Rocznik Instytutu Europy Środkowo-Wschodniej
(Yearbook of the Institute of East-Central Europe)

ISSN 1732-1395

Instrukcje dla autorów i Rocznik online:
https://ies.lublin.pl/rocznik

Transformacja systemów zarządzania bezpieczeństwem informacji w Polsce po 1989 r.

Małgorzata Szabaciuk[a]

[a] Uniwersytet Marii Curie Skłodowskiej

Opublikowano online: grudzień 2019

Sposób cytowania: M. Szabaciuk, *Transformacja systemów zarządzania bezpieczeństwem informacji w Polsce po 1989 r.*, „Rocznik Instytutu Europy Środkowo-Wschodniej" 17 (2019), z. 1, s. 319-332, DOI: 10.36874/RIESW.2019.1.15.

M. Szabaciuk, *Transformacja systemów zarządzania bezpieczeństwem informacji w Polsce po 1989 r.*„Rocznik Instytutu Europy Środkowo-Wschodniej" 17 (2019), z. 1, s. 319–332, DOI: 10.36874/RIESW.2019.1.15

Małgorzata Szabaciuk*

Transformacja systemów zarządzania bezpieczeństwem informacji w Polsce po 1989 r.

Transformation of Information Security Management Systems in Poland After 1989

Abstract: The article aims to draw attention to the problem of information security management after the political transformation in Poland after 1989, and to outline issues that result from the evolution of a comprehensive approach to the world around us and new threats in the 21st century. Information security management in the age of knowledge-based society is an extremely important problem. The very approach to this issue must be systemic and well thought out in every organization. Information security is primarily a form of trust, which is supported by proper analyzes and a specific attitude of a person, social group or the general society towards the accessibility and quality of acquired, stored, used and transmitted information. We must remember that the use of integrated solutions in the field of information and information systems is inevitable in a world with rapidly growing digital resources.
Keywords: information security, information management, personal data protection, cybersecurity

Wstęp

Zarządzanie bezpieczeństwem informacji w dobie społeczeństwa opartego na wiedzy jest niezwykle ważnym problemem. Samo podejście do tego zagadnienia musi być systemowe i dobrze przemyślane w każdej organizacji. Bezpieczeństwo informacji to przede wszystkim forma zaufania, która poparta jest odpowiednimi analizami oraz określonym tokiem rozumowania osoby czy też grupy społecznej bądź ogółu społeczeństwa na temat dostępności i jakości pozyskiwanej, przechowywanej, następnie wykorzystywanej oraz przekazywanej in-

* Dr Małgorzata Szabciuk – Uniwersytet Marii Curie-Skłodowskiej (Lublin, Polska), ORCID: 0000-0002-2119-134X, e-mail: malgorzata.szabaciuk@umcs.pl.

formacji[1]. Wraz z rozwojem technologii informatycznych zmienia się i cały czas ulega transformacji podejście do zarządzania bezpieczeństwem informacji. Trzydzieści lat temu, kiedy upadał ZSRR, dostęp do wszelkiego rodzaju wiadomości był utrudniony ze względu na formę, w której informacje[2] występowały. Były to przeważnie informacje utrwalone na papierze.

Każdy aktotwórca w postępowaniu z dokumentacją musi opierać się na przepisach prawa archiwalnego, przepisach wykonawczych do ustawy i resortowych aktach prawnych. W Polsce ciągle obowiązuje wielokrotnie nowelizowana ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach[3], jednak ostatnie dziesięciolecie XX w. otworzyło nową epokę w zarządzaniu dokumentacją[4]. Wiązało to się z przyśpieszeniem komputeryzacji, co zapoczątkowane zostało przez rozwój komputerów osobistych, a także Internetu. Do tego doszły przemiany w sposobach ujmowania rzeczywistości społecznej, gospodarczej, technologicznej itd. Wraz z rozwojem systemów informatycznych zmieniło się również podejście do zarządzania bezpieczeństwem informacji, które jest procesem bardzo złożonym i ciągle się rozwijającym. Artykuł ma za zadanie nakreślić kluczowe kwestie łączące się z ewolucją kompleksowego podejścia do tego problemu, w tym nowych zagrożeń w XXI w., takich jak np. cyberterroryzm.

