne podejście do tych zagrożeń jest nie tylko możliwe, ale również praktycznie użyteczne, albowiem wskazuje na pozytywne i negatywne aspekty ewentualnych działań wojennych na poziomie informatycznym. Wartość tego typu rozważań nad konfliktem w sferze informatycznej nie przekreśla okoliczność kryminalnych lub terrorystycznych organizacji stwarzających realne zagrożenie. W pierwszej kolejności należy jednak poruszyć istotne aspekty koncepcji wojny sprawiedliwej. W jej świetle dogodniejsze będzie określenie wojny informatycznej.

Koncepcja wojny sprawiedliwej

Etyczna refleksja nad zjawiskiem wojny jest czymś stałym, albowiem wywodzić ją można już z czasów starożytnych[24]. Nie bez racji jest ona sprzęgnięta ze sformułowaniami Tomasza z Akwinu, którego myśl przetrwała do czasów współczesnych[25]. W grę wchodzą dwie podstawowe kategorie: kryteria inicjowania wojny (*ius ad bellum*)

[22] *Ibidem*.

[23] M. Libicki, *What is Information Warfare?*, Washington, D.C, 1996, p. 6.

[24] J. Ober, *Classical Greek Times* [in:] M. Howard, G. Andreopoulos, M. R. Shulman, *Why men fight*, New York 1916.

[25] M. H. Russell, *op. cit*.

oraz kryteria prowadzenia działań wojennych (*ius in bello*). Podstawowe zasady wojny sprawiedliwej to: a) słuszna przyczyna (*causa iusta*): u podstaw leży zasadnicze pojęcie obrony, które nie wyklucza idei operacji interwencyjnej, co jednak nie oznacza akceptacji wojny prewencyjnej[26]; wyklucza się wszelkie formy wojny zmierzające do podbojów lub aneksji; b) uprawniony autorytet: decyzja podjęcia działań wojennych musi być podjęta przez legalną władzę, nie może być podejmowana przez jednostkę – stąd też dziewiętnastowieczny zakaz prowadzenia tzw. wojen prywatnych; c) ostateczność: wojna jest sprawiedliwa tylko po wyczerpaniu wszelkich innych możliwych pokojowych sposobów rozwiązania zaistniałego konfliktu. Przykładem tego jest wojna peloponeska, jak też wojna w Zatoce Perskiej. Kolejne zasady sprawiedliwego prowadzania działań wojennych są następujące: a) ochrona ludności cywilnej: strona podejmująca działania wojenne nie powinna atakować ludności cywilnej ani też walczących, którzy dostali się do niewoli lub zaprzestali wszelkich aktów zbrojnych. Wycofujące się oddziały przeciwnika nieposiadające zdolności do działań zbrojnych (*vide* oddziały irackie) znajdować się mogą w tzw. szarej strefie, w której dopuszczalne są działania zbrojne[27]. Lotnictwo strategiczne, jak też zbrojne środki nuklearne, stwarzają oczywiste zagrożenia dla ludności cywilnej. Rozwiązaniem jest tu dopuszczalność jedynie ataków na centra strategiczne, w których straty wśród ludności cywilnej mogą być traktowane jako skutek uboczny[28]; b) proporcjonalność: istnieje wiele aspektów tej zasady. W pierwszej kolejności chodzi o użycie przemocy zbrojnej w odpowiednich rozmiarach; po drugie, stosowanie przemocy zbrojnej w odpowiedniej proporcji do przeciwnika musi jednak służyć osiągnięciu zwycięstwa. Tak więc w grę wchodzi użycie odpowiedniej siły zbrojnej, jak też odpowiedniego jej rodzaju[29]; c) czynienie dobra niż szkodzenie: istotnie właściwa zasada Tomasza z Akwinu. Jej stosowanie implikuje, że etyczne działania zbrojne wymagają uprzedniej oceny celu, który ma być osiągnięty z zastosowaniem odpowiedniej siły zbrojnej. Przykładem tej kalkulacji, aczkolwiek zaciemnionego przez wyrządzone szkody ludności cywilnej, jest amerykańska decyzja zrzucenia bomby atomowej na Hiroszimę, co miało zapobiec kosztownej inwazji Japonii[30].

W świetle powyższych etycznych konstrukcji widać, że zasady drugiej kategorii, mające zastosowanie w trakcie prowadzonych działań zbrojnych, mogą również stanowić istotną bazę do rozważań przed przystąpieniem do działań wojennych. Obie kategorie stanowią więc wzajemnie się warunkujące jakości prezentowanej teorii wojny sprawiedliwej. Jednak, z perspektywy etycznej wydaje się, że zasady *ad bellum* muszą być uwzględnione w pierwszej kolejności przez tych, którzy podejmują decyzje o wojnie czy pokoju. Przedstawione zasady stanowią wystarczającą bazę konceptualną, która umożliwia pełną analizę jakichkolwiek różnic między powinnością a użytecznością, jak też potencjalności eskalacji konfliktu z poziomu wojny informatycznej

---

[26] D.A. Rosenberg, *Nuclear War Planning* [in:] *The Laws of War: Constraints on Warfare in the Western World*, eds. M. Howard, G. Andreopoulos, M. R. Shulman, New Haven, Conn 1994, p. 160 n.

[27] M. Walzer, *Just and Unjust Wars*, New York 1977, p. 129.

[28] *Ibidem*, pp. 255–260.

[29] J.T. Johnson, *Just War Tradition and the Restraint of War*, Princeton 1981, p. 21 n.

[30] G.E. Moore, *Principia Ethica*, London 1993; J. Rawls, *A Theory of Justice*, Cambridge 1971.

do poziomu wojny konwencjonalnej, a nawet do poziomu wojny nuklearnej. W oparciu o wymienione zasady istnieje możliwość stworzenia perspektyw kontroli zbrojeń[31].

Obecnie możemy odnieść wieloaspektową teorię wojny sprawiedliwej do pojęcia informacji, a następnie do zasadniczego pojęcia wojny informatycznej.

Informacja

Pojęcie informacji w sensie przekazu jakiejś wiedzy, używane w języku potocznym, odgrywa coraz większą rolę w życiu współczesnych społeczeństw. Rozwój i upowszechnienie stosowania maszyn cyfrowych, a od końca II wojny światowej połączenie ich w sieć, a także pojawienie się pod koniec lat pięćdziesiątych XX wieku informatyki jako nowej dyscypliny nauki jest tego zjawiska dowodem. Chociaż wiedza i jej przekaz stanowią podstawowe wyznaczniki każdej społeczności, to jednak rozwój technologii informatycznej i jej wpływ na ludzkie życie w skali globalnej w szczególny sposób charakteryzuje współczesne życie społeczne, kreując społeczeństwo informacyjne. Przyjmuje się, że informacja obok kapitału, pracy i surowców stanowi warunek rozwoju ekonomicznego. Informacja w postaci zapisu cyfrowego posiada tym większe znaczenie. Od wielu lat ożywione dyskusje wywołuje kwestia oddziaływania technologii informatycznej na nauki społeczne. Znaczący wpływ na ten rodzaj dyskusji miało dzieło C. Shannona, *A Mathematical Theory of Communication*. W istocie chodzi o fakt, iż semantyczne i pragmatyczne aspekty informacji zostały w tym dziele zdefiniowane w języku matematycznym. Pomimo to, wszelkie rozważania o jakimkolwiek przekazie wiedzy w kontekście omawianego terminu informacji nie może obejść się bez odniesień lingwistycznych[32].

Początkowo informatyka za punkt wyjścia obrała obiektywistyczne teorie cybernetyczne, ale w miarę rozwoju dominować zaczęły inne stanowiska, m.in. stosowanie i interpretacja jako podstawowe aspekty pojęcia informacji. Nie oznacza to wcale zwrotu ku teoriom subiektywistycznym, ale raczej uznanie istnienia różnych perspektyw, które mogą w pewnym kontekście stanowić o informacyjnym charakterze jakiejś rzeczy lub dokumentu. Nie bez znaczenia dla informatyki jest również fakt, że informacja jest zasadniczym czynnikiem sprawczym w życiu społecznym, stąd też za teleologiczne uznaje się wszelkie systemy, w których przetwarzana jest informacja.

Duże znaczenie posiada umiejętność rozumienia przez ludzi używanych przez nich samych terminów. Znalazło to wyraz w teorii znaczenia L. Wittgensteina. Filozof ten uznaje, że znaczenie terminu jest zależne od jego użycia[33]. Można to odnieść również do pojęcia informacji.

Słowo informacja posiada swój źródłosłów w łacińskim słowie *informatio*. Przedmiotem rozważań będą przede wszystkim dwa podstawowe konteksty, w których informacja jest stosowana, a mianowicie jako akt kształtowania umysłu i jako akt przekazywania wiedzy. Te dwie strony aktywności są ze sobą ściśle powiązane.

---

[31] T. Ślipko, *op. cit.*, s. 328.

[32] R. Capurro, B. Hjørland, *The Concept of Information*, ed. B. Cronin, "The Annual of Information Science and Technology" 2003, 37.

[33] L. Wittgenstein, *The Blue and Brown Books*, Oxford 1958.

W myśli filozoficznej Kartezjusza (1596–1650) znajdujemy ślady tej rewolucyjnej w skutkach zmiany stosowania pojęcia informacji: od nadawania formy materii do komunikowania komuś czegoś. Oświeceniowy filozof, określając idee jako formy myśli, odrzuca tym samym scholastyczną koncepcję bezpośredniości percepcji ludzkiej: bezpośredniej relacji poznawczej pomiędzy intelektem a rzeczywistością. Idea jest uobecniona w ludzkim umyśle jako: obraz, reprezentacja.

Od lat pięćdziesiątych ubiegłego wieku zaznacza się intensywny proces rozwoju teorii informacji w cybernetyce oraz komunikacji. W oparciu o te dziedziny rozwinęła się technologia informatyczna. Nie oznacza to, że zostały rozwiązane wszelkie problematyczne kwestie. W konsekwencji teoria C. Shannona pozostawała nadal wpływową koncepcją w różnych obszarach aktywności społecznej. Świadczyć o tym może fakt, że teoria ta była konceptualnym odniesieniem w wielu obszarach badawczych, łącznie z psychologią i socjologią. Z czasem pojawiły się istotne pytania nie tyle o precyzję pomiaru informacji, fizyczne jej gromadzenie i transmisję, ale o kontekst znaczenia przekazu informacyjnego.

Uwzględniając różne zastosowanie terminu informacji, M.K. Buckland dokonał podziału informacji ze względu na relację do: rzeczy, procesu i wiedzy. Istotne dla naszych potrzeb jest to, że autor ten, analizując pojęcie informacji, w konsekwencji wprowadza termin dokumentu (*information as a thing*) oraz wskazuje na jego subiektywny charakter. I tak np. słoje na pniu drzewa zawierają informację o jego wieku, jak też o zmianach klimatycznych w ciągu całej jego żywotności. W podobny sposób każda rzecz może stać się informacyjną. Jeśli bowiem jakiś przedmiot może być symbolem, to tak samo może być jakością informacyjną.

Rewolucja informacyjna poprzez dostarczanie przedsiębiorstwom nowych sposobów walki z rywalami ułatwia osiąganie przewagi konkurencyjnej. Technologie informatyczne w szczególności wpływają na procesy produkcyjne – nie tylko ułatwiają przedsiębiorstwom wymianę wartości, ale przekształcają sposoby tworzenia wartości oraz ich powiązania. Nie tylko stymulują aktywność jednostki ludzkiej, ale, poprzez nowe sposoby przepływu informacji powodują, że w organizacjach gospodarczych tworzą się lepsze powiązania między indywidualnymi działaniami zarówno w ich obrębie, jak i na zewnątrz; a wreszcie – technologie te powodują zmiany w sposobach dystrybucji produktów[34].

Pojęcie wojny informatycznej

Przed podjęciem próby zgłębienia etycznego wymiaru zjawiska wojny informatycznej, niezbędna jest uprzednia refleksja nad samym tym pojęciem. Czy mamy do czynienia z prawdziwą postacią wojny, czy też z przejawem działań o charakterze kryminalnym lub terrorystycznym, albo też tajnych operacji wywiadowczych? Należy również uwzględnić ewolucję, która pociąga za sobą rozszerzenie zakresu pojęcia o aktywności, które nie są *stricte* działaniami wojennymi, a przez to nie powodują żadnej konieczności odnoszenia ich do teorii wojny sprawiedliwej. Mając to na uwadze, możemy uznać, iż termin „operacje informatyczne" odnosi się do szerokiego spektrum

[34] M. K. Buckland, *Information and Information Systems*, New York 1991, p. 50.

zagadnień informatycznych, w tym obejmujących operacje psychologiczne, zarządzanie danymi informatycznymi, bezpieczeństwo informatyczne oraz stosowne działania o charakterze wojennym. Takie uporządkowanie ułatwia właściwe odniesienie terminu wojny informatycznej do działań wojennych, które z kolei można rozpatrywać w kontekście teorii wojny sprawiedliwej.

Na czym polega więc wojna informatyczna? Ogólnie rzecz biorąc, ta forma działań wojennych dotyczy ataku na system komunikacyjny, jego węzły i infrastrukturę. Stosowane w tym przypadku środki zbrojne to te, jakich używa się w cyberprzestrzeni, a więc bomby logiczne, wirusy. Obejmują one również zastosowanie szeregu ofensywnych narzędzi, poczynając od konwencjonalnych, a kończąc na energii elektromagnetycznej, które mogą być skierowane na węzły informatyczne. Oczywiście w grę wchodzić może zastosowanie konwencjonalnych środków rażenia. Jednak można je wykluczyć, ze względu na niski poziom oryginalności[35].

Zakres operacji, które mogą być przeprowadzane w ramach wojny informatycznej jest dość szeroki, albowiem obejmuje pole walki zbrojnej i głębokie zaplecze przeciwnika. Tak więc militarne operacje informatyczne mogą służyć jako bezpośrednie wsparcie aktywnych sił zbrojnych. Mogą być również zastosowane w strategicznych przedsięwzięciach ukierunkowanych na zasoby przeciwnika. W ostatnim przypadku mamy do czynienia ze szczególną jakością militarnych operacji informatycznych. Pod pewnym względem przypominają one strategiczne działania lotnicze, na temat których dyskutowano w latach dwudziestych i trzydziestych XX wieku. Pomimo wyraźnych podobieństw militarne operacje informatyczne posiadają własne właściwości oraz powodują odmienne skutki. Przede wszystkim, w przeciwieństwie do ataku lotnictwa strategicznego, atak informatyczny, nawet z zastosowaniem konwencjonalnych środków rażenia, nie powoduje podobnej destrukcji. W grę wchodzi raczej blokada systemów informatycznych na określonym obszarze geograficznym, nawet gdy przeciwnik podejmuje pewne przeciwdziałania. Inną jeszcze różnicą jest to, że strategiczne bombardowanie lotnicze z konieczności prowadzi do strat w ludności cywilnej, nawet przy obecnie stosowanych precyzyjnych środkach rażenia, natomiast broń informatyczna nie stwarza takich zagrożeń. Niski poziom niszczącego efektu broni informatycznej powoduje jednak pewne trudności w ocenie skutków, jak też uniemożliwia stosowanie zasady proporcjonalności. Z tego też powodu uważa się, że strategiczne środki informatyczne w pewnych obszarach mogą powodować większą destrukcję niż środki masowego rażenia. Taka perspektywa efektywności sprawia, że broń informatyczna staje się szczególnie atrakcyjna w wywoływaniu konfliktów.

Przedmiotem debat wśród specjalistów jest niejasność rozróżnienia między walczącymi stronami, aktami wojny. W przypadku ataku lotniczego ustalenie sprawcy nie nastręcza większych trudności. Tak samo łatwo zidentyfikować, że stroną walczącą przeciwnika są jego siły zbrojne. Pewnemu zamazaniu ulega już wojna partyzancka, w której aktywną rolę odgrywają często osoby cywilne. W operacjach informatycznych o charakterze wojennym może uczestniczyć dowolna osoba. Z etycznego punktu widzenia, istotne zatem jest rozróżnienie między osobami, które posiadają dostęp do zaawansowanych technologii informatycznych a osobami, które je wykorzystują w celach wojennych. Atak w cyberprzestrzeni jest trudny do zdefiniowania, albowiem

[35] M. Libicki, *op. cit.*

mogą go powodować organizacje kryminalne, terrorystyczne oraz mogą być przejawami właściwych działań militarnych. Dlatego też zasadniczym zadaniem jest często ustalenie sprawcy ataku, jego tożsamości. Czym innym jest epizodyczne zdarzenie, a czym innym zorganizowana akcja ukierunkowana na określony cel.

Teoria wojny sprawiedliwej a wojna informatyczna

Na podstawie powyższych rozważań wprowadzających w złożoną problematykę działań wojennych, istnieje obecnie sposobność odniesienia formy wojny informatycznej do uwarunkowań etycznych. W gruncie rzeczy chodzi o odpowiedź na pytanie: w jakim zakresie wojna informatyczna może być uznana za sprawiedliwą?

Obrona konieczna, albo też interwencyjna w przypadku wojny informatycznej, posiada inną wartość niż w przypadku klasycznych działań wojennych. Obrona z użyciem broni informatycznej posiada szerszy zasięg destrukcyjnego oddziaływania. Środki informatyczne mogą być szczególnie użyteczne w zapobieganiu niebezpiecznemu rozwojowi siły militarnej, rozbudowie arsenału broni masowego rażenia przeciwnika. Broń informatyczna wymyka się spod kontroli autorytetu państwa, przechodzi coraz bardziej w obszar działań organizacji alternatywnych. W jakiś sposób znajduje tu potwierdzenie teoria, że rewolucja informatyczna spowodowała rozproszenie władzy do organizacji i ośrodków pozapaństwowych zarówno pokojowych, jak też terrorystycznych i kryminalnych. Pojawienie się nowych aktorów na scenie politycznej świata, którzy są skłonni stosować broń informatyczną, sprawia, że państwa również wprowadzają ją do swojego arsenału militarnego. Warto dodać, że fakt istnienia nowych podmiotów politycznych jest poniekąd korzystny, gdyż ułatwia utajnienie operacji informatycznych podejmowanych przez poszczególne państwa. Paradoksalnie, słabe państwo może przeprowadzić atak na mocarstwo bez obawy wykrycia, unikając akcji odwetowej. Jednak jest to tylko sytuacja hipotetyczna, albowiem obecnie zaawansowane środki detekcji informatycznej nie ułatwiają tego rodzaju posunięcia. Pozostaje jednak łatwość podejmowania militarnych działań informatycznych, co powoduje, że moc traci coraz bardziej zasada wojny jako ostatecznego odwołania. Destrukcyjny charakter informatycznych narzędzi w działaniach wojennych przywołuje raczej podobieństwo sankcji ekonomicznych. Podobieństwo to z kolei powoduje wykluczanie pewnych działań informatycznych z zakresu działań wojennych.

Celami wojny informatycznej są często sieci transportowe, energetyczne, telekomunikacyjne oraz infrastruktura finansowa. W bezpośrednim zasięgu oddziaływania jest więc ludność cywilna, która dogłębnie odczuwa skutki ataków informatycznych. Ten typ wojny informatycznej podważa wolę oporu, walki. W dużym zakresie przypomina to wcześniej rozważane strategiczne bombardowanie obiektów cywilnych. Nie wyklucza się jednak możliwości planowania ataków wyłącznie na cele militarne, co tym bardziej upoważnia do prowadzenia ocen etycznych ewentualnych działań wymierzonych przeciwko ludności cywilnej.

Interesującym zagadnieniem jest możliwość stosowania zasady proporcjonalności. Uznaje się, że przemyślane zastosowanie broni informatycznej może być w pełni zgodne z tą zasadą, albowiem zaatakowany przeciwnik może odpowiedzieć, atakując w sposób precyzyjny wybrane obiekty adwersarza. Pojawiają się jednak określone

problemy, gdy strona atakująca niszczy żywotną infrastrukturę strony przeciwnej, a sama nie posiada żadnej, albo posiada, ale na niskim poziomie zaawansowania technologicznego. W jaki sposób można przeprowadzić, zgodnie z zasadą proporcjonalności, działania odwetowe? Czy można zastosować klasyczne środki rażenia w odwecie? Innym jeszcze krytycznym zagadnieniem jest sytuacja hipotetyczna, gdy strona zaatakowana bronią informatyczną nie może dokonać odpowiednich działań odwetowych z powodu braku narzędzi informatycznych. Rosyjscy specjaliści wojskowi, rozważając podobną sytuację, uznali konieczność odpowiedzi siłowej za pomocą wszelkich środków militarnych przeciwko atakującemu. W takich okolicznościach, z powodu braku respektowania zasady proporcjonalności, istnieje niebezpieczeństwo asymetrycznej eskalacji działań wojennych. Prócz tego pojawia się problem skali zniszczenia spowodowanego przez różne narzędzia militarne: uderzenie bomby precyzyjnej a infekcja systemu komputerowego wirusem. Trudnością realną jest to, że nie jest łatwo jednoznacznie przypisywać odpowiedzialność za atak komuś, gdy brak jest wystarczających danych[36].

Pomimo tych i wielu innych trudności w odwoływaniu się do zasad etycznych ułatwieniem jest idea wojny informatycznej, która powoduje mniejszą destrukcję materialną, jak też nie wywołuje strat wśród ludności. W przeciwieństwie do hamletowskiego dylematu, przed jakim został postawiony prezydent H. Truman, zastosowanie narzędzi wojny informatycznej prowadzi nie tylko do mniejszych zniszczeń, ale również ułatwia rozwiązywanie konfliktów, które w innych przypadkach mogłyby prowadzić do wyniszczającej wojny konwencjonalnej[37].

Podsumowanie

Zasadniczym celem niniejszego artykułu był wgląd w problematykę działań wojennych, prezentacja fundamentalnych pojęć, stanowisk i definicji, która jednak nie wyczerpuje interesującego pola badawczego, a następnie odniesienie się do współczesnego zjawiska wojny informatycznej. W pierwszej kolejności dokonano przybliżenia jej specyficzności w obszarze działań wojennych, a następnie naświetlono z punktu etyki. W tym ostatnim przypadku została przeprowadzona analiza porównawcza z zasadami teorii wojny sprawiedliwej. Tego rodzaju zabieg poznawczy posiada swoje uzasadnienie w wartości stanu bezpiecznego, jakim jest stan pokoju. Ewentualna polityka oraz doktryny bezpieczeństwa muszą uwzględniać zagrożenia płynące z cyberprzestrzeni. W grę wchodzi potrzeba wypracowania procedur obronnych i odwetowych, przy jednoczesnym starannym uwzględnieniu prawa międzynarodowego oraz zasad etycznych. W pierwszym rzędzie chodzi o unikanie ataków na cele cywilne, a następnie o stosowanie środków militarnych w sposób proporcjonalny. Kategoria wojny informatycznej przyczynia się, z różnych względów, do ponownych przemyśleń, konceptualizacji i wytyczania nowych perspektyw działań wojennych. Wojna informatyczna wywołuje określone zniszczenia, niemniej charakteryzuje się zmniejszoną skalą destrukcji, w przeciwieństwie do konwencjonalnych narzędzi zbrojnych. Współczesne

[36] Th. C. Schelling, *Arms and Influence*, New Haven 1966.

[37] J. T. Johnson, *Just War Tradition...*, *op. cit.*

wojny, nasycone zaawansowanymi technologiami, w szczególności informatycznymi, nadal mogą być rozpatrywane w świetle fundamentalnych zasad etycznych.

Bibliografia

Aron R., *Peace and war. A theory of international relations*, Praeger, New York 1966.

Ashworth A., *The sociology of trench warfare 1914–1918*, British Journal of Sociology, 19, 4, 1968.

Barbera H., *Rich nations and poor in peace and war*, Lexington, MA: Lexington Books, 1973.

Bozeman, A., *War and the clash of ideas*, Orbis, 20, 1, 1976.

Barringer R., *War: patterns of conflict*, Cambridge, MA: MIT Press, 1972.

Brodie B., *War and politics*, Cassell, London 1973.

Buckland M.K., *Information and Information Systems*, Praeger, New York 1991.

Capurro R., Hjørland B., *The Concept of Information*, ed. B. Cronin, "The Annual of Information Science and Technology" 2003, 37.

Van der Dennen J., *On War: Concepts, Definitions, Research Data – A Short Literature Review and Bibliography* [in:] UNESCO Yearbook on Peace and Conflict Studies 1980, Greenwood Press, Westport CT, 1981.

Eccles H., *Military concepts and philosophy*, Rutgers University Press, New Brunswick 1965.

Eagleton, C., *International government*, Ronald Press, New York 1948.

Grieves F., *Conflict and order: an introduction to international relations*, Houghton Mifflin, Boston 1977.

Johnson A., *War*, Encyclopedia of the Social Sciences, 15, Macmillan, New York 1935.

Johnson J. T., *Just War Tradition and the Restraint of War*, Princeton University Press, Princeton, NJ, 1981.

Libicki M., *What is Information Warfare?*, National Defense University Press, Washington, D.C, 1996.

Lider J., *On the nature of war*, Saxon House, Westmead 1977.

Moore G. E., *Principia Ethica*, Cambridge University Press, London 1993.

Ober J., *Classical Greek Times* [in:] M. Howard, G. Andreopoulos, M.R. Shulman, *Why men fight*, The Century Co., New York 1916.

Rawls J., *A Theory of Justice*, Cambridge, MA: Belknap Press, 1971.

Rosenberg D.A., *Nuclear War Planning* [in:] M. Howard, G. Andreopoulos, M. R. Shulman (eds.), *The Laws of War: Constraints on Warfare in the Western World*, Yale University Press, New Haven, Conn., 1994.

Russell B., *Why men fight*, The Century Co., New York 1916.

Russell F.H., *The Just War in the Middle Ages*, Cambridge University Press, Cambridge 1975.

Schelling Th.C., *Arms and Influence*, Yale University Press, New Haven, Conn., 1966.

Sorel G., *Réflections sur la violence*, Rivičre, Paris 1912.

Ślipko T., *Zarys etyki szczegółowej*, t. 2, Wydawnictwo WAM, Kraków 2005.

Wallace M., *War and rank among nations*, Lexington Books, Heath, MA 1973.

Walzer M., *Just and Unjust Wars*, Basic Books, New York 1977.

Wells D., *The war myth*, Pegasus, New York 1967.
Wittgenstein L., *The Philosophical Investigations*, G.E.M. Anscombe (trans.), Blackwell, Oxford 1958.
Wittgenstein L., *The Blue and Brown Books*, R. Rhees (ed.), Blackwell, Oxford 1958.
Wright Q., *A study of war*, Chicago University Press, 2nd ed., Chicago 1965.

Część II
Edukacja na rzecz bezpieczeństwa

Ewa Waligóra
Jacek Witkowski

Bezpieczeństwo w programach nauczania realizowanych w Centrum Szkolenia Policji

> Zapobieganie błędom kosztuje znacznie mniej niż naprawianie wyrządzonych w ich efekcie szkód.
> C.N. Parkinson

Współczesna nauka daje podstawy, by twierdzić, że poczucie bezpieczeństwa jest jedną z najbardziej podstawowych potrzeb człowieka zarówno w wymiarze indywidualnym, jak i zbiorowym (społecznym). Nawiązując do tej wiedzy, zarówno władza ustawodawcza, jak i wykonawcza określiły priorytety, na których muszą koncentrować się wysiłki samorządów zmierzające do wykonania zadań publicznych oraz zaspokojenia zbiorowych potrzeb z zakresu porządku publicznego i bezpieczeństwa.

Obowiązujące prawo nakłada szczególne obowiązki na samorząd terytorialny i policję – umundurowaną i uzbrojoną formację służącą społeczeństwu, przeznaczoną do ochrony bezpieczeństwa ludzi oraz do utrzymywania bezpieczeństwa i porządku publicznego, do której zadań należy w szczególności: ochrona życia i zdrowia ludzi oraz mienia przed bezprawnymi zamachami naruszającymi te dobra, a także bezpieczeństwa i porządku publicznego, inicjowanie i organizowanie działań mających na celu zapobieganie popełnianiu przestępstw i wykroczeń oraz zjawiskom kryminogennym, jak również współdziałanie w tym zakresie z organami państwowymi, samorządowymi i organizacjami społecznymi. Wynika z tego potrzeba tworzenia szeroko rozumianej koalicji na rzecz bezpieczeństwa. Jest to działanie uzasadnione oczywistym faktem, że surowe prawo i nawet najbardziej skuteczna policja działająca w osamotnieniu nie są w stanie poprawić stanu bezpieczeństwa.

Wiedząc, że elementarnym warunkiem poprawy bezpieczeństwa obywateli jest skuteczne ograniczanie przyczyn i zwalczanie zjawisk godzących w porządek prawny, autorzy zdają sobie sprawę, że częściowa odpowiedzialność za niewystarczający poziom tych działań wynika ze sfery funkcjonowania różnych podmiotów. W praktyce bowiem zdarzało się, że wiele instytucji w ramach działań własnych gromadziło istotne informacje, które po poddaniu analizie mogłyby służyć do konstruowania konkretnych wniosków prewencyjnych. Niestety bardzo rzadko wykorzystywano tę wiedzę do minimalizacji zagrożeń. U podłoża tego stanu leży niewielka aktywność wynikająca z niskiej świadomości roli i potencjalnego znaczenia swych działań, brak koordynacji przedsięwzięć i wymiany informacji pomiędzy zainteresowanymi podmiotami oraz niski poziom zachowań obywatelskich w społeczeństwie.

O zasobności pojęciowej prewencji kryminalnej świadczą próby jej zdefiniowania. Badacze zjawiska – W. Czapiewski i R. Głowacki – określają prewencję kryminalną jako ogół bezpośrednich działań instytucji państwowych, społecznych i obywateli, ma-

jących na celu uniemożliwienie lub utrudnienie podjęcia akcji przestępczej, poprawę bezpieczeństwa jednostki przez eliminowanie poczucia strachu przed staniem się ofiarą i w konsekwencji podniesienie jakości życia.

Oczekiwania społeczne oraz specyficzne zadania w zakresie prewencji kryminalnej sprawiają, że policjanci powinni sprostać szczególnym wymaganiom. Dotyczy to zarówno predyspozycji psychofizycznych, jak i specjalistycznej wiedzy oraz umiejętności. W związku z tym, w ostatnich latach dokonano gruntownej przebudowy programów szkoleniowych, wprowadzono treści nauczania, które przygotowują policjantów do wykonywania zadań z zakresu prewencji kryminalnej. Są to m.in.:

1) przygotowanie i zaprezentowanie wystąpienia publicznego, spotkania profilaktycznego z różnymi grupami odbiorców;
2) inspirowanie do działań i przedsięwzięć z zakresu prewencji kryminalnej oraz uczestnictwo w nich;
3) inicjowanie wspólnych spotkań z samorządami, organizacjami i instytucjami mogącymi przyczynić się do poprawy bezpieczeństwa;
4) propagowanie sposobów unikania zagrożeń;
5) rozpoznawanie i analizowanie stanu bezpieczeństwa pod kątem organizowania przedsięwzięć profilaktycznych;
6) udzielanie pomocy ofiarom przestępstw;
7) inicjowanie i prowadzenie działań w zakresie zapobiegania patologiom społecznym i ich zwalczania;
8) prowadzenie działań w ramach zwalczania i zapobiegania demoralizacji i przestępczości nieletnich;
9) podejmowanie działań zapobiegawczych dotyczących przemocy w rodzinie;
10) organizowanie pomocy oraz podejmowanie działań w celu zapewnienia bezpieczeństwa osobom zaliczanym do grup szczególnego ryzyka.

W programach szkoleń uwzględniono również kształcenie umiejętności tworzenia atmosfery życzliwości, otwartości i zaufania oraz aktywnego słuchania i zapamiętywania, gromadzenia informacji, analizowania, wyciągania wniosków i podejmowania decyzji, a także radzenia sobie ze stresem, psychomanipulacją, krytyką i sprzeciwem.

System przygotowania policjantów do zadań w zakresie prewencji kryminalnej został opracowany w ten sposób, aby w procesie dydaktycznym wykształcić pożądane umiejętności. Część zajęć to symulacje przeprowadzane na podstawie opracowanych założeń dotyczących zdarzeń, z jakimi policjanci mają do czynienia podczas codziennej służby.

Grupy szkoleniowe w Centrum Szkolenia Policji na różnych rodzajach kursów liczą średnio około 20 słuchaczy, co umożliwia stosowanie aktywizujących metod nauczania, takich jak: zajęcia demonstracyjne, pokazy, instruktaże, ćwiczenia praktyczne z dokumentowania wykonywanych czynności.

Szkolenia specjalistyczne policjantów o profilu: specjalista do spraw nieletnich, prowadzone w Zakładzie Służby Prewencyjnej CSP od 1997 r., ewoluują w kierunku psychologiczno-prawnym, zgodnie z trendem ogólnoświatowym.

W zakres tego typu szkoleń wchodzi wiedza interdyscyplinarna, niezbędna do wykształcenia konkretnej umiejętności i stosowania jej w praktyce. W realizacji wybranych zagadnień biorą udział wykładowcy spoza CSP, reprezentujący różne specjalizacje, w tym psycholodzy z Fundacji „Dzieci Niczyje", a także biegły psycholog Sądu Okręgowego w Warszawie.

Fundacja „Dzieci Niczyje" opracowała 21-godzinny program szkolenia warsztatowego „Przemoc wobec dziecka", którego celem jest poszerzenie wiedzy i umiejętności policjantów dotyczących diagnozy i interwencji w przypadku krzywdzenia dzieci oraz pracy z nimi – ofiarami tych czynów, rozwijanie umiejętności współpracy z instytucjami uczestniczącymi w procesie pomocy dzieciom krzywdzonym i ich rodzinom.

CSP specjalizuje się w promowaniu i propagowaniu wiedzy o przemocy w rodzinie i pomocy jej ofiarom. Czyni to poprzez organizowane seminaria, konferencje naukowe i szkolenia. Szkolenia te posiadają dodatkowy walor profilaktyczny – nie jest bowiem tajemnicą, że policjanci, ze względu na szczególnie stresujący charakter pracy, są grupą ryzyka skłonną także, chociaż w niewielkim stopniu, do stosowania przemocy wobec najbliższych.

W ramach tego szkolenia, blok prewencji kryminalnej zatytułowany „Prowadzenie działań profilaktycznych" realizowany jest przez 42 godziny. Obejmuje on m.in.:

1) przygotowanie się do spotkania profilaktycznego z różnymi grupami odbiorców (uczeń, nauczyciel, rodzice),
2) przeprowadzenie takiego spotkania,
3) zagadnienia autoprezentacji,
4) zasady udzielania informacji środkom masowego przekazu,
5) wiedzę na temat podmiotów pozapolicyjnych działających na rzecz dzieci i rodziny,
6) Krajowy Program Zapobiegania Niedostosowaniu Społecznemu i Przestępczości wśród Dzieci i Młodzieży,
7) Krajowy Program „Razem Bezpieczniej".

Program ten obejmuje także problematykę profilaktyki wczesnej przestępczości.

Dzięki systematycznej współpracy ze szkołami, znajdującymi się na terenie środowiska lokalnego autorów, instytucjami i placówkami, ustawowo i statutowo zajmującymi się sprawami wychowania dzieci i młodzieży, podnoszona jest świadomość prawna odnośnie do zasad postępowania w sprawach nieletnich, praw dziecka czy zapobiegania handlowi ludźmi.

Programy szkoleniowe realizowane są zgodnie z zasadami pedagogiki, uwzględniają także aktualne unormowania prawne i praktykę policyjną. Stosuje się ponadto nauczanie problemowe z wykorzystaniem scenariuszy zajęć np. dotyczących praw dziecka, zawierających potencjalne zagrożenia w tym zakresie. Uczestnik szkolenia otrzymuje w efekcie kompendium wiedzy służącej prawidłowemu rozwiązywaniu konkretnych kwestii na zasadzie funkcji: znać – ćwiczyć – umieć. Taki sposób postępowania dydaktycznego prowokuje słuchacza do aktywności, dostrzegania problemów, formułowania pytań i hipotez oraz ich weryfikowania przez podejmowanie odpowiednich działań.

Oferta programowa szkoleń w zakresie prewencji kryminalnej, pozwalająca kształtować najbardziej przydatne samorządom terytorialnym umiejętności policjantów, nie jest zamknięta – będzie ona modyfikowana i rozszerzana wraz z pojawiającymi się potrzebami i oczekiwaniami społecznymi.

W dniach 28–29 listopada 2007 r. w Centrum Szkolenia Policji w Legionowie odbyła się konferencja pt.: „Interwencja kryzysowa wobec małoletniej ofiary przestępstwa", której organizatorem był Zakład Służby Prewencyjnej Centrum Szkolenia Policji.

W konferencji wzięło udział około 140 osób, a wśród nich m.in.:
- specjaliści ds. nieletnich i patologii z KWP,
- sędziowie i prokuratorzy,
- starostowie powiatów legionowskiego, nowodworskiego, pułtuskiego i płońskiego,
- dyrektorzy PCPR,
- prelegenci,
- Sztab Główny Policji,
- Biuro Prewencji i Ruchu Drogowego KGP,
- KSP,
- Policyjna Izba Dziecka,
- Dyrektor Zespołu Szkół Ogólnokształcących,
- studenci Wyższej Szkoły im. Kardynała Stefana Wyszyńskiego (45 osób) – Wydział Filozofii Chrześcijańskiej, Instytut Psychologii, studenci realizujący specjalizację z psychologii sądowej i pomocy psychologicznej,
- Zespół Psychologa Koordynatora KGP,
- przedstawiciele szkół policyjnych.

Podczas konferencji dokonano uroczystego otwarcia komisariatu szkoleniowego. Komisariat ten wyposażony jest m.in. w pokój przyjaznego przesłuchania dziecka, który ma służyć nie tylko do celów szkoleniowych, ale także, a może przede wszystkim, instytucjom wykonującym czynności procesowe z małoletnią ofiarą przestępstwa.

W ciągu dwóch dni odbyły się sesje plenarne oraz zajęcia warsztatowe, w czasie których omawiano problemy związane z tematyką małoletniej ofiary przestępstwa, zwracano uwagę na poszanowanie jej praw i co ważniejsze, poruszano kwestię stworzenia interdyscyplinarnej koalicji działającej na rzecz krzywdzonego dziecka.

