Lidia Więcaszek-Kuczyńska

Wybrane regulacje prawne w obszarze zagrożeń bezpieczeństwa informacyjnego : część pierwsza

Obronność - Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Obrony Narodowej nr 3(11), 139-155

2014

AUTOR
mgr Lidia Więcaszek-Kuczyńska
lidiakuczynska@neostrada.pl

WYBRANE REGULACJE PRAWNE W OBSZARZE ZAGROŻEŃ BEZPIECZEŃSTWA INFORMACYJNEGO. CZĘŚĆ PIERWSZA

Wstęp

Efektywne funkcjonowanie w różnych dziedzinach życia społecznego i gospodarczego jest we współczesnym świecie uwarunkowane nieustannie rosnącym znaczeniem informacji oraz rozwojem środków umożliwiających ich zbieranie i przesyłanie[1].

Zaawansowane technologicznie społeczeństwa wieku informacji, które swój status i rozwój wiążą coraz silniej z informacją przetworzoną, archiwizowaną i przesyłaną w systemach teleinformatycznych, rozpatrują informację jako towar, nierzadko o znaczeniu strategicznym, jako składnik procesów biznesowych w przedsiębiorstwach komercyjnych, a także w organizacji, jaką jest państwo[2]. Bez wątpienia zatem nieodzowne staje się zwrócenie szczególnej uwagi na problematykę zagrożeń bezpieczeństwa informacyjnego we wszystkich dziedzinach, gdzie przepływ informacji stanowi istotny czynnik decyzyjny i determinujący osiągnięcie założonych celów: od wielkiej polityki poprzez wojsko, energetykę, finanse, logistykę, media, po indywidualne wybory konsumenta dóbr.

Wraz ze wzrostem roli informacji wiek XXI, w literaturze przedmiotu nazwany wiekiem informacji, przyniósł zmianę postaci zagrożeń na świecie, gdyż w czasach powszechnego dostępu do technik informatycznych, rodzą się nowe zagrożenia[3] blisko powiązane z wykorzystywaniem sieci informatycznych, np. przestępstwa, w których komputer jest narzędziem, a utrata informacji to skutek włamań do komputerów, często użycia złośliwych kodów i wirusów, aktów sabotażu, wandalizmu, szpiegostwa[4]. Zidentyfikowanie, osiągnięcie, utrzymanie i optymalizowanie bezpieczeństwa informacyjnego staje się zatem konieczne do zapewnienia przewagi kon-

[1] A. M. Dereń, *Prawna ochrona informacji w krajowym ustawodawstwie, wybrane zagadnienia,* Zeszyt 2008, OPO Bydgoszcz 2001, s. 11.

[2] K. Liderman, *Bezpieczeństwo informacyjne*, Wydawnictwo Naukowe PWN, Warszawa 2012, s. 18-19.

[3] *Zagrożenie (…) to najbardziej klasyczny czynnik środowiska bezpieczeństwa.* Zob., S. Koziej, *Teoria sztuki wojennej*, Bellona, Warszawa 2011, s. 268.

[4] K. Liderman, *Bezpieczeństwo…,* wyd. cyt., s. 24.

kurencyjnej podmiotów gospodarczych, ich płynności finansowej, rentowności, pozostawania w zgodzie z normami prawa[5].

Celem niniejszego opracowania, składającego się z dwóch części, jest przedstawienie wybranych przepisów prawa w obszarze zagrożeń bezpieczeństwa informacyjnego, stanowiących regulacje szczególnie istotne w praktyce organizacji będącej przedsiębiorstwem komercyjnym, narażonej na szereg zagrożeń dotykających bezpośrednio cennego zasobu firmy[6], jakim jest informacja.

Zagrożenia bezpieczeństwa informacyjnego

Zanim zostanie nakreślony zarys regulacji prawnych w sferze zagrożeń bezpieczeństwa informacyjnego, zasadne wydaje się przybliżenie definicji zagrożeń bezpieczeństwa informacyjnego, poprzez próbę odpowiedzi na pytanie: jak rozumieć pojęcie *bezpieczeństwo* oraz pojęcie *zagrożenie*.

Analizując stanowisko badaczy, należy stwierdzić, że termin *bezpieczeństwo* jest do zdefiniowania niełatwy, gdyż bezpieczeństwo to nie tylko stan możliwy do opisania jedynie w ustalonym miejscu i czasie (tu i teraz), ale także zmieniający się w czasie proces[7], jednocześnie *bezpieczeństwo można określić, jako pewność istnienia i przetrwania, posiadania oraz funkcjonowania i rozwoju podmiotu. Pewność jest wynikiem nie tylko braku zagrożeń (…), ale także powstaje w skutek kreatywnej działalności danego podmiotu i jest zmienna w czasie, czyli ma naturę procesu społecznego*[8].

S. Koziej charakteryzuje bezpieczeństwo podmiotu jako proces, tj. *tę dziedzinę jego aktywności, która zmierza do zapewnienia możliwości przetrwania, rozwoju i swobody realizacji własnych interesów w konkretnych warunkach, poprzez wykorzystanie okoliczności sprzyjających (szans), podejmowanie wyzwań, redukowanie ryzyka oraz przeciwdziałanie (zapobieganie i przeciwstawianie się) wszelkiego rodzaju zagrożeniom dla podmiotu i jego interesów*[9].

W opinii K. Lidermana bezpieczeństwo informacyjne do obecnej chwili nie doczekało się jednoznacznej wykładni i razem z towarzyszącym mu

[5] A. Nowak, W. Scheffs, *Zarządzanie bezpieczeństwem informacyjnym*, AON, Warszawa 2010, s. 22.

[6] Zob., R. Zygała, *Podstawy zarządzania informacją w przedsiębiorstwie*, Wydawnictwo Akademii Ekonomicznej im. Oskara Langego, Wrocław, 2007, s. 7, 16.

[7] T. Łoś-Nowak, *Bezpieczeństwo,* [w:] A. Antoszewski i R. Herbut (red.), *Leksykon politologii*, Alta 2, Wrocław 2004, s. 37-38.

[8] R. Zięba, *Wprowadzenie. Pozimnowojenny paradygmat bezpieczeństwa międzynarodowego,* [w:] R. Zięba (red.), *Bezpieczeństwo międzynarodowe po zimnej wojnie*, Wydawnictwa Akademickie i Profesjonalne, Warszawa 2008, s. 16.

[9] S. Koziej, *Teoria sztuki wojennej*, Bellona, Warszawa 2011, s. 255.

terminem *bezpieczeństwo informacji*[10] jest używane w różnych znaczeniach[11], dotykając wszystkich form, również werbalnych, wymiany, przechowywania oraz przetwarzania informacji[12].