1. Zarządzanie bezpieczeństwem informacji w kontekście rewolucji informatycznej

Polska, podobnie jak inne państwa, weszła w fazę rewolucji informatycznej, której symbolami stały się komputer, Internet, a dziś przede

1 P. Zaskórski, K. Szwarc, *Bezpieczeństwo zasobów informacyjnych determinantą informatycznych technologii zarządzania*, „Zeszyty Naukowe Warszawskiej Wyższej Szkoły Informatyki" 2013, R. 7, nr 9, s. 41.

2 Słowo „informacja" pochodzi z języka łacińskiego i oznacza powiadomienie, zakomunikowanie, wiadomość, pouczenie. W rozumieniu potocznym informacją nazywa się dowolną wiadomość, na podstawie której odbiorca podejmuje określone działania. Zob. J. Penc, *Skuteczne zarządzanie organizacją*, Łódź 1999, s. 526.

3 Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. 2018, poz. 217).

4 M. Wnuk, *Kancelaria współczesna – zarządzanie dokumentacją – records management, punkt widzenia archiwisty*, [w:] J. Poraziński, K. Stryjkowski (red.), *Archiwa w nowoczesnym społeczeństwie. Pamiętnik V Zjazdu Archiwistów Polskich, Olsztyn 6–8 września 2007 r.*, Warszawa 2008, s. 503–507.

wszystkim smartfon. Żadne narzędzie nie zdominowało naszego życia bardziej niż komputer i sieć, oraz wszystko, co ma z nimi związek. W państwach rozwiniętych znaczenie komputeryzacji uświadamiają sobie praktycznie wszystkie grupy społeczne. Powoli zaczynamy dostrzegać zmiany, jakie rewolucja ta wywołała w mentalności ludzi, a przede wszystkim młodzieży. Wydaje się, że choć nasza kultura nadal opiera się na wartościach tradycyjnych, to jednak powoli do przeszłości odchodzi ta jej część, której symbolem przez wieki była książka jako główne źródło informacji i sposób przeżywania wrażeń estetycznych. Oczywiście, jest to zagadnienie, a właściwie splot zagadnień niezwykle rozbudowanych i złożonych, wymagających pogłębionych studiów interdyscyplinarnych. Nie ulega jednak wątpliwości, że dzisiejsze społeczeństwo oparte jest na wiedzy i informacji, a co za tym idzie – na zarządzaniu tymi dwoma instrumentami oraz na należytym zabezpieczaniu tego, co wiemy i co przechowujemy w systemach informatycznych. Kluczowe jest zatem pytanie, jak rozwój społeczeństwa oraz nowej dziedziny zarządzania, jaką jest zarządzanie bezpieczeństwem informacji, wpływa na przemiany dostępu do informacji prywatnej i publicznej[5] oraz na jej dalsze wykorzystywanie[6].

Różne prace badawcze przyjmują niejednolite perspektywy podczas dyskusji dotyczących zarządzania bezpieczeństwem informacji[7]. Pierwsza perspektywa to przyjęcie rozwoju technologicznego jako głównego czynnika transformacji społeczeństw. Druga podnosi, że zmiana społeczna wywołana jest przez rozwój dziedzin przemysłu opartych na informacji i wiedzy. O bezpieczeństwie informacji piszą zarówno naukowcy, jak i futurolodzy. Coraz częściej można natknąć

5 Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. 2019, poz. 1429). Zgodnie z ustawą organy władzy państwowej (i inne podmioty) muszą udostępniać każdą informację o sprawach publicznych, tj. informację publiczną (art. 1, ust. 1). Wyjątek stanowią informacje niejawne (art. 5, ust. 1).

6 G. Sibiga, *Ponowne wykorzystywanie informacji sektora publicznego 2017. Akty prawne i ich omówienia*, Wrocław 2017.

7 Zob. m.in. J. Brdulak, P. Sobczak (red.), *Wybrane problemy zarządzania bezpieczeństwem informacji*, Warszawa 2014; A. Gałach, R. Wójcik, *Zarządzanie bezpieczeństwem informacji w Sektorze Publicznym*, Warszawa 2009; T. Kifner, *Polityka bezpieczeństwa i ochrony informacji*, Gliwice 1999; K. Liedel, P. Piasecka, T. R. Aleksandrowicz, *Analiza informacji w zarządzaniu bezpieczeństwem*, Warszawa 2013; K. Liderman, *Bezpieczeństwo informacyjne. Nowe wyzwania*, Warszawa 2017; J. Łuczak, M. Tyburski, *Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC 27001*, Poznań 2009.

się w Internecie na specjalne strony dedykowane tej problematyce, które na bieżąco poruszają kwestie wycieku danych i dają wskazówki, jak chronić nasze dane firmowe lub prywatne[8].

