Ewelina Machura

Informacja i jej znaczenie we współczesnym świecie w kontekście ochrony informacji niejawnych w Polsce

Obronność - Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Obrony Narodowej nr 1(5), 155-167

2013

AUTOR
Ewelina Machura
evemach@interia.pl

INFORMACJA I JEJ ZNACZENIE WE WSPÓŁCZESNYM ŚWIECIE W KONTEKŚCIE OCHRONY INFORMACJI NIEJAWNYCH W POLSCE

Współczesny świat podlega stałemu postępowi cywilizacyjnemu, którego cechami obecnie są już nie tylko szybkość i dynamika, lecz także globalizm, czyli światowy zasięg. Rozwój społeczny, ekonomiczny i technologiczny stopniowo zaciera wszelkie granice, staje się bardziej dostępny dla wszystkich, a kluczową wartością staje się informacja. Coraz częściej słyszymy stwierdzenie, że stajemy się *społeczeństwem informacyjnym*. Termin ten po raz pierwszy pojawił się już w 1963 roku w artykule japońskiego socjologa Tadao Umesao dotyczącym teorii ewolucji społeczeństwa[1]. Społeczeństwo informacyjne, oparte na technologiach informatycznych, gdzie nacisk kładzie się na narzędzia komunikacji, magazynowania oraz przetwarzania informacji, postrzegał jako następstwo społeczeństwa przemysłowego, propagował w rozprawie pt. *Wprowadzenie do teorii informacji* z 1968 roku inny japoński teoretyk mediów Kenichi Koyama. Cechą społeczeństwa informacyjnego jest rozwój intelektualny oparty na wiedzy, a więc na informacji.

Czym więc jest owa informacja, której ranga ciągle wzrasta? Jest wiele definicji i określeń tego pojęcia, nie ma jednej uniwersalnej i jednoznacznej. Informacja (łac. *informatio – przedstawienie, wizerunek; informare – kształtować, przedstawiać*) odmiennie postrzegana jest w różnych dziedzinach nauki, bo to pojęcie interdyscyplinarne. W znaczeniu ogólnym informacja postrzegana jest jako porcja danych, które mogą być przekazywane, przetwarzane i magazynowane – przydatne w wielu sektorach działalności ludzkiej. Z punktu widzenia ekonomicznego postrzega się ją jako zasób – *współcześnie, piątą podstawową kategorią ekonomiczną jest informacja. Informację należy traktować jako zasób podobny do innych zasobów, które mają wartość i wymagają poniesienia określonych kosztów w trakcie ich*

[1] T. Umesao (wersja oryginalna „jōhōka shakai") opracował unikatową teorię dotyczącą rosnącego znaczenie informacji jako zjawiska społecznego, łączącą koncepcje embriologii zwierząt i historii cywilizacji. Twierdził, że wraz z rozwojem mediów i komputerów, informacje staną się ważnym czynnikiem gospodarczym. Swoją teorię zawarł w artykule pt. *Information Industry Theory: Dawn of the Coming Era of the Ectodermal Industry,* opublikowanym 1963 roku w japońskim dzienniku *Hoso Asahi.*

wykorzystania. Informacja jest zasobem niezużywalnym i niewyczerpywalnym[2]*.*

Informacja może też być narzędziem komunikacji – *jest zjawiskiem społecznym, służy do społecznego komunikowania się*[3]*.* Równie ważną rolę odgrywa w życiu wirtualnym, o czym przekonuje M. Karciarz słowami: *Informacja jest dziś najważniejszym elementem cyberprzestrzeni. Jest generowana z danych, które – przetwarzane, komentowane i rozpowszechniane – tworzą nowy wymiar naszej rzeczywistości*[4]*.* Nowym wymiarem informacji staje się we współczesnym świecie traktowanie jej jako *towaru – dobra konsumpcyjnego*[5], które jak każde inne dobro można kupić i sprzedać. Rosnąca ranga i znacznie informacji zarówno w dziedzinie gospodarki, jak i bezpieczeństwa narodowego, stopniowo podnoszą jej cenę. Podsumowując powyższe rozważania, musimy się zgodzić, że współczesna informacja jest obecna we wszystkich dziedzinach i aspektach życia.