Jacek Grzechowiak

Rola szkoleń w zarządzaniu bezpieczeństwem

Na stronach internetowych firm szkoleniowych odnaleźć można wiele szkoleń o bardzo zróżnicowanej tematyce, skierowanych do niemal wszystkich branż. Rynek szkoleniowy w Polsce zadziwia bogactwem ofert, znaleźć bowiem możemy zarówno szkolenia adresowane do osób pracujących w danym zawodzie, które ukierunkowane są na rozwijanie kompetencji (np. „Innowacyjne rozwiązania dla logistyki"[1]), jak i szkolenia skierowane do osób niebędących specjalistami w obszarze, którego dotyczy szkolenie („Finanse dla menedżerów niefinansistów"[2]). Niestety, przeglądając oferty szkoleniowe, dość trudno zidentyfikować ten sam mechanizm w odniesieniu do branży ochrony. Rodzi się więc pytanie, czy bezpieczeństwo biznesowe jest niedoceniane, postrzegane jako mało istotny element prowadzenia działalności gospodarczej, czy też brak na rynku specjalistów od tego rodzaju szkoleń? Odpowiedź na to pytanie nie jest łatwa, bowiem z jednej strony branża ochrony od wielu lat plasowana jest na czołowych miejscach wśród branż najlepiej rozwijających się, z drugiej zaś wciąż wiele firm w swoich strukturach nie posiada osoby zarządzającej – w pełnym tego słowa znaczeniu – bezpieczeństwem. Można by więc postawić hipotezę, iż uboga oferta w zakresie tego rodzaju szkoleń wynika z dość niskiej świadomości bezpieczeństwa i *vice versa*.

Zanim jednak szczegółowo omówiona zostanie tematyka szkoleń, należy zastanowić się, dlaczego są one tak ważne, skoro jest ich taka mnogość i rozmaitość?

Szkolenie jest działaniem mającym na celu uzupełnienie lub pogłębienie wiedzy, kształtowanie umiejętności oraz odpowiednich postaw pracowników[3]. Jak widać, cel szkolenia jest jasno zdefiniowany, podobnie jak rola szkolenia w funkcjonowaniu organizacji biznesowych (i nie tylko). Podnoszenie kwalifikacji pracowników poprzez ich szkolenie jest jednym z podstawowych elementów rozwoju organizacji. Dążenie do rozwoju kompetencji, szczególnie kompetencji kluczowych najbardziej widoczne jest w organizacjach uczących się. Takie postępowanie stanowi także jeden z elementów kształtowania trwałej przewagi konkurencyjnej poprzez osiągane dzięki rozwojowi kompetencji odpowiednie wykorzystanie zasobów przedsiębiorstwa. Tak więc organizacje zainteresowane są rozwojem kompetencji swoich pracowników, ponieważ im lepiej wykształcona kadra (zwłaszcza menedżerska), tym lepsze wykorzystanie zasobów organizacji.

Zarządzenie bezpieczeństwem jest jednym z elementów prowadzenia działalności operacyjnej przez organizacje biznesowe. Proces ten w coraz większym stopniu wpływa na wyniki firm, dlatego jego poziom i jakość winny być analogiczne do innych procesów operacyjnych. Współczesne firmy coraz częściej postrzegają zarządzanie

---

[1] http://www.biznespolska.pl/konferencje/kalend.php?conferenceid=27691 (2008.09.12).

[2] http://www.szkolenia.com.pl (2008.09.12).

[3] *Leksykon zarządzania*, red. M. Adamska, Warszawa 2004, s. 576.

bezpieczeństwem jako istotny komponent swojej działalności operacyjnej. Wynika to z wielu czynników, z których zagrożenia kryminalne czy terrorystyczne to tylko niektóre niebezpieczeństwa, na jakie narażone są podmioty gospodarcze. Każda organizacja podlega jednak indywidualnym zagrożeniom, wynikającym z charakteru jej działalności, lokalizacji, pozycji na rynku czy choćby walki konkurencyjnej. Dlatego rozwój systemu zarządzania bezpieczeństwem powinien iść w parze z ogólnym rozwojem organizacji. Rozwój kompetencji jest narzędziem wspierającym ten proces. Dotyczy to zarówno osób zarządzających elementami systemu bezpieczeństwa (w praktyce więc *security manager*'ów), jak i pracowników korzystających z tego systemu. Niebagatelna jest także znajomość potrzeb w zakresie bezpieczeństwa oraz możliwości oferowanych przez współczesne systemy ochrony, rozwiązania organizacyjne, proceduralne, czy wreszcie możliwości pracowników działów ochrony i dostawców usług w tym zakresie.

Tak rozumiane podejście do zarządzania bezpieczeństwem wymaga zorganizowania odpowiedniego wsparcia szkoleniowego, które dostarczyłoby wiedzy podstawowej oraz aktualizowałoby ją wraz z rozwojem organizacji oraz zmianą zagrożeń, na jakie jest ona narażona. Rozwój kompetencji w zakresie bezpieczeństwa jest jednym z ważniejszych zadań *security manager*'a, ponieważ to on jest osobą odpowiedzialną w praktyce za tworzenie i zarządzanie systemem bezpieczeństwa organizacji. Jednocześnie poprzez szkolenia *security manager* tworzy nową jakość bezpieczeństwa w organizacji i podnosi efektywność tego procesu. W różnych przedsiębiorstwach istnieją różne systemy szkoleń pracowników. Z reguły jednak składają się one z trzech komponentów:

- szkolenia podstawowe (wstępne) – dostarczające bazowej wiedzy, umożliwiającej sprawne „poruszanie się" po organizacji oraz swoim obszarze odpowiedzialności;
- szkolenia doskonalące (uzupełniające) – rozwijające kompetencje kluczowe oraz umiejętności pomocnicze;
- szkolenia specjalistyczne – skierowane do wybranej grupy odbiorców, potrzebujących specjalistycznej wiedzy.

Szkolenia podstawowe bardzo często organizowane są w ramach obowiązkowych szkoleń BHP. Ten rodzaj szkoleń adresowany jest do pracowników rozpoczynających pracę. W ten sposób otrzymują oni podstawową wiedzę z wielu obszarów działania przedsiębiorstwa, w tym także z zakresu bezpieczeństwa. Udział *security manager*'a w tego rodzaju szkoleniach wydaje się więc oczywisty, choć organizacja tego szkolenia może przybierać różną postać w zależności od rodzaju i kultury przedsiębiorstwa, np. w firmach, zlokalizowanych w wielu miejscach może przybierać formę oddzielnego szkolenia. Dość często – zwłaszcza w dużych przedsiębiorstwach – ten typ szkoleń zastępowany jest przez drukowane broszury, wydawane nowemu pracownikowi przez dział ochrony lub personalny. Z doświadczeń autora wynika jednak, że kontakt osobisty *security manager*'a z nowymi pracownikami pozwala nawiązać bliższe relacje i wykorzystać kulturę organizacyjną do zainspirowania ich do aktywnego współdziałania w kreowaniu polityki bezpieczeństwa organizacji, a także poznać praktyki stosowane w innych firmach. Wszystkie metody szkoleń mają swoje zalety. Jednak zarówno metody, jak i zakres szkoleń podstawowych muszą odpowiadać potrzebom organizacji tak, aby nowi pracownicy nabyli przekonania, że system bezpieczeństwa wnosi konkretną wartość dodaną w sukces organizacji.

Szkolenia doskonalące przeznaczone są dla pracowników z dłuższym stażem, szczególnie gdy obejmują oni nowe obowiązki w ramach wewnętrznego awansu, np.:
- zmian prawnych, powodujących konieczność wprowadzenia nowych rozwiązań w zakresie bezpieczeństwa;
- zmian w poziomie bezpieczeństwa organizacji, np. wynikających ze zmiany lokalizacji bądź zmian stanu bezpieczeństwa w dotychczasowej lokalizacji;
- rozpoczynania realizacji nowych, innowacyjnych projektów bądź wprowadzania szczególnie ważnych – z biznesowego punktu widzenia – produktów.

Powyższe sytuacje są przykładowe, zaś faktyczne potrzeby szkoleniowe powinny być analizowane na bieżąco przez *security manager*'a w kontekście zmieniającego się stanu bezpieczeństwa firmy i jej otoczenia. Niestety ten rodzaj szkoleń rzadko jest stosowany, a pozwala rozwinąć kompetencje pracowników, dając przy tym *security manager*'owi możliwość zweryfikowania swojej wizji bezpieczeństwa przez pryzmat potrzeb pracowników. Brak szkoleń doskonalących najczęściej wynika z faktu, iż zarządzanie bezpieczeństwem wciąż nie jest postrzegane w kategoriach potrzeb organizacji, a sprowadzane jest jedynie do poziomu ochrony fizycznej (czasami także technicznej). Szkolenia doskonalące wymagają z reguły zewnętrznych trenerów, dlatego w tym przypadku rola *security manager*'a polega na tworzeniu programu szkoleń, ich organizowaniu oraz wspieraniu trenerów, choć oczywiście może on (i powinien) prowadzić część szkoleń osobiście. W ramach szkoleń doskonalących celowe jest wykorzystanie doświadczeń współpracujących firm ochrony z jednoczesnym włączeniem w proces szkolenia części pracowników tych firm (np. szefowie ochrony obiektu, dowódcy zmian), którzy powinni być zaznajomieni z potrzebami przedsiębiorstwa, w którym wykonują zadania ochronne. Zakres szkolenia i jego częstotliwość należy jednak w tym przypadku uzależnić od kilku czynników, m.in. profilu szkolenia, zakresu zadań, formy ochrony czy rotacji pracowników ochrony.

Szkolenia specjalistyczne – są formą szkoleń, skierowaną do wyselekcjonowanej grupy pracowników narażonych na specyficzne rodzaje niebezpieczeństw, czyli:
- najwyższe kierownictwo firmy, które z uwagi na swoją pozycję zawodową i społeczną może być narażone na porwanie, napaść bądź szantaż;
- pracownicy o szczególnym znaczeniu dla firmy, np. posiadający unikalne kompetencje i w ten sposób narażeni na różne zagrożenia, takie jak np. korupcja czy szantaż. Lista tych osób może być długa – wśród nich z pewnością powinni znaleźć się członkowie zespołów zarządzania kryzysowego;
- pracownicy, którzy z racji wykonywanych obowiązków mogą podlegać różnym zagrożeniom, z reguły kryminalnym, tacy jak: kasjerzy, pracownicy niektórych typów sklepów i zakładów (np. jubilerskich);
- pracownicy działów ochrony bądź osoby odpowiedzialne za bezpieczeństwo organizacji. Dotyczy to nie tylko *security manager*'ów (szefów bezpieczeństwa) lub osób odpowiedzialnych za ochronę fizyczną i techniczną, lecz także osób zajmujących się bezpieczeństwem teleinformatycznym.

Profil szkoleń specjalistycznych jest z reguły „szyty na miarę", uwzględnia potrzeby przedsiębiorstwa, poziom i rodzaj zagrożeń, wreszcie jego możliwości finansowe.

Najczęściej szkolenia specjalistyczne koncentrują się na takich zagadnieniach, jak:

- zasady bezpieczeństwa osobistego, np. wykrywanie obserwacji, zachowanie w sytuacjach ekstremalnych zagrożeń (napad, porwanie);
- zarządzanie kryzysowe: system wczesnego wykrywania zagrożeń, algorytm postępowania w sytuacji kryzysowej, tworzenie, szkolenie oraz praca zespołu zarządzania kryzysowego;
- wykrywanie symptomów podwyższonego zagrożenia;
- nowoczesne metody i środki bezpieczeństwa; technologie wspomagające ochronę osób, mienia i informacji; trendy w zarządzaniu bezpieczeństwem.

Podobnie jak w przypadku szkoleń doskonalących przedstawione powyżej obszary szkoleniowe są jedynie przykładami, toteż program szkoleń należy dopasować do potrzeb i kultury organizacji tak, aby osiągnięte cele w maksymalnym stopniu pokrywały się z celami przedsiębiorstwa. Szkolenia specjalistyczne, z uwagi na swój charakter oraz potrzeby w zakresie bazy szkoleniowej, w zdecydowanej mierze przeprowadzane są przez firmy specjalistyczne. Ta właśnie cecha sprawia, że ich przygotowanie wymaga od *security manager*'a zarówno kreatywności, jak i przezorności, by szkolenie rzeczywiście spełniało swoją rolę i przynosiło organizacji faktyczną – a nie wirtualną – wartość dodaną. Stąd wybór partnera do przeprowadzenia szkolenia specjalistycznego jest procesem, który należy przeprowadzić z najwyższą rzetelnością, w sposób analogiczny jak wybór firmy świadczącej usługi ochrony, dbając przede wszystkim o uwiarygodnienie doświadczenia w tym zakresie przez partnera szkoleniowego poprzez m.in.:

- Zweryfikowanie kwalifikacji trenerów (zarówno w zakresie zasad bezpieczeństwa, jak i kwalifikacji metodycznych);
- Przeprowadzenie wizji lokalnej bazy szkoleniowej;
- Uzyskanie referencji z przeprowadzonych szkoleń dla innych firm.

Równie istotny jest dobór osób szkolonych, który nie powinien opierać się jedynie na potrzebach wynikających z zajmowanego stanowiska, lecz powinien uwzględniać także cechy psychiczne i fizyczne pracowników. Ważnym aspektem szkoleń specjalistycznych jest także możliwość znalezienia przez samych szkolonych (a także *security manager*'a) zagadnień szczególnie trudnych, dzięki czemu możliwe jest podjęcie działań organizacyjnych wspomagających osoby, którym pewne aspekty bezpieczeństwa sprawiają szczególną trudność. Można to uzyskać m.in. za pomocą ankiet wypełnianych przez osoby szkolone po zakończeniu kursu, a także dokonanie oceny osób szkolonych przez trenerów. W ten sposób opracowanie planu szkoleń i ich programu będzie dużo bardziej efektywne[4]. W kontekście tworzenia planu szkoleń niezbędne jest uzyskanie przez *security manager*'a informacji na temat planów jego firmy jako podstawy do opracowania planu szkolenia[5].

Coraz większa grupa przedsiębiorstw postrzega szkolenia z zakresu bezpieczeństwa jako element kształtowania trwałej przewagi konkurencyjnej. Jest to niewątpliwie znak czasu, żyjemy bowiem w erze globalizacji i związanych z nią zamachów terrorystycznych czy przestępczości zorganizowanej. Dlatego właśnie „dojrzałe" firmy traktują zarządzanie bezpieczeństwem na równi z innymi procesami dokonującymi się w ramach ich funkcjonowania. Dzięki takiemu podejściu do zarządzania ponoszą

[4] *Ibidem.*

[5] *Rozwój personelu*, red. A. Szałkowski, Kraków 2002, s. 56.

one wymierne korzyści nie tylko w postaci niskich strat, lecz przede wszystkim – poprzez osiągnięcie stanu harmonijnego, niezakłócanego incydentami, funkcjonowania. Jest to wartość wpływająca zdecydowanie pozytywnie na ich rozwój, wizerunek stabilnego, bezpiecznego partnera biznesowego, a dzięki temu także na wyniki finansowe. Duża w tym zasługa pracowników, którzy, znając zasady bezpieczeństwa, jasno definiują swoje potrzeby i lepiej wykorzystują zasoby systemu zarządzania bezpieczeństwem.

Bibliografia

Leksykon zarządzania, red. M. Adamska, Difin, Warszawa 2004.
Rozwój personelu, red. A. Szałkowski, Wydawnictwo Akademii Ekonomicznej, Kraków 2002.

Strony internetowe:
http://www.biznespolska.pl/konferencje/kalend.php?conferenceid=27691 (2008.09.12).
http://www.szkolenia.com.pl (2008.09.12).

Część III
Bezpieczeństwo biznesu, gospodarki i społeczeństwa

Robert Kucęba
Leszek Kiełtyka

Analiza i projektowanie systemów bezpieczeństwa energetycznego

Wprowadzenie

Jednym z warunków egzystencji współczesnego świata jest ciągłe dążenie do zmniejszenia zużycia energii w różnych jej postaciach, praktycznie we wszystkich procesach energetycznych, co bezpośrednio wiąże się z poprawą bezpieczeństwa energetycznego. W ostatnich latach, po transformacji polskiej gospodarki energetycznej oraz krajów Unii Europejskiej, w okresie dynamicznych zmian politycznych zauważa się przejście od przeważającej w początkowej fazie transformacji krótkookresowego spojrzenia na gospodarkę energetyczną i politykę gospodarczą do zainteresowania problemami rezultatów przemian długookresowych. Zmiany w sektorze energetycznym szczególnie związane są z decentralizacją rynków energii, a jednocześnie ich integracją wewnątrz Unii Europejskiej. Zauważa się, że zmiany te wpływają na realizację transferu wiedzy, transferu technologii oraz wprowadzanie innowacji technologicznych i organizacyjnych w obszary gospodarki energetycznej. Daje to w efekcie istotne oszczędności zużycia energii, poprawie ulegają świadczone usługi, jak również zmniejszają się koszty prowadzonej działalności. Zmiany zachodzące w energetyce stymulują również powstawanie konkurencyjnych rynków energii w różnych podsystemach sektora energetycznego. Nasuwają się jednak elementarne pytania: czy ta konkurencyjność nie jest za bardzo kontrolowana? Czy rozwiązana strona legislacyjna przekłada się na rzeczywiste funkcjonowanie rynku energii? Prawne rozwiązania są opracowane, natomiast ich realizacja jest zbyt spowolniona przez dużych uczestników rynku, a także zmiany sił politycznych.

Mówiąc o transferach wiedzy i technologii, warto również wspomnieć o transferze politycznym. Może on być traktowany jako przechodzenie przez kolejne ekipy rządzące fundamentalnych kierunków strategicznych w gospodarce narodowej i ich realizacji, niezależnie od miejsca tych ugrupowań na scenie politycznej. Pomimo wysokiego postępu, wzrostu innowacji, otwarcia polityki energetycznej na Europę – na świat, transfer polityczny, zwłaszcza w obszarach gospodarki energetycznej, jest bardzo rozproszony, by nie powiedzieć – niski. Od 10 kwietnia 1997 roku, czyli od momentu uchwalenia pierwszej Ustawy Prawo energetyczne, upłynęło zaledwie 12 lat, a już kilkanaście razy była nowelizowana. Największe i najczęstsze zmiany w tym zakresie zachodziły przy przeobrażeniach pierwszej sceny politycznej, a co za tym idzie – ekip rządzących. Faktem jest, że zmiany jako jeden z elementów innowacji są bardzo istotne, jednak w sferze decyzji strategicznych, a zwłaszcza w polityce energetycznej, powodują częste restarty realizacji kierunków strategicznych. Wpływa to

negatywnie na realizację spójnej, kompatybilnej polityki bezpieczeństwa energetycznego, która ma znaczenie priorytetowe i powinna być przedmiotem integrującym cały zróżnicowany politycznie i etnicznie świat.

Istota projektowania Zintegrowanych Systemów Bezpieczeństwa Energetycznego

Znaczenie bezpieczeństwa energetycznego jest niewątpliwie pierwszorzędne. Można je uznać za filar bezpieczeństwa egzystencji na świecie, w każdym możliwym wymiarze. Z punktu widzenia legislacji, bezpieczeństwo energetyczne definiowane zarówno w perspektywie globalnej, jak i lokalnej to realizowane procesy w gospodarce, umożliwiające pokrycie bieżącego i perspektywicznego zapotrzebowania odbiorców na paliwa oraz różne postacie energii bezpośredniej i finalnej. Oczywiście, zakłada się, że procesy w omawianym obszarze realizowane są w sposób technicznie i ekonomicznie uzasadniony, z zachowaniem ciągłości (niezawodności) dostaw, odpowiednich parametrów jakościowych, warunków ochrony środowiska, po społecznie akceptowalnych cenach. Bardzo ważnym akceleratorem bezpieczeństwa energetycznego jest również transfer polityczny – dążenie do stabilności i kompatybilności politycznej w omawianym zakresie.

Bezpieczeństwo energetyczne uzależnione jest od wielu czynników, m.in. wielkości potencjału źródeł energii, stanu technicznego systemu zaopatrzenia i form własności jego infrastruktury, lokalizacji i stopnia dywersyfikacji, wykorzystania krajowych i zagranicznych źródeł zaopatrzenia (szczególnie złóż gazu ziemnego i ropy naftowej), zróżnicowania bazy paliwowej dla elektroenergetyki i ciepłownictwa, możliwości magazynowania paliw, stopnia rozwoju i przepustowości krajowych i międzynarodowych połączeń systemów energetycznych (elektroenergetycznego i gazowniczego) oraz warunków wewnętrznej i międzynarodowej stabilności[1].

Wysoka złożoność i wymagany duży stopień korelacji pomiędzy czynnikami wejściowymi i wyjściowymi wpływającymi na bezpieczeństwo energetyczne, świadczą o konieczności projektowania i wdrażania wielowymiarowych, kompatybilnych podsystemów bezpieczeństwa energetycznego, wchodzących w skład Zintegrowanego Systemu Bezpieczeństwa Energetycznego (ZSBE). Zintegrowany System Bezpieczeństwa Energetycznego to zbiór powiązań funkcjonalnych podsystemów, realizujących poszczególne funkcje cząstkowe w celu optymalizacji bezpieczeństwa energetycznego w badanym obszarze, zabezpieczające pokrycie bieżącego i perspektywicznego zapotrzebowania na energię pierwotną i bezpośrednią.

Każdy podsystem w strukturach ZSBE to zbiór obiektów, które realizują cząstkowe procesy/funkcje optymalizacji bezpieczeństwa energetycznego. Zatem każdy obiekt opisany jest atrybutami wejściowymi, zwanymi wymuszeniami, funkcjami opisującymi procesy realizowane przez obiekt pod wpływem zadanych atrybutów wejściowych oraz odpowiedziami obiektu (atrybuty wyjściowe) na zadane wymuszenia. Opty-

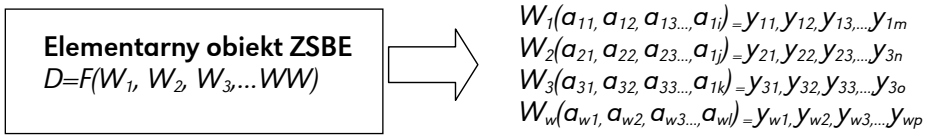
[1] M. Kwiatkowski, *Proces formułowania strategii rozwoju firmy obrotu energią elektryczną*, Warszawa 2006; J. Machowicz, A. Wieloński, *Bezpieczeństwo energetyczne Polski*, Warszawa 2007; J. Malko, A. Wilczyński, *Rynki energii – działania marketingowe*, Wrocław 2006.

malizacja bezpieczeństwa energetycznego w ZSBE wymaga uwzględnienia zarówno na wejściu i wyjściu poszczególnych podsystemów, w tym obiektów – atrybutów wejściowych uwzględniających czynniki technologiczne, produktowe, ekonomiczne, ekologiczne, jak również kompatybilność polityczną. Dlatego też istotą w procesie optymalizacji bezpieczeństwa energetycznego jest dopasowanie metodologii i metod modelowania oraz analizy i projektowania ZSBE, w odniesieniu do wielopoziomowych zbiorów atrybutów wejściowych i wyjściowych uzależnionych od wymienionych grup czynników. Zasadniczo, analiza i projektowanie ZSBE to proces adaptacji nowych technologii – transfer technologii, nowych rozwiązań legislacyjnych i przedmiotowych – transfer wiedzy, integralności politycznej – transfer polityczny.

Fazy projektowania systemów bezpieczeństwa na przykładzie ZSBE

Zgodnie z założoną definicją, ZSBE to zbiór powiązań funkcjonalnych podsystemów bezpieczeństwa, które z kolei prezentowane są przez zbiór obiektów będących podzbiorami ZSBE. Złożoność takich zbiorów ze względu na rozmiar i zakres działania ZSBE jest wielopoziomowa. Zatem w procesie projektowania ZSBE w pierwszej fazie tworzy się elementarne obiekty, definiując atrybuty wejściowe, funkcje obiektu oraz atrybuty wyjściowe. Uproszczony model elementarnego obiektu przedstawiono na rysunku 1.

Rysunek 1. Elementarny obiekt ZSBE – model uniwersalny



Źródło: opracowanie własne na podstawie: L. Kiełtyka, R. Kucęba, *Design and Analysis of Intelligent System of Electro-energetic Blocks Motion Management*, International Conference on Engineering Optimization, Rio de Janeiro, Brazil, June 1–5, 2008.

Powyższy model to prezentacja zbioru warunków decyzyjnych określonych mianem funkcji/procesów generowanych w poszczególnych projektowanych obiektach implementowanych w strukturach ZSBE. Liczebność argumentów wejściowych a_{wl}, oraz odpowiednich argumentów wyjściowych y_{wp}, są wielkościami zmiennymi dla poszczególnych warunków decyzyjnych W_w. Nieustalona zmienność liczebności wynika z różnorodności warunków decyzyjnych generowanych przez ekspertów dziedzinowych w rzeczywistym środowisku decyzyjnym. Należy zaznaczyć, że generowane funkcje/procesy zależą od zróżnicowanych grup czynników wpływających na bezpieczeństwo energetyczne, takie jak m.in.: technologiczne, ekonomiczne, ekologiczne oraz kompatybilności politycznej. Dlatego w procesach definiowania warunków decyzyjnych oraz generowanych odpowiedzi powinna być określona jednoznaczna funkcja celu odwzo-

rowań projektowanego obiektu w odniesieniu do optymalizowanych elementarnych funkcji zgodnych z istotą bezpieczeństwa energetycznego[2].

W rezultacie, w procesach projektowania i wdrażania ZSBE dokonuje się integracji pomiędzy poszczególnymi obiektami. Integrowanie polega na łączeniu w całość, zatem istotą integracji w strukturze ZSBE jest utworzenie nowej jakościowo całości, której elementy połączone są odpowiednimi relacjami – asocjacjami i powiązane odpowiednim stopniem zależności od całości. W praktyce rozróżniamy kilka typów integracji, m.in. takie jak: projektowa (metodologiczna), organizacyjna, techniczna, technologiczno-konstrukcyjna oraz istotna z punktu widzenia projektowania systemów bezpieczeństwa energetycznego – integracja (kompatybilność) polityczna. W niniejszym referacie skoncentrowano się na integracji projektowej, która bezpośrednio dotyczy całego cyklu projektowania, składającego się z następujących faz: założenia projektowe, cele projektu, analiza obiektowo-procesowa, generowanie warunków decyzyjnych – funkcji procesów, formułowanie i generowanie baz wiedzy, projektowanie i wdrażanie oraz weryfikacja. W tabeli 1 zdefiniowano poszczególne fazy całego proponowanego cyklu projektowania poszczególnych składowych ZSBE, jak również całego systemu.

Zgodnie z przyjętymi założeniami projektowymi, fundamentalnym elementem projektowanego systemu bezpieczeństwa energetycznego jest wygenerowanie funkcji celu oraz jej podfunkcji.

Wyznaczona funkcja celu oraz jej składowe opisywane są przez warunki decyzyjne, które w rzeczywistości są nieustalone i ulegają mutacjom pod wpływem zmieniającego się otoczenia i uwarunkowań, takich jak m.in.: prawnych, politycznych, technicznych, organizacyjnych, jak również ekologicznych. Po zdefiniowaniu funkcji celu i jej składowych należy określić i zdefiniować podejście metodologiczne projektowania i wdrażania proponowanego ZSBE lub jego składowych (podsystemów, obiektów).

Podejścia metodologiczne projektowania ZSBE

Podejścia metodologiczne projektowania ZSBE mogą być mapowane na podstawie ogólnych zasad projektowania systemów adaptowanych w różnych obszarach działalności zróżnicowanych grup społecznych. System bezpieczeństwa energetycznego, jak każdy inny system, to zbiór powiązanych funkcjonalnie i fizycznie obiektów, opisanych odpowiednimi procesami, które wymuszane są pod wpływem sygnałów wejściowych, generując na wyjściu sygnały wyjściowe zwane odpowiedziami. Prezentowana uogólniona definicja, którą można również adaptować jako uogólnioną definicję systemu bezpieczeństwa energetycznego, pozwala wnioskować i przyjąć założenie słuszności mapowania podejść metodologicznych z innych obszarów projektowania systemów.

W praktyce stosowane są dwa zasadnicze podejścia metodologiczne: diagnostyczne i prognostyczne. Podejście diagnostyczne polega na modernizacji istniejącej struktury systemu i dopasowaniu do wymagań otoczenia wewnętrznego oraz zewnętrznego.

[2] L. Kiełtyka, R. Kucęba, *Design and Analysis of Intelligent System of Electro-energetic Blocks Motion Management*, International Conference on Engineering Optimization, Rio de Janeiro, Brazil, June 1–5, 2008.

Tabela 1. Cykl projektowania ZSBE – opis poszczególnych faz

Etapy realizacji projektu	**Umowne oznaczenie**	**Zadania cząstkowe**
Założenia projektowe	Z	Określenie przedmiotu i podmiotu projektu; Wygenerowanie grupy obiektów przedmiotowo-podmiotowych w projekcie; Określenie przewidywanych rezultatów projektowych i wdrożeniowych w odniesieniu do poprawy bezpieczeństwa energetycznego; Określenie znaczenia projektu z punktu jego utylitarności.
Cele projektu	C	Uzyskanie obiektywnego, opartego na rzetelnej analizie opisu bieżącego stanu zarządzania bezpieczeństwem energetycznym w ściśle określonym środowisku projektowym. Informacje dotyczące stanu obecnego umożliwiają określenie optymalnych metod modyfikacji lub wdrożenia nowego systemu wspierającego poprawę bezpieczeństwa energetycznego. Bezpośrednio realizacja tej fazy projektowej umożliwia określenie m.in. funkcji celu dla ZSBE oraz opracowanie harmonogramu rzeczowego i finansowego wdrożenia ZSBE lub jego składowych.
Analiza obiektowo-procesowa	A	Określenie i zdefiniowanie podejścia metodologicznego projektowania ZSBE; Opracowanie specyfikacji funkcjonalnej i środowiskowej; Opracowanie projektu infrastruktury fizycznej (implementacyjnej); Opracowanie prognozy efektów wdrożenia ZSBE, w tym poszczególnych jego składowych; Opracowanie harmonogramu wdrażania ZSBE.
Generowanie warunków decyzyjnych	D	Określenie i zdefiniowanie atrybutów decyzyjnych a_{wl} oraz wartości (*decyzji*) y_{wp} opisujących poszczególne obiekty ZSBE; Określenie i opracowanie zbioru funkcji definiujących przykładowe rzeczywiste warunki decyzyjne w odniesieniu do opracowanej funkcji celu; Określenie zbioru i klasyfikacja asocjacji pomiędzy projektowanymi obiektami.
Formułowanie i generowanie baz wiedzy	W_w	Formułowanie i generowanie baz wiedzy z zakresu definiowanych rzeczywistych warunków decyzyjnych, opisujących wybrany zakres poprawy bezpieczeństwa energetycznego.
Projekt i wdrożenie	P	Opracowanie modeli funkcjonalno-implementacyjnych ZSBE wraz z ich opisem; Zestawienie serii diagramów przepływu danych; Zestawienie serii diagramów asocjacji pomiędzy obiektami ZSBE; Opracowanie słownika systemu opisującego poszczególne obiekty, przepływy i asocjacje – stanowiące dziedzinę działania systemu ZSBE; Wdrażanie składowych systemu wg określonego harmonogramu.
Weryfikacja	W	Określenie i analiza porównawcza rzeczywistych wartości decyzyjnych z modelowanymi wartościami decyzyjnymi – propozycja zastosowania mierników błędów ex-post.

Źródło: opracowanie własne na podstawie: L. Kiełtyka, R. Kucęba, *op. cit.*; R. Kucęba, *Chosen Aspects of Electricity Market Structure's Reconversing – Functions and Place of Small Power Industry* [in:] *The Challenges for Reconversion. Innovation – Sustainability – Knowledge Management*, ed. P. Pachura, Belgium 2006, p. 193–198.

Z kolei podejście prognostyczne to proces analizy, projektowania i wdrażania systemu od podstaw. Obydwa podejścia integrowane są poprzez stosowane metody projektowania, takie jak: sekwencyjna, ewolucyjna, przyrostowa przez cele oraz spiralna.

Wszystkie prezentowane metody charakteryzuje się tymi samymi fazami projektowania (punkt 2), różnica polega na realizacji funkcji celu, jej składowych oraz poszczególnych obiektów wchodzących w skład projektowanej struktury ZSBE. W przypadku metody sekwencyjnej następuje chronologiczna realizacja wszystkich faz projektowania systemu, z uwzględnieniem wszystkich jego obiektów/podsystemów oraz realizacji wszystkich składowych zdefiniowanej funkcji celu.

Metoda ewolucyjna polega na określeniu harmonogramu projektowania i wdrażania poszczególnych obiektów/podsystemów ZSBE, z uwzględnieniem harmonogramu ich integracji funkcjonalno-fizycznej. W metodzie tej chronologicznie realizuje się wszystkie fazy projektu dla pojedynczych obiektów bądź podsystemów ZSBE (kolejność projektowania obiektów/podsystemów określona według założonego harmonogramu). Zakłada się, że projektowane obiekty/podsystemy są autonomiczne, które mogą podlegać integracji funkcjonalnej i fizycznej w ujęciu ewolucyjnego rozwoju ZSBE[3].

Metoda przyrostowa przez cele polega na określeniu funkcji celu oraz jej składowych, które w następnym kroku są selekcjonowane i porządkowane (malejąco) według wyznaczonych wag ich istotności. Wagi istotności ustalane są na podstawie przyjętych kryteriów oceny istoty realizowanego celu cząstkowego, w odniesieniu do celu zasadniczego realizowanego przez złożenie funkcji składowych w zasadniczej funkcji celu. Po procesie selekcji następuje realizacja poszczególnych funkcji składowych celu, według wag ich istotności (malejąco). Realizacja poszczególnych celów cząstkowych wymaga określenia odpowiednich obiektów (niejednokrotnie wielodziedzinowych), które w procesie projektowania przechodzą wszystkie jego fazy, a ich weryfikacja polega na audycie i pomiarze „odpowiedzi" projektowanej części ZSBE, w odniesieniu do realizacji założonego celu cząstkowego. W metodzie przyrostowej przez cele poszczególne elementy ZSBE projektowane są według określonego harmonogramu realizacji celów cząstkowych.

Metoda spiralna to modyfikacja metody sekwencyjnej polegająca na iteracji wszystkich jej sekwencji i faz. Cechą charakterystyczną jest realizacja kolejno poszczególnych zakresów działania systemów. W tym przypadku cały system podzielony jest na etapy i dla każdego z nich opracowuje się całościowy projekt[4].

Reasumując, należy zwrócić uwagę, że przy każdej prezentowanej metodzie kładzie się nacisk na inną dziedzinę projektowanego ZSBE lub jego składowych.

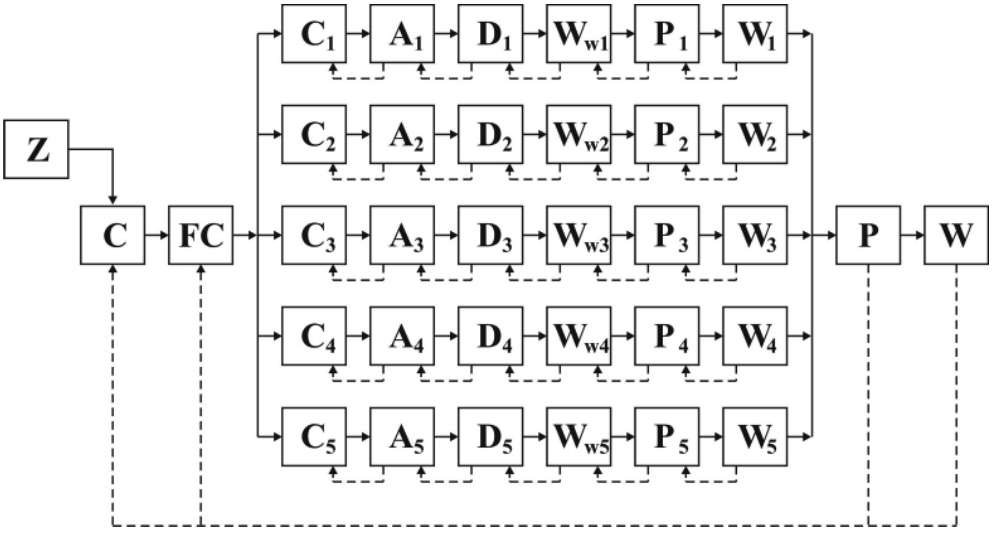
Ze względu na wysoką złożoność i wymagany duży stopień korelacji pomiędzy czynnikami wejściowymi oraz wyjściowymi wpływającymi na bezpieczeństwo energetyczne, w przypadku projektowania ZSBE proponuje się rozdzielenie poszczególnych składowych funkcji celu i opracowanie autonomicznych, dla realizacji tych funkcji, modułów realizujących poszczególne zadania (C_1–C_5) – patrz: rys.1. W celu zwiększenia niezawodności systemu bezpieczeństwa proponuje się z kolei zastosowanie funkcji

[3] L. Kiełtyka, R. Kucęba, *op. cit.*; J. Kisielnicki, H. Sroka, *Systemy informacyjne biznesu*, Warszawa 2005.

[4] J. Kisielnicki, *op. cit.*

MINIMUM zadaniowego (dla elementarnych obiektów ZSBE). Zastosowanie funkcji MINIMUM dla definiowanych elementarnych obiektów umożliwia także indywidualne dopasowanie metod i generatorów optymalizacji bezpieczeństwa energetycznego. W odniesieniu do realizacji głównej funkcji celu bezpieczeństwa energetycznego (punkt 1), proponuje się podejście prognostyczne projektowania z wykorzystaniem metody hybrydowej przyrostowo-sekwencyjnej. Na rysunku 2 przedstawiono etapy tworzenia projektu według proponowanego podejścia metodologicznego projektowania ZSBE.

Rysunek 2. Model zastosowanego podejścia ewolucyjno-kaskadowego projektowania ISZBE



Źródło: opracowanie własne na podstawie: L. Kiełtyka, R. Kucęba, *op. cit.*

Metoda hybrydowa przyrostowo-sekwencyjna umożliwia oddzielną realizację poszczególnych składowych zasadniczej funkcji celu bezpieczeństwa energetycznego poprzez modelowanie i projektowanie poszczególnych autonomicznych obiektów/podsystemów ZSBE. Wszystkie pojedyncze realizowane moduły integrowane są fizycznie i funkcjonalnie. Struktura ZSBE w każdej fazie wzrostu weryfikowana jest w odniesieniu do realizowanych odpowiednich składowych funkcji celu.