Nie istnieje tylko jedna definicja bezpieczeństwa informacji. Definicje te ulegają z czasem modyfikacji wraz z kierunkami rozwoju technologicznego, zmianami politycznymi i kulturowymi. Większość jednak kładzie duży nacisk na znaczenie informacji w procesie jej zabezpieczania[9]. Samo bezpieczeństwo informacji (ang. *information security*) określane jest jako bezpieczeństwo polegające na zachowaniu poufności, integralności i dostępności informacji[10]. Tak pojmowane bezpieczeństwo informacji jest wartością, która pozwala działać sprawnie i celowo oraz podejmować odpowiednie decyzje w procesie zarządczym. W celu lepszego zrozumienia specyfiki pojęcia należy odpowiedzieć na dwa kluczowe pytania: dlaczego bezpieczeństwo informacji stało się tak ważne? oraz dlaczego właśnie teraz? Odpowiedzi wcale nie są proste. Przede wszystkim nowe technologie sprawiły, że jednostki są poddawane większej kontroli. Jesteśmy śledzeni na każdym kroku, niejednokrotnie nie zdając sobie z tego sprawy. Kiedy nosimy przy sobie smartfon, który ma wbudowany GPS, ktoś może odtworzyć miejsca naszego pobytu. Doświadczenia ostatnich lat prowadzą do wniosku, że informacja jest niejednokrotnie cenniejsza niż kapitał i ma kluczowe znaczenie w procesie zarządzania przedsiębiorstwami, jednostkami terytorialnymi czy państwem[11]. Należyte jej zabezpieczenie i opracowanie jest gwarantem dobrobytu i rozwoju naszego społeczeństwa.

Uznaje się dość często, że zarządzanie bezpieczeństwem informacji ma wymiar uniwersalny. Z chwilą, gdy komputery stały się powszechnie dostępne i służą nam na co dzień, kwestie zabezpieczania dostępu do informacji znalazły się wśród kluczowych problemów cywilizacyjnych. Odpowiednie zarządzanie bezpieczeństwem informacji stało się obecnie atutem, który obok zasobów finansowych, rzeczowych i pra-

8 Zob. m.in. https://niebezpiecznik.pl/ [10.08.2019].

9 Jest to przekazywanie przez nadawcę pewnej treści będącej opisem, poleceniem, nakazem, zakazem, zaleceniem, prośbą itd. Zob. B. Stefanowicz, *Informacja*, Warszawa 2004, s. 13.

10 PN-ISO/IEC 27001:2007 *Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania*, Warszawa 2007.

11 M. Wnuk, *Zastosowanie komputera w zarządzaniu dokumentacją współczesną – uwagi problemowe*, [w:] K. Narojczyk (red.), *Metody komputerowe w badaniach i nauczaniu historii*, Olsztyn 2005, s. 59.

cowniczych może mieć wpływ na istnienie i rozwój przedsiębiorstwa, urzędu, czy też każdej, nawet najmniejszej organizacji.

Duży wpływ na kształt procesu odpowiedniego zarządzania bezpieczeństwem informacji ma norma ISO/IEC 27001, opublikowana w Polsce 4 stycznia 2007 r., która wprowadziła uniwersalny model systemu zarządzania bezpieczeństwem informacji, możliwy do zastosowania w każdej firmie, podmiocie publicznym czy dowolnej organizacji. Należy zaznaczyć, że właściwa implementacja systemu zarządzania bezpieczeństwem informacji powinna być decyzją strategiczną danej jednostki, kształtującą jej wydajność i sprawność funkcjonowania. Jeśli podmiot podejmie decyzję o wdrożeniu normy ISO 27001, nie może dokonywać żadnych wyłączeń[12]. Trzeba podkreślić, że omawiana norma nie wskazuje jednostce, w jaki sposób ma zrealizować wymagania, które nie są w niej określone.