K. Liderman bezpieczeństwo informacyjne[13] opisuje jako należyte zaufanie podmiotu do jakości i dostępności pozyskiwanej i wykorzystywanej informacji, pojęcie bezpieczeństwa informacyjnego obejmuje zatem podmiot (człowiek, organizacja), który może być zagrożony utratą zasobów informacyjnych lub otrzymaniem informacji o niewłaściwej jakości[14].

Bezpieczeństwo informacyjne określa się w literaturze przedmiotu także jako stan, w którym ryzyko wystąpienia zagrożeń związanych z prawidłowym funkcjonowaniem zasobów informacyjnych jest ograniczone do akceptowalnego poziomu[15].

Bezpieczeństwo informacyjne staje się gwarantem bezpieczeństwa militarnego, finansowego, gospodarczego zarówno w skali lokalnej, pojedynczego państwa, jak i na arenie międzynarodowej[16], co znajduje odpowiedź w opracowanych i wdrażanych przez państwo polskie strategiach oraz programach rządowych w zakresie bezpieczeństwa informacyjnego.

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej[17], dokument *Rządowy program ochrony cyberprzestrzeni RP na lata 2009-2011*, oraz dokument pod nazwą *Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej* odnoszą się do obszarów bezpieczeństwa informacyjnego, wskazując, iż *w dobie rosnącego znaczenia bezpieczeństwa informacyjnego, w tym wzrostu znaczenia procesów gromadzenia, przetwarzania i dystrybuowania informacji w certyfikowanych systemach teleinformatycznych, rośnie (…) rola bezpieczeństwa informacyjnego*

[10] Por., *Kiedy mówimy o bezpieczeństwie informacyjnym, to zawsze dotyczy to podmiotu, który jest zagrożony przez brak informacji (…). Natomiast bezpieczeństwo informacji to ochrona informacji będącej w posiadaniu tego właśnie podmiotu.* A. Nowak, W. Scheffs, *Zarządzanie…,* wyd. cyt. s. 25.

[11] K. Liderman, *Bezpieczeńswo…,* wyd. cyt., s. 13.

[12] Tamże, s. 22.

[13] Zob., *(…) bezpieczeństwo informacji oznacza uzasadnione (…) zaufanie, że nie zostaną poniesione potencjalne straty wynikające z niepożądanego (przypadkowego lub świadomego) ujawnienia, modyfikacji, zniszczenia lub uniemożliwienia przetwarzania informacji przechowywanej, przetwarzanej i przesyłanej w określonym systemie jej obiegu.* Tamże, s. 22.

[14] Tamże, s. 22.

[15] M. Wrzosek, *Procesy informacyjne w zarządzaniu organizacją zhierarchizowaną*, AON, Warszawa 2010, s. 150.

[16] K. Liderman, *Bezpieczeństwo…,* wyd. cyt., s. 23.

[17] Strategia Bezpieczeństwa Narodowego RP w Rzeczypospolitej Polskiej, Warszawa 2007, pkt. 3.8. stanowi: *Zwalczanie zagrożeń rządowych systemów teleinformatycznych i sieci telekomunikacyjnych ma na celu przeciwdziałanie przestępczości komputerowej oraz innym wrogim działaniom wymierzonym w infrastrukturę telekomunikacyjna, w tym zapobieganie atakom na elementy tej infrastruktury. Szczególne znaczenie ma ochrona informacji niejawnych przechowywanych lub przekazywanych w postaci elektronicznej.* Źródło: http://www.iniejawna.pl/pomoce/przyc_pom/SBN_RP.pdf, [dostęp: 22.02.2014].

w aspekcie cybernetycznym. Szczególną dziedziną bezpieczeństwa informacyjnego jest ochrona informacji niejawnych, a zatem takich, których nieuprawnione ujawnienie powoduje lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne[18]*.*

W definiowaniu terminu *bezpieczeństwo informacyjne* słuszne wydaje się odwołanie do norm PN-ISO/IEC 27001: 2007 oraz PN-ISO/IEC 17799: 2007, posługujących się terminem bezpieczeństwo informacji, gdzie jest on opisany, jako *zachowanie poufności, integralności i dostępności informacji; dodatkowo mogą być brane pod uwagę inne własności, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność*[19]*.*

Norma ISO/IEC 17799[20] odnosi się do bezpieczeństwa informacji kompleksowo i dostarcza rozwiązań, dzięki którym eliminuje się nawet najczęściej marginalizowane zagadnienia w tworzeniu procedur bezpieczeństwa[21]*,* a regulacje lokalne wszystkich państw korzystają z tego dokumentu jako pewnego rodzaju referencji[22].

Pojęcie *zagrożenie* możemy zaś scharakteryzować za P. Bączkiem podającym m.in. definicję leksykalną pojęcia, jako: *postraszyć kogoś, zapowiedzieć coś złego, ostrzec pod groźbą jakichś konsekwencji* oraz *stać się niebezpiecznym, groźnym dla kogoś, czegoś* oraz definicje politologiczne, w których *zagrożenia to wyzwania niepodejmowane lub podejmowane za późno*[23]*.*

S. Koziej opisuje zagrożenie jako pośrednie lub bezpośrednie destrukcyjne oddziaływanie na podmiot, wyodrębniając zagrożenie potencjalne lub realne, subiektywne i obiektywne, zewnętrzne i wewnętrzne, militarne i niemilitarne (lokując zagrożenia informacyjne w grupie zagrożeń niemilitarnych, razem z zagrożeniami politycznymi, ekonomicznymi, społecznymi, ekologicznymi)[24].

Lokalizacja źródeł zagrożenia pozwala wyodrębnić zagrożenia bezpieczeństwa informacyjnego wewnętrzne, powstające wewnątrz organizacji, takie jak: zagrożenie utratą, uszkodzeniem danych lub brakiem możliwości

[18] *Biała Księga Bezpieczeństwa Narodowego RP*, źródło: http://www.spbn.gov.pl/, [dostęp: 22.02.2014].

[19] Por., K. Liderman, *Bezpieczeństwo…,* wyd. cyt., s. 19-20.

[20] PN-ISO/IEC 17799: 2007 Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zarządzania bezpieczeństwem informacji – Zakres: *Przedstawiono zalecenia i ogólne zasady dotyczące inicjowania działań, wdrażania, utrzymania i doskonalenia zarządzania bezpieczeństwem informacji w organizacji. Cele stosowania zabezpieczeń przedstawione w normie są powszechnie akceptowanymi praktykami zarządzania bezpieczeństwem informacji.* Źródło: http://www.pkn.pl/ [dostęp 22.04.2014].

[21] A. Nowak, W. Scheffs, *Zarządzanie…,* wyd. cyt., s. 35.

[22] Tamże, s. 35-36.

[23] P. Bączek, *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Wydawnictwo Adam Marszałek, Toruń 2006, s. 31.