Kto ma informację ten ma władzę – co raz częściej słychać ten slogan i trudno się z nim nie zgodzić. Aby zyskać przewagę nad konkurencją, trzeba być szybkim w działaniu, zaś sprawne i trafne podejmowanie decyzji wymaga szybkiej, wiarygodnej i najświeższej informacji. Dostępność niemal całego świata dla wszystkich zainteresowanych, co jest efektem globalnego postępu cywilizacyjnego, pociągnęła za sobą nowe zagrożenie dla bezpieczeństwa narodowego, które przybiera formę niekontrolowanego wycieku informacji o znaczeniu nie tylko gospodarczym, politycznym, ale nawet strategicznym. Nowe zagrożenie wymaga podjęcia radykalnego działania w celu jego wykluczenia bądź minimalizacji. Pojawia się więc konieczność stałego monitoringu sytuacji, a tym samym powołania służb, instytucji czy organizacji, która w oparciu o odpowiednie regulacje prawne zapewni bezpieczeństwo państwa na tej płaszczyźnie. Także Polska, z uwagi na swój rozwój w ostatnich latach, wzrost znaczenia w Europie i na arenie międzynarodowej oraz w dużej mierze poprzez członkostwo w Unii Europejskiej i NATO, stała się podatna na zagrożenie wycieku informacji. Wyciek taki może być efektem niewłaściwego zarządzania zasobami informacyjnymi lub celowego działania służb wywiadowczych i specjalnych, a nawet organizacji terrorystycznych nieprzychylnych Polsce oraz jej polityce wewnętrznej i zagranicznej. Szczególnie ważne i poszukiwane są dane nie tylko te dotyczące wojskowości i obronności państwa, lecz także prowadzonej działalności gospodarczej, techniki i technologii, badań naukowych, a w głównej

[2] D. Dziuba, *Gospodarki nasycone informacją i wiedzą. Podstawy ekonomiki sektora informacyjnego,* Uniwersytet Warszawski, Warszawa 2000, s. 30.

[3] J. Oleński, *Elementy ekonomiki informacji,* Uniwersytet Warszawski, Warszawa 2000, s. 40.

[4] M. Karciarz, *Informacja w Internecie*, Wydawnictwo Naukowe PWN, Warszawa 2010, s. 60.

[5] J. Oleński, *Ekonomika informacji. Podstawy,* Polskie Wydawnictwo Ekonomiczne, Warszawa 2001, s. 310.

mierze polityki wewnętrznej i zewnętrznej państwa, co potwierdzają wnioski zawarte w ogólnie dostępnych raportach, sprawozdaniach, a nierzadko też doniesieniach medialnych.

W odpowiedzi na nowe zagrożenie, w celu zapewnienia bezpieczeństwa informacji szczególnie ważnych dla państwa, we wszystkich krajach powołuje się instytucje, odpowiednio przygotowane i przeszkolone służby, których zadaniem jest stały monitoring stanu bezpieczeństwa informacji oraz eliminacja bądź ograniczanie ich wycieku. Sprawność organów rządzących państwa wiąże się głównie z szybkością i trafnością podejmowanych decyzji, a to z kolei zależy od dostępności dużej ilości wiarygodnych i szczegółowych informacji w danej dziedzinie, dlatego też zarządzanie bezpieczeństwem musi być tak zorganizowane, aby informacje były łatwo dostępne dla osób uprawnionych, a jednocześnie chronione przed nieprawnym wykorzystaniem ich przez postronnych, mogących działać na szkodę państwa.

Skuteczna walka z takim zagrożeniem wymaga odpowiedniej klasyfikacji informacji głównie ze względu na ich wartość, a także ograniczenia dostępu do nich poprzez odpowiednie utajnienie. Oczywiście tak ważny aspekt bezpieczeństwa państwa jak ochrona informacji wymaga odpowiednich regulacji prawnych. Obowiązującym w Polsce normatywem w tej dziedzinie jest wprowadzona dnia 1 stycznia 2011 r. *Ustawa z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych* (Dz.U. z 2010r. nr 182, poz. 1228). Ustawa ta, wraz z wydanymi do niej rozporządzeniami, określa zasady ochrony informacji mających szczególne znaczenie dla państwa – zwanych informacjami niejawnymi, w sytuacji gdy organizacja, przedsiębiorstwo, inny podmiot prawny czy osoba fizyczna prowadzi działalność lub realizuje zadania, w których niezbędny jest dostęp do takich danych. Chcąc więc uzyskać dostęp do pewnych informacji, których nieprawne ujawnienie może stworzyć niebezpieczeństwo dla państwa (w myśl ustawy w celu potwierdzenia przestrzegania zasad ochrony informacji niejawnych), osoba fizyczna musi uzyskać, w toku tak zwanego postępowania sprawdzającego lub kontrolnego, poświadczenie bezpieczeństwa o stosownej klauzuli. Podobnie jest z przedsiębiorcami, którzy poddając się postępowaniu bezpieczeństwa przemysłowego, uzyskują świadectwo bezpieczeństwa przemysłowego, które pozwala im na dostęp do informacji ogólnie niedostępnych, czyli chronionych.