Podsumowanie

Prezentowane podejścia metodologiczne, metody i poszczególne fazy analizy oraz projektowania ZSBE potwierdzają, że ich podstawą jest określenie funkcji celu i jej dziedziny (funkcji składowych – procesów, obiektów i ich atrybutów wejściowych oraz wyjściowych, asocjacji pomiędzy obiektami – sygnałów sterujących). Za funkcje celu można przyjąć zasadniczy zakres, jaki obejmuje bezpieczeństwo energetyczne, a mia-

nowicie realizowane procesy w gospodarce umożliwiające pokrycie bieżącego i perspektywicznego zapotrzebowania odbiorców na paliwa oraz różne postacie energii bezpośredniej i finalnej. Przy realizacji tak przyjętej funkcji celu istnieje konieczność opracowania funkcji cząstkowych (składowych funkcji celu) obejmujących zakresem działania takie czynniki wpływające na poprawę bezpieczeństwa energetycznego, jak: ekonomiczne, techniczne, ekologiczne, a zarazem uwzględniając ciągłe zmiany zachodzące w tym obszarze. Dlatego też, mówiąc o bezpieczeństwie energetycznym, należy w procesach analizy i projektowania ZSBE uwzględniać transfer wiedzy, technologii i również transfer polityczny w omawianym zakresie. W szczególności wśród funkcji cząstkowych (składowych funkcji celu) należy uwzględniać realizację zasadniczych procesów energetycznych i społecznych, które wpływają na poprawę bezpieczeństwa energetycznego. Do tej grupy procesów zaliczyć można m.in.: stworzenie mechanizmów ekonomicznych stymulujących modernizację energochłonnych technologii i zmniejszających marnotrawstwo energii; priorytet dla rozwiązań prowadzących do racjonalnego zużycia i produkcji energii oraz zmniejszenie udziału paliw stałych, a zwiększenie udziału gazu, oleju i wszystkich rodzajów energii ze źródeł odnawialnych, dywersyfikacja paliw i źródeł energii; zwiększenie podaży gazu ziemnego ze źródeł własnych i importu, uporządkowanie systemu cen energii; wprowadzenie standardów użytkowania paliw i energii, opłat, podatków, preferencyjnych kredytów, rynku handlu zaoszczędzoną energią, zapewnienie działań społecznych na rzecz poszanowania energii i rozwoju odnawialnych źródeł energii; doprowadzenie do zgodności polityki energetycznej z polityką ekologiczną; wprowadzenie powszechnej edukacji energetyczno-ekologicznej społeczeństwa.

Autorzy referatu w swoich badaniach koncentrują się na procesie dywersyfikacji paliw i źródeł energii z wykorzystaniem generacji rozproszonej i rozsianej. Zaznaczyć należy, że w procesie analizy i projektowania proponują oni prezentowaną metodę hybrydową przyrostowo-sekwencyjną[5].

Bibliografia

Kiełtyka L., Kucęba R., *Design and Analysis of Intelligent System of Electro-energetic Blocks Motion Management*, International Conference on Engineering Optimization, Rio de Janeiro, Brazil, June 1–5, 2008.

Kisielnicki J., Sroka H., *Systemy informacyjne biznesu*, Placet, Warszawa 2005.

Kucęba R., *Chosen Aspects of Electricity Market Structure's Reconversing – Functions and Place of Small Power Industry* [in:] *The Challenges for Reconversion*. *Innovation – Sustainability – Knowledge Management*, ed. P. Pachura, Institut Superieur Industriel Pierrard, HEC du Luxemburg, VIRTON, Belgium 2006.

Kucęba R., *Wartość organizacyjna sieci powiązań informacyjnych elektrowni małych mocy*, VII Międzynarodowa Konferencja Multimedia w Biznesie, Częstochowa 2008.

[5] L. Kiełtyka, R. Kucęba, *op. cit.*; R. Kucęba, *Chosen Aspects of Electricity...*, *op. cit.*; R. Kucęba, *Wartość organizacyjna sieci powiązań informacyjnych elektrowni małych mocy*, VII Międzynarodowa Konferencja Multimedia w Biznesie, Częstochowa 2008.

Kwiatkowski M., *Proces formułowania strategii rozwoju firmy obrotu energią elektryczną*, Oficyna Wydawnicza Szkoły Głównej Handlowej w Warszawie, Warszawa 2006.
Machowicz J., Wieloński A., *Bezpieczeństwo energetyczne Polski*, Wydawnictwo Raabe, Warszawa 2007.
Malko J., Wilczyński A., *Rynki energii – działanie marketingowe*, Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław 2006.

Piotr Migas

Osobowe źródła informacji wewnętrznej w przedsiębiorstwie

Wprowadzenie

Nowoczesne zarządzanie bezpieczeństwem w przedsiębiorstwie wymaga wykorzystania szeregu rozwiązań technicznych i organizacyjnych. Zintegrowany system bezpieczeństwa wewnętrznego oparty jest na pełnym współdziałaniu zastosowanych podsystemów. Coraz większą popularnością w polskich przedsiębiorstwach cieszą się różnego rodzaju rozwiązania techniczne, stosowane w celu pozyskiwania informacji o rzeczywistych nastrojach, zamiarach i działaniach zatrudnionego personelu.

Organizacyjne metody kontroli pracowników pozostają niejako w cieniu. Taki stan rzeczy wydaje się w pełni uzasadniony – o ile szereg kontrowersji natury etycznej i prawnej budzą same rozwiązania techniczne, o tyle metody organizacyjne, oparte na pozyskiwaniu i wykorzystywaniu wewnętrznych informatorów narażają stosujące je przedsiębiorstwo na społeczny ostracyzm.

Spośród metod organizacyjnych kontroli lojalności personelu możemy wyróżnić dwa główne rozwiązania, polegające na wykorzystywaniu źródeł wewnętrznych informacji, posiłkujące się informatorami ulokowanymi w zespołach pracowniczych. Pierwszym z nich jest organizowanie systemów opartych o sprawdzone w krajach zachodnich rozwiązania Crime Stoppers[1]. Polegają one na anonimowej współpracy społeczności ze strukturami odpowiedzialnymi za bezpieczeństwo. Głównym ich założeniem jest anonimowość informatora, dobrowolność współpracy oraz wynagradzanie współpracujących za ujawnienie informacji przydatnych w wykryciu czynu lub sprawców. Drugim rozwiązaniem organizacyjnym jest wykorzystywanie informatorów pozyskiwanych z grona zatrudnionego personelu. Informatorzy współpracujący w ramach prezentowanej metody nie zachowują anonimowości w stosunku do prowadzących program, a ich udział w przedsięwzięciu nie zawsze jest dobrowolny. Wynagradzanie „życzliwych" za dostarczenie przydatnych informacji nie zawsze odbywa się w drodze gratyfikacji finansowej. W zależności od osoby poszczególnego informatora, przyczyn dołączenia do przedsięwzięcia oraz motywów osobistych, gratyfikacja może przybierać formę pochwał i wyróżnień, profitów finansowych, pomocy w rozwiązaniu prywatnych problemów, ułatwienia awansu czy przyznania podwyżki. Może również dotyczyć wymazania z akt pracowniczych nagan lub kar, czy też odstąpienia od wyciągnięcia konsekwencji dyscyplinarnych.

Rozwiązanie oparte na wykorzystaniu informatorów lokowanych w zespołach pracowniczych budzi szereg kontrowersji. Przeciw prezentowanej metodzie wysuwane są zarzuty natury historycznej, społecznej, etycznej oraz prawnej. Celem niniejszego

[1] Więcej szczegółów na temat programu zob. J. Konieczny, *Wprowadzenie do bezpieczeństwa biznesu*, Warszawa 2004, s. 75–79.

opracowania jest wyjaśnienie przytoczonych wątpliwości oraz uchylenie rąbka tajemnicy, jaką obrósł sposób pozyskiwania „życzliwych" informatorów w celu zwiększenia skuteczności wdrożonego systemu bezpieczeństwa wewnętrznego przedsiębiorstwa.

Historia wywiadu

Wykorzystanie tajnych informatorów budzi szereg wątpliwości przede wszystkim natury moralnej. Jest to temat niezwykle drażliwy, najczęściej traktowany jako swoiste tabu. W polskiej rzeczywistości społecznej obraz „kapusia" został wykreowany i utrwalony w latach 1939–1989. Początkowo był to zdrajca i sługus okupanta pomagający mu w eksterminacji ludności, by następnie przeistoczyć się w ogniwo aparatu represji politycznych. Pobudki, jakie kierowały tajnymi współpracownikami, były zróżnicowane – indywidualnie rozumiany patriotyzm, chęć zysku czy poprawy swojej sytuacji zawodowej, społecznej, rządza władzy czy, z drugiej strony, szantaż, przymus, groźby wobec samego informatora czy jego bliskich. Powodów podejmowania współpracy było tyle, ile samych współpracujących.

Powyższe wydarzenia wykreowały w oczach społeczeństwa negatywny obraz informatora, który pokutuje do dnia dzisiejszego. Należy jednak zauważyć, że zagadnienie to nie pojawia się w momencie wybuchu II wojny światowej.

Historia wywiadu i kontrwywiadu zaczyna się z chwilą powstawania pierwszych zorganizowanych struktur społecznych. Już na etapie społeczności plemiennych władcy wykorzystywali szpiegów i donosicieli w celu osiągnięcia przewagi politycznej, militarnej i gospodarczej.

Rozkwit wywiadu wewnętrznego datowany jest na początek monarchii absolutystycznych pojawiających się od początku XVII w. Prekursorem w dziedzinie tworzenia tajnych policji był niezaprzeczalnie kardynał Armand Richelieu[2], I minister Ludwika XIII. Od czasów monarchii absolutnej obserwujemy rozrost teorii „kontrwywiadu" mającego za zadanie zwalczać wrogą aktywność na terenie państwa, jak również tropić i neutralizować jednostki czy grupy rodzimych dysydentów.

Jak już wspomniano, wykorzystywanie tajnych informatorów, mimo że nie jest ono metodą nową, zostało w polskim społeczeństwie nacechowane negatywnie. Dla równowagi należy podkreślić, że w krajach zachodnich współpraca z organami ochrony porządku publicznego jest – w najgorszym wypadku – traktowana jako neutralny obowiązek obywatelski.

Abstrahując od stosunku psychicznego społeczeństwa do omawianego zagadnienia, należy stwierdzić, że stanowi ono jedną ze skuteczniejszych metod pozyskiwania informacji. Skoro instytucje państwowe od zarania dziejów wykorzystują informacje pochodzące od tajnych, osobowych źródeł informacji, to zastosowanie ich w rzeczywistości biznesowej jest jak najbardziej uzasadnione.

[2] http://pl.wikipedia.org/wiki/Armand_Jean_Richelieu (09.08.2008).

Kontrwywiad w biznesie

Jak powszechnie wiadomo, działalność kontrwywiadu oparta jest na tworzeniu i utrzymywaniu siatki informatorów lokowanych w odpowiednich grupach społecznych[3]. Informatorzy mają za zadanie zbierać określone informacje i przekazywać je do centrali, która na ich podstawie podejmuje stosowne działania. Jest to jeden z najstarszych, a zarazem najlepszych sposobów na walkę z zakonspirowanym przeciwnikiem wewnętrznym, jaki dotąd wynaleziono. Należy zauważyć, że pomimo olbrzymiego postępu technologicznego, nadal nic nigdy nie będzie w stanie zastąpić człowieka zbierającego i analizującego informacje w terenie[4].

Za wdrażaniem sprawdzonych wzorców dla ochrony interesów przedsiębiorstwa przemawia kilka argumentów. Pierwszym z nich jest niezaprzeczalny fakt, że ludzie wiedzą znacznie więcej, niż w określonych warunkach mówią. Kolejnym, że ludzie zdradzają więcej sekretów osobom zaufanym (przyjaciołom, kolegom czy innym osobom wzbudzającym zaufanie), niż swoim przełożonym. Oraz, na koniec – każdy ma swoją cenę, jak również – nie ma osób niewinnych. Na podstawie powyższych „zasad" działa każdy państwowy wywiad i kontrwywiad. Jak się okazuje, nie tracą one również aktualności w odniesieniu do przedsiębiorstwa.

Zakres obowiązków kontrwywiadu w przedsiębiorstwie jest bardzo szeroki. Tematem niniejszego opracowania jest jedynie pewien wycinek działalności przywołanej struktury, a mianowicie przeciwdziałanie przestępstwom pracowniczym, w znaczeniu wszelkich umyślnych i nieumyślnych przejawów działalności na szkodę przedsiębiorstwa dokonywanych przez jego personel[5].

Należy ponadto zauważyć, że pomimo swej kontrowersyjności rozwiązanie to nie jest niczym przełomowym. W każdym przedsiębiorstwie – od mikroprzedsiębiorstw po korporacje obejmujące swym zasięgiem całość globu, organizowane są podobne systemy. Różnica tkwi jedynie w celach, jakie się przed nimi stawia, oraz środkach, jakimi się je realizuje. Nie będzie przesadą stwierdzenie, że większość przełożonych wykorzystuje w mniejszym lub większym stopniu informatorów pozyskiwanych z podległych im zespołów pracowniczych w celu pozyskiwania informacji o aktualnych działaniach podwładnych, ich intencjach, celach czy planach.

Ograniczenia prawne

Na samym początku należy wskazać, że pomimo niezaprzeczalnych korzyści, jakie może przynieść stworzenie wewnętrznego systemu pozyskiwania informacji, nie jest to zadanie proste, szczególnie w kontekście przestrzegania obowiązującego porządku prawnego. Kwestia zgodności z prawem podejmowanych działań dotyczy naśladowania instytucji ochrony porządku publicznego. Opisanymi metodami, określanymi

---

[3] Zob. P. Migas, *Kontrola lojalności personelu w organizacji gospodarczej*, red. J. Konieczny, Kraków 2008, s. 186–194.

[4] O trafności przytoczonego stwierdzenia szczególnie boleśnie przekonało się w latach 70. CIA, która popadła w niejako „zachłyśnięcie się" możliwościami współczesnej techniki – jak się okazało, początkowy zachwyt i rezygnacja z agentów terenowych była błędna.

[5] P. Migas, *Kontrola lojalności personelu...*, *op. cit.*, s. 49.

mianem czynności operacyjno-rozpoznawczych, posługują się zarówno policja, jak i służby wywiadowcze czy kontrwywiadowcze. W wypadku tworzenia „prywatnej" siatki informatorów można narazić się na poważną odpowiedzialność karną, choćby pod zarzutem podszywania się pod instytucje państwowe. Nie można też zapominać o ewentualnych zarzutach dotyczących naruszania dóbr osobistych pracowników, zastraszania czy mobbingu, w wypadku ujawnienia tego typu działań. W celu uniknięcia zarzutu bezprawnego kopiowania rozwiązań stosowanych przez uprawnione instytucje ochrony porządku publicznego, „kopiując" rozwiązania organizacyjne, nie należy robić tego dosłownie. Pod żadnym pozorem nie można werbować agentów, przydzielać oficerów prowadzących, budować akt, kartotek, nadawać kryptonimów itd. Zobrazowaniu omawianej sytuacji służy poniższy przykład:

(1) Notatka służbowa oficera prowadzącego: *Agent „Kowal" informuje, że obserwowany sprzedaje informacje przedsiębiorstwa. Rozpocząć inwigilację środkami elektronicznymi, powiadomić odpowiedzialnego dyrektora, wypłacić agentowi nagrodę.*

(2) Notatka kierownika działu: *Informuję kierownika X, że jeden z moich podwładnych poinformował o możliwości kradzieży informacji przez jednego z pracowników. Jeżeli informacja okaże się prawdziwa, wnioskuję o przyznanie panu Y premii.*

W wypadku przeniknięcia na zewnątrz notatki nr 1, odpowiedzialność karna byłaby praktycznie gwarantowana. Wchodziłyby tu w grę zarzuty tworzenia własnej organizacji wywiadowczej, podszywanie się pod służby państwowe, wreszcie o nielegalne zbieranie i przetwarzanie informacji. Biorąc pod uwagę notatkę nr 2, nie można znaleźć w niej nic niezwykłego – zwyczajne pismo kierownika do swojego przełożonego o podejrzeniu zagrożenia bezpieczeństwa tajemnic przedsiębiorstwa. W związku z powyższym, organizując systemy wykorzystywania ukrytych, pracowniczych źródeł informacyjnych w przedsiębiorstwie, nie należy traktować ich dosłownie jako strukturę wywiadowczą.

Organizacja systemu

Znając ograniczenia formalne, można przejść do zagadnień technicznych wykorzystywania omawianej metody w praktyce.

Tak jak w przypadku programów Crime Stoppers, organizacja dodatkowej struktury informacyjnej powinna należeć do pionu bezpieczeństwa i być nadzorowana przez członka najwyższych władz przedsiębiorstwa. Przydzieleni do tego zadania pracownicy winni posiadać doświadczenie w pracy z ukrytymi informatorami, posiadać umiejętność nawiązywania odpowiednich kontaktów, umieć odpowiednio zachęcać do pomocy, jak i chronić swoich „podwładnych".

Profesjonalna realizacja przedsięwzięcia bezapelacyjnie wpływa na jego skuteczność oraz bezpieczeństwo osób w nie zaangażowanych. Niestety, budowa profesjonalnego pionu bezpieczeństwa w oparciu o doświadczoną kadrę jest bardzo kosztowna i zarezerwowana jedynie dla dużych przedsiębiorstw.

W praktyce często spotyka się systemy pozyskiwania informacji wewnętrznych powstające samoczynnie, najczęściej z inspiracji kierownictwa średniego szczebla. Problemem obok braku elementarnej wiedzy dotyczącej kierowania tego typu przed-

sięwzięciami są również nie zawsze czyste intencje samych organizatorów. Doświadczenie wskazuje, że informacje pozyskiwane z „prywatnych" systemów budowanych przez niektórych przełożonych wykorzystywane są głównie do wspierania partykularnych interesów samego realizatora.

Bez wątpienia, utworzona struktura musi mieć charakter tajny. O przedsięwzięciu i zaangażowanych w niego pracownikach powinny wiedzieć jedynie osoby odpowiedzialne za pracę „życzliwych". Nawet najmniejszy przeciek czy choćby podejrzenie istnienia takiego „tworu" może skutecznie zniweczyć wszelkie podjęte działania, a zaangażowane w projekt jednostki pogrążyć społecznie i zawodowo. Należy także zauważyć, że tożsamość „życzliwych" podwładnych biorących udział w przedsięwzięciu musi być również chroniona w wymiarze wewnętrznym, tzn. pomiędzy samymi uczestnikami. Innymi słowy, informatorzy nie mogą znać tożsamości ani nawet lokacji hierarchicznej innych osób współpracujących w ramach programu. Każdy z informatorów powinien znać tylko i wyłącznie tożsamość swojego bezpośredniego przełożonego, czyli osoby, z którą ma się kontaktować.

W celu realizacji omawianego projektu, oprócz wydzielenia zespołu mającego za zadanie znalezienie i nakłonienie do współpracy[6] odpowiednich członków personelu przedsiębiorstwa, potrzebni są sami „życzliwi". Pracownicy nadający się do wzięcia udziału w prezentowanym „programie" mogą zostać podzieleni na cztery grupy[7], charakteryzujące się własnymi motywami współpracy, oczekiwaniami, jak również zróżnicowanym poziomem jakości dostarczanych informacji.

Charakterystyka osobowych źródeł informacji

Ukrytych informatorów można wstępnie podzielić według kryterium stałości współpracy z prowadzącymi projekt[8]. W ramach tego podziału wyróżnia się informatorów stałych, czasowych oraz podejmujących współpracę tylko w celu wyjaśnienia konkretnej sprawy. Kolejnym kryterium będzie umiejscowienie „życzliwego" współpracownika w strukturze firmy. W związku z tym wyróżnia się informatorów ulokowanych bezpośrednio w zespołach pracowniczych, w strukturach kierownictwa lub wśród personelu pomocniczego (w cateringu, ochronie, serwisie sprzątającym, serwisie technicznym czy obsłudze sekretariatu). Powyższy podział nie jest oczywiście wyczerpujący. Współpracowników bowiem można także dzielić według wykonywanych zadań, specjalizacji oraz pobudek, z jakich podejmują współpracę w ramach programu. Warto przyjrzeć się nieco dokładniej ostatniemu z podanych podziałów.

Pierwszą, najbardziej pożądaną, a zarazem najmniej liczną grupę „życzliwych" będą stanowili pracownicy cechujący się daleko idącą lojalnością wobec firmy i działający dla jej dobra. W ich przypadku zachęta do pomocy komórce bezpieczeństwa jest praktycznie zbędna. Jeżeli tylko będą wiedzieli, do kogo mogą zwrócić się ze swoimi spostrzeżeniami, oraz będą mieli gwarancję, że informacja o odbytej rozmowie nie

---

[6] J. Konieczny [w:] *Kryminalistyka*, red. J. Widacki, Warszawa 2008, s. 129.

[7] P. Migas, E. Koszel, P. Fiszer, S. Piekoszewski, *Etyczne granice kontroli lojalności personelu* (praca w druku), Kraków 2007.

[8] *Kryminalistyka*, *op. cit.*, s. 139–140.

ujrzy światła dziennego, wtedy będziemy mogli powiedzieć, że pozyskaliśmy dobre osobowe źródło informacyjne. Pracownicy cechujący się wysoką lojalnością mogą być porównywani z ideowcami. Informując przełożonych o wykrytych (czy zasłyszanych) nieprawidłowościach, nie oczekują nagrody – uważają, że dobro firmy przekładające się na dobro ich samych będzie wystarczającą nagrodą. W odniesieniu do dostarczanych informacji wydaje się, że powinny one być „najczystsze", tzn. pozbawione cech rozgrywek prywatnych, chęci zemsty czy zaszkodzenia drugiej osobie. Jednak, pomimo względnie dobrej jakości dostarczanych przez omawianą grupę informacji, należy podchodzić do nich z daleko idącą rezerwą. J. Widacki zauważa, że instytucje państwowe podchodzą do „ideowców" z dużą ostrożnością z uwagi na ograniczoną możliwość kontroli informatora[9]. Jest to postulat jak najbardziej słuszny, który szerzej omówiony zostanie w dalszej części opracowania.

Drugą grupę współpracowników, którzy mogą przystąpić do „programu", stanowią pracownicy cechujący się w szczególności takimi cechami negatywnymi jak: złośliwość, zawiść czy żal do całego świata. Omawiana grupa będzie bardzo chętnie dostarczała negatywnych informacji o swoich kolegach i szefach celem np. zrobienia im na złość, wyrządzenia przykrości, zaszkodzenia w karierze zawodowej. W tym wypadku pozyskanie do współpracy może polegać na zachęceniu do zwierzeń, obietnicy pomocy w realizacji „chorych ambicji" czy marzeń źródła informacji. O ile omawiany rodzaj współpracowników jest stosunkowo „tani w utrzymaniu", o tyle informacje przez nich dostarczane mogą mieć różną wartość użytkową. Przy ocenie dostarczanych w tym przypadku materiałów należy mieć na uwadze motywy, jakie kierowały danym informatorem. Jeżeli motywy już same z siebie budzą niejako „obrzydzenie", to można się spodziewać, że ukryte fakty zostały w odpowiedni sposób obudowane „stekiem bzdur" mającym podnieść dramatyzm informacji.

Kolejna grupa potencjalnych, przychylnych programowi pracowników jest bardzo podobna do wyżej omówionej. Mogą się do niej zaliczać tzw. „złośliwcy", jak i zwykli ludzie jednakże nastawieni na osiągnięcie określonych korzyści majątkowych obok ewentualnej satysfakcji z cudzego nieszczęścia. Nakłonienie ich do pomocy formacji ochrony bezpieczeństwa będzie się głównie sprowadzać do przyznawania różnych gratyfikacji finansowych i materialnych, premii, podwyżek, niekiedy przyśpieszania awansów. Na podstawie powyższego można stwierdzić, że prezentowana grupa „kandydatów" posiada jedną cechę zbieżną z kategorią „ideowców" – ich „służba" będzie cechowała się daleko idącą skutecznością i oddaniem. U podstaw tego założenia leży czysta umowa handlowa: informacja za pieniądze. Im wyższy poziom użyteczności i rzetelności danej informacji, tym większa gratyfikacja. Biorąc pod uwagę fakt, że omawiani informatorzy w większości cechować się będą pazernością, można powiedzieć, że ich aktywność będzie dość duża.

Owa aktywność wiąże się jednak z pewnym niebezpieczeństwem. Po pierwsze, współpracownicy starający się pozyskać jak najwięcej cennych informacji mogą w pewnym momencie przekroczyć dopuszczalne granice, narażając się na tzw. „wpadkę". Po drugie, co kreatywniejsi mogą próbować „sprzedawać" kierownictwu informacje spreparowane, licząc na to, że niewielkim wysiłkiem szybko zdobędą pożądaną nagrodę. W celu niwelacji obu zagrożeń konieczne jest więc, aby kierowaniem

[9] J. Widacki, *Kryminalistyka*, wyd. 2, Warszawa 2002, s. 140.

prezentowanym „programem" zajęli się doświadczeni profesjonaliści, którzy będą w stanie w porę wykryć niebezpieczeństwo i mu przeciwdziałać. Warto podkreślić jeszcze jedną, bardzo ważną cechę omawianej grupy „kandydatów". Z uwagi na to, że wszyscy uwzględniani współpracownicy działają z pobudek ekonomicznych, kontrola nad nimi powinna być stosunkowo prosta – ludzie szybko przyzwyczajają się do wyższego wynagrodzenia, zgodnie z którym planują swoje wydatki. Ograniczenie dodatkowych pieniędzy będzie dla wielu z nich bardzo dotkliwe, a zarazem będzie działało jako dodatkowy bodziec z jednej strony motywujący do działania, a z drugiej jako swoisty ogranicznik przed wystąpieniem z „programu".

Ostatnią grupę będą stanowili pracownicy posiadający nieczyste sumienie. W szczególności chodzi tu o osoby, które zostały przyłapane na drobniejszych czynach niedozwolonych lub w sytuacjach kompromitujących ich w oczach kolegów czy przełożonych. Pozyskanie do współpracy tej kategorii pracowników polega na zwykłym szantażu – informacja za milczenie, pracę, ewentualnie – wynagrodzenie.

Dane o „chińskich ochotnikach" typowanych na informatorów można czerpać z prowadzonych postępowań lub odczytów systemów elektronicznych. Natomiast problematyczne jest nakłonienie ich do samej współpracy. To, czy określony pracownik „zechce" dołączyć do „programu", będzie zależało od indywidualnego poczucia zawinienia określonego czynu stanowiącego podstawę oferty oraz stopnia przywiązania do pracy. Może zdarzyć się tak, że w odczuciu samego podmiotu waga czynu oraz przywiązanie do aktualnej pracy będzie tak niskie, że odmówi współpracy, a ponadto niejako „na odchodne" ujawni próbę nakłonienia do współpracy jako zamach na wolność i dobra osobiste. Takie działanie może zagrozić całemu „programowi" oraz osobom w niego zaangażowanym od strony personelu przedsiębiorstwa. Skuteczność działania zwierzchników zależy tu przede wszystkim od dokonania właściwej analizy sytuacji i dostosowania oferty kierowanej do potencjalnego źródła informacji.

Opisana metoda pozyskiwania do współpracy budzi wiele wątpliwości natury etycznej. Dodatkowo sprawę komplikuje fakt, że za podstawę „oferty" współpracy mogą w niesprzyjających okolicznościach posłużyć informacje, jakich w żadnym wypadku nie należy gromadzić, a tym bardziej wykorzystywać. Mowa tu w szczególności o informacjach wymienionych w art. 11^3 k.p[10], stanowiących podstawę dyskryminacji. W związku z powyższym, należy jasno powiedzieć, że podstawą „oferty" współpracy mogą stać się tylko i wyłącznie informacje dotyczące realizacji obowiązków pracowniczych pozyskane w drodze kontroli czy prowadzonych postępowań. W żadnym wypadku nie wolno wykorzystywać informacji o charakterze dyskryminującym, jak również informacji niezwiązanych z działalnością zawodową pracownika. Pozostaje jeszcze kwestia wagi czynu, która może lec u podstaw „oferty". Należy przyjąć, że taką podstawą mogą być tylko czyny lekkiej oraz średniej wagi, przy czym korzyści z pozyskania pracownika obciążonego takimi czynami muszą być większe od strat spowodowanych przez ten czyn. Do obowiązków prowadzących „program" należy analiza omawianej podstawy oraz decyzja – pozyskiwać czy usunąć potencjalnego kandydata w drodze postępowania lojalnościowego.

Należy zastanowić się również nad zagadnieniem typowania współpracowników dla omawianego przedsięwzięcia na etapie naboru personelu. Część potrzebnych in-

[10] Ustawa z dnia 26 czerwca 1974 r. Kodeks Pracy (tekst jednolity Dz.U. z 1998 r., Nr 21, poz. 94 z późn. zm.).

formacji można pozyskać już w fazie rekrutacji. Chodzi tu w szczególności o stwierdzanie występowania u kandydata określonych cech charakteru czy poglądów na niektóre sprawy związane z życiem zawodowym. Niektórzy „specjaliści" od naboru personelu przestrzegają przed zatrudnianiem osób nastawionych tylko i wyłącznie na zysk. Jest to pogląd w mniemaniu autora błędny. Niezaprzeczalny jest fakt, że ludzie podejmują pracę zarobkową nie dla idei tylko dla odpowiedniej gratyfikacji finansowej. Jeżeli dany kandydat wykazuje daleko idące zainteresowanie kwestiami finansowymi, może to być dobry znak dla osób prowadzących program pozyskiwania informacji wewnętrznej – z biegiem czasu, zwerbowanie takiej osoby poprzez dodatkowe profity może być stosunkowo łatwe. Podobnie będzie w przypadku wykrycia u danego kandydata cech, które będą świadczyć o łatwości „przekształcenia" go w pracownika cechującego się dużym oddaniem firmie. Opieka połączona z odpowiednim szkoleniem pozwoli pozyskać go dla programu w odpowiednim momencie. Prezentowane metody nie powinny być stosowane w odniesieniu do grupy drugiej („złośliwców") oraz czwartej („czarnych charakterów"). W wypadku wykrycia takich osób na etapie postępowania rekrutacyjnego, powinni oni zostać bezwzględnie odrzuceni dla dobra przedsiębiorstwa. Lepiej nie pozyskać w przyszłości informatora, niż wprowadzać chaos w firmie.

Warto jeszcze zauważyć, że w ramach omówionej grupy trzeciej (pracownicy nastawieni na dodatkowy zysk) oraz pierwszej („ideowcy") można pozyskiwać współpracowników „technicznych" dla pionu bezpieczeństwa. Chodzi tutaj przede wszystkim o administratorów, techników oraz inne osoby pomocne w realizacji odpowiednich przedsięwzięć. Oprócz pozyskiwanych współpracowników, pion bezpieczeństwa w celach redukcji zatrudnienia bezpośredniego, a zarazem redukcji kosztów może prowadzić tzw. podwójne zatrudnienie w ramach firmy – poszczególni, wytypowani fachowcy świadczą pracę w innych działach firmy, a w razie potrzeby jako tajni, etatowi pracownicy pionu bezpieczeństwa wykonują odpowiednie zadania zlecone.

System w działaniu

Jak już wspomniano, systemy wewnętrznego pozyskiwania informacji można podzielić na profesjonalne i amatorskie.

Systemy profesjonalne tworzone są w drodze przemyślanej i w pełni świadomej decyzji najwyższych władz przedsiębiorstwa, angażują personel o odpowiednich kwalifikacjach i doświadczeniu, natomiast celem ich powstania jest ochrona przedsiębiorstwa przed zagrożeniami wewnętrznymi i zewnętrznymi.

Systemy amatorskie budowane są najczęściej z prywatnej inicjatywy kierownictwa różnych szczebli i prowadzane przez osoby o niewielkiej wiedzy praktycznej, ich celem z kolei jest najczęściej pozyskiwanie informacji przydatnych samemu prowadzącemu.

Omawiane systemy mają również miejsce w małych i średnich przedsiębiorstwach, których organizatorami są najczęściej właściciele lub inne osoby zajmujące stanowiska szczebla kierowniczego. W tym przypadku cel realizacji przedsięwzięcia jest taki sam jak systemów profesjonalnych, jednakże ich wykonanie i zarządzanie nosi cechy systemu amatorskiego.

Podstawową różnicą pomiędzy wyżej wymienionymi formami organizacyjnymi jest ich skuteczność oraz bezpieczeństwo osób zaangażowanych. Nie oznacza to, że systemy amatorskie lub półprofesjonalne z góry skazane są na niepowodzenie. Paradoksalnie, systemy profesjonalne stanowią zdecydowaną mniejszość, podczas gdy pozostałe królują w większości podmiotów gospodarczych. Systemy profesjonalne, z uwagi na siły i środki w nich angażowane cechują się oczywiście większą skutecznością, jednakże nawet im mogą przytrafić się spektakularne klęski.

Działanie każdego systemu, niezależnie od jego stopnia profesjonalizmu jest takie same. „Życzliwy" pracownik przekazuje zdobyte (zaobserwowane, zasłyszane) informacje osobie kontaktowej. Przełożony ma za zadanie zebrać informacje od swoich „podwładnych" i, w zależności od organizacji, przekazać je dalej lub samemu zweryfikować, pozostawiając jedynie materiał wartościowy. Informator za przekazanie użytecznego materiału powinien zostać wynagrodzony, zgodnie z przyjętymi wcześniej ustaleniami.

Użyteczność pozyskiwanych informacji jest problematyczna. Z uwagi na swoje źródło pochodzenia oraz formę, jaką przybierają, ich walor dowodowy jest niestety bardzo niski. W przypadku wykrycia nieprawidłowości lub czynu wymierzonego w przedsiębiorstwo, użycie informacji pochodzącej bezpośrednio z omawianego systemu jest praktycznie niemożliwe. Co prawda można by posłużyć się w trakcie ewentualnego postępowania dowodem z zeznań świadka, którym byłby przychylny programowi pracownik dostarczający określonych informacji, jednakże tego rodzaju wykorzystanie osobowego źródła informacji mogłoby zaważyć na dalszym istnieniu systemu.

W związku z powyższym, można przyjąć, że informacje pozyskiwane w ramach omawianego systemu są analogonem wiedzy operacyjnej[11], która, co prawda nie posiada waloru dowodowego, jednak nadaje kierunek prowadzonemu postępowaniu oraz wskazuje źródła dowodowe w znaczeniu procesowym.

Wykorzystanie pozyskanych informacji

Systemy pozyskiwania informacji wewnętrznej dostarczają jedynie nieoficjalnych informacji o zdarzeniach, osobach i faktach z nimi związanych. W związku z powyższym, sam system pozyskiwania informacji wewnętrznych powinien pełnić rolę wsparcia organizacyjnego dla jawnych lub półjawnych systemów kontroli pracy oraz wykrywania nieprawidłowości.

Informacje pozyskiwane w drodze korzystania z usług wewnętrznych informatorów powinny być wykorzystywane jako swoisty system wczesnego ostrzegania o nadchodzących lub zaistniałych wydarzeniach. Dzięki pozyskanym danym osoby nadzorujące program są w stanie uruchomić pozostałe systemy, mające za zadanie pozyskać pełnowartościowy materiał dowodowy w określonej sprawie. Pozyskane informacje są szczególnie istotne, gdy w przedsiębiorstwie działa zintegrowany system kontroli pracy, wykorzystujący szerokie spektrum środków technicznych. Jak wiadomo, systemy techniczne zbierające informacje prewencyjnie dostarczają olbrzymich ilości

[11] Zob. J. Widacki, *Kryminalistyka*, *op. cit.*, s. 142–143.

nieistotnych danych. Analiza tzw. szumu informacyjnego jest długotrwała, żmudna i nie zawsze przynosi spodziewane rezultaty. Wykorzystanie odpowiednio opracowanych danych, pochodzących z systemu pozyskiwania informacji wewnętrznych umożliwia skupienie uwagi operatorów środków technicznych na precyzyjnie oznaczonych osobach lub grupach. Znając potencjalne zagrożenie, łatwiej jest dobrać odpowiednie środki oraz skupić uwagę na określonych zachowaniach typowanych sprawców (przyszłych lub obecnych). Innymi słowy, wdrożenie i wykorzystywanie omawianego rozwiązania podnosi skuteczność wszystkich implementowanych systemów prewencyjnych i dochodzeniowych.

Warto wspomnieć, że system pozyskiwania informacji wewnętrznych może być również wykorzystywany w celach „pokojowych". Mianowicie, może być stosowany do diagnostyki nastrojów pracowników, ich oczekiwań oraz przyszłych zamiarów zawodowych. Innymi słowy, system ten może być wykorzystywany do standardowych działań kadrowych, jako narzędzie wczesnego ostrzegania choćby o planach zmiany miejsca zatrudnienia. Każdy pracodawca ma świadomość tego, że w określonych okolicznościach i w odniesieniu do odpowiedniej grupy pracowników informacja o planowanym odejściu na własne życzenie może okazać się bezcenna. Pomimo funkcjonowania instytucji rozwiązania umowy o pracę z zachowaniem okresu wypowiedzenia, ustawowe czy umowne terminy mogą okazać się zbyt krótkie na znalezienie kompetentnego następcy. W związku z powyższym, powzięcie informacji o dalszych planach zawodowych danego pracownika może ułatwić zachowanie ciągłości pracy na określonym stanowisku.

Zastosowań pozyskiwanych informacji może być znacznie więcej. W każdym wypadku należy jednak pamiętać o ustawowych zakazach i ograniczeniach w odniesieniu do zakresu pozyskiwanych informacji.

Należy też zwrócić uwagę na wykorzystywanie poszczególnych „życzliwych" pracowników do pozyskiwania odpowiedniego rodzaju informacji. Z teorii organizacji wywiadu gospodarczego[12] wynika, że działa on skutecznie jedynie wówczas, gdy wyznaczane są mu precyzyjnie określone zadania. Planując pracę informatorów, należy więc zawsze mieć powyższą zasadę na uwadze. Zlecając określonemu uczestnikowi programu tylko obserwację jego otoczenia bez wskazania konkretnych zdarzeń lub osób, na które powinien zwracać uwagę, istnieje prawdopodobieństwo otrzymania albo „szumu informacyjnego" albo braku jakichkolwiek informacji, gdy obserwator dojdzie do wniosku, że, w jego opinii, nie zachodzi żadne istotne zdarzenie. Z kolei informatorzy z precyzyjnie określonymi zadaniami mogą przez dłuższy czas zachowywać milczenie, w oczekiwaniu na odpowiednie wydarzenia.

Kolejną zasadą dotyczącą wyznaczania zadań dla osób zaangażowanych w program jest pozyskiwanie przez nich informacji z tzw. „naturalnego otoczenia"[13]. Innymi słowy, zlecając danemu pracownikowi zdobycie informacji, do których nie ma on fizycznie dostępu, a próba uzyskania dostępu mogłaby ściągnąć na niego czyjąś, „niezdrową" ciekawość, naraża się jego osobę, wyznaczone zadanie oraz cały system.

[12] J. Konieczny, *Wprowadzenie...*, *op. cit.*, s. 159–161.

[13] *Ibidem*, s. 163–164.

