Roczniki Administracji i Prawa nr XVIII(1), s. 187-199

Oryginalny artykuł naukowy
Original article

Data wpływu/Received: **21.01.2018**
Data recenzji/Accepted: **5.04.2018**
Data publikacji/Published: **30.06.2018**

Źródła finansowania publikacji: **Wyższa Szkoła Humanitas**

DOI: 10.5604/01.3001.0012.5998

Authors' Contribution:
(A) Study Design (projekt badania)
(B) Data Collection (zbieranie danych)
(C) Statistical Analysis (analiza statystyczna)
(D) Data Interpretation (interpretacja danych)
(E) ManuscriptPreparation (redagowanie opracowania)
(F) **LiteratureSearch (badania literaturowe)**

Dorota Fleszer*

WOKÓŁ PROBLEMATYKI BEZPIECZEŃSTWA INFORMACJI

Realizacja normatywnie wyznaczonych zadań publicznych wymaga posiadania określonego zasobu informacji. Ich zakres przedmiotowy bywa również normatywnie kształtowany, uwzględniający oczywiście możliwość wykonania konkretnego zadania. Nie sposób jednak pominąć problematyki społecznego zapotrzebowania na informację i roli, jaką ma dostęp do niej. Jak bowiem słusznie zauważa K. Liderman, rozwój elektroniki, homogenicznych sieci teleinformacyjnych (Internet), powszechność urządzeń dostępowych, powstanie sieci społecznościowych, wykorzystywanie sieci publicznych do przesyłania informacji dla systemów przemysłowych powoduje, iż informacja staje się kluczowym czynnikiem wyznaczającym wiedzę, władzę, ale i decydującym o bezpieczeństwie obywateli, organizacji, całych państw[1].

* dr; Wydział Administracji i Zarządzania Wyższej Szkoły Humanitas w Sosnowcu.
[1] K. Liderman, *Bezpieczeństwo informacyjne,* Warszawa 2012, s. 11-12.

Szybki rozwój społeczeństwa informacyjnego, w którym wytwarzanie, gromadzenie, przekazywanie, przechowywanie i wykorzystanie informacji należy do ważnych dziedzin życia społecznego i gospodarczego, sprawił, że coraz większą wagę zaczęto przywiązywać do problematyki zapewnienia bezpieczeństwa informacyjnego[2]. Stąd też bezpieczeństwo informacji to już nie tylko norma i wymóg czasu, ale obowiązek każdej organizacji będącej w posiadaniu informacji[3]. Mając świadomość roli i znaczenia informacji w społeczeństwie informacyjnym, kluczową kwestią staje się budowanie systemu jej bezpieczeństwa. Zdając sobie sprawę z tego, jak jest on złożony, ustawodawca nie stara się nawet konstruować konkretnych, szczególnych wymagań. Nakazuje jedynie podjąć działania odpowiednie, skuteczne, adekwatne, uwzględniające stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania[4]. Tym samym niezbędne staje się sięgnięcie do rozwiązań wypracowanych na gruncie innych dziedzin nauki, w szczególności organizacji i zarządzania.

W niniejszym opracowaniu podjęto problematykę bezpieczeństwa informacji w kontekście identyfikacji zagrożeń związanych z jej wykorzystywaniem i kształtowaniem umiejętności przeciwdziałania ich powstaniu. Działania tak określone są podejmowane w ramach procedur szacowania ryzyka bezpieczeństwem informacji, mających na celu nieustanne podejmowanie działań związanych z zabezpieczeniem informacji. Jest to proces, który wymaga stałego doskonalenia i ewaluacji.