Ustawa o ochronie informacji niejawnych określa sposoby i zasady ochrony informacji niejawnych, poprzez określenie:

1) klasyfikacji informacji niejawnych;
2) zasad organizacji ochrony informacji niejawnych;
3) zasady prowadzenia postępowań sprawdzających i kontrolnych, czy osoba daje rękojmię zachowania tajemnicy oraz postępowania bezpie-

czeństwa przemysłowego określającego, czy przedsiębiorca, prowadząc działalność, właściwie chroni informacje niejawne;

4) zasady przetwarzania informacji niejawnych;

5) sposobu prowadzenia kontroli ochrony informacji niejawnych;

6) zasady ochrony informacji niejawnych w systemach teleinformatycznych;

7) zasady i sposobów stosowania fizycznych zabezpieczeń ochrony informacji niejawnych.

Przepisy ustawy dotyczą wielu organizacji, jednostek organizacyjnych i instytucji, a w szczególności:

1) organów władzy publicznej, w tym:
- Sejmu i Senatu,
- Prezydenta Rzeczypospolitej Polskiej,
- organów administracji rządowej,
- organów jednostek samorządu terytorialnego oraz jednostek przez nie nadzorowanych,
- sądów i trybunałów,
- organów kontroli państwowej i ochrony prawa;

2) jednostek organizacyjnych podległych lub nadzorowanych przez Ministra Obrony Narodowej;

3) Narodowego Banku Polskiego;

4) innych państwowych osób prawnych oraz jednostek organizacyjnych podległych władzy publicznej;

5) przedsiębiorców, w działalności których niezbędny jest dostęp do informacji niejawnych.

Przepisy zawarte w ustawie nie stoją w sprzeczności z przepisami innych ustaw o ochronie tajemnicy prawnie chronionej, np. tajemnicy zawodowej. Ustawodawca podkreśla fakt, iż informacje niejawne mogą być udostępniane tylko osobom dającym rękojmię zachowania tajemnicy i to dodatkowo tylko w zakresie niezbędnym do wykonywania pracy, czy zadania. Aby zrozumieć i właściwie zinterpretować ten zapis, należy koniecznie wyjaśnić pojęcie rękojmia zachowania tajemnicy. W myśl ustawy owa rękojmia to nic innego jak zdolność osoby do spełnienia narzuconych przez ustawę wymogów zapewnienia ochrony informacji niejawnych przed ujawnieniem, a stwierdza się ją w efekcie przeprowadzenia postępowania sprawdzającego. Postępowanie takie prowadzone jest w zakresie zależnym od kategorii informacji niejawnych, do których dostęp jest zainteresowanemu niezbędny. Obecnie istnieją cztery kategorie informacji niejawnych, którym odpowiadają cztery klauzule: *ściśle tajna*, *tajna*, *poufna* i *zastrzeżona*, a ich nadanie konkretnym informacjom zależy od tego, jaki wpływ na bezpieczeństwo państwa może mieć ich nieprawne ujawnienie. Ujawnienie informacji o różnych klauzulach powoduje różne zagrożenie dla bezpieczeństwa państwa:

– ściśle tajne – wyjątkowo poważna szkoda dla Rzeczypospolitej Polskiej;
– tajne – poważna szkoda dla Rzeczypospolitej Polskiej;
– poufne – szkoda dla Rzeczypospolitej Polskiej;
– zastrzeżone – szkodliwy wpływ na wykonywanie zadań.

Przez wyjątkowo poważną szkodę dla RP rozumie się:
– zagrożenie niepodległości, suwerenności bądź integralności terytorialnej RP;
– zagrożenie bezpieczeństwa wewnętrznego (w tym porządku konstytucyjnego);
– zagrożenie sojuszu i pozycji międzynarodowej;
– osłabienie gotowości do obrony RP;
– przyczynianie się do identyfikacji pracowników wywiadu, kontrwywiadu i osób udzielających im pomocy;
– zagrożenie życia lub zdrowia osób wykonujących czynności operacyjno-rozpoznawcze bądź udzielających im pomocy w tym zakresie;
– zagrożenie życia lub zdrowia świadków koronnych lub osób im najbliższych.

Poważną szkodę dla RP stanowią działania, które mogą doprowadzić do:
– uniemożliwienia realizacji zadań ochrony suwerenności państwa i porządku konstytucyjnego;
– pogorszenia stosunków międzynarodowych;
– zakłócenia funkcjonowania Sił Zbrojnych RP;
– utrudnienia wykonywania zadań operacyjno-rozpoznawczych;
– zakłócenia działania organów ścigania i wymiaru sprawiedliwości;
– spowodowania znacznej straty ekonomicznej RP.