Informacje, jakie posiada każdy podmiot, mają swoją wartość i są podatne na różne zagrożenia, m.in. kradzież[13]. Podmioty powinny umieć z nich odpowiednio korzystać i zarządzać informacją w sposób pozwalający im zareagować na określone zagrożenia szybciej niż konkurencja. Firma, która jako pierwsza dokona strategicznych posunięć, wkraczając na nowe obszary działalności, umocni swoją pozycję wobec konkurencji. W dobie rewolucji informatycznej bezpieczną informacją może być fakt, pogłoska czy też spekulacja. Informacja daje władzę i przewagę jednostce, która nią rozporządza, niemniej jednak pod warunkiem, że zostanie stosownie użyta i należycie zabezpieczona[14]. Wartościowa informacja i efektywne zarządzanie nią to bez wątpienia jeden z najważniejszych aktywów organizacji rynkowej[15].

12 Norma ISO/IEC, wymagania określone w rozdziałach 4–8.

13 Zob. https://www.iso.org.pl/uslugi-zarzadzania/wdrazanie-systemow/zarzadzanie-ryzykiem/iso-iec-27001/ [10.08.2019].

14 R. Schaarschmidt, *Archivierung in Datenbanksystemen. Konzept und Sprache*, Stuttgart – Leipzig – Wiesbaden 2001, s. 18.

15 E. Górska, E. Lewandowska, *Podstawy zarządzania i kształtowania środowiska pracy*, Warszawa 2002, s. 116.

2. Czynnik ludzki w zarządzaniu bezpieczeństwem informacji

Cały czas największym zagrożeniem sprzyjającym wyciekom danych pozostaje jednak człowiek. Najczęściej to błędy ludzkie powodują ujawnienie informacji, które nie powinny ujrzeć światła dziennego. Pamiętajmy, że system bezpieczeństwa jest tak silny, jak jego najsłabszy element. Dużo firm przyznaje, że ich środki zabezpieczające są niewystarczające, pomimo stosowania ciągle nowych rozwiązań w zakresie bezpieczeństwa[16]. Transformacja ustrojowa, która miała miejsce w Polce po 1989 r., zmieniła perspektywę zarządzania zarówno dokumentacją, jak i informacją, jednak pracownicy nie zawsze stosują się do różnych polityk bezpieczeństwa korporacyjnego, co jest dużym wyzwaniem z punktu widzenia kadry kierowniczej[17].

Właściwe zarządzanie danymi zapewnia ich odpowiednie przechowywanie i stały dostęp dla organizacji, która je wytwarza lub zbiera, jednocześnie niszcząc lub usuwając z systemu dane zbędne po upływie ich czasu ważności. Takie działania podnoszą efektywność organizacji, a zarazem wzmacniają jej bezpieczeństwo.

Wraz z wprowadzaniem systemu Elektronicznego Zarządzania Dokumentacją w 2011 r.[18] administracja publiczna ma możliwość przejścia na zupełnie nowy system zarządzania dokumentacją, przez co możemy śledzić całościowy obieg dokumentacji w urzędzie w oparciu o nowe zasady. Właśnie takie elektroniczne zarządzanie informacją pełni kluczową rolę w systemowym nadzorze nad dokumentacją w trakcie jej cyklu życiowego – od momentu wpływu aż do archiwizacji wieczystej lub jej wybrakowania[19]. Tak więc droga do strategicznego systemu zarządzania informacją prowadzi przez budowę centralnego systemu zarządzania danymi w taki sposób, by inne systemy, w tym zarządzania informacją, mogły w pełni korzystać ze zgromadzonych w nim dokumentów.

16 Zob. https://www.kaspersky.pl/o-nas/informacje-prasowe/2155/rola-czynnika-ludzkiego-w-bezpieczenstwie-it-jest-calkowicie-zaniedbywana [10.08.2019].

17 Ibidem.

18 Rozporządzenie Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (Dz. U. 2011, nr 14, poz. 67).

19 Brakowanie to trwałe niszczenie dokumentacji.

Inaczej sprawa przedstawia się w firmach prywatnych, które nie muszą korzystać ze skomplikowanych jednolitych rzeczowych wykazów akt i mogą posługiwać się systemami klasy Enterprise Content Management, dostosowując je do swoich potrzeb. W efekcie właściwej organizacji obiegu informacji przedsiębiorstwo zyskuje rozliczne korzyści dotyczące sfery relacji międzyludzkich i organizacji pracy. Dzięki niej pracownicy mogą mieć dostęp do potrzebnych informacji, bez zalewnia ich zbędnymi danymi. W założeniu staną się przez to bardziej samodzielni, w większym zakresie będą poczuwać się do odpowiedzialności i będą przejawiać większe zaufanie do kierownictwa.