BEZPIECZEŃSTWO INFORMACJI

Termin „bezpieczeństwo" kojarzone jest ze stanem, w którym określone dobra są zabezpieczone, nie grozi im utrata lub zniszczenie. Zdaniem K. Liedela bezpieczeństwo informacyjne rozumiane jest przez praktyków jako ochrona informacji przed niepożądanym (przypadkowym lub świadomym) ujawnieniem, modyfikacją, zniszczeniem lub przetwarzaniem[5]. Także M. Beskosty zauważa, że „informacja może być dostarczana z wielu źródeł, niekoniecznie wiarygodnych, a ponadto w czasie swojej „wędrówki" może ulegać wielu przekształceniom, a tym samym zmniejsza się jej wartość. Dlatego należy chronić takie atrybuty informacji jak poufność, dokładność i dostępność. Poufnością informacji nazywamy zdolność do dzielenia się informacją wyłącznie z tymi instytucjami lub grupami osób, którym jest to niezbędne, oraz do odmowy dostępu do informacji tym osobom, które nie są do tego powołane. Natomiast dokładność przekłada się na wiarygodność informacji, tzn. mówi o tym, że informacja pochodzi z wia-

[2] A. Suchorzewska, *Rozdział I. Społeczeństwo w dobie rozwoju sieci teleinformatycznych 6. Współczesne zagrożenia informacyjne,* [w:] A. Suchorzewska, *Ochrona prawna systemów informatycznych wobec zagrożeń cyberterroryzmem,* Oficyna 2010 LEX.

[3] J. Kowalewski, M. Kowalewski, *Polityka bezpieczeństwa informacji w praktyce,* Wrocław 2004, s. 21.

[4] Por. art. 25 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 (Dz.U.UE.L. z 2016 nr 119, poz. 1).

[5] K. Liedel, *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Toruń 2005, s. 19.

rygodnego i sprawdzonego źródła i wiąże się z jej integralnością, czyli pewnością, że z upływem czasu nie została ona zniekształcona bądź nie straciła swojej pierwotnej wartości wskutek modyfikacji. O dostępności mówimy zaś wtedy, gdy wszystkie osoby mające pozwolenie na dostęp do danej informacji korzystają z niej, ponieważ należy ona do zasobów informacyjnych przedsiębiorstwa[6]. Również Polski Komitet Normalizacyjny definiuje bezpieczeństwo informacji jako zachowanie atrybutów informacji, którymi są:

- poufność – zapewnienie, że informacja dostępna jest jedynie upoważnionym osobom,
- integralność – zapewnienie dokładności i kompletności informacji oraz metod przetwarzania,
- dostępność – zapewnienie, że osoby upoważnione mają dostęp do informacji i aktywów zawsze wtedy, gdy są im one potrzebne[7].

P. Bączek stawia tezę, zgodnie z którą bezpieczeństwo informacyjne to bardzo szerokie pojęcie, określające taki stan wewnętrzny i zewnętrzny, w którym nie są zagrożone strategiczne zasoby informacyjne państwa, władze podejmują decyzje dotyczące problematyki wewnętrznej i zewnętrznej w oparciu o prawdziwe, sprawdzone, wiarygodne i aktualne informacje, zaś organizacja ich przepływu nie jest zakłócona, bezpieczeństwo publicznych sieci teleinformatycznych, prawnych systemów ochrony informacji oraz ochrona danych osobowych obywateli są z mocy prawa gwarantowane przez państwo, obywatele mają prawo do prywatności, instytucje publiczne i prywatne, zbierając informacje o obywatelach, organizacjach i ich działalności, nie naruszają ustalonych norm prawnych, a obywatele i ich przedstawiciele (media, organizacje pozarządowe, parlamentarzyści, organy kontrolne) posiadają w swoim zakresie dostęp do informacji o działalności władz[8].

Z kolei E. Nowak i M. Nowak bezpieczeństwo informacyjne utożsamiają ze stanem warunków zewnętrznych i wewnętrznych dopuszczających, aby państwo swobodnie rozwijało swoje społeczeństwo informacyjne, zaś warunki osiągnięcia bezpieczeństwa informacyjnego to:

- niezagrożone strategiczne zasoby państwa,
- decyzje organów władzy podjęte na podstawie wiarygodnych, istotnych informacji,
- niezakłócony przepływ informacji pomiędzy organami państwa,
- niezakłócone funkcjonowanie sieci teleinformatycznych tworzących krytyczną infrastrukturę teleinformatyczną państwa,
- zagwarantowana przez państwo ochrona informacji niejawnych i danych osobowych obywateli,
- zasada, że prawo do prywatności obywateli jest nienaruszane przez instytucje publiczne,

[6] M. Beskosty, *Zarządzanie bezpieczeństwem informacji,* „Studia nad Bezpieczeństwem" 2017, nr 2, s. 164-165 i podana tam literatura.
[7] Polski Komitet Normalizacyjny. „Technika informatyczna. *Praktyczne zasady zarządzania bezpieczeństwem informacji"*. PN-ISO/IEC 17799, Warszawa 2003.
[8] P. Bączek, *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego,* Toruń 2006, s. 74.