Szkoda dla Rzeczypospolitej Polskiej to z kolei:
– utrudnienia w prowadzeniu bieżącej polityki zagranicznej;
– negatywne wpływanie na zdolność bojową i obronność RP;
– zagrożenie bezpieczeństwa obywateli i zakłócenie porządku publicznego;
– zakłócanie i utrudnianie pracy organizacjom odpowiadającym za ochronę bezpieczeństwa i interesów państwa;
– utrudnienie wykonywania zadań instytucjom wymiaru sprawiedliwości, organom ścigania i odpowiedzialnym za utrzymanie porządku publicznego;
– zagrożenie systemu finansowego RP;
– negatywny wpływ na gospodarkę narodową.

Poprzez szkodliwy wpływ na wykonywanie zadań rozumie się – szkodliwy wpływ na wykonywanie zadań przez organy władzy publicznej i inne organizacje w zakresie obronności, polityki zagranicznej, przestrzegania porządku konstytucyjnego, wymiaru sprawiedliwości bądź interesów ekonomicznych państwa.

Stosowną klauzulę dokumentowi – czyli każdej utrwalonej informacji niejawnej – nadaje osoba uprawniona do jego podpisania. Podobnie traktowane są materiały według ustawy stanowiące dokumenty lub przedmioty bądź dowolną ich część, które są chronione jako informacje niejawne, a w szczególności urządzenia, wyposażenie, broń wyprodukowane oraz w trakcie produkcji, jak również składniki użyte do ich produkcji. Szczegółowo zasady i sposoby oznaczania materiałów i umieszczania na nich klauzul tajności określa Rozporządzenie Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. (Dz.U. z 2011r., nr 288, poz.1692). Natomiast zniesienie lub zmiana klauzuli może nastąpić jedynie za pisemną zgodą osoby, która dokument podpisała bądź jej przełożonego tylko w sytuacji ustania lub zmiany ustawowych przesłanek ochrony. W przypadku otrzymania w mocy umów danych niejawnych od innych państw bądź organizacji międzynarodowych nadaje im się polski odpowiednik posiadanej klauzuli. Wszystkie informacje niejawne, którym zostały nadane odpowiednie klauzule, mogą być udostępniane tylko osobom uprawnionym posiadającym odpowiednie poświadczenia, muszą być przetwarzane w taki sposób, aby nie nastąpiło nieprawne ich ujawnienie oraz muszą być odpowiednio chronione z wykorzystaniem środków bezpieczeństwa. Szczegółowe rozwiązania prawne w tym zakresie określają odrębne przepisy wykonawcze. Obecnie obowiązują:

1) w zakresie poświadczeń bezpieczeństwa:

– Decyzja nr 119/MON Ministra Obrony Narodowej z dnia 23 kwietnia 2012 r. w sprawie szczegółowych zasad oraz trybu prowadzenia i dokumentowania postępowań sprawdzających w resorcie obrony narodowej;

– Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie wzorów zaświadczeń stwierdzających odbycie szkolenia w zakresie ochrony informacji niejawnych oraz sposobu rozliczania kosztów przeprowadzenia szkolenia przez Agencję Bezpieczeństwa Wewnętrznego lub Służbę Kontrwywiadu Wojskowego (Dz. U. z 2010 r., nr 258, poz. 1751);

– Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie wzorów poświadczeń bezpieczeństwa (Dz.U. z 2010 r., nr 258, poz. 1752);

– Rozporządzenie Prezesa Rady Ministrów z dnia 22 marca 2011 r. w sprawie wysokości i trybu zwrotu zryczałtowanych kosztów ponoszonych przez Agencję Bezpieczeństwa Wewnętrznego albo Służbę Kontrwywiadu Wojskowego za przeprowadzenie sprawdzenia przedsiębiorcy oraz postępowań sprawdzających (Dz.U. z 2011 r., nr 67, poz. 356);

– Rozporządzenie Rady Ministrów z dnia 5 kwietnia 2011 r. w sprawie wzorów kwestionariusza bezpieczeństwa przemysłowego, świadectwa bezpieczeństwa przemysłowego, decyzji o odmowie wydania świadectwa bezpieczeństwa przemysłowego oraz decyzji o cofnięciu świadectwa bezpieczeństwa przemysłowego (Dz.U. z 2011 r., nr 86, poz. 470);

– Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie wzoru decyzji o odmowie wydania poświadczenia bezpieczeństwa (Dz.U. z 2010 r., nr 258, poz. 1753);

– Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie wzoru decyzji o cofnięciu poświadczenia bezpieczeństwa (Dz.U. z 2010 r., nr 258, poz. 1754);

2) w zakresie przetwarzania, przechowywania, przekazywania informacji niejawnych:

– Rozporządzenie Prezesa Rady Ministrów z dnia 28 grudnia 2010 r. w sprawie przekazywania informacji, udostępniania dokumentów oraz udzielania pomocy służbom i instytucjom uprawnionym do prowadzenia poszerzonych postępowań sprawdzających, kontrolnych postępowań sprawdzających oraz postępowań bezpieczeństwa przemysłowego (Dz.U. 2010 r., nr 258 poz. 1750);

– Rozporządzenie Prezesa Rady Ministrów z dnia 7 grudnia 2011r. w sprawie nadawania, przyjmowania, przewożenia, wydawania i ochrony materiałów zawierających informacje niejawne (Dz. U. 2011 r., nr 271, poz. 1603);

– Rozporządzenie Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych (Dz. U. 2011 r., nr 276, poz. 1631);

– Zarządzenie nr 57/MON Ministra Obrony Narodowej z dnia 16 grudnia 2011 r. w sprawie szczegółowego sposobu organizacji kancelarii tajnych oraz innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za przetwarzanie informacji niejawnych, sposobu i trybu przetwarzania informacji niejawnych oraz doboru i stosowania środków bezpieczeństwa fizycznego;

3) w zakresie bezpieczeństwa teleinformatycznego:

– Rozporządzenie Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz.U. 2011 r., nr 159, poz. 948);

– Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie wzoru świadectwa akredytacji bezpieczeństwa systemu teleinformatycznego (Dz.U. 2011 r., nr 156, poz. 926);

– Decyzja nr 7/MON Ministra Obrony Narodowej z dnia 20 stycznia 2012 r. w sprawie organizacji ochrony systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych w resorcie obrony narodowej.

Powyżej przedstawione zostały tylko główne rozporządzenia i decyzje. Oprócz nich istnieje szereg zarządzeń i wytycznych, które również obowiązują. Należy je stosować w przypadku kontaktów z informacjami, którym nadano klauzulę tajności. Proces przetwarzania, udostępniania, przechowywania informacji niejawnych oraz inne czynności z nimi związane wyma-

gają ciągłego nadzoru i kontroli realizowanych na wszystkich poziomach. W Polsce powołane zostały dwie instytucje nadzorujące funkcjonowanie systemu ochrony informacji niejawnych z ramienia państwa. Są to:

1) Służba Kontrwywiadu Wojskowego (SKW), która wykonuje zadania w stosunku do:

– Ministerstwa Obrony Narodowej oraz jednostek organizacyjnie podległych i nadzorowanych przez Ministra Obrony Narodowej;
– ataszatów obrony w placówkach zagranicznych;
– żołnierzy służby czynnej służących w jednostkach innych niż podporządkowane Ministrowi Obrony Narodowej;

2) Agencja Bezpieczeństwa Wewnętrznego (ABW), nadzorująca wszystkie pozostałe jednostki organizacyjne i osoby.

Do głównych zadań SKW i ABW ustawodawca zaliczył:

– prowadzenie kontroli ochrony informacji niejawnych i przestrzeganie obowiązujących przepisów;
– wykonanie zadań dotyczących bezpieczeństwa teleinformatycznego;
– prowadzenie postępowań sprawdzających i kontrolnych oraz postępowań bezpieczeństwa przemysłowego;
– zapewnienie bezpieczeństwa informacji niejawnych w sytuacji wymian międzynarodowych;
– prowadzenie szkoleń i doradztwa w zakresie ochrony informacji niejawnych.

Dodatkowo Szef ABW pełni rolę krajowej władzy bezpieczeństwa. Krajowa władza bezpieczeństwa jest organem przeznaczonym do nadzorowania systemu ochrony informacji niejawnych w stosunkach Rzeczypospolitej Polskiej z innymi państwami lub organizacjami międzynarodowymi i wydawania dokumentów upoważniających do dostępu do informacji niejawnych NATO, Unii Europejskiej lub innych organizacji międzynarodowych, zwanych dalej „informacjami niejawnymi międzynarodowymi". Szef ABW pełni funkcję krajowej władzy bezpieczeństwa w sferze cywilnej oraz w sferze wojskowej – za pośrednictwem Szefa SKW. Zakres, tryb i sposób współpracy Szefa ABW z Szefem SKW określa Prezes Rady Ministrów w drodze rozporządzenia.