Pozyskiwanie informacji – zagrożenia

Powyżej omówiony został jeden z możliwych podziałów „sympatyków" wdrażanego programu ze względu na motywy podejmowania współpracy. Należy zauważyć, że każdy rodzaj informatorów może dostarczać informacji prawdziwych, jak również wprowadzać dezinformację. Przekazywanie informacji fałszywych może być powodowane szeregiem czynników, zależnych lub niezależnych od samego informatora.

Czynnikami niezależnymi od zaangażowanych „życzliwych" mogą być samoistne zniekształcenia pozyskiwanych informacji w toku ich gromadzenia oraz świadome wprowadzenie go w błąd przez osoby trzecie. Jak wiadomo, informator (nawet organów państwowych) jest tylko człowiekiem z pełnymi tego konsekwencjami. W związku z powyższym mogą zaistnieć przesłyszenia, zniekształcenia odebranego przekazu, niewłaściwe zrozumienie słów czy intencji, jak również upływ czasu, warunki obserwacji, stan emocjonalny czy fizyczny[14]. Nie należy zapominać, że żadna ze współpracujących w ramach systemu osób nie jest odpowiednio wyszkolonym agentem wywiadu, a jedynie zwykłym człowiekiem, który z takiego czy innego powodu wziął udział w tym przedsięwzięciu. Jeżeli natomiast w toku weryfikowania pozyskanych informacji nastanie podejrzenie, że dany uczestnik programu został świadomie wprowadzony w błąd przez swojego rozmówcę, to może oznaczać, że w najlepszym przypadku systemowe źródło informacyjne zostało zdemaskowane. Analizując kolejne informacje napływające od potencjalnie zdemaskowanego, należy zachować szczególną ostrożność oraz w miarę możliwości poddawać je dodatkowej weryfikacji. W przypadku gdy omawiany informator zacznie ustawicznie dostarczać informacji sfałszowanych, a okoliczności towarzyszące wykażą brak jego winy, należy jak najszybciej wyłączyć go z programu, zawieszając jego działalność.

O ile zniekształcenia dostarczanych informacji spowodowane czynnikami niezależnymi od danego informatora mogą, ale nie muszą oznaczać wystąpienia problemów organizacyjnych, o tyle występowanie czynników zależnych należy traktować z najwyższą powagą. Jak już wspomniano, celowe zniekształcenia lub wręcz fabrykowanie informacji może wynikać z chęci szybkiego osiągnięcia określonych korzyści, próby zniechęcenia przełożonych przekładającego się na wykluczenie danego informatora z programu lub nawet całkowitej zmiany frontu.

Specyfiki działania kierowanego chęcią zysku nie trzeba tłumaczyć. Nawet w świecie prawdziwego wywiadu zdarzało się, że „asy" dostarczały wytworzone przez siebie, rewelacyjne informacje cechujące się całkowitym brakiem pokrycia z rzeczywistością. Motyw był tylko jeden – wyłudzić jak największą gratyfikację przy jak najmniejszym narażaniu własnej osoby. Konsekwencje operowania na tak spreparowanych danych zwykle były opłakane dla samego nabywcy, natomiast wykrycie takiego procederu – opłakane dla jego twórcy. Niestety, prowadząc program pozyskiwania informacji wewnętrznych, nie można pozwolić sobie na podobne zakończenie współpracy, a konsekwencje wykorzystywania informacji przekoloryzowanych lub zupełnie fałszywych mogą doprowadzić do zamknięcia programu – razem z przedsiębiorstwem.

Kolejną przyczyną fabrykowania informacji może być próba maskowania własnej, nielegalnej działalności w celu zmylenia ewentualnego postępowania wyjaśniającego. Informator, prowadząc niejako podwójną grę, może swobodnie manipulować

[14] Zob. *Kryminalistyka*, *op. cit.*, s. 101.

określonymi informacjami zwłaszcza, gdy jego współpraca była dotychczas oceniana wysoko.

Niska jakość przekazywanych informacji, oceniana pod kątem ich wiarygodności może wynikać z chęci zakończenia współpracy w ramach omawianego przedsięwzięcia. Taka sytuacja może mieć miejsce wtedy, gdy uczestnik został włączony do programu niekoniecznie z własnej woli lub, gdy, co prawda przyłączył się dobrowolnie, ale osiągnąwszy swój cel, postanawia zaprzestać ryzykownych działań. Innym powodem może być również wewnętrzne wypalenie danego uczestnika, a zarazem strach przed zakomunikowaniem swojej decyzji przełożonemu. Stopniowy lub nagły spadek jakości dostarczanych informacji w szczególności, gdy następuje to po okresie owocnej współpracy, należy potraktować jako ważny sygnał do podjęcia działań weryfikujących dalszą przydatność danego źródła. Powyższa uwaga nie dotyczy sytuacji, gdy dany informator zakończył określone zadanie, a nowego jeszcze nie otrzymał.

Najgroźniejszy przypadek fabrykowania informacji występuje wówczas, gdy określony uczestnik przedsięwzięcia zmienia swój stosunek psychiczny do przełożonych, swojego otoczenia zawodowego, wykonywanej pracy, a w rezultacie – do całego przedsiębiorstwa. Lojalność pracownicza nie jest niestety zjawiskiem stałym. W zależności od występujących czynników, stosunek psychiczny pracownika do przedsiębiorstwa może ulegać stopniowym, acz ukierunkowanym zmianom[15]. Alteracja owego nastawienia występująca u uczestnika programu, szczególnie gdy wcześniej uważany był za osobę lojalną i godną zaufania, może doprowadzić do zachwiania całego systemu. Powodem takiego obrotu sprawy jest najczęściej osłabienie czujności przełożonych oraz zbyt głęboka wiara w uczciwość i rzetelność zaangażowanego w program, lojalnego pracownika. Omawiane zjawisko przybiera najgroźniejszą formę, gdy dawny pracownik postanawia wykorzystać cały kredyt zaufania, jakim został obdarzony do osiągnięcia własnych, niekoniecznie szczytnych celów. Przytoczona działalność uczestnika programu będzie tu prowadzona pod „przykrywką" solidnej i lojalnej współpracy, podczas gdy dostarczane informacje o osobach i wydarzeniach będą dostosowywane do aktualnych potrzeb ich autora. Analizując przypadki wyżej omówionej działalności, należy zauważyć, że cele „zdrajców" bywają mocno zróżnicowane. O ile większość z nich można nazwać pragmatycznymi (zemsta, zysk), to niektóre bywają nader irracjonalne (wywołanie wewnętrznego chaosu, próby przejęcia kontroli nad przedsiębiorstwem).

Abstrahując od celów i motywów omawianej grupy przypadków, należy zauważyć, że wystąpienie przytoczonego zjawiska jest bardzo niebezpieczne zarówno dla programu, jak i całego przedsiębiorstwa. Niewykrycie celowej dezinformacji, a nawet poddanie się manipulacji przez informatora może w łatwy sposób unicestwić całe przedsięwzięcie, pogrążyć prowadzących, a w rezultacie doprowadzić do poważnego uszkodzenia lub zniszczenia systemu bezpieczeństwa wewnętrznego.

W ramach wyżej wymienionego przykładu celowego zniekształcania dostarczanych informacji może się również zawierać umyślna działalność wywiadowcza, inspirowana przez podmioty konkurencyjne. Przypadek ten jest o tyle skomplikowany, że podejrzany uczestnik programu mógł przejść na stronę konkurencji w trakcie trwania zatrudnienia w danym przedsiębiorstwie lub mógł zostać w nim ulokowany z precyzyjnie określonymi zadaniami. Niezależnie od genezy współpracy z konkurencją,

[15] P. Migas, *Kontrola lojalności personelu...*, *op. cit.*, s. 46.

szkody wyrządzone przez „podwójnego agenta" będą olbrzymie i podwójnie dotkliwe. Może się okazać, że „zdrajca" nie dość, że wykonał swoje zadanie (pozyskał odpowiednie informacje lub osoby), to dodatkowo zinfiltrował program, a tym samym większą część systemu bezpieczeństwa wewnętrznego.

Na koniec rozważań o zagrożeniach, jakie niesie pozyskiwanie informacji z wykorzystaniem ukrytych wśród pracowników informatorów należy przeanalizować przypadek demaskacji programu, a zarazem przedostania się informacji o nim do osób trzecich.

Z ujawnieniem informacji o istnieniu systemu możemy mieć do czynienia w przypadku nieudanej próby naboru uczestnika programu. Nieumiejętnie przeprowadzona rozmowa wstępna, złe zaklasyfikowanie kandydata, nieadekwatność wynagrodzenia do rzeczywistych celów przyszłego współpracownika może zaowocować jego odmową, a ponadto ujawnieniem próby angażu. Przedostanie się informacji o próbie budowania struktury informacyjnej do wiadomości społeczności firmowej może skutkować diametralną zmianą nastrojów pracowników. Swój stosunek do przełożonych mogą zmienić osoby nieuczestniczące w programie (gdyż się ich szpieguje i nakłania do donosicielstwa na kolegów i koleżanki) oraz już pozyskani „sympatycy" (skoro ujawniono informacje o istnieniu programu, to tylko kwestią czasu może być ujawnienie tożsamości jego uczestników).

Kolejnym przypadkiem demaskacji programu jest celowe ujawnienie informacji o jego istnieniu poprzez byłego informatora lub osoby nadzorującej jego działanie, która odeszła z firmy, szczególnie w ramach wyciągniętych wobec niej konsekwencji dyscyplinarnych. Przedostanie się do opinii publicznej informacji, że w danym przedsiębiorstwie stosuje się omawiane praktyki, nie dość, że wpłynie negatywnie na całość jego struktur wewnętrznych, to dodatkowo może zrujnować jego wizerunek w oczach klientów, kontrahentów czy przyszłych kandydatów na pracowników. Nie należy również zapominać o ewentualnych konsekwencjach prawnych, które już wcześniej sygnalizowano.

Celowa lub nieumyślna dezinformacja, ujawnienie danych o istnieniu systemu wewnątrz lub na zewnątrz przedsiębiorstwa, jak również infiltracja programu przez podmioty trzecie jest poważnym zagrożeniem dla istniejącego systemu bezpieczeństwa. Niektóre z omówionych przykładów, obok paraliżu struktur wewnętrznych oddziałują wprost na główną działalność całego przedsiębiorstwa. Konstruując system pozyskiwania informacji wewnętrznej, należy koniecznie uwzględnić powyższe przestrogi. Na każdym etapie działalności trzeba również analizować fakty oraz w miarę możliwości zabezpieczać się przed ewentualnymi konsekwencjami popełnionych błędów. Bagatelizowanie potencjalnych zagrożeń jest niewybaczalne, w szczególności gdy kierujący programem pretenduje do miana profesjonalisty.

Przykład z praktyki

Dla lepszego zobrazowania poruszanych zagadnień warto opisać wydarzenia, jakie miały miejsce w jednym z mikroprzedsiębiorstw branży usług paramedycznych. Prezentowana firma nie należy co prawda do grona potentatów w branży, nie zatrudnia setek pracowników, jednakże, posiadając dobrą reputację wśród swoich klientów,

dąży do utrzymywania wysokiego standardu ich obsługi. Jak każde małe przedsiębiorstwo, także i to jest wysoce wrażliwe na fluktuacje zatrudnienia, szczególnie że pozyskanie odpowiednio wykwalifikowanych pracowników jest niezmiernie trudne.

W związku z pojawiającymi się problemami z zatrudnionym personelem, wdrożone zostały techniczne środki kontroli pracy w formie monitoringu wizyjnego i dźwiękowego. Oba systemy legły u podstaw budowy zintegrowanego systemu bezpieczeństwa wewnętrznego. Efekty pracy systemów zostały zarejestrowane już w pierwszym miesiącu ich funkcjonowania. Na podstawie odczytów z kamer i mikrofonów wykryto działania na szkodę przedsiębiorstwa, przybierające postać działalności konkurencyjnej poza godzinami pracy firmy, połączonej z niszczeniem wizerunku przedsiębiorstwa i „wyprowadzaniem" klientów. Zgromadzony materiał dowodowy został wykorzystany podczas przeprowadzonego postępowania wyjaśniającego, czego efektem było usunięcie winnych nadużyć w trybie dyscyplinarnym.

W późniejszym czasie kierownictwo omawianego przedsiębiorstwa powzięło decyzję o utworzeniu systemu pozyskiwania informacji wewnętrznych w oparciu o informatorów ulokowanych pośród pracowników. W krótkim czasie pozyskano do współpracy kilka osób cechujących się wysoką (jak mniemano) lojalnością wobec firmy. System zaczął dość szybko przynosić imponujące rezultaty, dzięki czemu wykryto kilka pomniejszych aktów nadużyć pracowniczych, działalności konkurencyjnej oraz czynów wymierzonych w wizerunek przedsiębiorstwa.

Pozytywne rezultaty, jakie zaczął przynosić wdrożony system informacji wewnętrznej, odbił się niestety negatywnie na pozostałych podsystemach. W wyniku „zachłyśnięcia" się przez kierownictwo odniesionym sukcesem, systemy monitoringu zostały zaniedbane, co doprowadziło do ich stopniowej demaskacji, a w rezultacie do wycofania z użytku. Należy również podkreślić, że kierownictwo opierało się głównie na informacjach dostarczanych przez najlepszego, jak mniemano, informatora, którego w dodatku poczytywano za osobę najbardziej oddaną przedsiębiorstwu. Właśnie owo podejście do osoby wskazanego informatora legło u podstaw następnych wydarzeń, które o mało nie doprowadziły do całkowitej porażki wdrożonych rozwiązań z zakresu bezpieczeństwa wewnętrznego.

Wyżej wspomniany informator popadł w bezgraniczny samozachwyt, na co wpływ miał m.in. stosunek kierownictwa do jego osoby. Odkrył, że manipulując dostarczanymi informacjami, może dowolnie kształtować decyzje kierownictwa. Pozostając samemu poza wszelkimi podejrzeniami, rozpoczął działalność konkurencyjną oraz powziął przygotowania do przejęcia głównych klientów firmy. Kolejnym punktem jego planu było pozyskanie kilku z najlepszych pracowników oraz otworzenie własnej, konkurencyjnej wobec przedsiębiorstwa macierzystego działalności gospodarczej.

Prawdopodobnie założone przez niego działania odniosłyby sukces, gdyby nie pewien splot wydarzeń, który zmusił kierownictwo firmy do zmiany swojego stosunku wobec wspomnianego informatora oraz skuteczności użytkowanych rozwiązań. Pierwszym sygnałem o nieprawidłowościach mających miejsce w przedsiębiorstwie był odpływ klientów. Spadek obrotów firmy zmusił jej kierownictwo do głębokiej analizy sytuacji, w wyniku której odkryto przyczyny zaistniałego stanu rzeczy. Nieoczekiwanie pojawiły się anonimowe telefony, informujące o zachowaniu wyżej wspomnianego „asa wywiadu" w stosunku do klientów. Owe anonimy posiadały dwie zadziwiające cechy. Po pierwsze, treść i tematyka przekazywanych informacji dotyczyły przede wszystkim

jakości obsługi świadczonej przez poszczególnych pracowników, ich słów, ujawnionych zamiarów oraz przedstawianych propozycji. Po drugie, wyżej wymieniony rodzaj informacji wskazywał bezpośrednio na źródło ulokowane poza strukturami przedsiębiorstwa. Z biegiem czasu okazało się, że anonimy te pochodziły bezpośrednio od stałych klientów, zaniepokojonych wydarzeniami wewnętrznymi w omawianej firmie.

Samoistne pojawienie się działalności noszącej cechy systemu Crime Stoppers zmusiły władze przedsiębiorstwa do rewizji swoich poglądów na temat „wybitności" systemu pozyskiwania informacji wewnętrznej. Bardzo szybko do łask wróciły systemy technicznej kontroli pracy w postaci głęboko zmodernizowanych systemów monitoringu wizyjnego i dźwiękowego. Informacje zgromadzone dzięki samorzutnemu systemowi Crime Stoppers pozwoliły na precyzyjne wyznaczenia zadań dla systemów technicznych. W rezultacie podjętych działań zgromadzono bardzo szeroki wachlarz dowodowy, który umożliwił definitywne rozwiązanie problemu nielojalnego informatora, poprzez wyciągnięcie odpowiednich konsekwencji dyscyplinarnych.

Dla ścisłości należy dodać, że dostarczane anonimowo informacje na temat sytuacji wewnętrznej w omawianej firmie pochodziły od klientów, którzy sami prowadzili własne przedsiębiorstwa i doskonale rozumieli problematykę nielojalności pracowniczej.

Podsumowanie

Powyższy przykład może wprowadzić w pewnego rodzaju zdziwienie. Wystąpiły w nim praktycznie wszystkie czynniki, jakie zostały omówione w niniejszym opracowaniu. Opisana historia wskazuje w sposób jednoznaczny, jakie konsekwencje rodzi pokładanie zbyt wielkich nadziei tylko w jednym, w dodatku trudnym do weryfikacji źródle informacji wewnętrznych. Należy jednoznacznie stwierdzić, że wyznacznikiem skuteczności każdego systemu bezpieczeństwa wewnętrznego jest konsekwencja w jego stosowaniu, stała modernizacja jego podsystemów oraz wzajemna weryfikacja pozyskiwanych danych. Rezygnacja z wykorzystywania któregoś z ogniw wdrożonego systemu może odbywać się tylko w momencie, gdy istnieje możliwość zastąpienia go innym rozwiązaniem, w dodatku o obiektywnie wyższej skuteczności. Opieranie bezpieczeństwa wewnętrznego przedsiębiorstwa tylko na jednym ogniwie pociąga za sobą dość duże ryzyko operacyjne.

Wykorzystywanie systemów pozyskiwania informacji wewnętrznej bezspornie podnosi poziom bezpieczeństwa firmy. Dzięki informacjom dostarczanym przez zaangażowanych informatorów można zwiększyć skuteczność stosowanych środków kontroli pracy. Pozyskiwane dane o sytuacji wewnętrznej przedsiębiorstwa, aktualnych nastrojach poszczególnych pracowników, ich zamierzeniach, nadziejach oraz obranych kierunkach realizacji prywatnych celów w znacznym stopniu ułatwiają wewnętrzne zarządzanie firmą. Niekiedy nawet pozornie nieistotny szczegół na temat odpowiedniej osoby może stać się podstawą do podjęcia działań wyprzedzających, ukierunkowanych na zapobieżenie potencjalnemu zagrożeniu lub zmiany aktualnej sytuacji na lepszą.

Informacje płynące kanałami nieoficjalnymi, pochodzące od osób obserwowanych lub z ich najbliższego otoczenia bywają bliższe rzeczywistości niż pozyskiwane drogą

oficjalnych badań satysfakcji z pracy czy kontroli wydajności. Pracownicy chętniej rozmawiają na niektóre, poniekąd ważne dla firmy tematy ze swoimi znajomymi z pracy niż z przełożonymi, posiadającymi uprawnienia decyzyjne. Stworzenie i zarządzanie systemem pozyskiwania informacji wewnętrznych jest niczym innym, jak analizowaniem prawdziwej rzeczywistości firmy. Owa analiza opiera się na informacjach pochodzących bezpośrednio z obserwowanego środowiska, a dokonują jej firmowe ośrodki decyzyjne.

Pomimo szeregu zalet omawianego rozwiązania nie należy również zapominać o jego wadach. Ogół niebezpieczeństw związanych z pozyskiwaniem informacji sfabrykowanych, dezinformacją, a nawet zewnętrzną inspiracją, jak również rozmyte granice prawne oraz szereg wątpliwości moralnych stawia proponowane rozwiązanie na pozycji przedsięwzięć bardzo ryzykownych.

Analizując plusy i minusy opisanej metody, należy stwierdzić, że przy zachowaniu wymaganych środków ostrożności, angażowaniu pozostałych systemów do weryfikacji danych oraz rygorystycznie przestrzegając narzuconych ram prawnych, program ma duże szanse powodzenia, a przez to dostarczania informacji strategicznych.

Należy jednak pamiętać, żeby informacje uznawane za prawdziwe miały potwierdzenie z kilku, niezależnych źródeł. Zanim więc podejmie się działania w oparciu o pozyskanego „newsa", warto uzyskać jego potwierdzenie przynajmniej przez innego informatora, a najlepiej przez operatora systemu technicznej kontroli personelu.

Bibliografia

Konieczny J., *Wprowadzenie do bezpieczeństwa biznesu*, Wydawnictwo Konsalnet S.A., Warszawa 2004.

Kryminalistyka, red. J. Widacki, C.H. Beck, Warszawa 2008.

Migas P., *Kontrola lojalności personelu w organizacji gospodarczej* (w druku).

Migas P., Koszel E., Fiszer P., Piekoszewski S., *Etyczne granice kontroli lojalności personelu* (w druku).

Ustawa z dnia 26 czerwca 1974 r. Kodeks Pracy (tekst jednolity Dz.U. z 1998 r., Nr 21, poz. 94 z późn. zm.).

Widacki J., *Kryminalistyka*, wyd. 2, C.H. Beck, Warszawa 2002.

Strona internetowa:

http://pl.wikipedia.org/wiki/Armand_Jean_Richelieu (09.08.2008).

Michał Matej

Przeciwdziałanie nadużyciom jako sposób na zwiększenie zysków przedsiębiorstwa

Wprowadzenie

Zapewnienie bezpieczeństwa podmiotów gospodarczych kojarzy się przede wszystkim z bezpieczeństwem fizycznym pracowników i mienia. Zagadnienia ochrony fizycznej są zarówno prawnie unormowane, jak i powszechnie znane, zaś pracownicy ochrony oraz zabezpieczenia techniczne stosowane są przez niemal każde przedsiębiorstwo. Dzięki rozwojowi technologii informatycznych oraz sieci Internet na znaczeniu zyskuje także bezpieczeństwo informacji i zabezpieczenia sieci teleinformatycznych. Na tym tle przestępstwa gospodarcze i nadużycia pozostają problematyką mniej znaną. O tym, że zasługują one na większą uwagę, przekonują policyjne statystyki – systematycznie spada liczba przestępstw z użyciem przemocy przeciwko mieniu, takich jak np. napady na banki, zaś te, które są dokonywane, przynoszą stosunkowo niewielkie straty. W wymiarze finansowym znacznie większym zagrożeniem są oszustwa i wyłudzenia. Prowadzi to do wniosku, że należy przeciwdziałać wystąpieniu tych zjawisk, a w przypadku, kiedy już się zdarzą minimalizować straty. Jednak każdy przedsiębiorca, który postrzega swoją działalność jako sposób na osiągnięcie zysku, może postawić pytanie: czy przeciwdziałanie nadużyciom finansowym jest opłacalne?

Zagrożenia dla przedsiębiorstw można podzielić na zewnętrzne – związane z czynami dokonywanymi przez klientów i kontrahentów na szkodę przedsiębiorstwa, i wewnętrzne – w postaci nadużyć dokonywanych przez pracowników firmy. Oczywiście wymieniony podział jest jedynie umowny i nie ma charakteru rozłącznego – w praktyce często spotyka się przypadki nadużyć popełnianych przez skorumpowanego pracownika w celu ułatwienia kontrahentowi lub klientowi przedsiębiorstwa dokonania przestępstwa na jego szkodę. W zakresie omawianej problematyki znajdą się typy czynów zabronionych penalizowanych przez kodeks karny w rozdziałach: XXXIV Przestępstwa przeciwko wiarygodności dokumentów i XXXVI Przestępstwa przeciwko obrotowi gospodarczemu oraz w art. 286 (oszustwo) w takim zakresie, w jakim mogą one prowadzić do pokrzywdzenia przedsiębiorstw prywatnych. Ponadto w niniejszym opracowaniu operować się będzie szerszym pojęciem „nadużycia", oznaczającym czyny będące złamaniem przyjętych zasad postępowania (przepisów prawa, regulacji wewnętrznych przedsiębiorstwa), dokonane za pomocą wprowadzenia w błąd lub niewłaściwego wykorzystania uprawnień w celu uzyskania korzyści przez sprawcę lub inny podmiot. Pojęcie to będzie bardzo bliskie definicji oszustwa/nadużycia zawodowego (ang. *occupational fraud*), wykorzystywanej przez Association of Certified Fraud Examiners (ACFE) – organizację biegłych badających nadużycia wewnętrzne

w przedsiębiorstwach, która w polskim wydaniu brzmi następująco: „Wykorzystanie wykonywanego zawodu w celu osobistego wzbogacenia się poprzez umyślne nadużycie bądź niewłaściwe zastosowanie środków lub aktywów należących do organizacji, w której jest się zatrudnionym”[1].

Problematyka przestępstw tzw. „białych kołnierzyków” jako specyficznej kategorii występków znana już jest od kilkudziesięciu lat. Termin ten ukuł w latach 40. XX w. amerykański kryminolog Edwin H. Sutherland. Omawiany rodzaj przestępstw charakteryzuje się bardzo wysoką ciemną liczbą, na co składają się następujące czynniki: działanie pod pozorem zwykłej aktywności zawodowej sprawców, trudność wykrycia przestępstwa, duża finezja działania sprawców oraz trudność w pociągnięciu ich do odpowiedzialności za popełnione czyny[2]. Dalsze badania poświęcone nadużyciom pracowniczym prowadzone przez D. Cresseya doprowadziły do stworzenia koncepcji „trójkąta nadużyć” – czyli zestawu czynników wpływających na sprawcę nadużycia: okazja, presja i racjonalizacja. Powstrzymując się od rozważań nad tymi klasycznymi już dla teorii nadużyć zawodowych badaniami, należy zaznaczyć, że już w latach 80. Cressey wyartykułował potrzebę stworzenia specjalnej profesji – kogoś w rodzaju „policjanta korporacyjnego”. Osoba taka winna posiadać wiedzę specjalistyczną na temat nadużyć zawodowych, co ma umożliwiać jej „nadążanie” za ich sprawcami, co z kolei było niezwykle trudne do osiągnięcia przez zwykłych policjantów czy księgowych[3]. Niejako realizacją tej idei stało się powołanie w 1988 r. w Stanach Zjednoczonych wspomnianego już Association of Certified Fraud Examiners – stowarzyszenia biegłych świadczących usługi doradcze i dochodzeniowe dla przedsiębiorstw.

Na gruncie rodzimym nadużycia gospodarcze stanowiące nieodłączny element nieracjonalnej, centralnie sterowanej gospodarki socjalistycznej i skierowane przeciwko mieniu państwowemu, po zmianie ustroju politycznego weszły w nową fazę rozwoju. Obecnie w warunkach globalizacji i rozwoju technologii informatycznych pojawiają się nowe możliwości popełniania przestępstw o znacznie większej skali. Przykładem może być choćby informacja z sierpnia 2008 roku o zatrzymaniu prezesa jednej z krakowskich spółek pod zarzutem okradania pozostałych udziałowców przez wyprowadzanie z niej kapitału. Mechanizm przestępstwa polegał na założeniu kilkunastu spółek-córek, które generowały koszty, przedkładając do zapłaty faktury na wysokie kwoty za fikcyjne usługi. Ze spółek zarządzanych przez wspólników sprawcy pieniądze trafiały na rachunki bankowe zakładane w Stanach Zjednoczonych i w rajach podatkowych[4]. Choć przypadki oszustw popełnianych z takim rozmachem nie są, na chwilę obecną, zbyt częste, należy liczyć się z tym, że w związku z łatwością przemieszczania się i zdalnego dokonywania operacji finansowych (np. za pośrednictwem sieci internetowej) mogą stać się powszechne.

---

[1] www.acfe.pl (05.09.2008).

[2] J. Błachut, A. Gaberle, K. Krajewski, *Kryminologia*, Gdańsk1999.

[3] J. T. Wells, *Nadużycia w firmach. Vademecum*, Warszawa 2006.

[4] www.onet.pl (15.09.2008).

Dlaczego przeciwdziałanie nadużyciom jest ważne?

Choć pytanie to wydaje się retoryczne, w praktyce osoby odpowiedzialne za przeciwdziałanie nadużyciom w przedsiębiorstwach (audytorzy, pracownicy komórek bezpieczeństwa) często stają przed koniecznością przekonywania kierownictwa firmy o potrzebie wprowadzenia zmian w procesach biznesowych lub wydania dodatkowych środków na zwiększenie bezpieczeństwa. Istnieją pewne kategorie przedsiębiorstw, w których masowe świadczenie usług związanych z przekazaniem klientom lub kontrahentom środków pieniężnych lub wartościowych przedmiotów niejako wymusza wprowadzenie rozwiązań organizacyjnych służących przeciwdziałaniu wyłudzeniom. Wskazać tu można działalność bankową, ubezpieczeniową czy związaną ze świadczeniem usług telekomunikacyjnych. Stosowane są takie procedury jak: rozszerzona identyfikacja tożsamości klienta (np. na podstawie więcej niż jednego dokumentu tożsamości), weryfikacja autentyczności informacji lub dokumentów (przez ich sprawdzenie w niezależnych źródłach), wymiana informacji o solidnych i niesolidnych, a czasem nawet nieuczciwych klientach lub kontrahentach (np. za pomocą baz danych, takich jak: Biuro Informacji Kredytowej czy rejestry długów) oraz utraconych dokumentach mogących posłużyć do przestępstwa (np. za pomocą systemu Dokumenty Zastrzeżone). Z drugiej strony, problem nadużyć dokonywanych przez pracowników jest często bagatelizowany lub w ogóle niedostrzegany, a wiedza na ich temat – niewielka. Niekiedy w organizacjach, w których kultura organizacyjna zakłada duże zaufanie do pracowników, wprowadzenie mechanizmów kontroli uważane jest za podkopanie fundamentów firmy. Zwykle najbardziej skutecznym argumentem przemawiającym do zarządów przedsiębiorstw jest doświadczenie na własnym przykładzie nadużycia powodującego znaczne straty finansowe lub poważny uszczerbek na reputacji. W niektórych firmach posiadających właścicieli zagranicznych można zauważyć zaszczepianie na gruncie rodzimym rozwiązań z zakresu przeciwdziałania nadużyciom funkcjonujących w firmie macierzystej (w przypadku przedsiębiorstw amerykańskich mogą to być np. środki kontroli wewnętrznej wprowadzone w związku z wymogami ustawy Sarbanesa-Oxleya[5]). Niektóre kategorie przedsiębiorstw (np. banki) zobowiązane są przez prawo lub zalecenia organów nadzorczych do ograniczania ryzyka operacyjnego (w którym to pojęciu mieści się również ryzyko nadużyć) oraz do utrzymywania komórek audytu wewnętrznego. W przypadku, kiedy nie występuje żadna ze wskazanych sytuacji, należy rozważyć argumenty finansowe dotyczące rzeczywistych, a zwykle niewidocznych strat wynikających z nadużyć.

Pewną wiedzę na temat kosztów zjawiska nadużyć pracowniczych wnoszą badania statystyczne. Stosunkowo najbardziej szerokim i kompletnym jest Report to the Nation publikowany corocznie od 2002 r. przez wzmiankowaną już organizację ACFE. Z raportów, których podstawą są dane dostarczane przez członków organizacji wynika, że koszty nadużyć pracowniczych sięgają 6% (a w raporcie z roku 2008 r. nawet 7%) zysków przedsiębiorstw. Odsetek ten może być dla osób nieznających zagadnienia zaskakujący, a w przeliczeniu na konkretne kwoty utraconych zysków – wręcz nie do pomyślenia. Raport obala także wiele pokutujących ciągle mitów o nadużyciach zawodowych mówiących, że popełniają je głównie pracownicy z małym stażem pracy

[5] http://pl.wikipedia.org/wiki/Ustawa_Sarbanes-Oxley (31.05.2010).

i zatrudnieni na niskich stanowiskach. Tymczasem największy odsetek sprawców notuje się w grupie pracowników w wieku 41–50 lat (35,5%) ze stażem pracy w danym przedsiębiorstwie wynoszącym 1–5 lat (40,5%), zaś w popełnianiu nadużyć managerowie niemal dorównują pracownikom szeregowym (37,1% nadużyć popełnianych przez managerów przy 39,7% nadużyć pracowników szeregowych), mimo ich niewielkiej liczebności w stosunku do innych pracowników. Ponadto w raporcie znalazły się dane dotyczące skuteczności środków przeciwdziałania nadużyciom. I tak w zakresie wykrywania nadużyć, według raportu za rok 2008, najskuteczniejsze okazały się zgłoszenia o popełnieniu nadużycia – w ten sposób wykryto aż 46,2% z nich. W 20% wykrycie nastąpiło na skutek przypadku, podczas gdy skuteczność mechanizmów kontroli wewnętrznej i audytu wewnętrznego wyniosła odpowiednio 23,3% oraz 19,4%[6]. Na podstawie badań można również sformułować wniosek, że w organizacjach niestosujących rozwiązań mających na celu przeciwdziałanie nadużyciom tego typu przestępstwa są nie tylko częstsze, ale także wykrywane są znacznie później i przynoszą niemal dwukrotnie większe straty.

Sposoby przeciwdziałania nadużyciom w przedsiębiorstwach

Jak już wspomniano, wiele przedsiębiorstw wdrożyło pewne – przynajmniej pojedyncze – rozwiązania, mające chronić je przed nadużyciami. Niewiele jednak posiada kompleksowy system przeciwdziałania nadużyciom, oddziałujący na całą organizację i obejmujący wszystkie aspekty działania w tym zakresie. Koncepcję takiego systemu określonego mianem „strategii zarządzania ryzykiem defraudacji i korupcji" przedstawili N. Iyer i M. Samociuk w swojej pracy pt. *Defraudacja i korupcja*, będącej w założeniu podręcznikiem wdrażania tego typu strategii w przedsiębiorstwach[7]. Na strategię składają się, według autorów:

1. Ton nadawany z góry.
2. Zrozumienie ryzyk.
3. Redukowanie ryzyk.
4. Monitorowanie i wykrywanie czerwonych flag.
5. Zarządzanie incydentami.
6. Zwiększanie odporności.

Wprowadzanie strategii rozpoczyna się od akceptacji przez zarząd przedsiębiorstwa zarówno samej strategii, jak i idei kultury uczciwości w przedsiębiorstwie. „Ton nadawany z góry" powinien znaleźć odzwierciedlenie nie tylko w komunikatach o charakterze ogólnym skierowanych do pracowników, ale także w sformalizowanym dokumencie regulującym sposób postępowania pracowników oraz w przyjęciu polityki przeciwdziałania nadużyciom. Kodeks postępowania ma na celu uświadomienie pracownikom oczekiwanych standardów zachowania i przez to wpływ na ich codzienną postawę. Polityka przeciwdziałania nadużyciom powinna wskazywać, jakie zjawiska i w jaki sposób są przez przedsiębiorstwo zwalczane. Wreszcie, nie bez znaczenia jest dawanie przez kierownictwo osobistego przykładu uczciwości – znane są bowiem

[6] www.acfe.com (07.09.2008).

[7] N. Iyer, M. Samociuk, *Defraudacja i korupcja*, Warszawa 2007, s. 28–30.

przypadki destrukcyjnego wpływu niewłaściwego zachowania przełożonych na morale pracowników[8]. Zrozumienie ryzyka nadużyć to kolejny krok wdrażania strategii. Należy badać ryzyka powiązane z określonymi rodzajami działań, a następnie uświadamiać je kierownikom właściwych jednostek oraz ich pracownikom. Można w tym celu przeprowadzić stosowne szkolenia bądź wykorzystać formułę warsztatów, gdzie, podczas analizy konkretnych scenariuszy nadużyć osoba odpowiedzialna za realizację strategii wymienia swoją wiedzę o nadużyciach z doświadczonymi zawodowo pracownikami. Na podstawie tej wiedzy należy przystąpić do ograniczania zidentyfikowanych rodzajów ryzyka. Można to uczynić, wprowadzając rozwiązania na poziomie procesów biznesowych lub dodatkowe mechanizmy kontrolne skierowane przeciwko określonym typom nadużyć. Niekiedy ryzyko nadużyć może wywierać wpływ na decyzje na poziomie strategicznym przedsiębiorstwa. Oczywiście całkowite wyeliminowanie ryzyka nie jest możliwe, należy jednak dążyć do jego minimalizacji do akceptowalnego poziomu. Po wprowadzeniu mechanizmów prewencji należy przystąpić do implementacji mechanizmów monitorowania i wykrywania „czerwonych flag" (symptomów wystąpienia nadużycia). Tu także niezbędne będą szkolenia dla pracowników, bowiem właśnie pracownicy liniowi będą mieli najwięcej okazji do wykrycia pierwszych oznak nadużycia.

Równie ważne jest stworzenie ścieżki przekazywania zgłoszeń o nadużyciach. System taki powinien zakładać możliwość swobodnego i pozbawionego zewnętrznej kontroli przekazywania informacji przez każdego pracownika przedsiębiorstwa bezpośrednio do jednostki organizacyjnej, której zadaniem jest podjęcie reakcji na wystąpienie nadużycia. W celu zachęcenia pracowników do przesyłania informacji można zapewnić ochronę tożsamości informatorów lub umożliwić przekazywanie zgłoszeń również anonimowo. Poza zbieraniem sygnałów od pracowników warto rozważyć wprowadzanie monitoringu funkcjonowania przedsiębiorstwa. Analiza odpowiednich raportów i zestawień przez wyspecjalizowanych pracowników pozwoli na wykrycie różnego rodzaju nadużyć. Wskazać tu można chociażby zestawienia faktur od kontrahentów, wydatków służbowych, strat w majątku, danych na temat pracowników czy skarg.

W momencie wykrycia nadużycia lub przynajmniej podejrzenia, że ono wystąpiło, sprawa powinna zostać przekazana do jednostki organizacyjnej przedsiębiorstwa, która w polityce przeciwdziałania nadużyciom została wskazana jako zobowiązana do podjęcia stosownej reakcji. Od tego momentu właściwa jednostka przejmuje koordynację działań i ponosi odpowiedzialność za ich wyniki. Po wykryciu „czerwonej flagi" konieczne jest przeprowadzenie postępowania wyjaśniającego (dochodzenia) w celu ustalenia, czy: nadużycie rzeczywiście miało miejsce, jaki był jego mechanizm, jakie są straty i kto jest sprawcą. W ramach prowadzonego dochodzenia powinny zostać także zabezpieczone dowody będące podstawą ustaleń, które następnie, w razie potrzeby, zostaną przekazane do właściwych organów zewnętrznych, o czym należy pamiętać już na etapie działań wewnątrz firmy. Ukoronowaniem dochodzenia jest zwykle konfrontacja poczynionych ustaleń z domniemanym sprawcą nadużycia, a następnie pociągnięcie go do odpowiedzialności (w zależności od sytuacji dyscyplinarnej, cywilnej, karnej). Ostatnim elementem kompleksowej strategii jest dalsze

[8] *Ibidem*.

zwiększanie odporności na nadużycia przez prowadzenie pomiarów odporności organizacji na wpływ działań nieuczciwych pracowników[9].