[24] S. Koziej, *Teoria…,* wyd. cyt., s. 269.

obsługi z powodu błędu jak i przypadku, zagrożenie utratą lub uszkodzeniem poprzez celowe działania nieuczciwych użytkowników oraz zewnętrzne powstające poza organizacją w wyniku celowego lub przypadkowego działania ze strony osób trzecich w stosunku do systemu. Eksperci wyodrębniają także zagrożenia fizyczne, w których szkoda jest spowodowana wypadkiem, awarią, lub innym nieprzewidzianym zdarzeniem wpływającym na system informacyjny[25].

W opinii P. Bączka zagrożenie bezpieczeństwa informacyjnego może mieć swe źródło w działalności człowieka lub organizacji i wyrażać się jako:

- nieuprawnione ujawnienie informacji tzw. wyciek lub przeciek;
- naruszenie przez władze praw obywatelskich;
- asymetria w międzynarodowej wymianie informacji;
- działalność grup świadomie manipulujących przekazem informacji;
- niekontrolowany rozwój nowoczesnych technologii bioinformatycznych;
- przestępstwa komputerowe;
- cyberterroryzm;
- walka informacyjna[26];
- zagrożenia asymetryczne;
- szpiegostwo[27].

A. Kwintowski zagrożenia bezpieczeństwa informacyjnego wiąże ze *szpiegostwem gospodarczym, hackerstwem, czy walką o utrzymanie się na rynku i zwalczanie konkurencji (…) ponadto pracownicy w sposób nieświadomy wyprowadzają cenne dane z siedziby firmy narażając je na udostępnienie osobom nieupoważnionym*[28]*.*

Bez wątpienia zgodzić się trzeba z J. Łuczakiem, iż *niewiele sytuacji kryzysowych firmy można porównać z utratą informacji,* szczególnie, że jak dowodzi praktyka, utrata informacji to incydenty coraz bardziej powszechne i trudne do wykrycia, przynoszące konsekwencje prawne, finansowe, utratę wiarygodności podmiotu dopuszczającego do nieuprawnionego dostępu osób trzecich do swoich danych[29]. Obserwowany we współczesnej rzeczywistości gospodarczej dynamiczny rozwój sieci komputerowych przyczynia się także do tego, iż zbiory danych przepływają między organi-

[25] A. Żebrowski, W. Kwiatkowski, *Bezpieczeństwo informacji III Rzeczypospolitej*, Oficyna Wydawnicza ABRYS, Kraków 2000, s. 65.

[26] Zob., J. Janczak, *Zakłócenia informacyjne*, AON, Warszawa 2001, s. 11. Autor definiuje istotę i techniki prowadzenia walki informacyjnej.

[27] P. Bączek, *Zagrożenia…,* wyd. cyt., s. 86-87.

[28] A. Kwintowski, *Realia wdrażania systemu zarządzania bezpieczeństwem informacji,* [w:] M. Cisek, T. Nowogródzka (red.), *Stabilność Organizacji we współczesnej gospodarce*, Studio Emka, Warszawa 2014, s. 69.

[29] J. Łuczak, (red.) *Zarządzanie bezpieczeństwem informacji*, Oficyna współczesna, Poznań 2004, s. 10-11.

zacjami w sposób nie zawsze należycie kontrolowany. Komputerowe przetwarzanie danych umożliwia centralizację przechowywania i przetwarzania zasobów informacyjnych, co powoduje niespotykane dotąd zagrożenie utraty zasobów informacyjnych[30].

Rozważając zagrożenia bezpieczeństwa informacyjnego, należy także zaznaczyć, iż pewne informacje stanowią w organizacji wiadomości chronione, a tajność to jeden z atrybutów ochrony informacji (obok m.in. integralności, dostępności, niezaprzeczalności i autentyczności) stanowiący o wymaganym stopniu ochrony informacji przed nieuprawnionym dostępem[31].

Bez wątpienia, za najbardziej wrażliwe na zagrożenia nieuprawnionym ujawnieniem informacji (wyciek lub przeciek) uznaje się takie obszary działalności, jak: planowanie polityczne, zarządzanie w skali makroekonomicznej, politykę obronną, wywiad i kontrwywiad wojskowy[32].

Ataki na zbiory danych stanowiących tajemnicę państwową lub służbową prowadzą do przejęcie niedozwolonego, nieuprawnionego nadzoru nad chronionymi systemami, do ingerencji w nie oraz do usunięcia dowodów takich działań. Ataki te mogą być prowadzone przez modyfikowanie strumienia danych, kreowanie danych zafałszowanych (ataki aktywne) lub na podsłuchiwaniu, monitorowaniu transmisji danych (ataki pasywne) i następnie do poznania zawartości przekazu[33].

W świetle jednej z definicji bezpieczeństwa informacyjnego[34], w której podkreśla się rolę podmiotu charakteryzującego się określonym poziomem zaufania do jakości i dostępności pozyskiwanej i wykorzystywanej informacji, trafne wydaje się odwołanie do opinii K. Lidermana, iż ze względu na znaczenie dla użytkownika wszystkie wykorzystywane przez niego informacje powinniśmy klasyfikować jako wrażliwe bądź niewrażliwe. Wrażliwe te informacje, które muszą być chronione, gdyż tak stanowią obowiązujące przepisy. Niewrażliwe zaś to takie, których nakaz ochrony nie jest zawarty w regulacjach prawnych, ale organizacjom wytwarzającym je i przetwarzającym są wskazywane przez właściwe organy w danej organizacji[35].

Osoby odpowiedzialne za ochronę informacji powinny zatem dbać o ochronę informacji wrażliwych, a nie *danych osobowych*, czy informacji niejawnych, gdyż te kategorie informacji są jedynie szczególnym przypadkiem informacji wrażliwej[36].

[30] M. Wrzosek, *Procesy…,* wyd. cyt., s. 152.
[31] K. Liderman, *Bezpieczeństwo*…, wyd. cyt., s. 19.
[32] A. Żebrowski, W. Kwiatkowski, *Bezpieczeństwo…,* wyd. cyt. s. 78.
[33] Tamże, s. 63.
[34] Zob., K. Liderman, *Bezpieczeństwo…,* wyd. cyt., s. 22.
[35] Tamże, s. 21.
[36] Tamże, s. 21.

System prawno-karnej ochrony informacji

Wolność słowa i dostęp do informacji stanowią fundament standardów cywilizacyjnych obowiązujących w państwach demokratycznych.

Od czasu uchwalonej w Rzymie Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności[37] podstawę tworzenia społeczeństwa demokratycznego stanowi poszanowanie swobodnego dostępu do informacji, a usiłowanie ograniczania tego prawa traktuje się jako atak na podstawowe prawa człowieka[38].