W ramach wykonywanych zadań upoważnieni funkcjonariusze ABW i SKW mają prawo w jednostkach kontrolowanych do:

– wstępu do pomieszczeń i obiektów, gdzie są przetwarzane informacje niejawne;
– wglądu w dokumenty związane z organizacją ochrony informacji niejawnych w jednostce;
– żądania dostępu do systemów teleinformatycznych służących do przetwarzania informacji niejawnych;
– prowadzenia oględzin obiektów oraz kontroli czynności związanych z ochroną informacji;

– żądania od kierowników jednostek organizacyjnych i ich pracowników pisemnych wyjaśnień;

– powoływania biegłych i specjalistów, jeżeli tego wymaga prowadzona kontrola;

– uczestniczenia w posiedzeniach kierownictwa, organów zarządzających lub nadzorczych oraz organów opiniodawczo-doradczych w sprawach dotyczących problematyki ochrony informacji niejawnych.

Na szczeblu jednostki organizacyjnej, w której przetwarzane są informacje niejawne, za bezpieczeństwo i ochronę informacji niejawnych, a w szczególności za zorganizowanie i zapewnienie funkcjonowania tej ochrony odpowiada jej kierownik. Ochrona informacji niejawnych w jednostce jest organizowana i realizowana w oparciu o plan ochrony informacji niejawnych, w tym postępowania z materiałami, które zawierają informacje o klauzuli *tajne* bądź *ściśle tajne*, w sytuacji wprowadzenia stanu nadzwyczajnego.

Nadzór i kontrola nad ochroną informacji niejawnych objąć musi szereg elementów, a w szczególności właściwe klasyfikowanie informacji niejawnych, organizację ochrony, przetwarzania i przechowywania informacji niejawnych, prowadzenie postępowań kontrolnych i sprawdzających oraz postępowania bezpieczeństwa przemysłowego, ochronę systemów teleinformatycznych, a także stosowanie środków bezpieczeństwa fizycznego. W jednostkach organizacyjnych, w których istnieje konieczność dostępu do informacji niejawnych, występują specjalne piony funkcjonalne oraz osoby funkcyjne odpowiadające za ochronę informacji niejawnych. Kierownik jednostki organizacyjnej zatrudnia pełnomocnika do spraw ochrony informacji niejawnych, który bezpośrednio mu podlega i odpowiada za zapewnienie przestrzegania przepisów o ochronie informacji niejawnych. Szczegółowe zadania i kompetencje pełnomocnika określa Rozporządzenie Ministra Obrony Narodowej z dnia 2 listopada 2011 r. w sprawie szczegółowych zadań pełnomocników ochrony w zakresie ochrony informacji niejawnych w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych (Dz.U. z 2011 r., nr 252, poz. 1519). Dodatkowo w jednostkach organizacyjnych może występować specjalnie wyodrębniona komórka organizacyjna, zwana pionem ochrony, wspierająca realizację zadań przez pełnomocnika ochrony w zakresie ochrony informacji niejawnych, która mu bezpośrednio podlega. Każdorazowo w sytuacji stwierdzenia naruszenia przepisów ochrony informacji niejawnych pełnomocnik ochrony zawiadamia o zaistniałym fakcie kierownika jednostki organizacyjnej oraz podejmuje niezwłocznie czynności zmierzające do wyjaśnienia przyczyn zaistniałej sytuacji, a także minimalizacji jej negatywnych skutków. Jeżeli naruszenie dotyczy informacji o klauzuli *poufne* i wyżej pełnomocnik zobowiązany jest powiadomić również ABW bądź SKW, stosownie do kompetencji.

W jednostkach organizacyjnych, gdzie przetwarzane są dane o klauzuli *tajne* i *ściśle tajne,* kierownik jednostki tworzy kancelarię tajną oraz zatrudnia jej kierownika, który podlega pełnomocnikowi ochrony. Za zgodą kierownika jednostki organizacyjnej może ona również przetwarzać materiały o klauzuli *poufne* i *zastrzeżone*. Kancelaria jest elementem wchodzącym w strukturę pionu ochrony, a jej pracownicy są pracownikami pionu ochrony. Kancelaria tajna jednostki organizacyjnej odpowiada za właściwą rejestrację, przechowywanie, obieg oraz wydawanie uprawnionym osobom materiałów niejawnych. Takie rozwiązanie organizacyjne pozwala w każdej chwili ustalić, gdzie znajduje się dokument *tajny* bądź *ściśle tajny,* a także kto miał do niego dostęp.