Oczywiście zastosowanie tego rodzaju strategii nie jest ani szybkie, ani proste. Wymaga to zrozumienia zarówno ze strony kierownictwa, jak i pracowników. Wdrożenie opisanych działań powinno zostać poprzedzone oceną ryzyka nadużyć w organizacji (identyfikacji obszarów zagrożonych i poziomu ryzyka), z kolei zarząd przedsiębiorstwa musi wykazać się determinacją w dążeniu do celu. Zapewne nie w każdej firmie konieczne i możliwe będzie wprowadzenie wszystkich opisanych rozwiązań. Należy jednak podkreślić, że realizacja części z nich może być stosunkowo prosta i mało kosztowna, a przez to mało uciążliwa dla działalności biznesowej. Należy wskazać tu następujące działania:

- Ton nadawany z góry – przekazanie przez zarząd czytelnego sygnału w zakresie etyki oraz wprowadzenie regulacji wewnętrznych.
- Monitorowanie i wykrywanie – stosunkowo efektywne i tanie jest wprowadzenie kanału informowania o nadużyciach – może to być nawet telefon do wyznaczonego pracownika lub przeznaczony do tego celu adres e-mail. To samo dotyczy przeszkolenia pracowników w wykrywaniu czerwonych flag i przeglądania raportów o działalności firmy.
- Redukowanie ryzyk i zarządzenie incydentami – w tym przypadku można wykorzystać istniejącą jednostkę przedsiębiorstwa. Choć zarządzanie incydentami jest czasochłonne, trudno wyobrazić sobie model przeciwdziałania nadużyciom pozbawiony tego elementu.

Podsumowanie – korzyści i zagrożenia dla przeciwdziałania nadużyciom

Podsumowując, należy wymienić korzyści płynące z wdrożenia rozwiązań z zakresu przeciwdziałania nadużyciom, a są to:

1. Ograniczenie strat związanych z nadużyciami – poprawa wyników finansowych przedsiębiorstwa.
2. Stworzenie klimatu braku akceptacji dla działań nieetycznych – poprawa morale uczciwych pracowników.
3. Większa wiedza o własnej organizacji i jej podatności na zagrożenia – możliwość usprawnienia procesów (prewencja).

By jednak uczciwie sprowadzić zagadnienie od teorii do praktyki funkcjonowania organizacji gospodarczych, należy wymienić również następujące zagrożenia związanie z realizacją przeciwdziałania nadużyciom:

1. Brak możliwości lub znacznie utrudniona możliwość wykazania efektywności prowadzonych działań przez wskazanie konkretnych oszczędności w związku z udaremnionymi nadużyciami.
2. Próby dyskredytacji działań komórki bezpieczeństwa przez pracowników nieuczciwych.

[9] *Ibidem*.

3. Obawa kierownictwa przed ujawnianiem przypadków nadużyć (ryzyko utraty reputacji, negatywnego odbioru tych informacji przez radę nadzorczą bądź udziałowców).

Pierwsze z wymienionych zagrożeń występować może w organizacjach, w których kierownictwo nie posiada wewnętrznego przekonania o konieczności mitygowania ryzyka nadużyć lub obowiązek ten nie jest mu narzucony z zewnątrz. W takiej sytuacji, szczególnie przy okazji różnego rodzaju działań związanych z poszukiwaniem oszczędności, może dojść do prób ograniczania (lub w ogóle nie dochodzi do powstania) działania komórek przeciwdziałających nadużyciom. W warunkach gospodarki rynkowej skuteczną metodą jest przedstawienie wykonanych przez komórkę bezpieczeństwa lub mechanizmy prewencji działań w przełożeniu na postać danych finansowych o rzeczywistych i potencjalnych stratach, którym zapobiegło udaremnienie nadużycia. Nie bez znaczenia są także argumenty pozafinansowe: obniżenie morale pracowników firmy w przypadku tolerowania przez kierownictwo przypadków nadużyć oraz zwiększenie ryzyka utraty reputacji w przypadku rozpowszechnienia informacji o bezkarności sprawców.

Do prób dyskredytowania komórki przeciwdziałającej nadużyciom może dojść w przypadku ujawnienia sprawstwa lub innej formy dokonania nadużycia przez członków wysokiego szczebla kierowniczego. Takie działania są często formą obrony nieuczciwego pracownika, który, jeśli posiada zaufanie zarządu firmy, może skutecznie zaszkodzić wynikom postępowania wyjaśniającego, a nawet uniknąć odpowiedzialności. Jest to szczególnie niebezpieczne na etapie kształtowania się systemu przeciwdziałania nadużyciom w przedsiębiorstwie, prowadzi bowiem do jego negatywnego postrzegania. Koniecznymi środkami przeciwdziałania są: podział dochodzenia na część niejawną i jawną, ścisła reglamentacja informacji dotyczących toczącego się dochodzenia, powstrzymanie się od działań dyscyplinarnych przed wyjaśnieniem najważniejszych okoliczności nadużycia, a nade wszystko – możliwość bezpośredniego i niezwłocznego kontaktu z osobą zarządzającą przedsiębiorstwem (właścicielem, prezesem zarządu). Szybka i rzetelna informacja pochodząca bezpośrednio ze źródła – czyli komórki prowadzącej postępowanie wyjaśniające – pozwala prezesowi spółki (szefowi firmy) na wyrobienie sobie opartej na faktach opinii, a w konsekwencji podjęcie obiektywnych decyzji.

Trzecie wskazane zagrożenie związane jest z oczywistą troską o ochronę dobrego imienia przedsiębiorstwa, która może stać się zagrożeniem dla komórki bezpieczeństwa, jeśli kierownictwo, w obawie o utratę reputacji, zdecyduje się ingerować w prowadzone postępowanie wyjaśniające w celu jego przedwczesnego zakończenia. Obawy takie zwykle nasilają się w przypadku ujawnienia nadużyć na szerszą skalę lub sprawców zajmujących wysokie stanowiska kierownicze. Sytuacja taka może prowadzić do braku rozpoznania mechanizmów nadużycia i wskazania jego rzeczywistych sprawców, a zatem nie będzie możliwa ani prewencja, ani represja w stosunku do nieuczciwych pracowników. Remedium na tego typu niebezpieczeństwo może być odpowiednie przygotowanie zarówno kierownictwa, jak i całej organizacji na możliwe skutki ujawnienia nadużycia. Należy liczyć się z faktem, iż wykrycie każdego poważnego przestępstwa pracowniczego, szczególnie jeśli jest ono przedmiotem postępowania karnego, odbija się echem w samej organizacji (w raportach, sprawozdaniach), jak i poza nią (zgłoszenia do organów nadzorczych, informacje w mediach). Choć

przedsiębiorstwa nie mają powodu, by rozpowszechniać tego rodzaju informacje na zewnątrz, muszą jednak być przygotowane na ich ujawnienie. Sprawne działanie rzetelnie poinformowanego kierownictwa (czego fundamentem powinien być raport z postępowania wyjaśniającego przygotowany przez jednostkę odpowiedzialną za przeciwdziałania nadużyciom), wspieranego przez dział komunikacji zewnętrznej (rzecznika prasowego) poprzez szybką publikację komunikatów przedstawiających: prawdziwy przebieg wydarzeń, wyniki pracy śledczych, podjętą współpracę z organami ścigania, wdrożone środki zaradcze itd., pozwala na uniknięcie wypaczania informacji i podkopywania reputacji przedsiębiorstwa. Podobnie w komunikacji wewnętrznej jasne przedstawienie przypadku nadużycia i stosunku do niego organizacji pozwala podnieść takie zdarzenie z poziomu pożywki dla korytarzowych plotek do poziomu egzemplifikacji polityki przeciwdziałania nadużyciom.

Należy zaznaczyć, że powyższe przykłady dotyczą jedynie zagrożeń na poziomie kierowniczym organizacji, pominięto tutaj problemy związanie z rozwiązaniami systemowymi przedsiębiorstwa oraz z samą organizacją komórki przeciwdziałania nadużyciom, które mogą stanowić temat na osobną publikację.

Podsumowując przeprowadzone rozważania, należy stwierdzić, że nadużycia pociągają za sobą poważne straty finansowe przedsiębiorstw, zaś wprowadzanie środków prewencji przyczynia się do znacznego zmniejszenia ewentualnych strat. Warto zatem aktywnie im przeciwdziałać, by w ten sposób, wprowadzając rozwiązania promujące postawy etyczne, zwiększać dochody przedsiębiorstw i przyczyniać się do ich bardziej uczciwego działania.

Bibliografia

Błachut J., Gaberle A., Krajewski K., *Kryminologia*, Wydawnictwo Arche, Gdańsk 1999.
Iyer N., Samociuk M., *Defraudacja i korupcja*, Wydawnictwo Naukowe PWN, Warszawa 2007.
Wells J. T., *Nadużycia w firmach. Vademecum*, LexisNexis, Warszawa 2006.

Strony internetowe:
http://pl.wikipedia.org/wiki/Ustawa_Sarbanes-Oxley (31.05.2010).
www.acfe.com (07.09.2008).
www.acfe.pl (05.09.2008).
www.onet.pl (15.09. 2008).

Michał Skorecki

Problematyka kradzieży w dużych centrach handlowych

Z plagą kradzieży sklepowych od dawna borykają się wszystkie obiekty handlowe, niezależnie od ich wielkości i wysokości obrotów. Kradzież sklepowa zdefiniowana została jako specyficzna forma zaboru mienia, która przejawia się w działaniu przestępczym osoby udającej klienta sklepu, dokonującej tych czynności podczas dziennych godzin jego otwarcia[1]. Obecnie zjawisko to staje się tak powszechne i nagminne, że przedsiębiorcy zaczynają dostrzegać, iż dopuszczalna tolerancja strat zaczyna przekraczać wytyczone granice, a interwencja i prewencja wydają się jedynymi skutecznymi narzędziami w walce z tym problemem. Zrozumiałe jest również to, że do tej pory wielkie sieci handlowe niechętnie przyznawały się do tego, iż są okradane zarówno przez swoich klientów, jak i samych pracowników, co naraża ich na straty o wiele większe niż rzeczywiście ujawnione (w tym również uszczerbek na prestiżu). Świadomie w artykule pominięte zostały kwestie kradzieży wewnętrznych dokonywanych przez samych pracowników oraz kradzieże z włamaniem, a to ze względu na specyfikę tych przestępstw i traktowanie ich przez znawców tematu jako odrębne zjawiska.

Postęp cywilizacyjny i technologiczny, jaki dokonał się na przełomie ostatnich 15 lat w całej Europie, spowodował jednocześnie poważne zmiany w strategii zarządzania i organizacji pracy obiektów handlowych. Niestety w wielu przypadkach doprowadziło to do powstania sytuacji, w której nieumiejętne wykorzystywanie tych narzędzi przez menedżerów i kadrę kierowniczą naraża handel komercyjny na ogromne straty, nie tylko finansowe. Prawie we wszystkich dużych obiektach handlowych zrezygnowano ze struktury magazyn przyjmie = magazyn wyda. Obecnie towar przyjmowany jest bezpośrednio z centrum dystrybucji, a jego ilość i jakość podlega wyrywkowej kontroli. Następnie towar przesuwany jest na halę sprzedaży z pominięciem procedur rejestracji. Ponadto wprowadzenie samoobsługowej formy sprzedaży zredukowało liczbę personelu w sklepie do absolutnie niezbędnej. Doprowadziło to ostatecznie do tego, iż osoby dokonujące kradzieży indywidualnie oraz grupy przestępcze o różnym poziomie organizacyjnym i funkcjonowaniu doskonale wykorzystały te uwarunkowania dla ułatwienia swojej wrogiej działalności.

Globalnie sieci handlowe tracą rocznie około 72,4 mld euro. W Polsce jest to 1,2 mld euro w skali roku. Jest to problem coraz poważniejszy, bowiem kradzieże sklepowe stanowią już 1,36% rocznych obrotów sieci handlowych i wskaźnik ten powoli, ale regularnie rośnie. W Polsce wzrost strat z tego tytułu w porównaniu z rokiem ubiegłym wyniósł 1,5%. Jednocześnie Polska ma najwyższy w Europie odsetek strat, za które odpowiadają pracownicy – aż 35,1%. Nieuczciwym klientom przypisuje się jednak 40,5% strat, zaś średnia europejska w tym zakresie to 48,5%[2].

---

[1] R. Hayes, C. Cardone, *Shoptheft* [in:] *The Handbook of Security*, ed. M. Gill, Boston 2006.

[2] www.rp.pl/artykul/102681,127342 (15.09.2008).

Jaki zatem wpływ ma omawiane zjawisko na otaczającą rzeczywistość? Oddziałuje ono zasadniczo na 3 sfery: biznesu, władzy i społeczeństwo jako zbiorowość[3]. Przedsiębiorca będzie tolerował kradzieże, dopóki nie spowodują one przekroczenia z góry wkalkulowanych w ryzyko prowadzenia interesu strat. Jeżeli jednak tak się stanie, powoduje to wzrost ponoszonych przez niego kosztów na zapewnienie bezpieczeństwa i ubezpieczenie, prowadzenie audytu wewnętrznego i wykrywanie wewnętrznych przestępstw gospodarczych, wdrażanie procedur postępowania z nieuczciwymi klientami bądź personelem oraz odpowiednie szkolenia dla kadry zarządzającej. Co za tym idzie, powoduje to wzrost cen produktów na sklepowych półkach, spadek produktywności i efektywności działania oraz problemy z zapewnieniem odpowiedniej jakości usług. Władza państwowa z tytułu kradzieży sklepowych ponosi z kolei większe koszty utrzymania skazanych sprawców tego rodzaju przestępstw, tworzenia i wdrażania programów prewencyjnych czy zwiększania i zaostrzania procedur bezpieczeństwa ogólnego. Nie bez znaczenia pozostaje także fakt wzrostu licznych, ukrytych w cenach produktów podatków i danin państwowych. Społeczeństwo natomiast najdotkliwiej odczuwa ogólny i zauważalny wzrost kosztów utrzymania.

Obecnie w Polsce przestępstwo kradzieży wskazane jest w art. 278 § 1 Kodeksu karnego (Ustawa z dnia 6 czerwca 1997 r. Kodeks karny, Dz.U. z 1997 r., Nr 88, poz. 553), jak i art. 119 § 1 Kodeksu wykroczeń (Ustawa z dnia 20 maja 1971 r. Kodeks wykroczeń, Dz.U. z 1971 r., Nr 12, poz. 114), które jednakowo penalizują zachowanie polegające na „zaborze cudzej rzeczy ruchomej w celu przywłaszczenia". Wszystkie znamiona dotyczące strony przedmiotowej i podmiotowej są identyczne w obu przepisach. Kryterium rozgraniczającym jest wartość skradzionego mienia. Zatem o rodzaju odpowiedzialności sprawcy (za przestępstwo czy wykroczenie) decyduje wyłącznie kryterium obiektywne w postaci wartości rzeczy ruchomej zabranej celem przywłaszczenia. Tą granicą jest obecnie kwota 250 zł. Przestępcy, którzy zawodowo zajmują się kradzieżami sklepowymi w ramach zorganizowanych grup przestępczych, doskonale zdają sobie sprawę z obowiązujących przepisów i zagrożeń prawnych, wobec czego stosują dwie metody: albo kradną przedmioty o wartości poniżej tej kwoty (znikoma szkodliwość czynu – zaledwie kara grzywny, którą można uiścić na miejscu), albo wykorzystują do wykonywania czynności przestępnych nieletnich bądź upośledzonych fizycznie lub umysłowo, którzy właściwie pozostają bezkarni.

Zjawisko kradzieży sklepowych zwłaszcza w Polsce ma silne przyzwolenie społeczne, co jest bardzo ciekawym zjawiskiem socjologicznym[4]. Czyn ten, zwłaszcza w mentalności tych grup społecznych, które nie zajmują się zawodowo dokonywaniem kradzieży, w ostatnich latach mocno się zdekryminalizował. W przekonaniu wielu osób racjonalne argumenty usprawiedliwiające to zjawisko są następujące:

1. Kradzież sklepowa to nie kradzież, a pożyczka.
2. To znak obecnych czasów.
3. Kradzież jest moralnie uzasadniona wobec ogólnego ubóstwa.
4. Jest zemstą za upokorzenia w pracy.
5. Jest aktem demonstracji przekonań i walki klasowej.

[3] P. C. Nemeth, *Private Security and the Investigative Process*, Boston 2000; R. Hayes, C. Cardone, *op. cit.*

[4] P. C. Nemeth, *op. cit.*, s. 231 i n.

Istnieje wiele przyczyn, dla których ludzie kradną w sklepach. To impuls, głód, zemsta, choroba, chęć zaimponowania rówieśnikom. Jednakże najpopularniejsza z nich to czysty zysk ekonomiczny.

Bardzo zróżnicowany jest również przekrój osobowy sprawców tego rodzaju przestępstwa. Wielu sprawców może należeć do kilku kategorii jednocześnie. W związku z tym można przyjąć ogólną strukturę, która przedstawia się następująco (nie jest to jednak katalog zamknięty):

1) osoby o wysokim statusie społecznym, które kradną dla emocji i popisu;
2) osoby niezamierzające popełnić przestępstwa, natomiast uważające „podjadanie" za formę degustacji;
3) nieletni, którzy traktują centra handlowe jako doskonałe miejsce pobytu na wagarach przy jednoczesnym dokonywaniu drobnych kradzieży często dla uzyskania poklasku wśród rówieśników;
4) osoby, które tego typu placówki traktują jako miejsca, w których można się najeść i napić (bezdomni, narkomani itp.);
5) osoby lub grupy zawodowo zajmujące się kradzieżami w celu dalszej odsprzedaży skradzionego towaru.

Omawiany proceder charakteryzuje się różnym stopniem organizacji, a decydują o tym różnorodne uwarunkowania, m.in. takie jak: wprowadzenie w podziemie kryminalne, poziom intelektualny uczestników kradzieży, poziom wiedzy technicznej i prawnej, doświadczenie zawodowe, determinacja i zwykła chęć zysku.

Wiele typologii sprawców kradzieży sklepowych powstało w Stanach Zjednoczonych. Jedną z ciekawszych, która znalazła potem swoich naśladowców, jest klasyfikacja zaproponowana w 1984 r. przez R. Moore'a. Wyróżnił on 5 podstawowych typów złodziei sklepowych[5]:

1. Kradnący impulsywnie. Kradną w sposób niezaplanowany jedną, tanią rzecz, kierując się pokusą. Po zatrzymaniu reagują zdziwieniem, zmieszaniem lub szokiem. Mają poczucie winy, zakłopotania, wstydu. Wykrycie kradzieży jest dla nich traumatycznym przeżyciem powodującym, że zaprzestają dalszych kradzieży.
2. Złodzieje okazjonalni. Kradną średnio od 3 do 10 razy w skali roku. Kradną głównie po to, by sprostać jakiemuś wyzwaniu, lub po to, by przypodobać się rówieśnikom. Względy ekonomiczne mają drugorzędne znaczenie. Po schwytaniu przyznają się do kradzieży, jednakże reagują z dystansem. Umniejszają szkodliwość dokonanego czynu.
3. Kradnący okresowo. Kradną okresowo specyficzne towary. Badane w tej kategorii osoby zdradzały problemy emocjonalne i psychiczne oraz odczuwały silną depresję oraz poczucie winy. Często wykazują skłonność do intrapunitywnego wyrażania agresywnych impulsów. Kradną nieregularnie z powodu nieustannego stresu. Po schwytaniu zachowują się pokornie i są świadomi tego, że ich czyn jest niemoralny.
4. Amatorzy. Kradną regularnie, głównie dla osobistego zysku. Kradzieży dokonują świadomie. Sięgają przede wszystkim po małe, łatwe do ukrycia rzeczy. Posługują się przy tym prostymi technikami kradzieży. Po aresztowaniu zwykle z trudnością

[5] R. Hayes, C. Cardone, *op. cit.*; T. Krasnovsky, R. C. Lane, *Shoplifting: a review of the literature*, Vol. 3, "Aggression and Violent Behavior" 1998.

przyznają się do popełnionego czynu oraz stosują różnorodne strategie manipulacyjne, aby uniknąć kary.

5. Profesjonaliści. Kradzież sklepowa jest częścią ich stylu życia. Dokonują jej z bardzo dużą częstotliwością, wykorzystując przy tym najbardziej wyszukane techniki kradzieży. Głównymi motywami przestępstwa w tym przypadku jest chęć zysku oraz kompensacja krzywd wyrządzonych przez społeczeństwo. Kradzież sklepowa jest dla nich sposobem radzenia sobie z frustracją życia codziennego i nudą. Dzięki sprzedaży skradzionych artykułów nie tylko mogą pozwolić sobie na luksus, ale także gromadzą środki na realizację innych celów w przyszłości. Nie postrzegają kradzieży jako prawnie lub moralnie niewłaściwej. Zmniejszają powagę tego przestępstwa i nie czują się winni. Po zatrzymaniu przez policję starają się zredukować ciężar odpowiedzialności prawnej w związku z dokonaną kradzieżą. Co więcej, wpadają wówczas w gniew, twierdząc, że są traktowani niesprawiedliwie.

W sklepach giną głównie: alkohol, kosmetyki, odzież damska, perfumy, sprzęt RTV i AGD oraz żywność. Dość powszechnym zjawiskiem jest również spożywanie rozmaitych artykułów spożywczych przez klientów, za które oczywiście nie płacą. Zgodnie z szacunkami specjalistów, w skali miesiąca klienci średniej wielkości supermarketu zjadają na terenie obiektu 1,5 tony różnego rodzaju produktów.

Bogaty jest również katalog metod, jakimi posługują się sprawcy kradzieży sklepowych – od bardzo wyrafinowanych do skrajnie prymitywnych.

Dla przykładu warto przytoczyć choćby kilka z nich[6]:

1) stosowanie folii aluminiowej, w którą sprawca owija produkt, aby stał się „niewidzialny" dla elektronicznych bramek zabezpieczających;
2) do jednej z kas podchodzi członek grupy przestępczej i informuje, że zamierza dokonać kradzieży z większą grupą np. 4–5 osób. Grupa ostentacyjne wchodzi na halę i zaczyna robić sporo zamieszania. Wkładając towar do koszyków i rozrzucając go po sklepie oraz zaczepiając klientów, absorbuje swoim zachowaniem obsługę monitoringu, ochronę i nieliczny personel sklepu. W tym samym czasie zupełnie inni członkowie grupy spokojnie dokonują kradzieży;
3) podobnie zachowują się grupy, w których jeden z jej członków nagle symuluje atak choroby (zawał, padaczka itp.), a pozostali w tym czasie plądrują sklep;
4) przestępca wkłada do koszyka różne towary np. odzież oraz kostkę masła lub sera, następnie bierze drogi kosmetyk i udaje się do przebieralni, gdzie drogi kosmetyk wciska do masła/sera. Z tak sporządzonym „produktem" wraca na halę sprzedaży, odkładając go z powrotem w taki sposób, aby nie zabrał go przypadkowy klient. Następnie przychodzi wspólnik, podejmuje ową spreparowaną kostkę masła/sera i udaje się do kasy. Jeżeli kosmetyk nie został pozbawiony zabezpieczenia i zostaje ujawniony, klient robi awanturę, grożąc doniesieniem do sanepidu o rzecz znajdującą się w maśle. W tym przypadku udowodnienie winy jest niemożliwe, w związku z czym personel sklepu i ochrona przepraszają klienta. Przedmioty o większych rozmiarach mogą być chowane do pojemników z proszkiem, farbą itp.;
5) sprawca zabiera do koszyka produkty umieszczone w miejscu monitorowanym przez kamery, które zlokalizowane są głównie w miejscach składowania towarów

[6] R. Hayes, C. Cardone, *op. cit.*

„wrażliwych". Następnie towar przenoszony jest do miejsc takich jak np. wystawy lodówek, mebli, zamrażarek i tam pozostawiany przez jednego uczestnika akcji, który już bez towaru opuszcza sklep. Następnie towar ten podejmuje wspólnik nienarażony na obecność kamer;

6) grupa przestępcza zaprzyjaźnia się z pracownikami marketu lub ochrony. Pracownicy dużych centrów handlowych to najczęściej ludzie młodzi pochodzący z małych miasteczek, z niskim wykształceniem, niezamożni, szukający szansy w większym mieście. Z łatwością przyjmują zaproszenie do wspólnego spędzania czasu w dyskotekach i na imprezach sponsorowanych przez przestępców, za co już po krótkim czasie żądają oni swoistego rewanżu. Przestępcy przychodzą do marketu w godzinach małego ruchu i nocnych. Do wózków wkładają towar o wysokiej cenie i łatwego zbycia (kosmetyki, alkohol, papierosy). Przy pomocy zastraszonego i „kupionego" wcześniej personelu lub ochrony bez dokonania zapłaty opuszczają sklep;
7) często osoby mające dokonać kradzieży to tzw. półświatek lub osoby zdemoralizowane, z marginesu społecznego, dla których wystarczającą zapłatą jest tani alkohol i żywność. Grupa 3–4 osobowa przewożona jest samochodem od obiektu do obiektu, a kierowca pozostaje w aucie, odbierając tzw. fanty. Całość łupu odbiera szef, przekazując go dalej osobom, które zajmują się sprzedażą;
8) na „wyrwę" – przestępcy biorą towar, przeskakują przez pustą kasę i gwałtownie uciekają z marketu, a na parkingu czeka w samochodzie ich wspólnik;
9) dość powszechnym zjawiskiem jest przemetkowanie cen na towarach. W grupach zorganizowanych jedni dokonują przemetkowania, a inni wynoszą towar. Jednocześnie dbają o to, aby w czasie wpadki mogli udowodnić, że niczego nie przyklejali. Mają pełne rozeznanie o lokalizacji kamer i robią wszystko, aby byli widoczni. Temu procederowi sprzyja współpraca z kasjerkami lub mechaniczne zachowania kasjerek, które często nie zwracają uwagi na korelację rzeczywistej wartości towaru z ceną podaną na metce.

Ciekawe są również sposoby upłynniania skradzionego towaru. Najczęściej jest on sprzedawany za pośrednictwem Internetu, na parkingach przed obiektami handlowymi, na bazarach, wśród znajomych. Dla zobrazowania owego zjawiska niech posłuży kilka przytoczonych niżej przykładów:

1) starsza pani siedzi przed dworcem kolejowym i sprzedaje po bardzo atrakcyjnej cenie markowy kosmetyk. Ma przy sobie jedną, dwie sztuki towaru, kiedy je sprzeda krążący wokół dworca wspólnik dostarcza kolejne sztuki;
2) na parkingu przy supermarkecie krąży człowiek proponujący w niskiej cenie np. odtwarzacz mp3. Po jego sprzedaży udaje się do samochodu zaparkowanego w odległym punkcie parkingu, gdzie od wspólnika otrzymuje kolejną partię, tym razem np. kosmetyków i ponownie powtarza czynność;
3) alkohol i kosmetyki od osób uzależnionych wykupują taksówkarze;
4) często miejscem odbioru towaru są małe sklepy wiejskie. Charakteryzują się one dobrym kontaktem ze swoimi klientami (małe środowisko, często patologiczne);
5) ten rodzaj towaru, który pakowany jest w sposób charakterystyczny dla konkretnej sieci handlowej (np. w plastikowych pudełkach) pozbawiany jest opakowania i sprzedawany luzem.

Najważniejsze jednak pytanie brzmi: co zrobić, by zlikwidować lub co najmniej zminimalizować omawiane zjawisko? Rozwiązań owego problemu jest wiele, wymagają one jednak ścisłej współpracy między sieciami handlowymi, organami ścigania i samym społeczeństwem. Niektóre z tych rozwiązań zostaną omówione szerzej[7].

A. Strategia działania sklepu

Każda z większych sieci handlowych wypracowuje własne standardy i procedury postępowania z nieuczciwymi klientami oraz pracownikami. Oczywiste jest, że mają one nie tylko charakter restrykcyjny, ale także prewencyjny. Ważnym czynnikiem redukującym zjawisko kradzieży sklepowych jest tutaj także odpowiednia polityka społeczna penalizująca takie zachowania, zwłaszcza wśród młodzieży i osób starszych (bowiem najlepszymi „sklepowymi policjantami" są uczciwi klienci).

B. Działania wobec personelu

Sprawnie zarządzany obiekt handlowy z powodzeniem wdraża nowoczesne procesy zarządzania personelem, szkolenia dla pracowników niższego szczebla, odpowiednie techniki motywacyjne (polityka cenowa i wynagrodzeń). Dba o ścisłą kontrolę obiegu towaru od momentu jego dostarczenia do sklepu do wydania klientowi. Wielką uwagę zwraca się także na personel ochrony, którego kryteria doboru i okresowej weryfikacji winny być podyktowane specyfiką danej placówki i jednocześnie spełniać najwyższe standardy bezpieczeństwa. Trzeba bowiem pamiętać, iż praca w ochronie jest naprawdę ciężka – wymaga nie tylko silnych mięśni, ale także krzty intelektu i zdolności interpersonalnych.

C. Odpowiednia przestrzeń

Rozkład pomieszczeń i półek z towarami w sklepie powinien być tak przemyślany, aby ryzyko kradzieży było jak najmniejsze, techniczne środki zabezpieczeń pracowały możliwie najbardziej wydajnie, a potencjalny złodziej czuł się przez cały czas pobytu na terenie obiektu obserwowany. Nie można też dopuścić do sytuacji, w której miałby on możliwość ukrycia zrabowanego przedmiotu (redukcja otwartej przestrzeni, dużo światła itp.).

D. Mechaniczne zabezpieczenia

Sieci handlowe coraz więcej inwestują w zabezpieczenia antykradzieżowe. Zgodnie z kategoryzacją dokonaną przez ekspertów z firmy EEA Checkpoint Systems, najpopularniejsze systemy zabezpieczające towary w polskich sklepach można podzielić na kilka rodzajów:

- elektroniczne systemy antykradzieżowe (EAS), do których należą bramki sygnalizujące wynoszenie towaru poza teren sklepu, a także etykiety i klipsy dołączane np. do odzieży;
- telewizja przemysłowa (CCTV); mogą to być zarówno proste systemy złożone z kilku kamer, jak i kompleksowe rozwiązania zintegrowane z kasami fiskalnymi (np. CheckView);
- mechaniczne systemy pętlowe, często wyposażone w zasilanie zabezpieczanych urządzeń prądem, stosowane m.in. w sklepach RTV;
- przezroczyste pudełka, w których umieszcza się np. kosmetyki czy płyty CD.

Nowoczesne sposoby zabezpieczania towarów przed kradzieżą mają w przyszłości zaoferować handlowcom kompleksowe rozwiązania, które będą nie tylko informować

[7] R. Hayes, C. Cardone, *op. cit.*; P. C. Nemeth, *op. cit.*

o kradzieży, ale również ułatwiać zakupy i analizować zachowania konsumentów. Od pewnego czasu na Zachodzie stosowane są zabezpieczania towarów implementowane już na etapie produkcji. Pozwala to kontrolować koszty związane ze stratami powstającymi już podczas transportu. Etykiety radiowe umożliwią stworzenie „inteligentnych sklepów", w których kasy staną się zbędne, a wartość produktów w koszyku obliczona zostanie po przejściu przez specjalną bramkę[8].

Na osobne omówienie zasługuje zjawisko tzw. detektywów sklepowych. To instytucja w Polsce dość nowa, na Zachodzie natomiast z powodzeniem funkcjonująca od lat. Detektyw sklepowy to osoba odpowiednio przeszkolona i wyposażona w specjalistyczne narzędzia czy urządzenia nadawczo-odbiorcze, działająca na terenie sklepu na ogół anonimowo, której zadaniem jest odpowiednio wczesne wychwycenie potencjalnego złodzieja spośród klientów i odpowiednia reakcja. Oczywiście współpracuje on z personelem oraz innymi służbami bezpieczeństwa operującymi na terenie obiektu handlowego. Detektyw sklepowy pełni rolę głównie prewencyjną. Aktywna obserwacja, natychmiastowa reakcja, odstraszanie potencjalnego amatora cudzej własności – to podstawowe jego funkcje. Gdy są one realizowane z pełnym sukcesem i stanowczością, ryzyko handlowe, jakie ponosi przedsiębiorca, jest wówczas minimalne. Często zatrudnienie wykwalifikowanej kadry do spraw bezpieczeństwa jest znacznie bardziej opłacalne niż zgoda na dopuszczalne straty, zwłaszcza w dużych obiektach handlowych. Detektyw jest także swoistym łącznikiem pomiędzy klientem, personelem, kadrą zarządzającą i menadżerską, a także organami ścigania. Musi znać również wszystkie procedury finansowe i rejestracyjne towarów obowiązujące w firmie, techniki komunikacji, podstawy prawa dowodowego oraz posiadać szeroką wiedzę ściśle powiązaną z procesem zapewnienia bezpieczeństwa wewnętrznego sklepu[9].

Jego zadaniem jest nie tylko uważna obserwacja i kontrola, ale także rola trenera i aktywizacja całego personelu w dążeniu do wspólnego dobra, jakim jest bezpieczeństwo pracy. Musi ponadto znać zespół metod, jakimi posługują się nieuczciwi klienci (katalog ten jest bardzo szeroki), techniki wnikliwej obserwacji, analizy ludzkich zachowań w szczególnych sytuacjach, a także posiadać wiedzę z zakresu negocjacji i prezentować wysoką kulturę osobistą[10].

Jednocześnie trzeba pamiętać, iż żadnemu z pracowników ochrony nie przysługuje prawo do zatrzymania sprawcy z wykorzystaniem przymusu fizycznego ani też prawo do przeszukania. Do tych czynności uprawniona jest jedynie policja, którą służby ochrony mają obowiązek wezwać natychmiast po stwierdzeniu podejrzenia dokonania kradzieży[11].

Ciekawym programem strategicznym osiągania celów zapewnienia bezpieczeństwa w przedsiębiorstwie jest tzw. POP FORMULA. Obejmuje ona sprzężone ze sobą 3 płaszczyzny porozumienia: polityka (wskazanie, co chce osiągnąć kadra kierownicza, propagowanie otwartej polityki wiedzy za pomocą edukacji personelu), cele (dlaczego chcą osiągnąć takie, a nie inne cele – przekazywanie informacji zwrotnej ze zrozumieniem) i procedury (jak cel może stać się rzeczywistością poprzez odpowiednie szko-

[8] http://www.rp.pl/artykul/159741.html (15.09.2008).

[9] R. Hayes, *Store detectives and loss prevention* [in:] *The Handbook of Security*, ed. M. Gill, Boston 2006.

[10] P. C. Nemeth, *op. cit.*

[11] http://hipermarkety.republika.pl/50_kradnie.html (15.09.2008).

lenia). Współzależność tych płaszczyzn tworzy nierozerwalną sferę porozumienia pomiędzy personelem a kadrą zarządzającą, co prowadzi ostatecznie do wypracowania wspólnej polityki bezpieczeństwa[12].

Podsumowując, aby osiągnąć zamierzony cel, jakim jest zlikwidowanie lub co najmniej minimalizacja zjawiska kradzieży w centrach handlowych spełnione muszą być jednocześnie następujące warunki:

1) sprawna i bezkompromisowa polityka bezpieczeństwa obiektu handlowego oparta na sprawdzonych wzorcach;
2) ścisła współpraca pomiędzy sieciami handlowymi celem eliminacji wspólnych zagrożeń;
3) ponoszenie adekwatnych nakładów finansowych na zapewnienie bezpieczeństwa (nabór do służby w ochronie, polityka prewencyjna, szkolenia dla personelu wszystkich szczebli, stosowanie mechanicznych zabezpieczeń itp.);
4) współpraca sieci sklepowych z organami ścigania i wypracowywanie wspólnej polityki bezpieczeństwa;
5) zmiany w przepisach karnych tak, aby traktowały kradzież jako przestępstwo bez względu na wartość przywłaszczonego mienia;
6) konsekwentne, wspólne i bezpośrednie współoddziaływanie przez przedsiębiorstwa handlowe na instytucje państwowe służące zwalczaniu przestępczości (podobnie jak to ma miejsce np. wśród producentów nagrań fonograficznych, w którym to środowisku polityka zapewnienia ochrony własności intelektualnej ma fundamentalne znaczenie i jest bardzo restrykcyjnie przestrzegana).

Największe zagrożenie spośród wszystkich kategorii złodziei sklepowych niosą ze sobą zorganizowane grupy przestępcze. Nie ma oficjalnych danych liczbowych, które obrazowałyby skalę strat finansowych sieci handlowych spowodowanych przez tego rodzaju organizacje, jednak można przypuszczać, że ich udział procentowy w ogólnej liczbie kradzieży jest znaczący. Za przyczyny takiego stanu rzeczy można uznać z pewnością ich wysoki stopień zorganizowania, świadomość prawną, doskonałą znajomość i perfekcyjne opracowanie różnorodnych metod kradzieży, bezwzględność w dążeniu do zamierzonego celu oraz ekonomiczną determinację. Najgorsze jest jednak to, iż tak zdobyte fundusze inwestowane są przez te grupy w przedsięwzięcia znacząco groźniejsze dla bezpieczeństwa ogólnego niż powodowanie strat finansowych, czyli handel narkotykami, prostytucję, nielegalny obrót bronią czy też budowanie fikcyjnych instytucji, których zadaniem jest „pranie brudnych pieniędzy". Dlatego tak ważne jest, aby organy ścigania były bezwzględne w egzekwowaniu prawa i prowadziły konsekwentną politykę eliminacji nielegalnego handlu skradzionymi towarami.

Osiągnięcie poziomu tzw. optymalnego bezpieczeństwa nie jest zadaniem łatwym, jednakże, przy sprawnej kooperacji wszystkich zainteresowanych stron, jak najbardziej możliwym do zrealizowania.

[12] A.C. Sennewald, *Effective Security Management*, Amsterdam 2000.

Bibliografia

Nemeth P.C., *Private Security and the Investigative Process*, Butterworth Heinemann, Boston 2000.
Sennewald A. C., *Effective Security Management*, Butterworth Heinemann, Amsterdam 2000.
Hayes R., *Store detectives and loss prevention*, [in:] *The Handbook of Security*, ed. M. Gill, Palgrave Macmillan, Boston 2006.
Hayes R., Cardone C., *Shoptheft*, [in:] *The Handbook of Security*, ed. M. Gill, Palgrave Macmillan, Boston 2006.
Krasnovsky T., Lane R. C., *Shoplifting: A Review of the Literature*, Vol. 3, „Aggression and Violent Behavior" 1998.
Ustawa z dnia 6 czerwca 1997 r. Kodeks karny, Dz.U. z 1997 r., Nr 88, poz. 553.
Ustawa z dnia 20 maja 1971 r. Kodeks wykroczeń, Dz.U. z 1971 r., Nr 12, poz. 114.