W systemie legislacyjnym Unii Europejskiej dostęp do informacji publicznej jest uregulowany w aktach prawnych związanych zarówno bezpośrednio, jak i pośrednio z tym rodzajem informacji. Art. 255 ust. 1 Traktatu ustanawiającego Unię Europejską[39] gwarantuje, iż każdy obywatel Unii i każda osoba fizyczna lub prawna z miejscem zamieszkania w jednym z krajów członkowskich ma prawo do dostępu do dokumentów Parlamentu Europejskiego, Rady i Komisji z zastrzeżeniem zasad przewidzianych w odrębnych przepisach[40]. Decyzja Rady 2000/23/WE orzeka, *iż dostęp do informacji nie jest dozwolony, jeżeli jej ujawnienie mogłoby zaszkodzić interesowi publicznemu, ochronie dóbr osobistych i prywatności, ochronie tajemnicy handlowej czy przemysłowej ochronie wspólnotowych interesów finansowych*[41]*.*

Na uniwersalny charakter zasady nieskrępowanego dostępu do informacji mają wpływ akty prawa międzynarodowego, wśród których, prócz wspomnianej uprzednio *Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności z roku 1950*, należy wymienić Powszechną Deklarację Praw Człowieka ONZ z roku 1948 oraz Międzynarodowy Pakt Praw Obywatelskich i Politycznych uchwalony w Nowym Jorku w roku 1966[42].

W krajowym systemie legislacyjnym prawo dostępu do informacji oraz jego ograniczenia wynikają bezpośrednio z Konstytucji Rzeczypospolitej Polskiej. Art. 61 ustawy zasadniczej przyznaje obywatelowi prawo do uzyskiwania informacji o działalności organów informacji publicznej oraz osób pełniących funkcje publiczne.

---

[37] Dz. U. 1993 nr 61 poz. 284 Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności sporządzona w Rzymie dnia 4 listopada 1950 r., zmieniona następnie Protokołami 3, 5 i 8 oraz uzupełniona Protokołem nr 2. Źródło: http://isap.sejm.gov.pl /DetailsServlet?id= WDU1993061028, [dostęp: 22.06.2014].

[38] A. M. Dereń, *Prawna ochrona informacji w krajowym ustawodawstwie, Wybrane zagadnienia*, Zeszyt 2008, OPO Bydgoszcz 2001, s. 9.

[39] Zob., http://europa.eu/eu-law/decision-making/treaties/indexpl.htm, [dostęp: 20.06. 2014].

[40] A. M. Dereń, *Prawna…,* wyd. cyt., s. 9.

[41] Tamże, s. 12.

[42] M. Ciecierski, M. Gajos (red.), *Ochrona Informacji niejawnych i biznesowych,* Materiały III Kongresu, Krajowe Stowarzyszeni Ochrony Informacji Niejawnych, Uniwersytet Śląski w Katowicach, Katowice 2007, s. 109.

W Polsce dostęp do informacji publicznej został zatem podniesiony do rangi norm konstytucyjnych, a wejście w życie ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej[43] powoduje ciągły wzrost dyspozycji o udostępnienie różnorakich informacji adresowanych do organów i jednostek organizacyjnych[44].

W opinii A. Żebrowskiego i W. Kwiatkowskiego[45] za system prawnokarnej ochrony informacji należy uznać przepisy zawarte w:

- ustawie zasadniczej – Konstytucji Rzeczypospolitej Polskiej (Konstytucji RP)[46];
- ustawie o ochronie informacji niejawnych[47];
- Kodeksie karnym[48];
- zarządzeniach resortowych;
- umowach międzynarodowych, których stroną jest Polska[49].

Art. 54 ust.1 Konstytucji RP gwarantuje każdemu obywatelowi wolność wyrażania swoich poglądów oraz pozyskiwania i rozpowszechniania informacji, legalizując wolę społeczeństwa, aby skonstruować porządek prawny respektujący wolność człowieka, szanujący jego przywilej do zdobywania, przekazywania, przetwarzania i odtwarzania informacji[50].

---

[43] Dz. U. 2001 nr 112 poz. 1198 *Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej*, źródło http://isap.sejm.gov.pl/DetailsServlet?id=WDU20011121198, [dostęp: 22.06.2014].

[44] M. Ciecierski, M. Gajos (red.), *Ochrona Informacji niejawnych i biznesowych. Materiały III Kongresu*, Krajowe Stowarzyszeni Ochrony Informacji Niejawnych, Uniwersytet Śląski w Katowicach, Katowice 2007, s. 111.

[45] Za ustawy obligujące *organizacje do zapewnienia bezpieczeństwa przetwarzanych informacji* A. Nowak i W. Scheffs przyjmują: ustawę o ochronie danych osobowych, ustawę o ochronie informacji niejawnych, ustawę o dostępie do informacji publicznej, ustawę o prawach autorskich i prawach pokrewnych. Zob., A. Nowak, W. Scheffs, *Zarządzanie…,* wyd. cyt., s. 6.

[46] W świetle aktualnie obowiązującej ustawy zasadniczej konstytucyjny obowiązek strzeżenia tajemnicy państwowej i służbowej przez obywateli wynika z niżej wymienionych zapisów Konstytucji RP: *art. 82 Obowiązkiem obywatela polskiego jest wierność Rzeczypospolitej Polskiej*, *art. 83 Każdy ma obowiązek przestrzegania prawa Rzeczypospolitej Polskiej*. Zob. http://www.sejm.gov.pl/prawo/konst/polski/kon1.htm, [dostęp: 11.12.2013].

[47] *Od 2 stycznia 2011 r. obowiązuje ustawa z 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. nr 182, poz.1228), która zastąpiła dotychczasową ustawę z 1999 r. Potrzeba wprowadzenia w tej materii nowej regulacji wynikała z konieczności dostosowania przepisów do zmieniającej się rzeczywistości, uaktualnienia przestarzałych i niefunkcjonalnych uregulowań wobec dzisiejszego poziomu technologicznego oraz dostosowania polskich rozwiązań do praktyk i reguł obowiązujących w instytucjach Unii Europejskiej i NATO. Wśród uregulowań nowej ustawy istotne jest m.in. zniesienie podziału na tajemnicę państwową i służbową. Ochronie podlegają obecnie te informacje, których ujawnienie przyniosłoby szkody interesom państwa*. Źródło: http://www.rp.pl/artykul/599343.html,[dostęp: 24.02.2014].

[48] Kodeks Karny, Dz. U. 1997 nr 88 poz. 553 Ustawa z dnia 6 czerwca 1997 r. - Kodeks karny.

[49] A. Żebrowski, W. Kwiatkowski, *Bezpieczeństwo…,* wyd. cyt., s. 110.

[50] A. M. Dereń, *Prawna…,* wyd. cyt., s. 10.

Konstytucja RP w art. 61 tę wolność ewidentnie podkreśla rozstrzygając, iż obywatel ma prawo do uzyskiwania informacji o działalności organów władzy publicznej oraz osób pełniących funkcje publiczne[51].