Pracownicy potrzebują dostępu do różnych informacji, szczególnie tych dotyczących bezpieczeństwa pracy. Brak rzeczowej i miarodajnej informacji sprzyja powstawaniu plotek, dezinformacji, budzi podejrzliwość wobec kierownictwa i współpracowników, nasila poczucie zagrożenia, podsyca destrukcyjnie współzawodnictwo, zachowania egoistyczne, dążenie do nielegalnego zdobywania informacji. Wszystko to tworzy niekorzystny klimat w przedsiębiorstwie i nie sprzyja osiąganiu dobrych wyników w pracy i trosce o interes firmy[20].

Zarządzanie bezpieczeństwem informacji to przede wszystkim zaspokojenie potrzeb jednostki poprzez tworzenie poczucia bezpieczeństwa podmiotu oraz jego otoczenia. Niezwykle ważnym zagadnieniem w tym kontekście jest polityka haseł dostępu, która powinna być osobno omówiona w Polityce Bezpieczeństwa instytucji. Zbyt rygorystyczne albo nazbyt pobłażliwe wytyczne mogą przyczynić się do niepowodzenia wdrożenia i realizowania systemu bezpieczeństwa informacji. Należy przede wszystkim skupić się na podnoszeniu świadomości pracowników w zakresie zarówno odpowiedniej ochrony haseł, jak i ich okresowego zmieniania oraz niestosowania takich, które mogłyby zostać szybko złamane[21].

20 U. Gros, *Zachowania organizacyjne w teorii i praktyce zarządzania*, Warszawa 2003, s. 173–174.

21 H. Aniszewska, *Rola czynnika ludzkiego w uwierzytelnianiu haseł w organizacji*, [w:] J. Brdulak, P. Sobczak (red.), *Wybrane problemy zarządzania bezpieczeństwem informacji*, Warszawa 2014, s. 161–162.

3. Zarządzanie bezpieczeństwem informacji a ochrona danych osobowych

Ochroną danych osobowych zaczęto zajmować się w drugiej połowie XX w. Związane to było z ideą prawa idącego w kierunku zapewnienia większej prywatności i ochrony dóbr osobistych[22]. Już wtedy obawiano się dużej automatyzacji, pojawienia się nowych technologii, które będą nie tylko gromadziły, ale przede wszystkim przetwarzały informacje, w tym dane osobowe obywateli[23]. Na skutek szybko rozwijających się w ostatnich dekadach technologii informatycznych możemy obserwować nowe podejście do ochrony danych osobowych.

Niewątpliwym przełomem było wydanie dyrektywy 95/46/WE Parlamentu Europejskiego i Rady (UE) z 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych[24]. W Polsce została ona wdrożona poprzez ustawę o ochronie danych osobowych z dnia 29 sierpnia 1997 r.[25] Kwestie ochrony danych osobowych są także poruszane w Konstytucji RP z dnia 2 kwietnia 1997 r.[26], a szczególnie w jej dwóch artykułach: 47[27] oraz 51[28].

Najnowsze regulacje w zakresie bezpieczeństwa danych osobowych to przede wszystkim Ogólne Rozporządzenie o Ochronie Da-

22 Mowa tu o Powszechnej Deklaracji Praw Człowieka, która została przyjęta przez Zgromadzenie Ogólne Organizacji Narodów Zjednoczonych w 1948 r. oraz o Europejskiej Konwencji Praw Człowieka z roku 1950. Tego typu działania miały za zadanie wyeliminowanie negatywnego wpływu na prawo do prywatności. Ponadto w 1967 r. powstała w ramach Rady Europy Komisja Konsultacyjna do spraw badania technologii informacyjnej i właśnie stworzenia prawa w kierunku do idei prywatności. Na początku lat 80. XX w. Rada Europy zajęła się ideą ochrony danych osobowych w kontekście szeroko rozwijanej informatyki. Przyjęto tekst Konwencji nr 108 Rady Europy, który sporządzono w Strasburgu 28 stycznia 1981 r. Dokument dotyczył ochrony osób w związku z automatycznym przetwarzaniem danych osobowych. W Polsce Konwencja weszła w życie 1 września 2002 r.