Jeżeli w jednostce przetwarzane są informacje o klauzuli *poufne* i wyżej, pełnomocnik opracowuje dokumentację określającą poziom zagrożeń związanych z nieuprawnionym dostępem do informacji niejawnych bądź ich utratą. W celu uszczegółowienia zasad stosowania przepisów o ochronie informacji niejawnych oraz sprecyzowania obiegu dokumentów pełnomocnik ochrony sporządza dokumenty określające: sposób i tryb przetwarzania informacji niejawnych o klauzuli *poufne* w podległych komórkach organizacyjnych, a także instrukcję dotyczącą sposobu i trybu przetwarzania informacji niejawnych o klauzuli *zastrzeżone* oraz zakres i warunki stosowania środków bezpieczeństwa fizycznego w celu ich ochrony. Oczywiście wszystkie te dokumenty zatwierdza kierownik jednostki organizacyjnej.

W celu dodatkowej ochrony informacji niejawnych jednostki organizacyjne stosują środki bezpieczeństwa fizycznego stosowne do istniejącego poziomu zagrożeń, których rolą jest zapewnienie ochrony przed: obcymi służbami specjalnymi i wywiadowczymi, zamachami terrorystycznymi i sabotażem, kradzieżą bądź zniszczeniem materiałów niejawnych, próbami wejścia do pomieszczeń, gdzie przetwarzane są materiały niejawne osób nieuprawnionych, a także próbami dostępu do informacji niejawnych o wyższej klauzuli tajności niż posiadane uprawnienia. Środki ochrony fizycznej to głównie strefy ochronne, system kontroli wejść i wyjść ze stref ochronnych oraz stosowne urządzenia i wyposażenie służące do ochrony informacji niejawnej, które posiadają certyfikat.

Jeżeli w jednostce organizacyjnej istnieją systemy teleinformatyczne służące do przetwarzania informacji niejawnych o klauzuli od *poufne* wzwyż, konieczne jest wykonanie akredytacji bezpieczeństwa teleinformatycznego. Akredytację bezpieczeństwa uzyskuje system teleinformatyczny na podstawie zatwierdzonej przez ABW bądź SKW dokumentacji bezpieczeństwa systemu oraz wyników audytu bezpieczeństwa systemu teleinformatycznego, który również prowadzi stosownie do właściwości ABW lub SKW. W celu weryfikacji i bieżącej kontroli zgodności funkcjonowania systemu teleinformatycznego ze szczególnymi wymaganiami bezpieczeństwa oraz przestrzegania procedur bezpieczeństwa teleinformatycznego, kie-

rownik jednostki organizacyjnej powołuje pracownika pionu ochrony do funkcji inspektora bezpieczeństwa teleinformatycznego. Ponadto stosownie do potrzeb powołuje się jednego bądź kilku administratorów systemów teleinformatycznych. Administrator systemu teleinformatycznego odpowiada za funkcjonowanie systemu teleinformatycznego oraz za przestrzeganie zasad i wymagań bezpieczeństwa przewidzianych dla systemu teleinformatycznego. Zasady powoływania oraz szczegółowe zadania osób funkcyjnych czuwających nad bezpieczeństwem teleinformatycznym określone zostało w odrębnych przepisach wykonawczych.

Jak powszechnie wiadomo w każdym systemie najsłabszym ogniwem z reguły jest człowiek, dlatego też duży nacisk kłaść należy na szkolenie oraz uświadamianie roli ochrony informacji niejawnych w funkcjonowaniu we współczesnej rzeczywistości. Zgodnie z obowiązującą normą prawną w jednostkach organizacyjnych, w których działalność wiąże się z dostępem do informacji niejawnych, prowadzi się trzy rodzaje szkoleń:

1) podstawowe – dla osób pełniących służbę lub zatrudnionych w jednostce organizacyjnej w celu zapoznania z obowiązującymi zasadami ochrony informacji niejawnych oraz obowiązującą dokumentacją – szkolenie organizuje i prowadzi pełnomocnik ochrony lub wyznaczony przez niego pracownik pionu ochrony;

2) uzupełniające – dla osób pełniących służbę lub zatrudnionych w jednostce organizacyjnej, realizowane w przypadku zaistnienia istotnych zmian przepisów dotyczących problematyki ochrony informacji niejawnych bądź w przypadku uzyskania negatywnych wyników w czasie kontroli przestrzegania przepisów – organizuje i prowadzi je pełnomocnik ochrony lub wyznaczony przez niego pracownik pionu ochrony;

3) specjalistyczne – dla kandydatów na pełnomocników ochrony, zastępców pełnomocników ochrony, administratorów systemów teleinformatycznych, inspektorów bezpieczeństwa teleinformatycznego oraz pracowników kancelarii tajnych oraz innych komórek odpowiedzialnych za przetwarzanie informacji niejawnych w celu przygotowania do wykonywania obowiązków służbowych – organizuje i prowadzi SKW.