Ustawa zasadnicza, nadając swobodzie dostępu do informacji szeroki charakter, ustanawia także klauzulę o możliwości wprowadzania restrykcji z przyczyn wyraźnie w ustawie ustalonych[52].

Szczególnie warte podkreślenia jest, iż na podstawie art. 61 ust. 3 Konstytucji RP wpisano do polskiego porządku prawnego dwie istotne dla podmiotów gospodarczych ustawy: o ochronie danych osobowych oraz o ochronie informacji niejawnych[53].

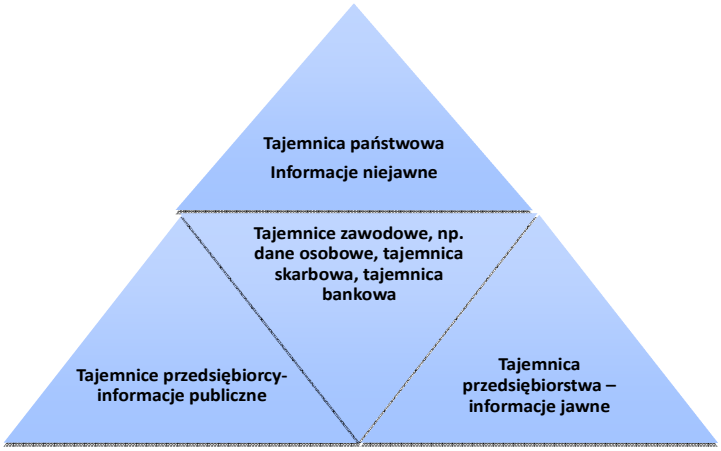
Ustawy te formułują skuteczną granicę dla niczym nieograniczonego dysponowania informacjami, wnosząc jednocześnie do polskiego systemu prawnego uznane w świecie standardy bezpieczeństwa[54].

Należy zaznaczyć, iż szczególnie ustawa o ochronie informacji niejawnych uchwalona w dniu 22 stycznia 1999, obowiązująca w nowym brzemieniu od 2 stycznia 2011, odpowiada potrzebie należytego, zgodnego z Konstytucją RP, uregulowania problematyki ochrony informacji i jest nadzwyczaj istotna z punktu widzenia żywotnych interesów Rzeczypospolitej Polskiej[55].

Identyfikowanie coraz to nowych zagrożeń dla bezpieczeństwa informacji generowało wdrażanie różnego rodzaju zastrzeżeń odnoszących się do postępowania z informacjami, jak i do odpowiedzialności karnej za ujawnienie informacji osobom do tego nieuprawnionym[56], stąd na początku zapisy związane z ochroną informacji pojawiały się w kodeksach karnych, a z biegiem czasu wprowadzono coraz bardziej szczegółowe instrukcje, zarządzania, rozporządzenia i ustawy, również o zasięgu międzynarodowym, w tym standardy dla ochrony informacji o szczególnej wadze[57].

Hierarchię ochrony informacji w Polsce przedstawia rysunek 1.

[51] Tamże, s. 10.
[52] Tamże, s. 11.
[53] Tamże, s. 11.
[54] Tamże, s. 11.
[55] B. Iwaszko, *Ochrona informacji niejawnych w praktyce*, Presscom Sp. z o.o., Wrocław 2012, s. 13.
[56] Tamże, s. 13.
[57] A. Żebrowski, W. Kwiatkowski, *Bezpieczeństwo…,* wyd. cyt., s. 13.



Źródło: Opracowanie własne na podst. B. Iwaszko, *Ochrona…*, wyd. cyt., s. 13.

Rys. 1. Hierarchia ochrony informacji w Polsce

Bardziej szczegółowe rozważania litery ustawy o ochronie danych osobowych i ustawy o ochronie informacji niejawnych przedstawiono w drugiej części opracowania, natomiast podejmując próbę nakreślenia ram systemu prawno-karnej ochrony informacji, należy przedstawić zarys zasad karnej odpowiedzialności za naruszenie tajemnicy państwowej i służbowej, powołując się na regulacje znajdujące się w Kodeksie karnym z 1997 roku (Dz. U. Nr.88 z 1997 r., poz. 553).

Kodeks karny to akt prawny określający najwyższe sankcje w stosunku do przepisów odrębnych ustaw dotyczących ochrony tajemnicy państwowej i służbowej oraz innych tajemnic prawnie chronionych[58].

Kodeks karny z mocą obowiązywania od 1 stycznia 1998 (Dz. U. Nr.88 z 1997 r., poz. 553), w odpowiedzi na wyzwania gwałtownego postępu naukowo-technicznego i technologicznego, szczególnie w dziedzinie automatycznego przetwarzania informacji, uregulował zagadnienia przestępstw komputerowych[59], uwzględniając obowiązujące *wytyczne Komitetu*

[58] Tamże, s. 121-122.

[59] *Mimo, iż zagadnienie bezpieczeństwa sieci komputerowych i obiegu informacji pozostaje przedmiotem zainteresowania organów ochrony prawnej już od kilku lat, to do niedawna w polskim ustawodawstwie brak było definicji przekładającej pojęcie przestrzeni wirtualnej – jako obszaru potencjalnych zagrożeń – na język prawny. Nawet przepisy Kodeksu karnego, znowelizowanego w 2004 r. w celu wprowadzenia na grunt polskiego prawa zapisów Konwencji Rady Europy o cyberprzestępczości (tzw. budapeszteńskiej), podpisanej przez Polskę w 2001 r., poza objęciem penalizacją przestępstw komputerowych oraz przestępstw godzących w bezpieczeństwo systemów informatycznych, nie zawierają w tej materii określeń definicyjnych. Problem bezpieczeństwa w cyberprzestrzeni wychodzi przy tym poza ramy tradycyjnie pojmowanego czynu o charakterze przestępczym, w rozumieniu Kodeksu karnego. W skrajnych przypadkach może on bowiem przybrać postać, która w świetle konstytucji stanowi podstawę do wprowadzenia jednego ze stanów nadzwyczaj-*

Ministrów Rady Europy z 1989 roku w sprawie przestępstw związanych z wykorzystaniem komputerów[60].

W rozdziale XVII Kodeksu karnego ustawodawca odniósł się do przestępstwa komputerowego ujmując je jako kwalifikowaną postać szpiegostwa. Zgodnie z art. 130 paragraf 3 kodeksu karnego karalne jest włączanie się do sieci komputerowej w celu uzyskania wiadomości, których udzielanie obcemu wywiadowi może wyrządzić szkodę Rzeczypospolitej Polskiej i podlega karze pozbawienia wolności na czas nie krótszy niż lat 3 (przestępstwo komputerowe).

Kolejnym przestępstwem spenalizowanym przez kodeks karny (art. 132) jest wprowadzanie w błąd polskiego organu państwowego przez osobę oddającą usługi wywiadowcze Rzeczypospolitej Polskiej, co podlega karze pozbawienia wolności od roku do 10 lat.