23 A. Mednis, *Ochrona danych osobowych w Konwencji Rady Europy i Dyrektywie Unii Europejskiej*, ODO 2000, nr 1, s. 9.

24 Dyrektywa 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 (Dz. Urz. WE L 281 z 21.11.1995 r., s. 31).

25 Ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r., poz. 922).

26 Konstytucja Rzeczypospolitej Polskiej z 2 kwietnia 1997 r. (Dz. U. z 1997 r., nr 78, poz. 483).

27 Art. 47 Konstytucji RP brzmi „Każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz decydowania o swoim życiu osobistym".

28 Art. 51 Konstytucji porusza szersze kwestie związane z ochroną danych osobowych i mówi o tym, że „Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawnienia informacji dotyczących jego osoby".

nych Osobowych, w skrócie RODO (ang. *General Data Protection Regulation*, GDPR)[29], obowiązujące od 25 maja 2018 r. Zawiera ono przepisy o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych oraz regulacje gwarantujące swobodny przepływ danych. Wraz z RODO uchwalono tzw. „dyrektywę policyjną"[30], która w przeciwieństwie do RODO nie jest stosowana bezpośrednio, lecz musiała zostać wprowadzona poprzez ustawę. W Polsce weszła w życie z opóźnieniem, bo dopiero 6 lutego 2019 r.[31] Głównym jej celem ma być zapewnienie skutecznej współpracy wymiaru sprawiedliwości oraz policji z innymi partnerami. Ustawa reguluje zasady ochrony danych osobowych, jeśli chodzi o czynności operacyjno-rozpoznawcze, dochodzeniowo-śledcze czy też administracyjno-porządkowe, które są związane z prewencją i zwalczaniem przestępczości[32]. Kolejnym aktem prawnym, który został wprowadzony wspólnie z RODO, jest ustawa o ochronie danych osobowych z 10 maja 2018 r. [33], która obowiązuje od 25 maja 2018 r. Oczywiście przepisy krajowe nie mogą podważać zapisów RODO, ale regulują m.in. kwestie związane z organem nadzorczym, którym w Polsce jest Urząd Ochrony Danych Osobowych[34], odpowiedzialnością i sankcjami, kwestiami proceduralnymi oraz sprawami związanymi z działalnością dziennikarską czy też funkcjonowaniem archiwów[35]. 4 maja 2019 r. weszła w życie ustawa o zmianie niektórych ustaw w związku z zapewnieniem zgodności z RODO. Dokonano w niej zmian aż w 162 aktach prawnych, w któ-

29 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L Nr 119, s. 1 ze zm.).

30 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz. Urz. L 119, s. 89).

31 Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. 2019, poz. 125).

32 Zob. https://odo24.pl/blog-post.dyrektywa-policyjna-wdrozona [10.08.2019].

33 Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2018, poz. 100).

34 Zob. https://uodo.gov.pl [10.08.2019].

35 G. Sibiga w opinii *Dostosowanie prawa polskiego do ogólnego rozporządzenia o ochronie danych*, Warszawa 2016, dostępnej w Internecie: http://michalboni.pl/mboni/wp-content/uploads/2016/11/Opinia.pdf [10.08.2019].

rych doprecyzowano, a niekiedy dodano nowe wymagania wiążące się z ochroną danych osobowych i ich należytym zabezpieczeniem[36].

Wraz z RODO zmieniała się też definicja danych osobowych, która została doprecyzowana. Artykuł czwarty RODO określa je jako: „informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej («osobie, której dane dotyczą»); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej"[37]. RODO bardzo duży nacisk kładzie na obowiązek informacyjny, w którym to zostajemy powiadamiani o swoich prawach m.in. do skargi do organu nadzorczego czy też żądania zaprzestania przetwarzania naszych danych. Z powodu niespełnienia obowiązku informacyjnego zgodnie z art. 14 RODO wymierzono już pierwszą karę finansową[38].