Strony internetowe:
http://www.rp.pl/artykul/159741.html (15.09.2008).
http://hipermarkety.republika.pl/50_kradnie.html (15.09.2008).
www.rp.pl/artykul/102681,127342 (15.09.2008)

Szczególne podziękowania dla pana Henryka Klechy za pomoc w tworzeniu niniejszego artykułu.

Mieczysław Morawski
Wojciech Topczewski

Wpływ wiedzy agenta ubezpieczeniowego na bezpieczeństwo ubezpieczeniowe klientów

Wprowadzenie

Od początku lat dziewięćdziesiątych, gdy zaczęła obowiązywać Ustawa o działalności ubezpieczeniowej[1], siłą rzeczy przemianom podlegał również cały rynek finansowy, a w szczególności także ubezpieczeniowy. Od momentu wprowadzenia przez wymienioną ustawę nowych rozwiązań systemowych, towarzystwa ubezpieczeniowe rozpoczęły działalność na rynku polskim. Od tego czasu powstało zapotrzebowanie na nowy zawód – agenta ubezpieczeniowego. Agenci ubezpieczeniowi (pośrednicy ubezpieczeniowi) stanowią część składową rynku ubezpieczeniowego obok różnego rodzaju stowarzyszeń i organizacji, biorących udział w obrocie ubezpieczeniowym, instytucji zewnętrznych oraz innych usługodawców wspomagających ten rynek[2]. To agenci ubezpieczeniowi penetrują rynek ubezpieczeniowy, docierając do pojedynczych klientów. To oni również próbują ożywić rynek ubezpieczeń grupowych. Działania te wpływają bezpośrednio na zaspokajanie potrzeb i bezpieczeństwa ubezpieczonych.

Dnia 1 stycznia 2004 r. weszła w życie nowa Ustawa o pośrednictwie ubezpieczeniowym, która doprecyzowała zasady wykonywania pośrednictwa ubezpieczeniowego w zakresie ubezpieczeń osobowych i majątkowych[3]. Dzięki tym regulacjom usankcjonowana została, pozostająca nadal w rękach kadry zarządzającej towarzystwami ubezpieczeniowymi, merytoryczna strona przygotowania agentów ubezpieczeniowych w zakresie zarówno wiedzy fachowej, jak i praktyki. Najważniejszym ogniwem w sprzedaży ubezpieczeń pozostali agenci ubezpieczeniowi.

Agent ubezpieczeniowy jako kluczowa postać w zapewnieniu bezpieczeństwa finansowo-ubezpieczeniowego klienta

Aby dokonać identyfikacji i personifikacji swoich klientów, należy prowadzić badania ich motywacji zakupu i stwarzać warunki dla nawiązania bliższego wzajemnego kontaktu. Pośrednicy ubezpieczeniowi odgrywają tutaj bardzo istotną rolę, stając się

[1] Ustawa z 28 lipca 1990 r. o działalności ubezpieczeniowej (Dz.U. Nr 50, poz. 344).

[2] H. Worach-Kardas, *Ubezpieczenia społeczne i na życie. Stan i perspektywy*, Łódź 2004, s. 151.

[3] Ustawa z 22 maja 2003 r. o pośrednictwie ubezpieczeniowym (Dz.U. Nr 124, poz. 1154).

doradcami finansowymi, jako profesjonaliści dobrze znający potrzeby konkretnych, obsługiwanych przez siebie, a zarazem zidentyfikowanych przez firmę klientów. Świadomość ubezpieczeniowa wśród pracowników i agentów zakładów ubezpieczeń, a także wśród klientów jest coraz wyższa. Agenci ubezpieczeniowi muszą uczestniczyć w szkoleniach z zakresu umiejętności sprzedażowych (techniki sprzedaży, proces sprzedaż, analizy potrzeb klienta itp.), po to, by móc zaspokoić potrzeby klienta zarówno pod względem ubezpieczeń, jak i finansów.

W centrum uwagi muszą się znaleźć potrzeby klienta, który na ogół domaga się natychmiastowej, zindywidualizowanej i kompleksowej obsługi. Warto pamiętać, że praktycznie żaden klient nie pogodzi się z brakiem kompetencji usługodawcy, mając nieograniczony wybór i możliwość porównywania konkretnych ofert lub rozwiązań oraz standardów stosowanych gdzie indziej. Wymagania współczesnego klienta rosną szybciej niż kiedykolwiek wcześniej. Oczekuje on profesjonalnych standardów oferowanego produktu, obsługi i serwisu. Jeśli stwierdzi, że konkurencja wypada lepiej, bez wahania zmieni dostawcę usługi. Przy czym wymaga on nie tylko wysokich standardów związanych z istotą produktu, ale także życzliwości, uprzejmości, a nawet troski o jak najlepsze zaspokojenie swoich indywidualnych preferencji. Do osiągania satysfakcjonujących wyników współpracy z klientami potrzeba bowiem silnie umotywowanych, zaangażowanych i kompetentnych pracowników, których zapał i entuzjazm oparte na rzetelnym, merytorycznym przygotowaniu będą z kolei budować zaangażowanie klientów. Dobry, odpowiednio merytorycznie przygotowany pracownik przyciąga zwykle dobrego, rentownego klienta. Nawet najlepszy produkt ubezpieczeniowy nie sprzeda się sam, musi mu towarzyszyć pracownik – ekspert czy konsultant, na bieżąco analizujący i odpowiadający na pytania klienta. Stan niewiedzy jest szczególnie widoczny w procesie świadczenia usług, gdy odbiorca oczekuje fachowej rady, rzetelnej i aktualnej informacji, szybkiej i skutecznej zdolności rozwiązywania bieżących problemów.

W tym kontekście, aby agent ubezpieczeniowy mógł być skuteczny w działaniu, musi posiadać odpowiednie kompetencje. Obecnie kompetencje należy rozumieć bardzo szeroko, jako „wszelkie cechy pracowników, które używane i rozwijane w procesie pracy prowadzą do osiągnięcia rezultatów zgodnych ze strategicznymi zamierzeniami przedsiębiorstwa"[4].

Postulowane kompetencje agenta przedstawia rysunek 1.

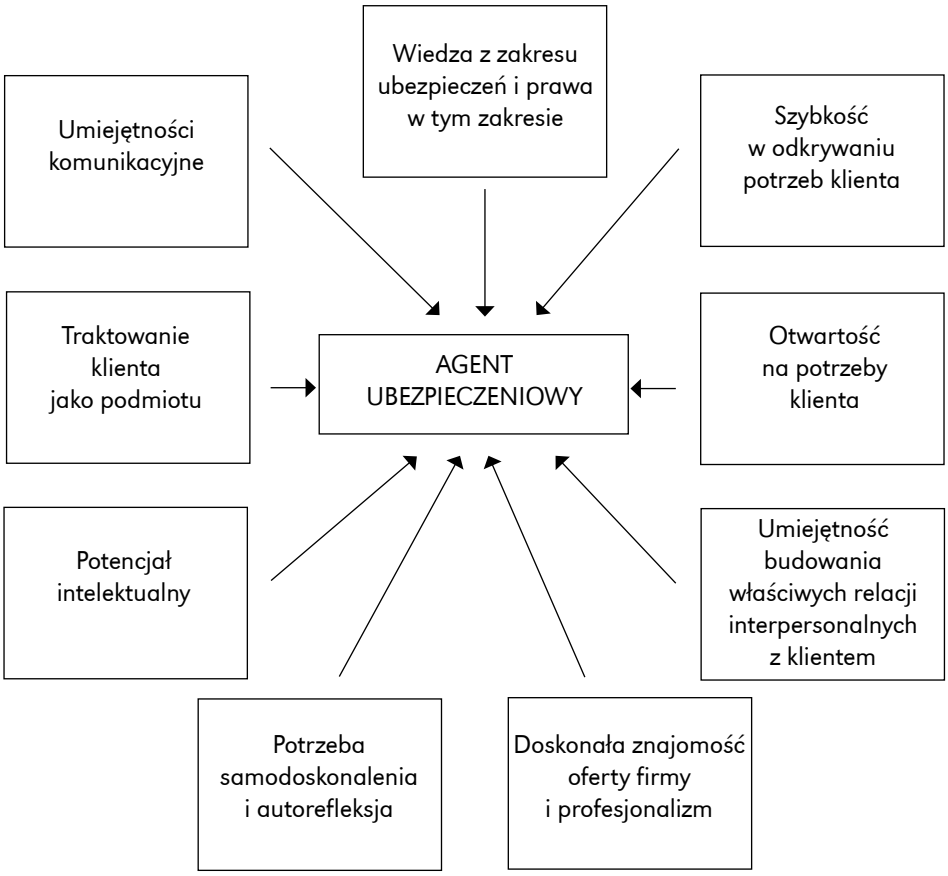
Powrót do oczekiwań klientów oraz możliwości ich spełnienia wydaje się aspektem podstawowym. Agent ubezpieczeniowy musi być dobrze przygotowany do nowej rzeczywistości. Potrzebni są agenci myślący, przewidujący, kreatywni i samodzielni. Zamiast usiłować sprzedawać, z różnym skutkiem, agent ubezpieczeniowy musi przede wszystkim nawiązywać dobre stosunki z klientem, musi doradzać. Aby spełnić te założenia, oprócz szkoleń, które organizowane są przez firmy ubezpieczeniowe, osoby pracujące w zawodzie agenta ubezpieczeniowego powinny cały czas angażować się w procesy samokształcenia, studiowania fachowej literatury związanej z zagadnieniami ubezpieczeniowymi oraz prasy[5]. Agenci ubezpieczeniowi powinni utożsamiać się z wizją i misją firmy zamiast manipulować klientem. Powinni oni przyzwyczaić się

[4] T. Oleksyn, *Zarządzanie kompetencjami*, Kraków 2006, s. 18.

[5] F.K. Reilly, K.C. Brown, *Analiza inwestycji i zarządzanie portfelem*, Warszawa 2001.

do coraz szybszego uczenia się rzeczy nowych[6]. Ważne jest, aby swoją postawą umieli pokazać, że klient, który powierza im ochronę swojego życia i mienia, miał poczucie bezpieczeństwa i chciał polecać ich obsługę innym.

Rysunek 1. Kompetencje skutecznego agenta ubezpieczeniowego



Źródło: opracowanie własne na podstawie J.M. Fijor, *Metody zdobywania klientów, czyli jak osiągnąć sukces w sprzedaży;* C.K. Prahalad, V. Ramaswamy, *Przyszłość konkurencji*, Warszawa 2005.

Wiedza agenta ubezpieczeniowego jako wykładnik bezpieczeństwa w ubezpieczeniach

W związku z rozwojem rynku ubezpieczeń, firmy działające w ramach tej branży zaczęły kierować swoją uwagę na pozyskiwanie i rozwój wiedzy swoich współpracowników. Wiedza agentów ubezpieczeniowych zaczyna odgrywać kluczową rolę w stra-

[6] E. Geffroy, *Clienting*, Warszawa 1996.

tegii działania firm ubezpieczeniowych. Agenci powinni posiadać wykształcenie co najmniej średnie, związane z ekonomią, prawem itp. Umiejętne zarządzanie kapitałem intelektualnym staje się dziś koniecznością dla każdej firmy ubezpieczeniowej, która chce przetrwać i być konkurencyjna dla innych firm. W związku z powyższym, istnieje żywa potrzeba ciągłego kształcenia agentów ubezpieczeniowych.

Autorzy niniejszego opracowania przeprowadzili badanie w firmach ubezpieczeniowych (próba 115 agentów ubezpieczeniowych różnych firm) dotyczące uszeregowania przejawów kwalifikacji agenta. Agenci ubezpieczeniowi jako najważniejsze zagadnienia wskazali umiejętność wyjaśnienia problematyki ubezpieczeniowej, jak również rozwiązywania problemów klienta. Chcą oni umiejętnie doradzać, jak również posiadać umiejętności komunikacyjne. Jako mniej ważne postrzegają osiągnięcia w dziedzinie ubezpieczeń, jak również tytuł i stopień naukowy. Wyniki badań przedstawia tabela 1.

Tabela 1. Ranking składowych kompetencji agenta ubezpieczeniowego

Proszę uszeregować w skali od 1 – najważniejsze do 12 – najmniej ważne Pani/Pana zdaniem niżej wymienione przejawy kwalifikacji agenta ubezpieczeniowego	
wyjaśnianie problematyki ubezpieczeniowej	1
rozwiązywanie problemów klienta	2
doradzanie	3
umiejętności komunikacyjne	4
doświadczenie w zawodzie agenta	5
tworzenie relacji opartych na zaufaniu	6
dyspozycyjność	7
wiedza produktowa	8
wykształcenie	9
osiągnięcia w dziedzinie ubezpieczeń	10
tytuł zawodowy	11
stopień / tytuł naukowy	12

W wyniku dokonanych badań nasuwają się różne spostrzeżenia. Mianowicie, zarządzanie wiedzą wszystkich pracowników może nie tylko zwiększyć efektywność towarzystwa ubezpieczeniowego, ale także może wpłynąć na poprawę jego innowacyjności i wzrost satysfakcji klienta. Główną funkcją systemu zarządzania wiedzą jest dostarczanie agentowi informacji, która po odpowiednim przetworzeniu zostanie efektywnie wykorzystana. Wiedza pozwala przewidywać, kojarzyć fakty i podejmować decyzje. Duża konkurencja na rynku ubezpieczeń (obecnie 36 firm ubezpieczeń na życie i 36 firm ubezpieczeń majątkowych)[7] spowodowała, że towarzystwa ubezpieczeniowe skupiły swoją uwagę na ciągłym poszerzaniu oferty, dodając różnorodne świadczenia oraz kalkulując możliwie niskie koszty własne, a także koszty ryzyka ubezpieczeniowego. Oczekiwano, iż skupienie uwagi na produkcie doprowadzi do wzrostu sprzedaży ubezpieczeń. Rozwiązywanie problemów klienta prowadzi również do prze-

[7] www.money.pl/ubezpieczenia (czerwiec 2008).

kazania sygnału, iż jest on dobrze zabezpieczony. W chwili gdy nowy agent rozpoczyna pracę samodzielnie, zaczyna tworzyć wiedzę indywidualną oraz współprzyczyniać się do tworzenia zbiorowej wiedzy organizacyjnej. W momencie odejścia z firmy ubezpieczeniowej zabiera on bezpowrotnie swoją wiedzę indywidualną, której ani firma, ani menedżerowie nie są w stanie odebrać i zatrzymać. Dla towarzystw ubezpieczeniowych o wysokim współczynniku rotacji kadr stanowi to poważne zagrożenie. W związku z powyższym, oprócz samego zarządzania wiedzą, potrzebna jest kontrola, a także umiejętne zarządzanie wiedzą chronioną i przepływem informacji.

Problemy implementowania bezpieczeństwa ubezpieczeniowego w towarzystwach ubezpieczeń

W kontekście pobierania wiedzy oraz jej wykorzystania w towarzystwach ubezpieczeniowych, nie można zapominać o dwóch problemach stanowiących, że:
1) zgromadzona w bazie wiedza nie zawiera informacji o relacjach zachodzących między danymi, faktami itp.;
2) informacje poufne zanikają tak dla wewnętrznych, jak i zewnętrznych użytkowników wiedzy.

Jednymi z kluczowych dóbr zgromadzonych w każdym przedsiębiorstwie, w tym również w firmie ubezpieczeniowej, są szeroko pojęte zasoby wiedzy. Można je podzielić na dwie kategorie:
1) zasoby materialne: dokumentacja, procedury firmowe, informacje o rynku, raporty, wyniki prac badawczo-rozwojowych, zawartość baz danych;
2) zasoby niematerialne: umiejętności, doświadczenie, indywidualna wiedza agentów, wiedza na temat przebiegu procesów sprzedaży, nieutrwalone w żadnej formie informacje o przedsiębiorstwie, wiedza o konkurencji czy rynku.

Według jednej z teorii[8], zarządzanie wiedzą często mylone jest z zarządzaniem informacją. Jej autor uważa, że konieczne jest wyróżnienie następującej triady: dane – informacje – wiedza. Dane dotyczą zjawisk samych w sobie; mają one charakter wysoce sterylny, źródłowy oraz nieprzetworzony. Informacje – to dane przetworzone w sposób strukturalizowany, wiedza zaś stanowi psychologiczne, indywidualne doświadczenie będące wynikiem intelektualnej refleksji teoretycznej nad bytami realnymi lub abstrakcyjnymi.

Innymi cechami wiedzy są[9]:
- niemożność przechowywania,
- nietransferowalność,
- wieloznaczeniowość interpretacyjna,
- możność tworzenia jej z wykorzystaniem różnorodnych procedur i metod.

Wykorzystując teorie i definicje, menedżerowie firm ubezpieczeniowych muszą zadbać o to, by informacje przekazywane były agentom w sposób kompetentny i zrozumiały. Agenci z kolei muszą przekazywać klientom informacje w sposób czytelny tak,

[8] K. Perechuda, *Dyfuzja wiedzy w przedsiębiorstwie sieciowym*, Wrocław 2005, s. 51.

[9] *Ibidem*.

aby nie budziły one obaw. Autorzy przeprowadzili badanie na klientach firm ubezpieczeniowych, w których wyodrębniono trzy grupy:

Grupa I (35 osób) – klienci z liczbą ubezpieczeń powyżej 3, z wysoką lokatą (powyżej 100 000,00 zł) lub/i wysoką sumą ubezpieczenia (powyżej 100 000,00 zł) tzw. VIP,

Grupa II (34 osoby) – klienci z liczbą 1–3 ubezpieczeń, lokaty 30 000–100 000 zł, suma ubezpieczenia również 30 000–100 000 zł – tzw. klienci „średni",

Grupa III (35 osób, bez nazwy) – klienci poniżej podanych wskaźników.

W wyniku badań okazało się, że Grupa I jako najważniejsze informacje, które chciała uzyskach od agentów, wskazała sposób inwestowania oraz wartość ich środków, a jako najmniej ważne – informacje o firmie. Grupa średnia oprócz wartości swoich środków, interesowała się informacją, jak one wpływają. Wyniki badań w Grupie III były identyczne jak w Grupie I (tab. 2).

Tabela 2. Ranking stopnia ważności informacji dla klienta

Jakich aktualnych informacji obecnie oczekuje Pani/Pan od firmy ubezpieczeniowej? Proszę ułożyć od najważniejszej – 1, do najmniej ważnej – 6.			
	Grupa I	Grupa II	Grupa III
wartość polisy	2	1	2
sposób inwestowania	1	3	1
jak wpływają składki	3	2	3
informacje o nowych produktach	4	4	4
informacje o firmie	5	5	5
inne	6	6	6

Główny wniosek, który nasuwa się w wyniku przeprowadzonych badań, to fakt, że bez względu na zasobność portfela klienci dla własnego bezpieczeństwa ubezpieczeniowo-finansowego dużą uwagę zwracają na informacje o sposobie inwestowania oraz dotyczące wartości zgromadzonych przez nich środków. Obecnie, gdy sytuacja na giełdzie jest niestabilna, agenci muszą ciągle obserwować rynek finansowy, muszą również umiejętnie kreować „portfel" klienta, tzn. reagować na każde pytanie z jego strony i potrafić udzielić na nie informacji. Z badań wynika również, że klientom bardziej zależy na prowadzeniu już zawartych ubezpieczeń, a mniej interesują się nowymi produktami.

Niestety, w swojej działalności marketingowej towarzystwa ubezpieczeniowe zagubiły zdezorientowanego klienta. A przecież to właśnie klient, jako główny podmiot oddziaływań ubezpieczeniowych powinien stanowić kluczowe ogniwo dla podniesienia sprzedaży ubezpieczeń na życie. Prowadzenie polityki inwestycyjnej towarzystw ubezpieczeniowych przez osoby niewykwalifikowane może okazać się brzemienne w skutkach dla klientów oraz dla samych towarzystw ubezpieczeniowych. Już dzisiaj obserwuje się spadek sprzedaży ubezpieczeń na życie, a przez to spada zainteresowanie ubezpieczeniami w ogóle. Czasy masowego klienta bezpowrotnie minęły. Dzisiaj i w przyszłości „klient masowy" to klient chcący się wyróżniać i żądający indywidual-

nego podejścia[10]. Wydaje się, że sytuowanie klienta w centrum uwagi, a więc postrzeganie go jako podmiotu transakcji, może doprowadzić do wzrostu zainteresowania produktami ubezpieczeniowymi. Dzięki temu klienci będą mogli obserwować wszelkie zmiany, jakie zachodzą w danej firmie ubezpieczeniowej, w proponowanych produktach ubezpieczeniowych, będą mogli dzielić się swoimi uwagami, pomysłami i propozycjami ulepszeń tych produktów. Aby możliwa była rzetelna współpraca między konsumentem a agentem, przejawiająca się przede wszystkim stałym przekazywaniem klientowi wiedzy, dającej poczucie bezpieczeństwa, komfortu psychicznego i zadowolenia, trzeba zwrócić uwagę na kompetencje agenta ubezpieczeniowego. Ich podstawą jest **rzetelna wiedza**, nieustannie poszerzana o nowe istotne wiadomości, **interpersonalne umiejętności kooperacji** z klientem oparte na otwartej komunikacji, dostępności i budowaniu indywidualnych, wręcz osobistych relacji, a także **osobiste predyspozycje**, które powinno się i trzeba w sobie rozwijać, by móc okazywać usługobiorcy życzliwość, troskę i autentyczną serdeczność.

Podsumowanie

Od momentu transformacji (początek 1991 roku) towarzystwa ubezpieczeniowe działały bardzo schematycznie – proponowały ubezpieczenia, unowocześniały je w trakcie zdobywania rynku, by trafić do większej liczby klientów. Od samego początku działania tych firm kluczowe zadania spełniali pośrednicy ubezpieczeniowi zwani doradcami ubezpieczeniowymi lub agentami ubezpieczeniowymi. W wyniku różnych czynników gospodarczych, na początku 2000 roku sprzedaż ubezpieczeń zaczęła spadać. Ważnym zatem czynnikiem poprawiającym koniunkturę rynku ubezpieczeniowego powinno być, oprócz podstawowych form marketingu, zarządzanie wiedzą. Tworzenie bazy klientów oraz informacji o ich potrzebach przyczyni się do poprawnej obsługi dotychczasowych klientów oraz pozyskiwania nowych[11]. Agenci ubezpieczeniowi muszą dbać o dobro klienta poprzez fachowe doradztwo, jak również dobry serwis. Dobra, fachowa obsługa powoduje wzrost zaufania do towarzystwa ubezpieczeniowego oraz poczucie bezpieczeństwa z tytułu współpracy z tym towarzystwem. Agent ubezpieczeniowy, mimo wielu zabiegów prowadzenia ubezpieczeń w formie *direct*, w dalszym ciągu pozostał najważniejszym ogniwem sprzedaży ubezpieczeń.

Bibliografia

Fijor J.M., *Metody zdobywania klientów, czyli jak osiągnąć sukces w sprzedaży*, Polskie Wydawnictwa Ekonomiczne, Warszawa 2005.

Geffroy E., *Clienting*, Agencja Wydawnicza Placet, Warszawa 1996.

[10] F. Mroczko, W. Topczewski, *Wykorzystanie wiedzy i umiejętności agenta ubezpieczeniowego w nowych warunkach rynku ubezpieczeń na życie*, [w:] P. Laskowski, M. Morawski, *Zarządzanie wiedzą i informacją w przedsiębiorstwie i jednostce samorządu terytorialnego*, Wałbrzych 2004.

[11] T. Szumlicz, *O kształtowaniu świadomości ubezpieczeniowej*, [w:] T. Kopczyńska, S. Nowak, *Ubezpieczenia w polskim obszarze rynku europejskiego. Wyzwania i oczekiwania*, Warszawa 2003.

Mroczko F., Topczewski W., *Wykorzystanie wiedzy i umiejętności agenta ubezpieczeniowego w nowych warunkach rynku ubezpieczeń na życie*, [w:] P. Laskowski, M. Morawski, *Zarządzanie wiedzą i informacją w przedsiębiorstwie i jednostce samorządu terytorialnego*, Wałbrzyska Wyższa Szkoła Zarządzania i Przedsiębiorczości, Wałbrzych 2004.
Oleksyn T., *Zarządzanie kompetencjami*, Oficyna Ekonomiczna, Kraków 2006.
Perechuda K., *Dyfuzja wiedzy w przedsiębiorstwie sieciowym*, Wydawnictwo Akademii Ekonomicznej im. Oskara Langego we Wrocławiu, Wrocław 2005.
Prahalad C.K., Ramaswamy V., *Przyszłość konkurencji*, Polskie Wydawnictwa Ekonomiczne, Warszawa 2005.
Reilly F.K., Brown K.C., *Analiza inwestycji i zarządzanie portfelem*, Polskie Wydawnictwo Ekonomiczne, Warszawa 2001.
Szumlicz T., *O kształtowaniu świadomości ubezpieczeniowej*, [w:] T. Kopczyńska, S. Nowak, *Ubezpieczenia w polskim obszarze rynku europejskiego. Wyzwania i oczekiwania*, Oficyna Wydawnicza BRANTA, Warszawa 2003.
Ustawa z 28.07.1990 r. o działalności ubezpieczeniowej (Dz.U. nr 50, poz. 344).
Ustawa z 22.05.2003 r. o pośrednictwie ubezpieczeniowym (Dz.U. nr 124, poz. 1154).
Worach-Kardas H., *Ubezpieczenia społeczne i na życie. Stan i perspektywy,* Wydawnictwo Wyższej Szkoły Humanistyczno-Ekonomicznej w Łodzi, Łódź 2004.

Strona internetowa:
www.money.pl/ubezpieczenia (czerwiec 2008).

Agnieszka Thier

Woda na wagę złota, czyli o współczesnym problemie bezpieczeństwa wodnego w skali globalnej

Ile kosztuje woda? Pytanie trywialne, można powiedzieć, po co w ogóle o to pytać, skoro przyzwyczajeni jesteśmy do tego, że woda jest i należy się każdemu. Czasem tylko złościmy się, kiedy nagle wskutek awarii następuje przerwa w jej dostawie. Co by jednak było, gdyby nagle woda przestała być dostarczana, gdyby zabrakło jej w naszych kranach? Zwykle nie zastanawiamy się nad tym bardzo istotnym faktem, kiedy odkręcamy kurek w umywalce lub polewamy się rzęsistym strumieniem pod prysznicem, a szkoda. Niestety w wielu miejscach naszego globu widok płynącej z kranu wody jest tylko marzeniem, za którego realizację zapłacono by niejedną sztabkę złota. Większość z nas traktuje wodę jako coś, co było, jest i będzie. To efekt przyzwyczajenia, który przysłania świadomość pewnych problemów – to jego wada zasadnicza. Korzystając z łazienki czy kuchni, zapewne niewielu pokusiło się o refleksję, ile w tym czasie zostało zużytej wody, ile to kosztowało?[1] Autorka zakłada, że takie myśli nie towarzyszą ludziom w życiu codziennym. Większość z nas nawet nie zauważa, że podczas takiej prozaicznej czynności jednorazowo wylewa się zupełnie niepotrzebnie 20, a nawet 30 litrów wody.

W XIX wieku nasi przodkowie gorliwie poszukiwali złota, w wieku XX takim złotem była i nadal jest ropa, określana przez niektórych jako czarne złoto. O nią też nierzadko wybuchały różnego rodzaju konflikty, które pochłonęły miliony istnień ludzkich. Dobrym przykładem są tutaj wojny w Iraku, Kuwejcie, gdzie jednym z motywów ich inicjowania, czasem skrzętnie przez polityków ukrywanym, jest właśnie chęć pozyskania dostępu do zasobów ropy naftowej. W niedalekiej przyszłości to nie złoto, o które tak zabiegali przedstawiani w westernach bohaterowie, ani też nie czarne złoto, dla zdobycia którego wielu polityków gotowych jest poświęcić tysiące swoich żołnierzy, ale właśnie woda będzie tym prawdziwym złotem, o który toczyć się będą konflikty różnej maści. Za około 50 lat woda w niektórych rejonach świata będzie prawdziwym skarbem. Jednak już teraz z płynącą w kranach wodą, nawet w Polsce, jest problem. Temu właśnie zagadnieniu poświęcony będzie niniejszy artykuł.

W roku 2003 Ogólne Zgromadzenie Narodów Zjednoczonych (ONZ) uroczyście proklamowało Rok Słodkiej Wody. Z tej okazji został także przedstawiony Raport o stanie gospodarki wodnej (*World Water Development Report – WWDR*). Lektura niniejszego raportu autorstwa największych specjalistów w tej dziedzinie napawa uczuciem niepewności o zbliżającą się przyszłość. Dokument ten bowiem stwierdza, że w ciągu najbliższych 20 lat, przeciętna ilość wody przypadająca na jednego miesz-

[1] Zob. http://www.eioba.pl/a75444/woda_na_wage_zlota (07.06.2010).

kańca globu ziemskiego zmniejszy się o jedną trzecią. Zgodnie z raportem, w latach 1970–1990, ilość wody przypadająca na osobę zmniejszyła się o jedną trzecią. Mimo że maleje liczba urodzin, do roku 2050 populacja na świecie i tak osiągnie 9,3 miliarda (w porównaniu do 6,1 w roku 2001). Dalej czytamy, że w ciągu ostatnich 50 lat spożycie wody niemal się podwoiło. Dziecko urodzone w kraju rozwiniętym spożywa od 30 do 50 razy więcej wody niż dziecko pochodzące z kraju rozwijającego się. Według najbardziej pesymistycznych prognoz, do roku 2050, siedem miliardów ludzi w 58 krajach będzie cierpieć z powodu chronicznego niedoboru wody. Według optymistycznych prognoz, będą to około 2 miliardy w 48 krajach. Wynik zależy od następujących aspektów: wzrost populacji, zużycie wody w przemyśle, rolnictwie i gospodarce wodnej, a także od czynników politycznych, społecznych i ekonomicznych. Zgodnie z raportem, wzrost niedoboru wody na świecie będzie w 20% skutkiem zmian klimatycznych. Podczas gdy w rejonach wilgotnych zwiększy się ilość opadów, w rejonach zagrożonych suszą, a nawet na niektórych obszarach tropikalnych i subtropikalnych, opady będą rzadsze i nieregularne. Ulegnie zmianie cykl hydrologiczno-meteorologiczny. Wzrost zanieczyszczeń i temperatury wody spowoduje pogorszenie jakości wody pitnej[2]. Wedle danych zawartych w raporcie, ludzkości grozi katastrofa, u której podstaw znajdował się będzie deficyt zasobów wodnych.

W literaturze przedmiotu pojawiło się nawet pojęcie *Water conflict* – obejmuje ono szereg działań o charakterze politycznym, gospodarczym, ekonomicznym, prawnym, a także militarnym, których celem jest rozwiązanie konfliktu w określonym rejonie świata. U podstaw każdego z tych konfliktów leży niezwykle istotne zjawisko, jakim jest poczucie zagrożenia bezpieczeństwa. Zarówno jednostki, jak i całe społeczności chcą czuć się bezpiecznie – to biologiczno-psychologiczne prawo, a zarazem potrzeba jest właściwe każdemu człowiekowi, tego też niezbywalnego prawa nie należy nikomu odmawiać. W kontekście przywołanych na początku ustaleń raportu, okazuje się, że wobec ludzkości, a dokładniej rzecz biorąc, wobec wybranych obszarów globu ziemskiego groźba zachwiania poczuciem bezpieczeństwa jest realna. Jeśli prognozy podawane w raporcie z 2003 roku się sprawdzą, a nic nie wskazuje na to, że będzie inaczej, świat stanie wobec poważnego problemu: jak poradzić sobie ze stale narastającym poczuciem zagrożenia bezpieczeństwa? Istnieje związek między zmniejszającym się deficytem wody w poszczególnych regionach świata a wzrastającym poczuciem zagrożenia bezpieczeństwa w różnych wymiarach. Związek ten nie ma charakteru tylko apriorycznego, lecz jest tezą potwierdzoną przez empiryczne badania tych rejonów świata. Badania te prowadzone były choćby przez takie instytucje jak ONZ czy Bank Światowy, czy też przez ekspertów z FAO. Omawiany związek można ująć następująco: deficyt zasobów wodnych generuje zaburzenie równowagi bezpieczeństwa w różnych aspektach życia. Kiedy mówimy o bezpieczeństwie, mamy na myśli różne jego wymiary, m.in.: bezpieczeństwo psychologiczne, państwowe, bezpieczeństwo żywnościowe, bezpieczeństwo zdrowotne, bezpieczeństwo związane z miejscem stałego zamieszkania. Mówiąc o bezpieczeństwie, należy uwzględnić wszystkie wymienione aspekty, w przeciwnym razie sprawę można potraktować marginalnie.

W niniejszym artykule problem ten potraktowano ogólnie. Nie chodzi zatem o analizę tego problemu na przykładzie jakiegoś konkretnego państwa, lecz o jego przy-

[2] http://www.unic.un.org.pl/iyfw/raport_gwns.php (07.06.2010).

bliżenie w skali globalnej. Dlatego autorka świadoma jest wielu uproszczeń, które są tutaj konieczne. Nie chodzi również o wyczerpanie tematu ani też o podanie antidotum na zniwelowanie problemu. Chodzi tylko – i może aż tylko – o swego rodzaju diagnozę problemu, aby poprzez to dotarł on do świadomości innych – że jest to problem pierwszorzędny XXI wieku. W artykule zweryfikowano tezy o związku zachodzącym między stale pogłębiającym się deficytem wody a zachwianiem poczucia bezpieczeństwa. Tak zdeterminowana problematyka wyznacza także odnośną strukturę opracowania. Wiadomo bowiem, że zasoby wodne znajdujące się obecnie na świecie nie są rozmieszczone równomiernie. Zadecydowały o tym przede wszystkim czynniki, które odgrywały główną rolę w ewolucyjnym procesie kształtowania się obecnego stanu powierzchni naszej planety oraz cykl hydrologiczno-meteorologiczny. Zasoby wodne są także uwarunkowane geograficznym położeniem różnych kontynentów i krajów. Za taki rozkład można już tylko „winić" samą naturę, która jednym kontynentom stworzyła większe zasoby wody i możliwości korzystania z nich, innym zaś mniejsze. Zgodnie z wynikami badań, największymi zasobami wodnymi dysponuje Azja i Ameryka Południowa. Druga w kolejności jest Ameryka Północna. Jeśli chodzi o pozostałe przedstawione na mapie kontynenty, to cechuje je stopniowy spadek zasobów wodnych. Okazuje się, że Australia i Oceania są tymi regionami, gdzie, ze względu na niski odpływ, zasobów tych jest najmniej[3].

Regiony o najuboższych zasobach wodnych, wedle raportu World Water Development Report, to: Kuwejt (gdzie rocznie na jednego mieszkańca przypada 10 m^3 wody), drugie miejsce zajmuje Rejon Gazy (52 m^3), Zjednoczone Emiraty Arabskie (58 m^3), Wyspy Bahama (66 m^3), Katar (94 m^3), Malediwy (103 m^3), Libia (113 m^3), Arabia Saudyjska (118 m^3), Malta (129 m^3) oraz Singapur (149 m^3). Kraje o najbogatszych zasobach wodnych (wyłączając Grenlandię i Alaskę) to: Gujana Francuska (812,121 m^3 wody przypadających na jednego mieszkańca w skali roku), Islandia (609,319 m^3), Gujana (316,698 m^3), Surinam (292,566 m^3), Kongo (275,679 m^3), Papua Nowa Gwinea (166,563 m^3), Gabon (133,333 m^3), Wyspy Salomona (100,000 m^3), Kanada (94,353 m^3) oraz Nowa Zelandia (86,554 m^3)[4]. Wszystkie te dane w roku 2050 ulegną, wedle prognoz, zmianie.

Jeśli zaś chodzi o Polskę, to należy ona do krajów o małych zasobach wodnych. Średni roczny odpływ wód powierzchniowych (jeziora, rzeki), łącznie z dopływami z zagranicy, w latach 1951–2000 wyniósł 62,4 km^3, w tym z obszaru Polski – 54 km^3. W przeliczeniu na 1 mieszkańca daje to roczny zasób wód ok. 1,6 dam^3 (dam^3 = dekametr sześcienny = 10 m*10 m*10 m = 1000 m^3). W innych krajach europejskich przeciętne zasoby wód powierzchniowych (odpływy) szacowane są na 4,6 dam^3/rok na jednego mieszkańca. Jest to średnio prawie 3 razy więcej wody rocznie na każdego mieszkańca niż w Polsce. Zasoby wodne Polski charakteryzuje duża zmienność sezonowa i nierównomierność rozmieszczenia terytorialnego. Zbiorniki retencyjne mają znikomą pojemność. Mogą zatrzymać tylko 6% rocznego dopływu wód, co nie zapewnia koniecznej ochrony wody przed okresowymi nadmiarami (powodzie), jak też deficytami wody (susze). Na podstawie obecnego stanu badań, ogólna ocena dotycząca ilości i jakości polskich zasobów wodnych jest wysoce niezadowalająca. Wody

[3] J.R. Craig, D.J. Vaughan, B.J. Skinner, *Zasoby ziemi*, Warszawa 2003.

[4] http://www.unic.un.org.pl/iyfw/raport_gwns.php (07.06.2010).

jest mało, ponadto jest ona zanieczyszczona mechanicznie, fizykochemicznie i bakteriologicznie. Zanieczyszczenie to ocenia się jako duże. Co więcej, pobór zasobów wodnych w Polsce stale maleje (z 14 300 hm^3 w 1990 r. do 10 000 hm^3 w roku 2003, co stanowi zmniejszenie aż o 30% w ciągu ostatnich 13 lat). Aktualnie całkowity pobór wody w Polsce jest 3 razy mniejszy niż we Francji, 4-krotnie mniejszy niż w Hiszpanii i Niemczech oraz 5-krotnie mniejszy niż we Włoszech[5].

Nierównomierne rozmieszczenie zasobów wodnych na kuli ziemskiej generuje różnego rodzaju konflikty, które mają charakter polityczny, gospodarczy, ekonomiczny, społeczny i psychologiczny. Ta nierównomierność powoduje także określoną reorientację w polityce gospodarki wodnej, która odpowiedzialna jest za zarządzanie tymi zasobami. Przede wszystkim jednak poznanie tego, jak rozmieszczone są na globie ziemskim zasoby wodne oraz na czym polega ich zużycie i jakie przyczyny decydują o ich deficycie, pozwala na przewidywanie zagrożeń, które ten deficyt niesie ze sobą oraz na skuteczne przeciwdziałanie pojawiającemu się zagrożeniu poczucia bezpieczeństwa. Przejdźmy teraz do omówienia poszczególnych sektorów, gdzie zagrożone jest bezpieczeństwo na skutek deficytu zasobów wodnych.