Przepisem będącym odpowiedzią na rozwój techniki informacyjnej jest art. 165 paragraf 1 pkt. 4 Kodeksu karnego stanowiący, iż za sprowadzenie niebezpieczeństwa dla życia lub zdrowia wielu osób albo mienia w wielkich rozmiarach, które jest następstwem zakłócania, uniemożliwiania lub wpływu w inny sposób na automatyczne przetwarzanie, gromadzenie lub przesyłanie danych informatycznych grozi kara pozbawienia wolności od 6 miesięcy do lat 8[61].

Odpowiedzialność za przestępstwo przeciw ochronie informacji regulują zapisy rozdziału XXXIII Kodeksu karnego, w tym art. 265 formułujący odpowiedzialność za ujawnienie lub wykorzystanie tajemnicy państwowej. W myśl art. 265 paragraf 1 kodeksu karnego, ujawnienie tajemnicy państwowej zagrożone jest karą pozbawienia wolności od 3 do 5 lat, natomiast paragraf 2 mówiący o ujawnieniu tajemnicy państwowej osobie działającej na rzecz podmiotu zagranicznego określa karę pozbawienia wolności od 6 miesięcy do 8 lat[62].

---

nych. Zob., M. Grzelak, K. Liedel*, Bezpieczeństwo Polski w cyberprzestrzeni,* [w:] *Bezpieczeństwo narodowe II-2012/22,* Biuro Bezpieczeństwa Narodowego, Warszawa 2012, s. 132

[60] A. Żebrowski, W. Kwiatkowski, *Bezpieczeństwo…,* wyd. cyt., s. 117.

[61] Tamże, s. 117.

[62] Przykładem naruszenia art. 265 kodeksu karnego był przypadek dwóch dziennikarzy oskarżonych o ujawnienie tajemnicy państwowej, w tym działalności szpiegowskiej kilku oficerów Wojskowych Służb Informacyjnych. *Warszawska prokuratura oskarżyła ich o to, że w 1999 r. ujawnili tajemnicę państwową, opisując zatrzymanie przez UOP trzech oficerów WSI pod zarzutem szpiegostwa na rzecz wschodniego sąsiada (skazanych potem na kary od trzech do czterech lat więzienia i degradacje). Drugi zarzut dotyczył ujawnienia przez nich sprawy innego oficera WSI, który miał współpracować z wywiadem USA, a został bez procesu wypuszczony z Polski do USA; potem wrócił do kraju. Ostatecznie uniewinnił go w 2007 r.* (..) *Z uwagi na małą „szkodliwość społeczną" stołeczny sąd umorzył proces w roku 2010.* Źródło: http://wiadomosci.wp.pl/kat,1342,title,Umorzono-proces-dziennikarzy-za-ujawnienie-tajemnicy-WSI,wid,12378330,wiadomosc.html?ticaid=112c56, [dostęp: 22. 05.2014]. Innym przykładem (rok 2013) jest postępowanie zapoczątkowane zawiadomieniami szefa Centralnego Biura Antykorupcyjnego. *Prokuratura Okręgowa w Lublinie zdecy-*

Odpowiedzialność za ochronę informacji, zgodnie z literą XXXIII rozdziału Kodeksu karnego, to także odpowiedzialność za ujawnienie tajemnicy innej niż państwowa, to jest tajemnicy *służbowej, zawodowej, oraz która nie posiadając atrybutów tajemnicy* służbowej ani *zawodowej wynika z przyjętego przez sprawcę zobowiązania do jej zachowania*. Powszechnie stosowana zasada poufności informacji uzyskanych w związku z wykonywaniem pewnych zawodów, np. tajemnica adwokacka, tajemnica lekarska, tajemnica dziennikarska, tajemnica biegłego rewidenta podlega regulacjom tego rozdziału Kodeksu karnego. Tajemnica zawodowa często może współistnieć z tajemnica służbową, a *Ustawodawca określił ją mianem tajemnicy powierzonej* (art. 266 kodeksu karnego)[63].

Paragraf 1 art. 266 kodeksu karnego określa podstawowy typ przestępstwa zagrożony karą grzywny, ograniczeniem wolności albo pozbawienia wolności do lat 2, natomiast paragraf 2 reguluje odpowiedzialność funkcjonariusza publicznego, który ujawnił osobie nieuprawnionej informacje stanowiące tajemnice służbową lub informacje, którą uzyskał w związku z wykonywaniem obowiązków służbowych, a której ujawnienie może narazić na szkodę prawnie chroniony interes[64].

W czasach gwałtownego rozwoju technologicznego, w skutek globalizacji gospodarki i związanej z nią potrzebą przekazywania danych pomiędzy podmiotami międzynarodowymi za pośrednictwem sieci informatycznej szczególnej wagi nabrało praktyczne znaczenie przepisów regulujących transfer danych osobowych do państw trzecich[65].

---

dowała się wszcząć śledztwo po doniesieniu szefa CBA w sprawie „bezpieczeństwa funkcjonariuszy oraz Biura". Śledztwo jest prowadzone w kierunku artykułów: 266 paragraf 1. i 265 paragraf 1. Kodeksu Karnego. Chodzi o bezprawne ujawnienie informacji, które uzyskało się w związku z pełnioną funkcją czy wykonywaną pracą (to przestępstwo zagrożone karą do 2 lat pozbawienia wolności). Źródło: http://m.tokfm.pl/Tokfm/1,110222, 13257248,Jest_sledztwo_ws__ujawnienia__Gazecie_Wyborczej__niejawnych.html, [dostęp: 28.01.2014]. Przykładem postępowania w kierunku m.in. art. 265 kodeksu karnego to umorzone w roku 2013 postępowanie *dotyczące ewentualnego ujawnienia – w postaci przecieku do mediów – informacji ze śledztwa w sprawie domniemanych tajnych więzień CIA w Polsce.* Jak wyjaśnił *(…)* naczelnik *wydziału śledczego Prokuratury Okręgowej w Gdańsku, w śledztwie badano sprawę pod kątem (…) art. 265 kodeksu karnego – wykorzystania informacji niejawnych o klauzuli „tajne" lub „ściśle tajne". Śledztwo w sprawie ewentualnego ujawnienia w mediach informacji ze ściśle tajnego, prowadzonego przez krakowską prokuraturę apelacyjną postępowania dotyczącego domniemanych więzień CIA w Polsce wszczęto 20 kwietnia ub. r. O wyjaśnienie, czy doszło do ujawnienia informacji z tego śledztwa, wystąpiła do prokuratora generalnego Prokuratura Apelacyjna w Krakowie. Z podobnym wnioskiem wystąpiła też do prokuratora generalnego w końcu marca ub. r. sejmowa komisja do spraw służb specjalnych. Postępowanie trafiło do Gdańska,* gdzie zostało umorzone. Źródło: http://www.tvn24.pl/pomorze,42/umorzono-sprawe-przeciekow-ws-domniemanych-wiezien-cia,302943.html, [dostęp: 28.01. 2014].