Zarządzanie ryzykiem, które w RODO jest poruszane, stanowi integralną część całościowego procesu zarządzania bezpieczeństwem informacji. Każda instytucja, która przetwarza dane, niekoniecznie tylko dane osobowe, wystawiona jest na wpływ zarówno czynników wewnętrznych, jak i zewnętrznych, które mogą spowodować naruszenie bezpieczeństwa informacji. Może nastąpić m.in. przypadkowe zniszczenie, zmodyfikowanie lub nieuprawnione ujawnienie osobom trzecim danych przetwarzanych. Mówimy wtedy o ryzyku niezrealizowania założeń organizacji na skutek np. wycieku danych, o których dowie się konkurencja[39].

Dobre zarządzanie bezpieczeństwem informacji zgodnie z RODO wymaga powołania przez organizację Inspektora Ochrony Danych.

36 Ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. 2019, poz. 730).

37 Art. 4 pkt 1 RODO.

38 Zob. https://www.rp.pl/Firma/190329577-Pierwsza-kara-za-RODO--milion-zlotych.html [10.08.2019].

39 Zob. https://blog-daneosobowe.pl/ocena-ryzyka-w-rodo/ [10.08.2019].

Reprezentuje on instytucję w kontaktach zewnętrznych. Podejmuje działania mające na celu realizację uprawnień podmiotów zajmujących się ochroną danych. Wyznaczenie Inspektora Ochrony Danych jest obowiązkowe we wskazanych przypadkach[40], przede wszystkim musi być wyznaczony w instytucjach sektora publicznego. W artykule 39 RODO zostały określone zadania Inspektora Ochrony Danych. Wśród nich możemy wyróżnić działania informacyjne, monitorowanie przestrzegania przepisów o ochronie danych oraz współpracę z organem nadzorczym.

4. Cyberbezpieczeństwo i jego rola w zarządzaniu bezpieczeństwem informacji

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[41] obowiązuje od 28 sierpnia 2018 r. i wdrożyła w Polsce dyrektywę w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych ma terytorium Unii (tzw. Dyrektywę NIS)[42]. W XXI w. cyberbezpieczeństwo jest jednym z podstawowych wyzwań stojących przed architektami i administratorami systemów zarządzania informacjami. Nie można zapewnić odpowiedniego poziomu bezpieczeństwa przepływu informacji bez posiadania właściwych narzędzi, które chroniłyby organizację przed wirusami, robakami czy też atakami hakerów.

Kwestia zarządzania bezpieczeństwem informacji może być rozpatrywana z punktu widzenia bezpieczeństwa zarówno poszczególnych podmiotów, jak i całego państwa. Skala zagrożenia sprawia, że pojedyncze firmy czy organizacje nie są w stanie same walczyć z cyberprzestępczością czy cyberterroryzmem. W ostatnich latach Unia Europejska i Sojusz Północnoatlantycki przywiązują coraz większą wagę do tego aspektu bezpieczeństwa, koordynując pracę dbających o nie instytucji w poszczególnych państwach członkowskich oraz two-

40 Art. 37 ust. 1 RODO.
41 Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. 2018, poz. 1560).
42 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE L 194 z 19.07.2016, s. 1).

rząc ponadnarodowe struktury ułatwiające skuteczne przeciwdziałanie tym zagrożeniom[43].

Bezpieczeństwo informacji i ochrona danych szczególnie ważnych z punktu widzenia państwa czy określonej instytucji mają obecnie znaczenie kluczowe. W celu minimalizowania ryzyka każdy podmiot musi rygorystycznie przestrzegać procedury obowiązującego systemu zarządzania bezpieczeństwem informacji, dbając o należyty stan sprzętu oraz odpowiednie przeszkolenie personelu.

Konkluzje

Problematyka zarządzania bezpieczeństwem informacji w Polsce jest zagadnieniem rozwojowym. Technologie informatyczne we współczesnym świecie zmieniają się na naszych oczach. Sposoby zabezpieczania informacji w systemach informatycznych są coraz lepsze. Należy jednak pamiętać, że hakerzy także zwiększają swoje umiejętności. Transformacja systemów zarządzania bezpieczeństwem informacji, którą mieliśmy okazję zaobserwować przez ostatnie 30 lat, jest ciągle niedokończona. Nie jesteśmy w stanie przewidzieć, jakich sposobów użyją cyberprzestępcy, aby wydobyć informacje z nośników elektronicznych. Coraz częściej trzymamy nasze zasoby w chmurze, zdając się na odpowiednie zabezpieczenia firm zewnętrznych, np. Google. W dobie systemów EZD czy też ECM, które przechowują ogromne zasoby danych i niejednokrotnie nie posiadają swojego odpowiednika papierowego, inaczej patrzymy na bezpieczeństwo informacji.