Bezpieczeństwo psychologiczne

Bezpieczeństwo to pojęcie, które funkcjonuje w wielu sektorach życia. Bliskie jest ono każdemu człowiekowi, gdyż związane jest z jedną z naturalnych potrzeb, jakie człowiek posiada. Bezpieczeństwo rozpatrywane w tym kontekście ma charakter biologiczno-psychologiczny, związane jest z przystosowaniem jednostki do otaczającego ją środowiska oraz zaspokojeniem podstawowych potrzeb[6]. Każdy człowiek chce czuć się bezpiecznie i robi wszystko, by ten stan osiągnąć. Człowiek jako jednostka dąży do zaspokojenia własnych potrzeb – taki obraz ukazuje nam współczesna psychologia. A. Maslow, przedstawiciel psychologii humanistycznej, zaprezentował interesującą hierarchię potrzeb[7]. Po bliższym wglądzie w jej strukturę możemy powiedzieć, że realizacja tych potrzeb służy przede wszystkim bezpieczeństwu jednostki, które to bezpieczeństwo polega, najogólniej mówiąc, na utrzymaniu właściwej homeostazy. Maslow, tworząc teorię potrzeb, inspirował się przemyśleniami szkoły stosunków społecznych Eltona Mayo. Twierdził on, że człowiek w swoim działaniu dąży do zaspokojenia zespołu różnych potrzeb, te zaś potrzeby konstytuują logiczną hierarchię. Na swojej liście amerykański psycholog wymienia m.in. potrzeby związane z poczuciem bezpieczeństwa. Poniżej postaramy się odnieść je do analizowanego w niniejszym opracowaniu problemu i pokazać, w jaki sposób brak zaspokojenia tych potrzeb powoduje wzrost obniżenia się psychologicznego poczucia bezpieczeństwa. Najpierw jednak kilka słów o samej teorii Maslowa i jej funkcjonowaniu.

Zachowanie każdego człowieka określone jest przez 2 prawa: prawo homeostazy i prawo wzmocnienia. Pierwsze mówi o dążeniu do równowagi potrzeb niższego rzędu. Oznacza to, że niezaspokojenie potrzeb niższego rzędu będzie prowa-

[5] http://www.npw.pl/STARE%20NUMERY/2005_01_02/Gospodarka.html (07.06.2010).

[6] Por. K. Obuchowski, *Galaktyka potrzeb*, Warszawa 2007.

[7] A. Maslow, *W stronę psychologii istnienia*, Warszawa 2004; A. Maslow, *Motywacja i osobowość*, Warszawa 2006.

dzić do naruszenia ustalonej równowagi organizmu człowieka, zaś ich zaspokojenie będzie tę równowagę przywracać i stan napięcia zniknie. Natomiast dla potrzeb wyższego rzędu ma zastosowanie prawo wzmocnienia. Zgodnie z tym prawem, zaspokojenie wyższych potrzeb nie powoduje ich zaniku, lecz przeciwnie, byt ludzki odczuwa je jako przyjemne i będzie dążył do ich wzmocnienia. Psychologiczne pojęcie poczucia bezpieczeństwa jest najbardziej podstawowe[8]. Zdaniem Maslowa, jeśli któraś z wyżej wymienionych potrzeb nie zostaje zaspokojona, zaczyna się proces zaburzania równowagi. Proces ten może przybrać rozmiary patologiczne wówczas, gdy większość z potrzeb znajdujących się na zaprezentowanej przez niego liście nie zostaje zaspokojona. Już samo niespełnienie potrzeb fizycznych przez dłuży czas, czyli tych z niższego rzędu, może powodować zaburzenie równowagi życia jednostki. Również środowisko zewnętrzne, które jest biologiczną niszą egzystowania człowieka, może skutecznie przyczynić się do tego, że będzie on miał większe lub mniejsze poczucie bezpieczeństwa.

Potrzeba przeżycia to potrzeba tak z rzędu potrzeb biologicznych, jak i psychicznych. Aby przeżyć w środowisku, konieczne są różne surowce naturalne, w które „matka natura" wyposażyła ziemię w długim procesie ewolucji kosmicznej. Woda jest surowcem zapewniającym przeżycie i zachowanie poczucia bezpieczeństwa w sensie biologicznym i psychologicznym. Można powiedzieć, że stałe i względnie równomierne zaspokajanie potrzeby wody powoduje, że psychologiczne poczucie bezpieczeństwa utrzymuje się w stanie równowagi. Homeostaza zostaje wówczas zachowana. Kiedy natomiast pojawia się problem w postaci ograniczonego dostępu do zasobów wodnych odczuwany przez poszczególne jednostki, wówczas, automatycznie, ograniczenie możliwości zaspokojenia tej potrzeby powoduje wzrost psychologicznego poczucia zagrożenia. Zgodnie z teorią A. Maslowa, homeostaza zostaje zachwiana. Rozmiar tego zagrożenia w razie długotrwałych trudności z zaspokajaniem potrzeby wody może prowadzić do różnych reakcji, określanych przez psychologów jako antyspołeczne. Brak zaspokojenia potrzeby posiadania stałego dostępu do zasobu wody może potęgować u jednostek frustrację oraz wzbudzać zachowania agresywne, z użyciem przemocy fizycznej wobec innych. Psychologiczną oznaką braku poczucia bezpieczeństwa jest przede wszystkim lęk generujący różne typy zachowań. W prostej linii może to prowadzić do powstawania konfliktów w skali nie tylko wewnątrzpaństwowej, ale także międzynarodowej. W celu redukcji zagrożenia psychologicznego poczucia bezpieczeństwa, człowiek od zawsze podejmował różne działania, które można określić jako działania regulacyjno-zachowawcze. Działania te mogą polegać np. na migracji całych grup społecznych w celu poszukiwania wody. Podejmowane działania mogą mieć zarówno charakter pokojowy, jak i destrukcyjny. Ten ostatni może polegać na odbieraniu innym grupom dostępu do zasobów wodnych. Tak silna jest w człowieku potrzeba przetrwania!

Zgodnie z przewidywaniami, należy się spodziewać, że w tych rejonach globu ziemskiego, gdzie wystąpi największy deficyt wodny (mowa o roku 2050), pojawi się również przyrost poczucia zagrożenia bezpieczeństwa psychicznego. Jeśli wierzyć przywołanym wcześniej prognozom, przyrost utraty bezpieczeństwa psychologicznego wystąpiłby najbardziej u mieszkańców niektórych krajów Afryki oraz Azji.

[8] Por. A. Maslow, *W stronę psychologii istnienia*, *op. cit.*

Kraje te bowiem znajdą się w klasie największego deficytu wody i zapaści gospodarki wodnej[9]. Świadomość możliwości zaistnienia takiej sytuacji już dziś powinna motywować opinię międzynarodową do dołożenia wszelkich starań, aby to poczucie bezpieczeństwa zostało w tych rejonach świata choćby w minimalny sposób zapewnione.

Deficyt zasobów wodnych generuje poczucie zagrożenia o życie własne oraz najbliższych. W następnej kolejności, powoduje poczucie zagrożenia bezpieczeństwa związanego ze zdrowiem, uruchamia mechanizm obaw o bezpieczeństwo socjalne i – rzecz jasna – o dach nad głową. Potrzeba ta szczególnie uaktywnia się podczas migracji powodowanych np. suszą czy zniszczeniem naturalnych zasobów wodnych przez ekstremalne zjawiska przyrodnicze. Można powiedzieć, że bezpieczeństwo związane z możliwością stałego dostępu do zasobów wodnych znajduje się na poziomie najbardziej podstawowym. Stąd też ma decydujące znaczenie dla zaspokajania innych potrzeb stojących na wyższych piętrach hierarchii. Trudno przecież wyobrazić sobie realizację np. potrzeby miłości czy przyjaźni bez uprzedniego zrealizowania potrzeby posiadania stałego dostępu do zasobów wodnych.

Bezpieczeństwo państwowe

Kolejnym wymiarem bezpieczeństwa, który zostaje zagrożony na skutek deficytu zasobów wodnych jest rozwój i bezpieczeństwo państwa. Trudno zaprzeczyć, jak bardzo zasoby wodne przyczyniają się do rozwoju państwa i decydują o jego wewnętrznym bezpieczeństwie. Oczywiście rozwój państwa z wykorzystaniem zasobów wodnych uzależniony jest od kilku czynników, zwłaszcza od ilości tych zasobów, położenia geograficznego, które w dużej mierze decyduje o tym, ile dane państwo posiada zasobów wodnych, klimatu oraz cyklu hydrologiczno-meteorologicznego.

Znaczenie zasobów wody we współczesnym świecie jest ogromne i tego nie trzeba dowodzić. Woda wykorzystywana jest niemal w każdym sektorze przemysłu. W różnych procesach produkcyjnych służy ona jako surowiec wchodzący w skład wytwarzanych produktów. Jest ona traktowana jako środek chłodzący urządzenia mechaniczne lub produkty w trakcie ich wytwarzania, a także jako pośrednik w przetwarzaniu energii cieplnej na mechaniczną i elektryczną. Wodę wykorzystuje się także do mycia surowców, półfabrykatów i produktów, służy ona również potrzebom transportowym itd. Ponadto, wodę jako surowiec wykorzystuje się w przemyśle spożywczym, browarniczym i spirytusowym. W pośrednictwie wody w przetwarzaniu energii cieplnej na mechaniczną bądź elektryczną pomocne są urządzenia, w których woda zamieniona w parę porusza tłoki maszyn albo wirniki turbin, a następnie produkuje za pomocą generatorów energię elektryczną. Z kolei w energetyce wodnej woda pełni funkcję czynnika energetycznego, z którego za pośrednictwem turbin i generatorów przetwarza się energię potencjalną lub kinetyczną na elektryczną. Zasoby wodne są więc niewyczerpalnym źródłem energii. Stąd też, można powiedzieć, ma ona przewagę nad innymi źródłami energii, np. węglem czy ropą naftową, których zasoby również ciągle maleją. Ważną własnością zasobów wodnych zwłaszcza płynących w ściekach jest

[9] Por. P. Kowalczak, *Konflikty o wodę*, Poznań 2007.

możliwość ich ponownego odzyskiwania. Dzięki procesom oczyszczania i samooczyszczania można przywrócić im wartości użytkowe.

Skalę wielkości potrzeb wodnych ustala się na podstawie dotychczasowych doświadczeń w użytkowaniu wód w miastach, osiedlach, przemyśle i rolnictwie. Aktualne zużycie wody nie zawsze jest równoznaczne z całkowitym zaspokojeniem wymagań w tym zakresie. Powodem tego jest często brak dostatecznej ilości czystej wody. Nierzadko zły stan zaopatrzenia w urządzenia, które ułatwiają pobór wody zmusza do ograniczenia jej zużycia. Fakt ten w znaczniej mierze ogranicza albo wręcz uniemożliwia gospodarczy rozwój wielu regionów świata. Deficyt zasobów wodnych w odniesieniu do rozwoju państwa ogranicza rozwój każdej jego sfery. Z zasobów wodnych korzysta m.in. przemysł, rolnictwo czy gospodarka komunalna – ograniczenie zasobów powoduje słaby rozwój tych sektorów.

O trudnościach rozwojowych państw z uwzględnieniem zasobów wodnych decyduje kilka czynników. Mają one charakter demograficzny, społeczny, polityczny, prawny, hydrologiczny bądź klimatyczny. Wzrost ludności np. państw afrykańskich powoduje deficyt wody, gdyż obecne już zasoby wskutek ciągłych zjawisk ekstremalnych ulegają zniszczeniu i nie są w stanie zaspokoić potrzeb obecnie żyjących tam ludzi, nie mówiąc już o tych, którzy dopiero mają się narodzić – znaczny wzrost demograficzny w obszarze państw afrykańskich przewidywany jest w XXI wieku. Czynnik demograficzny jest szczególnie akcentowany przez badaczy, jako jedna z przyczyn możliwych konfliktów o wodę. Problem ten występuje przede wszystkim w państwach afrykańskich. Tamtejszy szybki przyrost naturalny powoduje zwiększanie się aglomeracji miejskich, powstawanie tzw. slumsów na obrzeżach miast cechujących się chronicznym brakiem stałego źródła czystej wody. Powoduje to migracje i różnego rodzaju choroby przenoszone przez brudną wodę. Państwa, których nie stać na zorganizowanie sprawnej infrastruktury wodno-kanalizacyjnej borykają się z problemem ścieków zanieczyszczających pozostałości nadających się do wykorzystania zasobów wodnych.

Bezpieczeństwo każdego państwa może zostać zachwiane przez nagłe odcięcie od zasobów wodnych. Woda ma wpływ na różne gałęzie przemysłu także te tzw. strategiczne, które wchodzą w sektor polityki militarnej danego państwa. Oczywiście, świadomość zagrożonego bezpieczeństwa wodnego potęguje wzrost polityki prewencyjnej, której celem jest zapobieganie możliwym zagrożeniom generującym deficyt wody. To jednak nierzadko wymaga olbrzymich środków finansowych, których państwa ubogie, np. Afryka albo kraje rozwijające się, gdzie społeczeństwo jest zbyt spolaryzowane, nie posiadają.

Rozwój rolnictwa uzależniony jest w dużej mierze od naturalnych zasobów wód powierzchniowych i podziemnych. Rolnictwo jest dziedziną zużywającą największe ilości zasobów wodnych w skali globalnej. Wedle danych statystycznych, nawadnianie obszarów rolniczych pokrywa 70% wody zużywanej na ziemi. W wielu krajach rozwijających się nawadnianie wynosi około 95% zużywanych zasobów wodnych. Trzeba podkreślić, że przyszły rozwój gospodarki rolniczej w tych krajach będzie zależał od możliwości utrzymywania, ulepszania oraz rozprzestrzeniania rolnictwa, w którym stosowane jest nawadnianie. Z drugiej strony nieustannie rosnące w rolnictwie zapotrzebowanie na wodę spotyka się ze sprzeciwem ze strony innych regionów domagających się dużych ilości wody, co z kolei może stanowić zagrożenie dla środowiska naturalnego. Rolnictwo, w którym wykorzystuje się techniki na-

wadniające, powoduje zbyt dużą rywalizację, ponieważ zużywa od 70 do 90% wody stosowanej w tych krajach.

Problem ten jest zróżnicowany w zależności od poszczególnych kontynentów. W krajach, gdzie występuje susza, zachodzi konieczność melioryzacji gruntów. Jest to inwestycja droga, na którą wielu państw nie stać, zwłaszcza tych w Afryce. Dlatego tak ważna jest w tej kwestii współpraca międzynarodowa i odpowiednie regulacje prawne. Solidarna współpraca między państwami może w pierwszej kolejności przyczynić się do zagwarantowania bezpieczeństwa wobec możliwych konfliktów o wodę oraz skutecznie organizować akcje pomocy dla tych, którzy dochodzą lub też w przyszłości przejdą do klasy państw cechujących się deficytem zasobów wodnych i zapaścią polityki gospodarki wodnej.

Bezpieczeństwo żywnościowe

Kolejną płaszczyzną bezpieczeństwa, która może ulec zachwianiu przez deficyt zasobów wodnych, jest bezpieczeństwo związane z żywnością. Mogłoby się wydawać, że w XXI wieku – erze techniki i nauki, kiedy na własne oczy obserwujemy rozwój technologii roślin i coraz częściej zasypywani jesteśmy różnymi odmianami żywności genetycznie zmodyfikowanej, nie powinno być na globie ziemskim takiego kraju, w którym panowałby głód i nędza. Nic bardziej mylnego. Media dostarczają nam nierzadko szokujących obrazów, jak z braku pożywienia umierają ludzie, szczególnie drastycznych wówczas, gdy jest to śmieć małych dzieci i to przeważnie na rękach swoich również wycieńczonych z głodu matek. Co jest przyczyną takiego stanu rzeczy? Co powoduje wzrost zagrożenia bezpieczeństwa żywnościowego? Nie zagłębiając się w przyczyny, trzeba powiedzieć, że nie istnieje tylko jeden powód jednoznacznie rozstrzygający o zaistnieniu takiego stanu rzeczy. Przyczyn jest wiele. Są to m.in. warunki klimatyczne, polityczne, zarządzanie gospodarką wodną, nierzadko też przyczyny ideologiczne.

Wedle badań, populacja ludności do roku 2050 ma się zdecydowanie zwiększyć. Przyrost ludności, szczególnie na tych kontynentach, gdzie już teraz występuje deficyt wody, spowoduje konieczność zaspokojenia zwiększonych potrzeb żywnościowych. Zgodnie z prognozami ONZ, w roku 2025 będzie żyć na ziemi około 8 miliardów ludzi, czyli około 38% więcej niż obecnie. Oblicza się, że w związku z tym konieczny będzie przyrost zboża o jakieś 40% więcej niż w stanie obecnym. To z kolei będzie wiązało się z rozwojem rolnictwa i pozyskiwaniem nowych zasobów wodnych. Szacuje się, że konieczny będzie również wzrost około 30% obszarów powierzchni nawadnianych, w związku z czym wzrośnie zapotrzebowanie na wodę o 17%. Wedle badań[10], przeeksploatowanie zasobów wodnych zarówno powierzchniowych, jak i podziemnych występuje w Indiach, Pakistanie i USA. Najgorsza sytuacja panuje obecnie w Afryce, gdzie, według przeprowadzonych badań, w przyszłości może nie wystarczyć zasobów wodnych do wyżywienia stale zwiększającej się populacji mieszkańców. Ilość wody koniecznej do wyprodukowania żywności rozkłada się w sposób zróżnicowany w poszczególnych częściach globu. Z badań wynika, że stosunek poboru wód, które

[10] P. Kowalczak, *op. cit.*

konieczne są dla rozwoju rolnictwa nie jest proporcjonalny do możliwości ich odnawiania. Szczególnie taka sytuacja ma miejsce w państwach arabskich, zajmujących obszar północno-wschodniej Afryki, Półwyspu Arabskiego oraz Azji Centralnej. Szacuje się, że pobór wody przekroczył tam 40% zasobów odnawialnych. Odnawialność wód powierzchniowych i podziemnych uwarunkowana jest przede wszystkim czynnikami geograficznymi i klimatycznymi. W państwach o szczupłych zasobach wodnych i przy wzroście populacji, której należy zapewnić żywność, nieproporcjonalność ta prowadzi do katastrofy. Niektóre państwa znajdujące się w obszarze Afryki osiągnęły już ten poziom, a inne zbliżają się do równi pochyłej. Problem polega więc na tym, że odnawialność zasobów wodnych nie jest proporcjonalna do ich poboru, a ten do przyrostu naturalnego.

Polski badacz tych zagadnień P. Kowalczak pisze, że „brak dostępu do wody jest przyczyną braku możliwości produkcji rolnej na obszarach sfery suchej i półsuchej, wynika to często z niesprawiedliwego podziału zasobów wodnych, gdzie grupy uboższe społeczeństwa z reguły znajdują się na przegranych pozycjach”[11]. Autor porusza tutaj ważny problem dotyczący państw rozwijających się, gdzie występuje polaryzacja warstw społecznych. W takich krajach jak Chiny czy Indie większa procentowo, bo aż 69% ludności biednej znajduje się w obszarze deficytu zasobów wodnych, inaczej jest z ludźmi zamożnymi, tutaj aż 29% z nich zamieszkuje obszary nawadniane. Kowalczak przytacza szokujące fakty, które są konsekwencją takiego podziału społeczeństwa w rozwijających się państwach. Zacytujmy autora: „W latach 70. i 80. XX wieku w krajach obszaru saharyjskiego Afryki Zachodniej wystąpiły klęski głodu spowodowane długą suszą, ale w tym samym czasie znaleziono wystarczającą ilość wody do uprawy bawełny, warzyw, orzeszków ziemnych i innych artykułów rolniczych przeznaczonych na eksport do Europy i USA. Produkty te wysyłano tymi samymi statkami, którymi przywieziono do Dakaru pomoc żywnościową głodującym. Podobna sytuacja wystąpiła w 1985 roku w Etiopii, gdzie klęska suszy dotknęła znaczącą część kraju – w jej wyniku zginęło 300 tys. ludzi, ale jednocześnie w tym samym czasie na obszarze państwowych gospodarstw rolnych (zlokalizowanych w innej części kraju) uzyskano dobre plony z uprawy trzciny cukrowej i bawełny przeznaczone na eksport”[12]. Fakty te pokazują, że polaryzacja społeczeństwa wpycha jedną grupę w ubóstwo i doprowadza do katastrofy poprzez zaniechanie pomocy.

FAO (*Food and Agriculture Organization*) oszacowało liczbę ludności niedożywionej na kuli ziemskiej. Na podstawie tych analiz (raport – *Agriculture, Food and Water*) otrzymujemy niepokojące dane o kontynentach, które najbardziej borykają się z problemem niedożywienia. Należy do nich przede wszystkim Afryka, gdzie sytuację można ocenić jako bardzo trudną. Tragedią dla Afryki są bowiem nie tylko warunki klimatyczne, które dla odnawialności zasobów wodnych nie są sprzyjające, ale również brak właściwych technologii w rolnictwie. Państwa afrykańskie są pod względem ekonomicznym niewydolne i nie stać ich na wdrażanie nowych technologii ulepszających jakość gospodarki rolnej. Autorzy raportu wskazują, że najgorsza sytuacja jest w Somalii, gdzie 75% osób jest niedożywionych, Burundi – 65%, Kongo – 63%. Problem ten występuje także w Afganistanie – 58% i na Haiti – 55%. Raport zwraca uwagę

[11] *Ibidem*, s. 202.

[12] *Ibidem*, s. 206.

zwłaszcza na kraje Afryki, gdzie problem głodu nadotkliwiej jest odczuwalny na południe od Sahary. To właśnie tam znajduje się najwięcej ubogich, zdewastowanych przez konflikty krajów świata. Wedle badań, co trzeci mieszkaniec kontynentu afrykańskiego ma niewystarczającą ilość żywności, często na skutek nałożenia się wojen i suszy, braku dostępu do świeżej i zdatnej do picia wody. Sytuacja taka występuje również w takich krajach jak: Etiopia, Erytrea, Angolia, Burundia, Sierra Leone, Gwinea i Somalia. Miliony ludzi dotkniętych suszą mieszka w Tadżykistanie, Pakistanie, Iranie, Armenii i Gruzji, a także Afganistanie, Korei Północnej, Mongolii, Kambodży i Bangladeszu.

Niedożywionych jest 11% z 481 milionów mieszkańców Ameryki Łacińskiej i regionu Karaibów, głównie na Haiti, w Nikaragui, Boliwii, Hondurasie. Całe rzesze ludzi cierpi na niedożywienie w Azji. Na ogólną liczbę 826 milionów niedożywionych, 34 miliony żyją w krajach przechodzących transformację ustrojową, przede wszystkim w licznych państwach byłego ZSRR. Ofiarami niedożywienia są głównie jednostki z niższych warstw społecznych, a przede wszystkim dzieci. Według danych raportu FAO, aż 80% dzieci egzystuje w krajach rozwijających się, które mają nadprodukcję żywności[13].

Bezpieczeństwo zdrowotne i sanitarne

Brak dostępu do zasobów wodnych i notoryczne ich zanieczyszczenia są powodem różnego rodzaju chorób. Bezpieczeństwo zdrowotne to kolejna sfera, która może być zagrożona przez deficyty zasobów wodnych. Oczywiste jest to, że warunkiem zdrowego życia jest czysta woda. Jednakże dostęp do niej nie jest taki sam na wszystkich kontynentach, lecz rozkłada się nierównomiernie, co uzależnione jest od szeregu różnorodnych czynników.

Dostęp do świeżej, nadającej się do spożycia wody jest niezbywalnym prawem każdego człowieka. To jednak tylko postulat, faktycznie jest zupełnie inaczej, o czym przekonują nas dane statystyczne, które niejednego wygodnie żyjącego Europejczyka mogą przerazić. Znaczna część populacji (powyżej 1 miliarda, na 6 miliardów ludności zamieszkującej obecnie ziemię) nie posiada dostępu do czystej wody. Około 2,5 miliarda osób, czyli powyżej 1/3 ludzkości, nie posiada możliwości korzystania z urządzeń sanitarnych zaopatrzonych w wodę. Kwestia ta dotyczy zwłaszcza większej części kontynentu afrykańskiego, a także Azji. Nawet w krajach rozwiniętych takich jak Indie, szczególnie poza terenem dużych miast, znaczna część ludności nie ma dostępu do czystej wody. Największym problemem na dzień dzisiejszy nie jest sam brak wody, której źródłem są rzeki, wodospady i woda gruntowa, ale prawidłowa i sprawiedliwa jej dystrybucja do tych obszarów, w których występuje jej największy deficyt. Faktycznie, w Ameryce Łacińskiej, na Karaibach, Afryce Subsaharyjskiej, Europie czy Azji Centralnej istnieją olbrzymie zasoby wodne. Zasoby te nie wiążą się jednak z poziomem ekonomicznego rozwoju tych krajów. Np. w Kongo na jednego mieszkańca przypada ok. 291 tys. m^3 wody, Papui Nowej Gwinei – 170 tys. m^3, podczas gdy w Stanach Zjednoczonych jest to jedynie 9 tys. m^3, a w Kuwejcie 75 m^3 wody *per capita*.

[13] http://www.opoka.org.pl/biblioteka/Z/ZM/granice_glodu.html (07.06.2010).

Dramatyczna sytuacja dotyczy także dostępu do podstawowych urządzeń sanitarnych (kanalizacja, sanitariaty itp.) – nie ma go połowa ludności krajów rozwijających się. Najgorzej jest w Afryce Subsaharyjskiej i w Azji, gdzie dostępność ta obliczana jest na poziomie 36%.

Szczególne problemy z dostępem do urządzeń sanitarnych mają mieszkańcy dużych miast. Wynika to z faktu dysproporcji między wzrostem ludności a dostępem do zasobów wodnych. Prognozuje się, że w okresie 2000–2015 nastąpi przyrost ludności o 1,1 miliarda, z których 88% będzie stanowiła ludność żyjąca w aglomeracjach miejskich. Ten asymetryczny przyrost rodzi szereg problemów. Szczególnie tragicznie sytuacja ta wygląda na obszarze Afryki, np. w Haruna w Kenii. Wokół miast powstają tzw. slumsy, które mają problem nie tylko z dostępem do zasobów wodnych, ale także z odprowadzaniem ścieków. Pojęcie „slums" wywodzi się od XIX-wiecznych przemysłowych miast brytyjskich, których ponad 60% powierzchni zajmowały zatłoczone dzielnice mieszkaniowe, nierzadko o bardzo niskich standardach życia. Dzielnicami slumsowymi nazywa się także dzielnice w bogatszych i wysoko rozwiniętych krajach świata, które zamieszkuje ludność uboga. Najczęściej są to ogromne skupiska ludzi mieszkających w wysokościowcach, na terenach pozbawionych zieleni.

Przeprowadzone badania przedstawiają zatrważający obraz. Okazuje się bowiem, że większość potrzeb fizjologicznych jest po prostu załatwiana na otwartej przestrzeni[14]. Brak infrastruktury wodno-kanalizacyjnej odbija się zwłaszcza na stanie zdrowia mieszkańców. Ścieki to źródło różnego rodzaju bakterii, które powodują śmiertelne choroby. Badania pokazały także, że obszar Afryki i Azji jest pod względem skanalizowania najuboższy. Ocenia się, że około 80% litrów wody to poziom wymagany dla zdrowego stylu życia. Ponadto statystyki przeprowadzone przez badaczy pokazują, że zużycie wody przez jednostki egzystujące w krajach rozwiniętych przekracza ponad 500 litrów dziennie. Inna sytuacja, jakże rażąco odmienna, ma miejsce w krajach ubogich i rozwijających się. Tam ilość wody nie przekracza 50 litrów dziennie.

Wzrost liczby ludności, trudności w dostępie do świeżej i nadającej się do spożycia wody, brak odpowiedniej infrastruktury kanalizacyjnej (szczególnie w Afryce i Azji) powoduje powstawanie wielu chorób. Do rozwoju chorób zakaźnych przyczyniają się także warunki klimatyczne, migracja oraz nieudolna polityka państwowa. Poczucie bezpieczeństwa związane ze zdrowiem jest zachwiane szczególnie przez uniemożliwiony – z różnych przyczyn – dostęp do zasobów wodnych, jak i brak infrastruktury kanalizacyjnej. Statystycznie aż 75% chorób w krajach rozwijających się to choroby przenoszone przez wodę lub spowodowane brakiem dostępu do czystej wody, co uniemożliwia utrzymanie prawidłowego poziomu higieny, powodując łatwe ich rozprzestrzenianie. Zakażona, brudna woda zabija więcej ludzi niż AIDS, nowotwory czy wojny. Choroby zakaźne przenoszone są przez zanieczyszczone cieki wodne. Choroby te zabijają, zgodnie z danymi statystycznymi, powyżej 6 milionów dzieci rocznie (ok. 20 tys. dziennie). Główną przyczyną śmierci małych dzieci jest biegunka wywołana patogenami zawartymi w zanieczyszczonej wodzie (corocznie na całym świecie dzieci przechodzą 1,5 biliona epizodów biegunki, z tego 4 mln epizodów kończy się śmiercią). Przewiduje się, że do roku 2020 z powodu chorób przenoszonych przez wodę umrze

[14] „Latająca toaleta" to jedyny wynalazek, jaki z konieczności powstał w slumsie Kibera pod Nairobi. Na jedną toaletę klasyczną – dziurę wykopaną w ziemi – przypada tam 1500 osób. Zob. http://serwisy.gazeta.pl/swiat/ (07.06.2010).

135 mln ludzi. 1/3 populacji w krajach rozwiniętych zainfekowana jest pasożytami jelitowymi, co prowadzi do niedożywienia i niedorozwoju fizycznego dzieci. Schorzeniom tym łatwo można byłoby zapobiec, zapewniając dostęp do świeżej, zdatnej do spożycia wody. Poniższa tabela (tab. 1) przedstawia skrótowy opis chorób przenoszonych przez wodę.

Tabela 1. Skrótowy opis chorób przenoszonych przez wodę

Choroba	**Zgony na rok**	**Związek choroby z dostępem do wody lub urządzeń sanitarnych**
Ogółem	5,29 milionów osób	
Inwazje nicieniami przewodu pokarmowego	100 000	Ściśle związana z nieprawidłowym składowaniem fekaliów, złą higieną osobistą i domową.
Choroby biegunkowe	2 200 000 do 5 000 000	Ściśle związana z nieprawidłowym składowaniem fekaliów, złą higieną osobistą i domową.
Drakunkuloza		Ściśle związana z piciem niepewnej, skażonej wody.
Jaglica		Ściśle związana z niedostateczną higieną twarzy i rąk związaną z brakiem dostępu do wody.
Malaria	1 500 000	Związana z nieprawidłową gospodarką wodną, przechowywaniem wody, źle zabezpieczonymi punktami wodnymi.
Denga	20 000	Związana z nieprawidłowym składowaniem śmieci (zanieczyszczających wodę), nieprawidłowym przechowywaniem wody, zarządzaniem punktami wodnymi.
Poliomyelitis		Związana z zanieczyszczeniem wody fekaliami, niskim poziomem higieny, brakiem świeżej, pitnej wody.
Trypanosomoza	130 000	Związana z brakiem dostępu do bezpiecznych źródeł wody.
Filarioza wywołana W. bancrofti		Związana z nieprawidłowym składowaniem śmieci (zanieczyszczających wodę), nieprawidłowym przechowywaniem wody, zarządzaniem punktami wodnymi.
Onchocerkoza	40 000	Związana z nieprawidłową gospodarką dużymi zbiornikami wodnymi.

Na podstawie powyższej tabeli można stwierdzić, że wszystkie wyliczone choroby mają swoją przyczynę w „brudnej wodzie" i braku odpowiednich urządzeń sanitarnych oraz higienicznych. Na omawiany problem zwrócił uwagę w 2003 roku *World Water Development Report* – WWDR, zaprezentowany w przeddzień Światowego Forum Wody, które odbyło się w dniach 16–23 marca w Japonii. W raporcie pojawia się szczegółowa diagnoza omawianego problemu. Dokument postuluje konkretne działania, których celem jest przeciwdziałanie zaistniałej sytuacji. Zakłada, że aby osiągnąć Milenijne Cele Rozwoju (MDG – *Millennium Development Goals*), należy do roku 2015 usprawnić dostęp do wody pitnej dla 1,5 miliarda ludzi. Oznacza to, że

w latach 2000–2015 należałoby pomóc kolejnym stu milionom ludzi rocznie (274 tysiącom dziennie).

Polepszenie warunków sanitarnych wydaje się jeszcze bardziej nierealne. W raporcie podkreśla się konieczność usprawnienia dostępu do urządzeń sanitarnych dla kolejnych 1,9 miliarda ludzi, co oznacza, że w latach 2000–2015 należałoby pomóc 125 milionom obywateli rocznie (342 tysiącom dziennie). Raport stwierdza, że przeszkodą w tworzeniu odpowiednich warunków sanitarnych są nie tylko problemy natury logistycznej i finansowej, ale również czynniki kulturowe, obyczajowe, a często także i religijne. W raporcie zwraca się uwagę, że gdyby utrzymać obecny poziom inwestycji, można by zrealizować lub zbliżyć się do realizacji wyznaczonych celów we wszystkich regionach świata oprócz Afryki Subsaharyjskiej. Jednak w ogólnym ujęciu, to Azja potrzebuje więcej inwestycji niż Afryka, Ameryka Łacińska i Karaiby razem wzięte. Szacuje się, że koszt pierwszych interwencji wyniósłby około 12,6 miliarda dolarów[15].

Bezpieczeństwo związane ze stałym zamieszkaniem

Deficyt zasobów wodnych zagraża także bezpieczeństwu związanemu ze stałym miejscem zamieszkania. Powoduje on problem migracji jednostek i całych grup społecznych. Na problem migracji ludności zwrócił uwagę Raport UNFPA z 2004. Ze względu na ciągłą migrację ludności ze wsi do miast, liczba osób mieszkających w dużych aglomeracjach rośnie dwukrotnie szybciej w stosunku do całkowitego przyrostu ludności. Większość ludności świata do roku 2007 będzie mieszkała w miastach, a do roku 2030 we wszystkich regionach będą przeważały struktury miejskie. Rosną zarówno największe aglomeracje liczące 10 lub więcej milionów mieszkańców (ogółem 20, zaś 15 w krajach rozwijających się), jak i małe oraz średnie miasta, co nadwyręża lokalną infrastrukturę i sektor usług. Uczestnicy konferencji ICPD stwierdzili, że migracje ludności wewnątrz krajów są skutkiem nierównego podziału zasobów naturalnych, usług i możliwości. Zapewnienie opieki socjalnej z uwzględnieniem zdrowia reprodukcyjnego na ubogich obszarach miejskich jest działaniem niezbędnym, tak jak zaspokojenie potrzeb zaniedbanych społeczności wiejskich. W roku 2000 na świecie było 175 mln migrantów, którzy opuścili swój kraj (1 na 35 osób) – liczba ta wzrosła z 79 mln w roku 1960. Wielu ludzi, w tym coraz więcej kobiet, szuka pracy za granicą, co ma istotny wpływ zarówno na kraje ich pochodzenia, jak i na kraje przyjmujące. Obydwa kraje odczuwają także skutki ekonomiczne tego procesu. W trakcie konferencji ICPD wezwano państwa do zajęcia się podstawowymi przyczynami migracji, zwłaszcza ubóstwem. Trzy czwarte krajów poinformowało o działaniach podjętych w sprawie migracji międzynarodowych; w roku 1994 uczyniła to tylko jedna piąta. Niektóre kraje zacieśniły granice, podczas gdy inne dążą do lepszej integracji imigrantów. Wiele krajów popiera zwiększoną koordynację polityki migracyjnej, jakkolwiek kwestia ta pozostaje drażliwa[16]. Migracja związana jest ze zmianą miejsca zamieszkania. A. Maslow stwierdził, że jedną z potrzeb bezpieczeństwa jest potrzeba posiadania

[15] Zob. www.unic.un.org.pl/iyfw/raport_gwns.php (07.06.2010).

[16] http://www.unic.un.org.pl/swp/2004/streszczenie_raportu.php (07.06.2010).

stałego miejsca zamieszkania, innymi słowy – potrzeba posiadania tzw. „dachu nad głową". W ostatnich latach pojawiła się w literaturze przedmiotu specjalna kategoria określająca ten typ ludzi, którzy stale migrują pod wpływem czynników środowiskowych – jest to „uchodźca środowiskowy" (*environmental refugees*).

Kategoria „uchodźstwa środowiskowego" to kategoria polityczna, ekonomiczna, ekologiczna. Różnorodność ta wynika stąd, że w danym państwie, w którym występuje migracja, trudno jest wskazać jedną tylko przyczynę generującą tego typu zjawisko. Zazwyczaj u podstaw migracji leży kilka przyczyn jednocześnie, które w połączeniu decydują o zaistnieniu zjawiska migracji. Typ uchodźcy środowiskowego określa ludzi, którzy migrują z powodu gwałtownych zmian środowiska. Zmiany te mogą być spowodowane przez czynniki naturalne, jak i przez inwazyjną działalność człowieka. Jeśli chodzi o czynniki naturalne, są to różnego rodzaju kataklizmy, zjawiska ekstremalne, klęski żywiołowe zmuszające wielkie rzesze ludzi do przemieszczania się w poszukiwaniu bezpiecznych miejsc do rozwoju oraz egzystencji. Przyroda nie oszczędza człowieka i wymusza na nim tego typu zachowania. Do przyczyn wywoływanych przez człowieka należy np. wojna. Nie od dziś wiadomo, że prowadzone działania wojenne zmuszają miliony jednostek do migracji. Szacuje się, że największa obecnie migracja pod wpływem działań wojennych ma miejsce z Afganistanu, gdzie ponad 85% terenów zdatnych pod uprawę zostało zniszczonych. Oblicza się, że na dzień dzisiejszy około 174 mln ludzi żyje poza granicami własnych państw, niektórzy z nich nie mają już szans powrotu do swojej ojczyzny. Na straży praw uchodźców stoi Konwencja ONZ z 1951 roku. Migracja ludności może mieć charakter tak międzypaństwowy, jak i wewnątrzpaństwowy.