[63] A. Żebrowki, W. Kwiatkowski, *Bezpieczeństwo…,* wyd. cyt., s. 118.

[64] Tamże, s. 118.

[65] Państwa trzecie, zgodnie z literą ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, to państwa nienależące do Europejskiego Obszaru Gospodarczego (gru-

Pozostawiając jako niewątpliwie dopuszczalne przekazywanie danych na podstawie zgody osoby zainteresowanej, przekazywanie danych osobowych do państwa trzeciego może mieć miejsce, gdy państwo docelowe zapewnia na swym terytorium tzw. odpowiedni poziom ochrony danych osobowych[66] (art. 47 ust.1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych)[67].

Przyjmuje się, że odpowiedni poziom ochrony zapewniają kraje, co do których Komisja Europejska wydała decyzję stwierdzającą, że państwo to zapewnia poziom ochrony danych odpowiadający poziomowi ustanowionemu w dyrektywie 95/46/WE z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych[68].

Europejskie organy ochrony danych zrzeszone w ramach Grupy Roboczej[69] opracowały stosowne koncepcje tzw. BCR (ang. *Binding Corporate Rules*)[70], zawierające informacje i wytyczne, którym powinny odpowiadać reguły przesyłania danych oraz kryteria zatwierdzania reguł przez krajowe organy kontroli danych osobowych.

Dokumenty robocze (ang. *working paper*) o numerach WP74, WP107, WP108, WP154, WP155 odnoszą się do wiążących reguł korporacyjnych właściwych dla administratorów danych, a dokumenty robocze o numerach

---

py państw obejmującej państwa członkowskie Wspólnoty Europejskiej z wyłączeniem Chorwacji oraz Norwegię, Islandię i Lichtenstein). Zob., A. Szydlik, S. Paszek, *Przekazywanie danych osobowych w państwach trzecich*, Rocznik 2014, Wardyński i Wspólnicy, 2014, s. 85.

[66] Zob. art.47 ust.1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Dz. U. 1997 nr 133 poz. 883, http://isip.sejm.gov.pl/DetailsServlet?id=WDU19971330883, [dostęp: 24.05.2014].

[67] A. Szydlik, S. Paszek, *Przekazywanie…,* wyd. cyt., s. 86.

[68] Tamże, s. 86.

[69] *Grupa robocza ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych, zwana dalej Grupą Roboczą, powołana została na mocy art. 29 Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, jako niezależny podmiot o charakterze doradczym. W skład Grupy Roboczej wchodzą przedstawiciele organu lub organów nadzorczych, powołanych przez każde Państwo Członkowskie, przedstawiciel organu lub organów ustanowionych dla instytucji i organów wspólnotowych oraz przedstawiciel Komisji. Każdy członek grupy roboczej jest powoływany przez instytucję, organ lub organy, które reprezentuje. W przypadku gdyby Państwo Członkowskie powołało więcej niż jeden organ nadzorczy, organy te wyznaczają wspólnego przedstawiciela zasiadającego w Grupie Roboczej. Powyższa zasada dotyczy również organów utworzonych przez instytucje i organy wspólnotowe. Polska w Grupie Roboczej reprezentowana jest przez Generalnego Inspektora Ochrony Danych Osobowych.* Źródło: http://www.giodo.gov.pl/261/id_art/920/j/pl/ [dostęp: 22.06.2014].

[70] Zob., http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index_en.htm, dostęp 20.06.2014

WP 195 i WP 204 stanowią reguły dla podmiotów przetwarzających dane[71].

Aktualny stan prawny nie pozwala Polsce dołączyć do procedury zatwierdzania reguł w ramach wzajemnego uznawania wiążących reguł korporacyjnych, jednak w myśl obowiązujących przepisów Generalny Inspektor Ochrony Danych Osobowych może rozpatrzyć pozytywnie wniosek, w którym polski podmiot wystąpi o zgodę na transfer danych w oparciu o wiążące reguły korporacyjne[72].

Wielorakość i niesymetryczność zabezpieczeń formalnych oraz opracowywanych przez organizacje autorskich rozwiązań w obszarze ochrony przed zagrożeniami bezpieczeństwa informacyjnego przyczyniła się do tego, iż podmioty zaczęły poszukiwać jednorodnego systemu ochrony informacji. W odpowiedzi na te poszukiwania Międzynarodowa Organizacja Normalizacyjna – ISO (ang. *International Organization for Standarization* – ISO) opracowała i wprowadziła normalizację procesów dotyczących bezpieczeństwa informacji w postaci pierwszej wersji normy ISO/IEC 17799, w roku 2007 przemianowanej na normę ISO/IEC/27002, a Polski Komitet Normalizacyjny opublikował zmienioną normę ISO/IEC 17799 pod nazwą PN-ISO/IEC 17799. Norma wspomaga zatem procesy w przedsiębiorstwie, zapewniając realne podniesienie bezpieczeństwa informacji, kładąc nacisk na sferę organizacyjną oraz monitorując obszary szczególnego ryzyka, np.: dostęp do informacji, zabezpieczenia na poziomie organizacyjnym, kontrolę zasobów, działanie urządzeń informatycznych, przestrzeganie prawa i obowiązujących procedur, zabezpieczenie fizyczne organizacji i otoczenia[73].

Zakończenie

W części pierwszej opracowania będącego próbą przedstawienia wybranych regulacji prawnych w obszarze bezpieczeństwa informacyjnego przybliżono pojęcia i definicje z zakresu problematyki zagrożeń bezpieczeństwa informacyjnego oraz nakreślano ramy prawno-karnej ochrony informacji.

Analiza literatury przedmiotu pozwala stwierdzić, iż pojęcie bezpieczeństwa informacyjnego nie posiada jednoznacznej wykładni, razem z towarzyszącym mu terminem „*bezpieczeństwo informacji*”[74] jest używane w różnorakich znaczeniach.

[71] A. Szydlik, S. Paszek, *Przekazywanie…,* wyd. cyt., s. 86.

[72] Tamże, s. 87.

[73] A. Nowak, W. Scheffs, *Zarządzanie…,* wyd. cyt., s. 36.

[74] *Kiedy mówimy o bezpieczeństwie informacyjnym, to zawsze dotyczy to podmiotu, który jest zagrożony przez brak informacji (…). Natomiast bezpieczeństwo informacji to*

Szczególne zagrożenia dla bezpieczeństwa informacyjnego niesie za sobą gwałtowny postęp cywilizacyjny, powstanie zbiorów olbrzymich zasobów informacji oraz rozwój środków komunikowania[75], zaś katalog tych zagrożeń jest katalogiem otwartym, gdyż wraz z rozwojem społeczeństwa informacyjnego pojawiają się nowe możliwości i wyzwania.