Na zakończenie należy podkreślić, że stosowanie zintegrowanych rozwiązań w zakresie systemów informatycznych i informacyjnych jest nieuchronne i zespoły konstruujące takie systemy powinny kłaść odpowiedni nacisk na bezpieczny dostęp do danych, który jednocześnie nie będzie ograniczał możliwości korzystania ze zbiorów informacji.

43 Zob. N. Lee, *Counterterrorism and cybersecurity: total information awareness*, New York 2013, s. 143–210.

Bibliografia

Aniszewska H., *Rola czynnika ludzkiego w uwierzytelnianiu haseł w organizacji*, [w:] J. Brdulak, P. Sobczak (red.), *Wybrane problemy zarządzania bezpieczeństwem informacji*, Warszawa 2014.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE L 194 z 19.07.2016, s. 1).

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz. Urz. L 119, s. 89).

Dyrektywa 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 (Dz. Urz. WE L 281 z 21.11.1995 r., s. 31).

Gałach A., Wójcik R., *Zarządzanie bezpieczeństwem informacji w Sektorze Publicznym*, Warszawa 2009.

Górska E., Lewandowska E., *Podstawy zarządzania i kształtowania środowiska pracy*, Warszawa 2002.

Gros U., *Zachowania organizacyjne w teorii i praktyce zarządzania*, Warszawa 2003.

Kifner T., *Polityka bezpieczeństwa i ochrony informacji*, Gliwice 1999.

Konstytucja Rzeczypospolitej Polskiej z 2 kwietnia 1997 r. (Dz. U. z 1997 r., nr 78, poz. 483).

Lee N., *Counterterrorism and cybersecurity: total information awareness*, New York 2013.

Liderman K., *Bezpieczeństwo informacyjne. Nowe wyzwania*, Warszawa 2017.

Liedel K., Piasecka P., Aleksandrowicz T. R., *Analiza informacji w zarządzaniu bezpieczeństwem*, Warszawa 2013.

Łuczak J., Tyburski M., *Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC 27001*, Poznań 2009.

Mednis A., *Ochrona danych osobowych w Konwencji Rady Europy i Dyrektywie Unii Europejskiej*, ODO 2000, nr 1.

Penc J., *Skuteczne zarządzanie organizacją*, Łódź 1999.

PN-ISO/IEC 27001:2007 *Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania*, Warszawa 2007.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L Nr 119, s. 1 ze zm.).

Rozporządzenie Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (Dz. U. 2011, nr 14, poz. 67).

Schaarschmidt R., *Archivierung in Datenbanksystemen. Konzept und Sprache*, Stuttgart – Leipzig – Wiesbaden 2001.

Sibiga G., *Ponowne wykorzystywanie informacji sektora publicznego 2017. Akty prawne i ich omówienia*, Wrocław 2017.

Stefanowicz B., *Informacja*, Warszawa 2004.

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. 2018, poz. 1560).

Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. 2019, poz. 1429).

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2018, poz. 100).

Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. 2018, poz. 217).

Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. 2019, poz. 125).

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016, poz. 922).

Wnuk M., *Kancelaria współczesna – zarządzanie dokumentacją – records management, punkt widzenia archiwisty*, [w:] J. Poraziński, K. Stryjkowski (red.), *Archiwa w nowoczesnym społeczeństwie. Pamiętnik V Zjazdu Archiwistów Polskich, Olsztyn 6–8 września 2007 r.*, Warszawa 2008.

Wnuk M., *Zastosowanie komputera w zarządzaniu dokumentacją współczesną – uwagi problemowe*, [w:] K. Narojczyk (red.), *Metody komputerowe w badaniach i nauczaniu historii*, Olsztyn 2005.

Zaskórski P., Szwarc K., *Bezpieczeństwo zasobów informacyjnych determinantą informatycznych technologii zarządzania*, „Zeszyty Naukowe Warszawskiej Wyższej Szkoły Informatyki" 2013, R. 7, nr 9.