Szkolenia to bardzo istotny aspekt ochrony informacji niejawnych w każdej jednostce organizacyjnej, w której konieczny jest dostęp do tego typu informacji. Spoglądając poprzez pryzmat jednej z podstawowych zasad prawa, wywodzącej się z prawa rzymskiego, a brzmiącej: nieznajomość prawa szkodzi *(łac. Ignorantia iuris nocet),* należy podkreślić fakt, iż za łamanie przepisów prawa o ochronie informacji niejawnych grożą poważne sankcje karne. Odpowiedzialność karna za popełnione przestępstwa przeciwko ochronie informacji została określona w rozdziale XXXIII Kodeksu Karnego art. 265 – 269 (Dz. U. z 1997r., nr 88, poz. 553 z późniejszymi zmianami).

Podejmując problematykę roli informacji jako nowej wartości współczesnego świata oraz wynikającej z powyższego faktu konieczności ochrony informacji niejawnych na potrzeby zapewnienia bezpieczeństwa narodowego państwa, należy zdawać sobie sprawę ze złożoności, obszerności, a przy tym drażliwości prezentowanej tematyki.

Zagrożenia stanowią podstawową i pierwotną kategorię bezpieczeństwa narodowego. Dlatego też określenie ich współczesnego charakteru jest podstawowy krokiem w procesie tworzenia bezpieczeństwa narodowego[6]. Ważne jest zidentyfikowanie zagrożeń, a głównie tych nowych, wynikających z ciągłego postępu cywilizacyjnego. Takim też zagrożeniem jest niewątpliwie niekontrolowany wyciek informacji o znaczeniu politycznym, gospodarczym, a nawet strategicznym, a jego identyfikacja pociąga za sobą konieczność ciągłego monitoringu oraz poszukiwania nowych rozwiązań w celu sprawniejszej realizacji zadań z zakresu ochrony informacji, które nie powinny być ogólnie dostępne, a przez to zwane są informacjami niejawnymi.

Podstawą walki z każdym zagrożeniem jest dostosowany do realiów szczegółowy zbiór unormowań prawnych, który pozwoli na realizację zadań w celu przeciwdziałania zagrożeniu bądź zmniejszeniu jego negatywnych skutków. Polska uporała się z tym wymaganiem, gdyż w naszym prawodawstwie obecnie obowiązuje stosunkowo nowa ustawa z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych, a ponadto szereg aktów wykonawczych do ustawy, które przyjmują postać rozporządzeń, decyzji i zarządzeń. Ich rolą jest szczegółowe doprecyzowanie zapisów ustawy. Normatywy te są stale uaktualniane, a w miarę potrzeb powstają nowe, co niewątpliwie jest wyjściem naprzeciw potrzebie identyfikacji i monitoringu zagrożeń, w celu ich eliminacji bądź minimalizacji negatywnego wpływu na bezpieczeństwo narodowe.

Bibliografia:

1. Dziuba D., *Gospodarki nasycone informacją i wiedzą. Podstawy ekonomiki sektora informacyjnego,* Uniwersytet Warszawski, Warszawa, 2000.

2. Jakubczak R., Flis J. (red.), *Bezpieczeństwo narodowe Polski w XXI wieku, wyzwania i strategie,* BELLONA, Warszawa 2006.

3. Karciarz M., *Informacja w Internecie*, Wydawnictwo Naukowe PWN, Warszawa 2010.

[6] R. Jakubczak, J. Flis (red.), *Bezpieczeństwo narodowe Polski w XXI wieku. Wyzwania i strategie,* BELLONA, Warszawa 2006, s. 97.

4. Oleński J., *Ekonomika informacji. Podstawy,* Polskie Wydawnictwo Ekonomiczne, Warszawa 2001.
5. Oleński J., *Elementy ekonomiki informacji,* Uniwersytet Warszawski, Warszawa 2000.
6. *Ustawa z dnia 05 sierpnia 2010r. o ochronie informacji niejawnych* (Dz.U. 2010, nr 182, poz. 1228).

INFORMATION AND ITS IMPORTANCE IN THE MODERN WORLD IN THE CONTEXT OF CLASSIFIED INFORMATION PROTECTION IN POLAND

Abstract: This article deals with the role of information in the modern world, which has changed along with the civilization development adopting the role of a consumer good, the price of which constantly grows. This fact resulted in the emergence of a new threat to national security, i.e. uncontrolled leak of information. The article also touches on the issue of information protection as a means of counteracting the new threat to the Polish national security in the light of the binding law on classified information protection of 5 August 2010.