Mnogość i różnorodność regulacji prawnych[76] w obszarze zagrożeń bezpieczeństwa informacyjnego świadczy o tym, iż we współczesnym przedsiębiorstwie jednym z najważniejszych zagrożeń bezpieczeństwa informacyjnego jest możliwość niekontrolowanego dostępu i ujawnienia informacji stanowiącej tajemnicę[77],a zapewnienie ochrony takiej informacji to jedno z wyzwań, przed jakimi stoją współczesne organizacje.

Bibliografia

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

2. Ciecierski M., Gajos M. (red.), *Ochrona Informacji niejawnych i biznesowych,* Materiały III Kongresu, Krajowe Stowarzyszenie Ochrony Informacji Niejawnych, Uniwersytet Śląski w Katowicach, Katowice 2007.

3. Dereń A. M., *Prawna ochrona informacji w krajowym ustawodawstwie, wybrane zagadnienia,* Zeszyt 2008, OPO Bydgoszcz 2001.

4. Grzelak M., Liedel K.*, Bezpieczeństwo Polski w cyberprzestrzeni,* [w:] *Bezpieczeństwo narodowe II-2012/22,* Biuro Bezpieczeństwa Narodowego, Warszawa 2012.

5. Iwaszko B., *Ochrona informacji niejawnych w praktyce,* Presscom Sp. z o.o., Wrocław 2012.

6. Janczak J., *Zakłócenia informacyjne*, AON, Warszawa 2001.

---

ochrona informacji będącej w posiadaniu tego właśnie podmiotu. A. Nowak, W. Scheffs, wyd. cyt., s. 25.

[75] M. Wrzosek, *Współczesne zagrożenia w obszarze bezpieczeństwa europejskiego,* Wydawnictwo Menedżerskie PTM, Warszawa 2013, s. 179.

[76] Za autorami M. i R. Taradejna jako akty prawne regulujące obszar ochrony informacji należy wymienić także m.in. ustawy: Ustawa z dnia 23 kwietnia 1964 r. – Kodeks Cywilny, Ustawa z dnia 15 lutego 1962 r. o obywatelstwie polskim, Ustawa z dnia 30 czerwca 1970 r. o służbie wojskowej żołnierzy zawodowych, Ustawa z dnia 10 kwietnia 1974 r. o ewidencji ludności i dowodach osobistych, ustawa z dnia 26 czerwca 1974 r. – Kodeks Pracy, Ustawa z dnia 10 czerwca 1994 r. o zamówieniach publicznych, Ustawa z dnia 29 czerwca 1995 r. o statystyce publicznej, Ustawa z dnia 29 września 1994 r. o rachunkowości, Ustawa o zawodzie lekarza, Prawo bankowe, Ustawa z dnia 26 maja 1982 r. o adwokaturze, Ustawa z dnia 20 czerwca 1985 r. o prokuraturze, Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych, Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji. Zob., M. Taradejna, R. Taradejna, *Dostęp do informacji publicznej a prawna ochrona informacji dotyczących działalności gospodarczej, społecznej i zawodowej oraz życia prywatnego*, Adam Marszałek, Toruń 2003, s. 332-333.

[77] K. Liderman, *Bezpieczeństwo…,* wyd. cyt., s. 61.

7. Kodeks Karny Dz. U. 1997 nr 88 poz. 553 Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny.
8. Koziej S., *Teoria sztuki wojennej*, Bellona, Warszawa 2011.
9. Kwintowski A., *Realia wdrażania systemu zarządzania bezpieczeństwem informacji,* [w:] Cisek M., Nowogródzka T. (red.), *Stabilność organizacji we współczesnej gospodarce*, Studio Emka, Warszawa 2014.
10. Liderman K., *Bezpieczeństwo informacyjne*, Wydawnictwo Naukowe PWN, Warszawa 2012.
11. Łoś-Nowak T., *Bezpieczeństwo*, [w:] Antoszewski A., Herbut R. (red.), *Leksykon politologii*, Alta2, Wrocław 2003.
12. Łuczak J. (red.), *Zarządzanie bezpieczeństwem informacji*, Oficyna Współczesna, Poznań 2004.
13. Nowak A., Scheffs W., *Zarządzanie bezpieczeństwem informacyjnym*, AON, Warszawa 2010.
14. Szydlik A., Paszek S., *Przekazywanie danych osobowych w państwach trzecich*, Rocznik 2014, Wardyński i Wspólnicy, 2014.
15. Taradejna M., Taradejna R., *Dostęp do informacji publicznej a prawna ochrona informacji dotyczących działalności gospodarczej, społecznej i zawodowej oraz życia prywatnego*, Adam Marszałek, Toruń 2003.
16. Wrzosek M., *Procesy informacyjne w zarządzaniu organizacją zhierarchizowaną*, AON, Warszawa 2010.
17. Wrzosek M., *Współczesne zagrożenia w obszarze bezpieczeństwa europejskiego,* Wydawnictwo Menedżerskie PTM, Warszawa 2013.
18. Zięba R. (red.), *Bezpieczeństwo międzynarodowe po zimnej wojnie*, Wydawnictwa Akademickie i Profesjonalne, Warszawa 2008.
19. Zygała R., *Podstawy zarządzania informacją w przedsiębiorstwie*, Wydawnictwo Akademii Ekonomicznej im. Oskara Langego, Wrocław 2007.
20. Żebrowski A., Kwiatkowski W., *Bezpieczeństwo informacji III Rzeczypospolitej*, Oficyna Wydawnicza ABRYS, Kraków 2000.

Źródła internetowe

1. http://ec.europa.eu/justice.
2. http://europa.eu/eu-law.
3. http://isap.sejm.gov.pl.
4. http://isip.sejm.gov.pl.
5. http://m.tokfm.pl.
6. http://wiadomosci.wp.pl.
7. http://www.giodo.gov.pl.
8. http://www.iniejawna.pl.
9. http://www.pkn.pl/.
10. http://www.rp.pl.

11. http://www.sejm.gov.pl.
12. http://www.spbn.gov.pl/.
13. http://www.tvn24.pl.

ABSTRACT
SELECTED LEGAL REGULATIONS CONCERNING INFORMATION SECURITY THREATS. PART ONE

The article presents selected notions and definitions concerning information security threats as well as outlines legal and penal framework of information protection.

As the role of information grows in the 21st century, which is called the information age in the literature of the subject matter, new threats emerge that are closely connected with the use of IT networks.

These threats catalogue is open since new opportunities and challenges appear together with the development of information society.

According to experts, the notion of information society does not have an explicit interpretation and with accompanying term of information security is used in many meanings. A special threat to information security results from a rapid development of civilization progress, enormous information resources and development of different communication media.

Recognizing new threats to information security initiates various reservations relating to dealing with information and penal responsibility for disclosing information to unauthorized personnel.