O ile problem ten w mniejszej skali istnieje na terenie Europy, o tyle na szeroką skalę występuje na terenie państw afrykańskich. Szacuje się, że właśnie w tym obszarze migracja ludności jest największa. W literaturze przedmiotu[17] zwraca się uwagę na trudności diagnozy problemu migracji ludności na kontynencie afrykańskim. Afryka charakteryzuje się bowiem szczególnie dużą częstotliwością migracji wewnątrzpaństwowych. Ocenia się, że w samej Afryce migracja ludności przekracza 13 mln. Duża skala migracji występuje także w Demokratycznej Republice Konga, Ugandzie, Liberii, Wybrzeżu Kości Słoniowej i Somalii. Głównymi przyczynami, które decydują o tym, że na kontynencie afrykańskim mamy do czynienia z tak potężną falą migracji, są konflikty wojenne oraz częste klęski żywiołowe. Badacze najdokładniej przebadali właśnie ten typ uchodźstwa środowiskowego, u którego źródeł leżą przyczyny związane z realizacją wielkich budowli wodnych oraz wielkich systemów nawadniających. Na podstawie dokumentacji każdej z tych inwestycji można określić liczbę przesiedleńców. Część z nich rozpoczyna migrację w poszukiwaniu dostępnych i zdatnych do picia zasobów wodnych, ma zagwarantowane gdzieś miejsce zamieszkania, ale, statystycznie rzecz biorąc, większa część z tych migrujących grup społecznych nie przenosi się w kierunku konkretnego miejsca osiedlenia. W przeważającej mierze trafiają oni do slumsów i tam rozpoczynają nowe życie. Taka sytuacja nie stwarza jednak poprawy jakości ich życia ani też nie gwarantuje, że będą oni korzystali z dobrych jakościowo zasobów wodnych – o takie dobrodziejstwo w slumsach jest niestety trudno. Migracja, szczególnie na obszarze Afryki, doprowadziła w sensie socjologicznym do

[17] Por. P. Kowalczak, *op. cit.*

nowego rozumienia rodziny, innego niż to, do którego przywykli np. Europejczycy. „W Afryce pojęcie rodzina ma szczególny charakter, jest pojęciem szerszym niż w Europie i obejmuje bezpośrednio większą grupę krewnych. Ta grupa stanowi jednostkę ekonomiczną i produkcyjną o specyficznym dla Afryki systemie zabezpieczenia socjalnego, jest także grupą, wewnątrz której następuje przekaz dotyczący identyfikacji kulturowej. Wskutek migracji funkcje rodziny zostają zniszczone lub w poważnym stopniu zakłócone. Szczególnie widoczna jest rola rodziny właśnie podczas sytuacji ekstremalnych w obliczu zagrożenia. To właśnie organizacja rodzinna jest podstawą bezpieczniejszej egzystencji w zmienionych i bardzo trudnych warunkach kontynentu afrykańskiego”[18].

Przemieszczanie się nierzadko olbrzymich mas ludności powoduje szereg konfliktów i prowadzi do różnych niebezpieczeństw. Jeśli chodzi o konflikty, to w pierwszej kolejności mogą one powstawać między ludnością tubylczą żyjącą na określonej przestrzeni a ludnością, która wyemigrowała z jakiegoś innego obszaru – czy to danego państwa, czy z innych regionów wewnątrz tego samego kraju. Migracje pociągają za sobą olbrzymie straty w środowisku naturalnym. Np. w rejonie Kageru w Tanzanii uchodźcy spalają około 1200 ton drzewa dziennie. W zairskim Parku Narodowym Virunga, gdzie występują tzw. lasy dziewicze, tysiące uchodźców niszczy miliony drzew na opał. Migracje powodują także wzrost różnego rodzaju chorób zakaźnych. Prowadzą w prostej linii do poczucia zagrożenia bezpieczeństwa zdrowotnego. Emigranci zamieszkują albo wolne przestrzenie, o ile znajdują się tam wystarczające zasoby do ich wyżywienia, albo żyją w slumsach razem z inną ludnością. Brak dostępu do urządzeń sanitarnych zarówno na otwartych przestrzeniach, jak i w afrykańskich slumsach generuje problem z odprowadzaniem ścieków. Według badań, jest to bardzo poważny problem. Większe skupiska ludności oraz brak właściwej higieny powoduje bardzo szybkie rozprzestrzenianie się chorób przenoszonych drogą wodną.

Na podstawie tego, co powiedzieliśmy widać, że deficyt zasobów wodnych prowadzi do zachwiania poczucia bezpieczeństwa w wielu sektorach życia. Zagrożenie bezpieczeństwa w skali globalnej tak obecnie, jak i prognozowane w przyszłości, dotyczy przede wszystkim krajów położonych na kontynencie afrykańskim. Ten rejon jest szczególnie zagrożony zachwianiem równowagi bezpieczeństwa we wszystkich opisanych powyżej aspektach.

Podsumowanie

Podejmując konkluzję dotychczasowych rozważań, należy zauważyć, że:

1) Na podstawie przywołanych badań, stale rosnący deficyt wody jest realnym zagrożeniem szczególnie dla tych kontynentów, co do których prognozy pokazują, iż w 2050 roku znajdą się takie państwa, które będą cechowały się chronicznym brakiem wody, a ich gospodarka wodna dozna zapaści. Do takich terenów należy przede wszystkim Afryka oraz niektóre kraje Azji.
2) Wzrost zagrożenia poczucia bezpieczeństwa spowodowany jest faktem nierównomiernego rozłożenia zasobów wodnych na globie ziemskim. Za ten stan rzeczy

[18] *Ibidem*, s. 235.

odpowiedzialnych jest wiele czynników zwłaszcza geograficzne, związane z położeniem danego kontynentu, ukształtowanie terenu, warunki klimatyczne, cykl hydrologiczno-meteorologiczny, odnawialność zasobów wodnych oraz kwestia ich wykorzystania poprzez odpowiednio rozbudową gospodarkę wodną. Oprócz tych kwestii pojawiają się także problemy polityczne, ekonomiczne i prawne, problemy jeśli chodzi o dostęp do zasobów wodnych, a także kulturowo-religijne. Zapotrzebowanie na wodę nie maleje, ale wzrasta w sposób nieproporcjonalny do stale powiększającej się liczby ludności w niektórych obszarach globu, zwłaszcza w tych, które określa się mianem krajów trzeciego świata. Wzrost populacji rodzi potrzebę efektywniejszego korzystania z dostępnych zasobów wodnych. Tu jednak sprawa się komplikuje, bo w niektórych regionach świata (np. Afryka) występują takie miejsca, gdzie nie zachodzi równowaga między eksploatacją wody a jej odnawianiem. Na ten proces ma wpływ wiele czynników, ale decydujący jest klimat i warunkowany nim cykl hydrologiczny.

3) Rodzi się pytanie: *w jaki sposób można zaradzić stale wzrastającemu poczuciu zagrożenia bezpieczeństwa przez nieustannie zmniejszające się zasoby wodne?* Wydaje się, że same inicjatywny różnych państw (w ramach np. ONZ) czy regulacje prawne niewiele przyczyniają się do redukcji tego zagrożenia. Sprawa bowiem leży zupełnie gdzie indziej. Problem polega na tym, że największą przeszkodą w usunięciu tego zagrożenia jest przede wszystkim ubóstwo wielu społeczeństw i krajów. Ubóstwo to wynika stąd, że państwa te nie stać na podjęcie skutecznych działań w celu zapobiegnięcia kolejnym katastrofom związanym z deficytem zasobów wodnych. Brak środków finansowych uniemożliwia rozbudowanie infrastruktury, która pozwoliłaby nie tylko na efektywne eksploatowanie zdatnej do picia wody, ale także zapobiegłaby jej zanieczyszczaniu przez ścieki. Państwa, zwłaszcza afrykańskie, mają ograniczone możliwości, jeśli chodzi o politykę prewencyjną, która stanowi istotny czynnik zapobiegający pojawieniu się braku bezpieczeństwa w różnych sektorach życia. Chodzi tutaj szczególnie o państwa Afryki oraz Azji.
4) Trzeba powiedzieć, że rozwiązaniem problemów z bezpieczeństwem wodnym nie jest na pewno konflikt militarny. Takie rozwiązanie nie jest racjonalne i przynosi więcej strat niż pożytku. Zwracają na to uwagę teoretycy zajmujący się tym problemem. Np. Wolf twierdzi, że za cenę tygodniowych działań zbrojnych można wybudować np. pięć stacji odsalania wody i uzyskać nowy dostęp do zasobów wodnych bez straty w ludziach. Nie zawsze jednak działanie ludzkie jest tak racjonalne. Nierzadko tego typu konflikty starają się rozwiązywać właśnie drogą działań militarnych zwłaszcza politycy. W tym jednak przypadku bardziej chodzi o ambicje i strefy wpływów niż o pomoc tym, którzy najbardziej cierpią z powodu braku wody. Trafnym przykładem obrazującym ten problem jest wieloletni zatarg między Izraelem a państwami arabskimi.
5) W artykule zwrócono uwagę na to, że szczególnie trudna sytuacja w skali globalnej ma miejsce w Afryce. Afryka – to słowo brzmi jak synonim konfliktu o wodę. W państwach afrykańskich występuje największe zagrożenia bezpieczeństwa wodnego. Sytuację komplikuje również podział Afryki oraz brak realnej współpracy między państwami. Stałe konflikty, które mają charakter militarny, nie prowadzą do żadnego rozwiązania, wręcz pogarszają sytuację. Problem Afryki to problem na skalę światową. Wydaje się, że, aby zaradzić problemom bezpieczeństwa szczególnie

w tym zakątku globu ziemskiego, konieczne jest większe i szersze współdziałanie wspólnoty międzynarodowej. Same akty prawne i apele, a także pomoc humanitarna dostarczana do tych krajów, zdają się niewystarczające. W przypadku rozwiązania problemu Afryki i wielu innych państw, które po 2050 roku znajdą się w obliczu chronicznego braku dostępu do zasobów wodnych, konieczne jest podejście holistyczne, które uwzględni cały kompleks warunków politycznych, społecznych, ekonomicznych i prawnych, a także ekologicznych i kulturowych. Rozwiązania polityczne powinny finalizować się nawiązywaniem współpracy, która pomoże uporządkować pozostałe zagadnienia. Jak do tej pory, problem podzielonej Afryki nie został skutecznie rozwiązany. Nadal na to czekamy – oby tylko nie było to rozwiązanie militarne, które jeszcze bardziej pogorszy i tak już bardzo trudną sytuację w tym rejonie globu.

6) Można postawić pytanie, które wyraża pewną pesymistyczną postawę w stosunku do problemu deficytu wodnego: czy w ogóle istnieje możliwość zapobiegnięcia prognozowanej „katastrofie wodnej"? Wydaje się bowiem, że w tych rejonach świata, gdzie zasoby wodne uwarunkowane są czynnikami geograficznymi i klimatycznymi, gdzie odnawialność źródeł wody jest nieproporcjonalnie mniejsza do jej zużycia, gdzie ubóstwo danego kraju uniemożliwia rozwój gospodarki wodnej i wdrożenie skutecznych technik zarządzania zasobami wodnymi, zachodzi obawa, że nie ma żadnej możliwości pomocy. Czy można zapobiec temu, co przygotowała tym ludziom z jednej strony natura, a z drugiej nieudolna polityka w resorcie gospodarki wodnej? Gospodarka wodna ma zatem przed sobą trudny problem do rozwiązania. Co zrobić z żyjącymi na tych terenach ludźmi? W jaki sposób zapewnić im dostarczanie wody, która jest niezbędnym warunkiem do życia? Te i wiele innych pytań nasuwających się na kanwie powyższych rozważań zostawiamy bez odpowiedzi. Pozostaje tylko mieć nadzieję, że świadomość prognozowanych ubytków zasobów wodnych i problemów z tym związanych oraz humanistyczna świadomość współczesnego człowieka, deklarowana wrażliwość na jego godność i jego niezbywalne prawa – a takim jest prawo do wody – będzie silnym bodźcem do działania, aby nie pozwolić zginąć milionom ludzi, którzy za około 40 lat mogą znaleźć się w stanie permanentnego braku wody.

Bibliografia

Craig J. R., Vaughan D. J., Skinner, B. J., *Zasoby ziemi*, Wydawnictwo Naukowe PWN, Warszawa 2003.
Kowalczak P., *Konflikty o wodę*, Wydawnictwo Kurpisz, Poznań 2007.
Maslow A., *W stronę psychologii istnienia*, REBIS, Warszawa 2004.
Maslow A., *Motywacja i osobowość*, Wydawnictwo Naukowe PWN, Warszawa 2006.
Obuchowski K., *Galaktyka potrzeb*, Wydawnictwo Zysk i S-ka, Warszawa 2002.

Strony internetowe:
http://www.unic.un.org.pl/iyfw/raport_gwns.php (07.06.2010).
http://www.npw.pl/STARE%20NUMERY/2005_01_02/Gospodarka.html (07.06.2010).

http://www.eioba.pl/a75444/woda_na_wage_zlota (07.06.2010).
http://www.opoka.org.pl/biblioteka/Z/ZM/granice_glodu.html (07.06.2010).
http://serwisy.gazeta.pl/swiat/. (07.06.2010).
http://www.unic.un.org.pl/swp/2004/streszczenie_raportu.php (07.06.2010).

Mariusz Rozwadowski

Wykorzystanie metody SMED w procesie obsługi sprawcy wykroczenia drogowego

Wprowadzenie

Metoda Single Minute Exchange of Die (SMED) została opracowana w latach 50. i 60. XX wieku przez jedną z głównych postaci japońskiej szkoły zarządzania Shigeo Shingo i po raz pierwszy zastosowana w przemyśle samochodowym do skrócenia trwania procesów technologicznych (przezbrajania pras). Z czasem, dzięki skuteczności i uniwersalności, zaczęła ona przenikać do różnych innych branż oraz dziedzin gospodarki. Obecnie jest jedną z metod stosowanych do poprawy wydajności pracy i usuwania tzw. „wąskich gardeł" systemów produkcyjnych.

W celu poprawy procesów przezbrajania, zgodnie z metodą S. Shingo, należy zrealizować cztery etapy postępowania[1]:

- stadium przygotowawcze;
- rozgraniczenie przezbrojenia wewnętrznego i zewnętrznego;
- przekształcenie przezbrojenia wewnętrznego w zewnętrzne;
- racjonalizację wszystkich aspektów operacji przezbrajania.

Istota pierwszego etapu metody SMED sprowadza się do identyfikacji organizacji pracy istniejącej na danym stanowisku. W analizie poszczególnych zachowań można posłużyć się wywiadem z pracownikami, a także filmowaniem poszczególnych czynności na danym stanowisku. Na koniec wskazane jest przeprowadzenie rozmowy z bezpośrednimi wykonawcami poszczególnych czynności. W trakcie spotkania roboczego warto zadać następujące pytania: Co należy zmienić w dotychczasowej organizacji wykonywanej pracy? oraz: Co przeszkadza im w realizacji tego procesu?

Celem drugiego etapu jest wyodrębnienie dwóch kategorii czynności – czynności zewnętrznych, które mogą być wykonywane przed lub po zaistnieniu danego procesu czy usługi oraz czynności wewnętrznych, które muszą być realizowane w czasie danego procesu lub świadczenia usługi.

Celem stosowania metody SMED w sferze usług publicznych jest skrócenie czasu obsługi tzw. „klienta", przede wszystkim poprzez wyeliminowanie z procesu obsługi czynności zewnętrznych.

Przemysłowe zastosowania metody wykazały, iż dzięki oddzieleniu czynności zewnętrznych od wewnętrznych i ich wykonania poza cyklem uzyskuje się znaczną redukcję czasu procesu. Przekształcenie czynności wewnętrznych na zewnętrzne jest jednak zabiegiem dosyć trudnym, wymagającym poszukiwania nowych, niekonwencjonalnych rozwiązań organizacyjnych o charakterze jakościowym.

---

[1] Z. Martyniak, *Nowe metody i koncepcje zarządzania*, Kraków 2002, s. 91.

Stąd twórca metody zaleca w takim przypadku posługiwanie się zestawem pięciu pytań:

- Co się wykonuje?
- Kto to wykonuje?
- Jak się wykonuje?
- Gdzie się wykonuje?
- Kiedy się wykonuje?

Ostatnim krokiem powinno być opracowanie projektu usprawnionego procesu. W procesie projektowania należy zwrócić uwagę na kolejność, sposób oraz czas realizowanych czynności, określając odpowiednie wyposażenie stanowiska pracy.

Metodyka SMED w racjonalizacji procesu obsługi sprawcy wykroczenia

Mając na uwadze ukazanie możliwości i korzyści zastosowania metody SMED w racjonalizacji usług publicznych realizowanych przez funkcjonariuszy policji, zdecydowano się na przeprowadzenie analizy organizacji procesu związanego z obsługą sprawców wykroczeń drogowych. Głównym celem racjonalizacji było skrócenie czasu realizacji procesu. Przygotowując niniejsze opracowanie, przeprowadzono badania empiryczne wśród policjantów Sekcji Ruchu Drogowego Komendy Miejskiej Policji w Krakowie (SRD KMP). Analizie poddano proces obsługi sprawców wykroczeń drogowych w przypadku, gdy pojazd sprawcy wykroczenia zarejestrowany jest na terenie miasta Krakowa, właścicielem jest osoba fizyczna, która stawia się na pierwsze wezwanie do SRD KMP.

W odniesieniu do procesu związanego z ukaraniem sprawcy wykroczenia drogowego, pierwotnie zdefiniowany w metodzie SMED termin „przezbrajanie" wydaje się dalece niewłaściwy i wymaga modyfikacji. Sprawca ujawnionego wykroczenia drogowego staje się w pewnym momencie swego rodzaju „klientem", natomiast funkcjonariusz policji świadczy „usługę" związaną z ukaraniem. Występuje zatem klasyczny przypadek swoistego „procesu obsługi klienta". Odwołując się do analogii pomiędzy produkcją a obsługą klienta oraz do podziału procesu na czynności, operacje, ruchy robocze i ruchy elementarne[2], można stwierdzić, że w procesie ukarania sprawcy wykroczenia drogowego (przekroczenia dozwolonej prędkości) można zdefiniować i wyodrębnić czynności obsługi, które dzielą się z kolei na operacje obsługi. Reasumując, określenie „czynności obsługi" jest zatem właściwym odpowiednikiem dla pierwotnie zdefiniowanej czynności „przezbrajania".

W zastosowaniach produkcyjnych czynności związane z przezbrajaniem dzielą się na wewnętrzne i zewnętrzne. Zależy to od możliwości ich przeprowadzenia w trakcie ruchu maszyn – czynność zewnętrzna to taka, która jest przeprowadzona w trakcie postoju maszyny. W przypadku obsługi klienta – sprawcy wykroczenia drogowego – należy posłużyć się innym kryterium podziału, wyróżniając następujące czynności[3]:

---

[2] H. Mreła, *Technika organizowania pracy*, Warszawa 1965, s. 20.

[3] M. Walczak, *Próba zastosowania metody SMED w pracach administracyjno-biurowych na przykładzie okienka pocztowego*, Zeszyty Naukowe Akademii Ekonomicznej w Krakowie, nr 616, Kraków 2003, s. 100.

- wewnętrzne, przy których wymagana jest obecność klienta (kierującego pojazdem, którym popełniono wykroczenie drogowe),
- zewnętrzne, które mogą być wykonane pod nieobecność tzw. klienta (sprawcy wykroczenia drogowego).

Biorąc pod uwagę sformułowany cel zastosowania metody SMED oraz specyfikę usług świadczonych przez policję, dokonano uszczegółowienia toku postępowania badawczego prowadzącego do skrócenia czasu procesu związanego z ukaraniem sprawcy wykroczenia drogowego (tab. 1).

Tabela 1. Struktura i specyfikacja toku postępowania SMED w procesie obsługi sprawcy wykroczenia drogowego

Etapy	**Zadanie badawcze**
1. Stadium przygotowawcze	• Analiza organizacji pracy na stanowisku obsługi fotoradaru. • Wykonanie pomiarów czynności związanych z obsługą klienta. • Sporządzenie listy niesprawności w procesie. • Analiza i ocena procedur związanych z procesem ukarania sprawcy.
2. Podział czynności na wewnętrzne i zewnętrzne	• Sporządzenie listy czynności procesu. • Podział na czynności zewnętrzne i wewnętrzne. • Poszukiwanie nowych sposobów realizacji czynności zewnętrznych (przed lub po obsłudze klienta).
3. Przekształcenie czynności wewnętrznych na zewnętrzne	• Dokonanie szczegółowej analizy wyodrębnionej grupy czynności wewnętrznych. • Poszukiwanie nowych rozwiązań realizacji czynności wewnętrznych, mających na celu skrócenie czasu ich trwania.
4. Racjonalizacja procesu	• Końcowa analiza nowo zaprojektowanego procesu obsługi sprawcy wykroczenia z punktu widzenia optymalizacji czasu trwania poszczególnych czynności. • Określenie wyposażenia policjanta w odpowiednie środki organizacyjno-techniczne (komputer z dostępem do Internetu, materiały biurowe, druki procesowe).

Źródło: opracowanie własne na podstawie założeń teoretycznych metody SMED oraz empirycznej weryfikacji dla przypadku ujawnienia i ukarania sprawcy wykroczenie drogowego – przekroczenia dozwolonej prędkości (materiały i informacje SRD KMP w Krakowie).

Analiza i projektowanie usprawnień procesu obsługi sprawców wykroczeń drogowych

Analiza działań w stadium przygotowawczym

Przystępując do usprawnienia procesu obsługi klienta, należy postępować zgodnie z etapami wyszczególnionymi w metodzie SMED[4], zaczynając od stadium przygotowawczego. W pierwszej kolejności rozpoznano strukturę procesu, wyróżniając siedem czynności, które aktualnie realizowane są w obecności klienta i kształtują przebieg oraz czas jego realizacji. Dla obliczenia czasu realizacji wymienionych czynności zastosowano technikę szacunku ekspertów, w rezultacie czego wyznaczono trzy zmienne tej charakterystyki, a mianowicie czas minimalny, maksymalny i średni (pożądany). Zestawienie czynności i czasu ich trwania zawarto w tabeli 2.

Tabela 2. Wyniki pomiarów czasów realizacji czynności przy określonej próbie (w minutach)

Czynności obsługi	**Czas realizacji czynności w minutach**		
	minimalny	**maksymalny**	**średni**
Ustalenie tożsamości sprawcy wykroczenia – właściciela samochodu.	1	5	2,4
Przedstawienie wykroczenia (materiał fotograficzny).	1	20	8
Sprawdzenie osoby i pojazdu w ewidencji WI.	1	30	7,7
Zaproponowanie sprawcy wykroczenia mandatu karnego.	1	30	8,8
Wypisanie mandatu karnego.	2	15	6,5
Sporządzenie karty informacyjnej PRD 5.	2	10	7,5
Przesłuchanie sprawcy wykroczenia drogowego.	5	120	38
Razem	**13**	**230**	**79**

Źródło: opracowanie własne na podstawie analizy materiału empirycznego dotyczącego obsługi sprawcy wykroczenia drogowego – przekroczenia dozwolonej prędkości (materiały i informacje SRD KMP w Krakowie).

Na podstawie opinii ekspertów ustalono, że czas realizacji procesu obsługi uzależniony jest od szeregu czynników techniczno-organizacyjnych, a jego wydłużenie związane jest m.in. ze sprawnością funkcjonowania systemu komputerowego, jakością nośników informacji (dowód tożsamości, materiały fotograficzne). Zasadniczo jest on jednak determinowany kompetencjami merytorycznymi policjantów i skutecznością procesu komunikowania się w układzie sprawca wykroczenia drogowego – policjant.

[4] Z. Martyniak, *Zastosowanie metody SMED*, Zeszyty Naukowe Akademii Ekonomicznej w Krakowie, nr 486, Kraków 2001, s. 96.

Uwzględniając potrzebę racjonalizacji procesu obsługi sprawcy wykroczenia drogowego, przeprowadzono badania ankietowe wśród wszystkich wykonawców procesu[5] (dziesięciu pracowników sekcji), której celem była identyfikacja występujących niesprawności. Uzyskane wyniki umożliwiły określenie trudności w realizacji procesu oraz źródła marnotrawstwa czasu. Do czynników utrudniających zaliczono: niską jakość zdjęć fotograficznych, nieaktualność lub brak danych osobowych, brak umiejętności obsługi programu komputerowego przez policjantów. Można je uznać za źródła nieuzasadnionych strat czasu. Warto podkreślić daleko idącą zbieżność opinii respondentów.

Podział czynności procesu obsługi i określenie usprawnień

Etap ten rozpoczyna sporządzenie listy wszystkich operacji realizowanych w procesie obsługi sprawcy wykroczenia drogowego. Na podstawie analizy empirycznej dziesięciu przypadków poddanych obserwacjom bezpośrednim i rejestracji wideo ustalono następującą strukturę operacji uporządkowanych chronologicznie:

- zarejestrowanie sprawy w systemie komputerowym,
- ustalenie właściciela pojazdu w systemie CEPiK,
- ustalenie adresu i numeru telefonu właściciela pojazdu,
- powiadomienie właściciela o popełnionym wykroczeniu za pomocą telefonu, w przypadku jego posiadania[6],
- powiadomienie właściciela o popełnionym wykroczeniu za pomocą wezwania,
- ustalenie tożsamości sprawcy wykroczenia stawiającego się na wezwanie,
- przedstawienie wykroczenia drogowego (materiał fotograficzny),
- sprawdzenie osoby i pojazdu w ewidencji WI,
- zaproponowanie sprawcy wykroczenia drogowego mandatu karnego, informując go o możliwości odmowy przyjęcia,
- wypisanie mandatu karnego w przypadku, gdy strona przyznaje się do popełnienia wykroczenia drogowego,
- wypisanie karty informacyjnej PRD 5,
- sporządzenie protokołu przesłuchania sprawcy wykroczenia,
- zakończenie sprawy po zastosowaniu postępowania mandatowego,
- sporządzenie wniosku do Sądu Grodzkiego i zakończenie sprawy.

Najważniejszym elementem tego etapu, zgodnie z metodą SMED, jest właściwe rozgraniczenie czynności na zewnętrzne i wewnętrzne. Podział czynności występujących w procesie obsługi „klienta" zaprezentowano w tabeli 3.

[5] Ankiety sporządzone w trakcie badań realizowanych w Sekcji Ruchu Drogowego Komendy Miejskiej Policji w Krakowie w 2006 roku.

[6] Ustawa z dnia 24 sierpnia 2001 r. Kodeks postępowania w sprawach o wykroczenia.

Tabela 3. Podział czynności realizowanych w procesie obsługi sprawcy wykroczenia drogowego

Czynności zewnętrzne	Czynności wewnętrzne
• zarejestrowanie sprawy w systemie komputerowym, • ustalenie właściciela pojazdu w CEPiK, • ustalenie adresu i numeru telefonu właściciela pojazdu, • powiadomienie właściciela o popełnionym wykroczeniu za pomocą telefonu i wezwanie go do stawiennictwa (gdy posiada telefon), • powiadomienie właściciela o popełnionym wykroczeniu i wezwanie go do stawiennictwa za pomocą druku wezwania, • zakończenie sprawy po zastosowaniu postępowania mandatowego, • sporządzenie wniosku do Sądu Grodzkiego i zakończenie sprawy.	• ustalenie tożsamości właściciela pojazdu – sprawcy wykroczenia, • przedstawienie wykroczenia drogowego, • sprawdzenie osoby i pojazdu w ewidencji WI, • zaproponowanie przyjęcia mandatu karnego wraz z informacją o jego wysokości i prawie odmowy przyjęcia, • wypisanie mandatu karnego, • sporządzenie karty informacyjnej PRD 5, • sporządzenie protokołu przesłuchania sprawcy wykroczenia.

Źródło: opracowanie własne.

Przedstawione czynności zarówno zewnętrzne, jak i wewnętrzne z reguły wykonywane są w obecności sprawcy wykroczenia drogowego w Sekcji Ruchu Drogowego. W rezultacie często występują kolejki osób wezwanych na dany dzień oraz niezadowolenie sprawców wykroczeń.

Po rozgraniczeniu czynności na zewnętrzne i wewnętrzne należy określić metody realizacji czynności zewnętrznych. Na podstawie obserwacji i wyników przeprowadzonych badań ankietowych określono sposób ich realizacji, nośniki informacji, wykonawcę oraz czasowe uzależnienie od obecności petenta (tab. 4).

Uwzględniając dane zamieszczone w tabeli 4 oraz sugestie zmian zawarte w ankietach, można zaproponować następujące usprawnienia czynności zewnętrznych procesu obsługi sprawcy wykroczenia drogowego:

- skrócenie czasu ustalenia właściciela pojazdu w Centralnej Ewidencji Pojazdów i Kierujących możliwe jest poprzez usprawnienie funkcjonowania tego programu na szczeblu centralnym, nie na poziomie SRD KMP,
- bieżące uaktualnianie zawartych w CEPiK danych pojazdów i kierowców przy współpracy z wydziałami komunikacji w miastach i starostwach,
- poprawa wykonania zdjęć możliwa jest tylko i wyłącznie z użyciem sprzętu cyfrowego, a nie analogowego (fotoradary stacjonarne).

Usprawnieniu należy poddać także czynności wewnętrzne. Będzie to wyposażenie stanowiska obsługi w terminal z dostępem do bazy danych, dzięki czemu czas sprawdzenia osób i pojazdów wyniesie około minuty, co oznacza, że nastąpi trzydziestokrotne skrócenie czasu tej czynności. Występująca obecnie rozpiętość czasowa tejże czynności wynika ze znacznego obciążenia policyjnego systemu informatycznego.

Tabela 4. Specyfikacja czynności zewnętrznych

Czynność	Sposób realizacji	Nośniki informacji	Wykonawca	Czasowa zależność
zarejestrowanie sprawy w systemie komputerowym	wpisanie informacji do systemu za pomocą naciskania klawiatury komputera	dokument powstający po wpisaniu danych	policjant	przed
ustalenie właściciela pojazdu w CEPiK	rozmowa telefoniczna z operatorem WI	przekaz werbalny	policjant	przed
ustalenie adresu i numeru telefonu właściciela pojazdu	rozmowa telefoniczna z operatorem WI	przekaz werbalny	policjant	przed
powiadomienie właściciela o popełnionym wykroczeniu za pomocą telefonu i wezwanie go do stawiennictwa (gdy posiada telefon)	rozmowa telefoniczna z właścicielem pojazdu	przekaz werbalny	policjant	przed
powiadomienie właściciela o popełnionym wykroczeniu i wezwanie go do stawiennictwa za pomocą druku wezwania	wypełnienie ręcznie za pomocą długopisu odpowiedniego druku	druk wezwania	policjant	przed
zakończenie sprawy po zastosowaniu postępowania mandatowego	wpisanie ręcznie stosownych danych za pomocą długopisu do odpowiednich druków	odpowiednie druki	policjant	po
sporządzenie wniosku do Sądu Grodzkiego i zakończenie sprawy	naciskanie klawiatury komputera w celu wpisania konkluzji i danych sprawcy wykroczenia	odpowiednio wypełniony dokument	policjant	po

Źródło: opracowanie własne.

Przekształcenie czynności procesu obsługi z wewnętrznych na zewnętrzne oraz wprowadzenie zmian usprawniających

W przypadku obsługi sprawcy wykroczenia drogowego polegającego na przekroczeniu dozwolonej prędkości istnieją określone procedury i algorytmy postępowania[7], które muszą być zachowane. Działając zgodnie z procedurami, przekształceniu z wewnętrznych na zewnętrzne można poddać jedynie dwie czynności.

Pierwszą z nich będzie sprawdzenie w Wydziale Informatyki osoby i pojazdu. Opierając się na wytycznych SMED, ustalono czynniki determinujące czas tej czynności:

- kto dokonuje sprawdzenia osoby i pojazdu? – policjant,
- co się wykonuje? – wpisuje się stosowne dane na kartkę papieru,
- jak się to wykonuje? – pisze się ręcznie za pomocą długopisu,
- gdzie wykonuje się tę czynność? – w siedzibie SRD KMP,
- kiedy się ją wykonuje? – w trakcie wizyty sprawcy wykroczenia.

Przekształcenie czynności wewnętrznej na zewnętrzną sprowadza się do realizacji tej czynności bez zaangażowania klienta, a co za tym idzie – jej eliminację z bezpośredniej obsługi klienta. Obecnie minimalny czas tej czynności wynosi jedną minutę, natomiast maksymalny trzydzieści minut.

Następną czynnością wewnętrzną, która ulegnie przekształceniu na zewnętrzną, będzie wypisanie karty PRD 5 po wizycie „klienta" w siedzibie SRD KMP. Podobnie jak poprzednio ustalono czynniki jej realizacji:

- kto wypisuje kartę PRD 5? – policjant,
- co się wykonuje? – wpisuje się dane sprawcy wykroczenia,
- jak się to wykonuje? – naciska się przyciski klawiatury komputera,
- gdzie się to wykonuje? – w siedzibie SRD KMP,
- kiedy się to wykonuje? – w trakcie wizyty sprawcy wykroczenia.

Przekształcenie operacji z wewnętrznej na zewnętrzną będzie polegać na tym, że policjant wypełni tę kartę PRD 5 poza cyklem bezpośredniej obsługi. Czas ten zostanie wyeliminowany z czasu obsługi „klienta".

Wykaz czynności związanych z obsługą sprawcy wykroczenia drogowego po dokonanych usprawnieniach przedstawia się następująco:

- ustalenie tożsamości właściciela pojazdu – sprawcy wykroczenia,
- przedstawienie wykroczenia drogowego,
- zaproponowanie przyjęcia mandatu karnego wraz z informacją o jego wysokości i prawie odmowy przyjęcia,
- wypisanie mandatu karnego,
- sporządzenie protokołu przesłuchania sprawcy wykroczenia.

Efektem wykorzystania metody SMED jest optymalizacja procesu obsługi „klienta" poprzez eliminację oraz skrócenie czasu czynności wykonywanych w trakcie bezpośredniego kontaktu policjanta ze sprawcą wykroczenia drogowego. Dla wdrożenia zoptymalizowanego procesu, oprócz zmian podanych wyżej, należy również wprowadzić zmiany w algorytmie czynności procesowych.

---

[7] Zarządzenie nr 497 Komendanta Głównego Policji z dnia 25.05.2004 r. w sprawie pełnienia służby przez Policjantów wykorzystujących przyrządy kontrolno-pomiarowe służące do rejestracji zachowań uczestników ruchu drogowego.

Podsumowanie

Proponując wprowadzenie zmian w procesie obsługi sprawcy wykroczenia drogowego związanego z przekroczeniem dozwolonej prędkości, skupiono się jedynie na usprawnieniu przebiegu tych czynności, w stosunku do których istnieją organizacyjne, techniczne i proceduralne możliwości realizacji w obecnej dobie funkcjonowania jednostek policji.

Wyniki przeprowadzonych badań empirycznych obejmują zaledwie jedną z wielu procedur obsługi klientów, realizowanych w komórkach organizacyjnych Policji. Potwierdzają one jednak tezę o efektywności zastosowania metody SMED w realizacji procesów obsługi klientów. W rezultacie proponowanych rozwiązań następuje bowiem istotne skrócenie cyklu procesów, zwiększa się wydajność pracy policjantów, co znacznie poprawia wizerunek policji jako instytucji.

Jak wynika z przedstawionego przypadku, metoda SMED może być ze znacznymi korzyściami stosowana nie tylko w odniesieniu do procesów produkcyjnych, ale także prac administracyjno-biurowych. Daje ona możliwości skrócenia czasu oczekiwania petentów oraz pozwala właściwie organizować czynności osób obsługujących.

Bibliografia

Ankiety sporządzone w trakcie badań realizowanych w Sekcji Ruchu Drogowego Komendy Miejskiej Policji w Krakowie w 2006 roku.

Martyniak Z., *Nowe metody i koncepcje zarządzania*, Wydawnictwo Akademii Ekonomicznej w Krakowie, Kraków 2002.

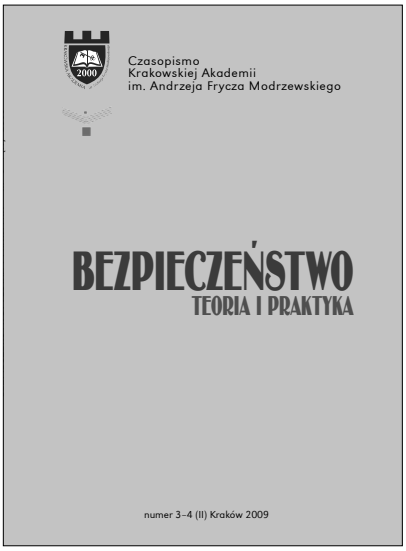
Martyniak Z., *Zastosowanie metody SMED*, Zeszyty Naukowe Akademii Ekonomicznej w Krakowie, nr 486, Kraków 2001.

Mreła H., *Technika organizowania pracy*, Wiedza Powszechna, Warszawa 1965.

Ustawa z dnia 24 sierpnia 2001 r. Kodeks postępowania w sprawach o wykroczenia.

Walczak M., *Próba zastosowania metody SMED w pracach administracyjno-biurowych na przykładzie okienka pocztowego*, Zeszyty Naukowe Akademii Ekonomicznej w Krakowie, nr 616, Kraków 2003.

Zarządzenie nr 497 Komendanta Głównego Policji z dnia 25.05.2004 r. *W sprawie pełnienia służby przez policjantów wykorzystujących przyrządy kontrolno-pomiarowe służące do rejestracji zachowań uczestników ruchu drogowego.*



Polecamy czasopismo Krakowskiej Akademii im. Andrzeja Frycza Modrzewskiego „Bezpieczeństwo. Teoria i Praktyka"

Oprócz aktualnych zagadnień dotyczących głównie bezpieczeństwa międzynarodowego każdy numer zawiera dział „Z kart historii" oraz „Recenzje". Nieodłącznym i cennym elementem czasopisma są streszczenia artykułów w językach polskim, angielskim i rosyjskim.

W numerze 1–2/2010 m.in.:

- Marian Banach, *Bezpieczeństwo ekologiczne a przebieg tras rurociągowych w Eurazji*
- Katarzyna Czajkowska, *Aksjonormatywne podstawy systemu globalnego bezpieczeństwa Organizacji Narodów Zjednoczonych*
- Anna Diawoł, *Znaczenie regionu śródziemnomorskiego w Europejskiej Strategii Bezpieczeństwa*
- Włodzimierz Fehler, *Bezpieczeństwo publiczne jako składnik wewnętrznego bezpieczeństwa państwa*
- Kazimierz Kraj, *Federalna Służba Ochrony Federacji Rosyjskiej*
- Jan A. Księżyk, *Pojęcie i klasyfikacja środków przymusu bezpośredniego stosowanych przez policję w Polsce*
- Bogdan Mucha, *Zakres ingerencji egzekutywy w prawa i wolności obywateli USA w dobie walki z terroryzmem*

Sprzedaż prowadzi:
Księgarnia „U Frycza"
Kampus Krakowskiej Akademii im. Andrzeja Frycza Modrzewskiego
ul. Gustawa Herlinga-Grudzińskiego 1, 30-705 Kraków
tel./faks: (12) 252 45 93
e-mail: ksiegarnia@kte.pl