- swobodny dostęp obywateli do informacji publicznej[9].

Nie ulega wątpliwości, że zapewnienie „bezpieczeństwa informacji" wymaga uwzględnienia specyfiki związanej z jej treścią oraz celów, dla realizacji których jest wykorzystywana. Istotny jest także rodzaj wykonywanych na informacji operacji, co z kolei ma swoje przełożenie na konieczność podjęcia działań chroniących informację przed zagrożeniami z tym związanymi. Jakkolwiek by nie ujmować problematyki bezpieczeństwa informacji, trzeba kłaść nacisk na bezpieczeństwo podstawowych i jednocześnie dla informacji właściwych atrybutów. Po pierwsze, należy zapewnić bezpieczeństwo treści informacji, co oznacza niedopuszczenie do nieuprawnionego ingerowania w jej brzmienie. Po drugie, należy zapewnić kontrolę nad tym, kto do informacji ma dostęp. W zależności od jej zawartości powinien on być limitowany ze względu na potrzebę posiadania wiedzy wynikającej z dostępu do informacji. Po trzecie zaś – w zależności od rodzaju informacji – zapewnienie możliwości zapoznania się z jej treścią i następnie wykorzystywanie tej wiedzy.

ZAGROŻENIA BEZPIECZEŃSTWA INFORMACJI

„Zagrozić" – jak wynika z definicji leksykalnej tego pojęcia – znaczy tyle, co: postraszyć kogoś, zapowiedzieć coś złego, ostrzec pod groźb*ą* jakichś konsekwencji, oraz stać się niebezpiecznym, groźnym dla kogoś, czegoś. Wedle definicji politologicznych zagrożenia to wyzwania niepodejmowane lub podejmowane za późno[10].

Najczęściej stosowaną w literaturze klasyfikacją zagrożeń bezpieczeństwa informacji jest podział ze względu na lokalizację ich źródła. Dzięki jego zastosowaniu uzyskujemy podział na zagrożenia:

- wewnętrzne (powstające wewnątrz organizacji), obejmujące zagrożenie utratą, uszkodzeniem lub brakiem dostępu do danych spowodowane błędem, przypadkiem albo celowym działaniem nieuczciwych użytkowników,
- zewnętrzne (powstające poza organizacją), które obejmują zagrożenie utratą, uszkodzeniem danych lub pozbawieniem możliwości obsługi przez celowe lub przypadkowe działanie ze strony osób trzecich w stosunku do sieci lub systemu,
- fizyczne, w których utrata, uszkodzenie danych lub brak możliwości obsługi następuje z powodu wypadku, awarii, katastrofy lub innego nieprzewidzianego zdarzenia wpływającego na system informacyjny bądź urządzenie sieciowe[11].

Nieco inne źródła zagrożeń wskazuje P. Bączek. Jego zdaniem zagrożenia bezpieczeństwa informacyjnego to:

- zagrożenia losowe – klęski żywiołowe, katastrofy, wypadki, które wpływają na stan bezpieczeństwa informacyjnego organizacji (np. pożar budynku, w którym przechowywane są nośniki informacji),

[9] E. Nowak, M. Nowak, *Zarys teorii bezpieczeństwa narodowego,* Warszawa 2011, s. 103.
[10] P. Bączek, *Zagrożenia informacyjne …*, s. 31.
[11] Szerzej: A. Żebrowski, M. Kwiatkowski, *Bezpieczeństwo informacji III Rzeczypospolitej*, Kraków 2000; por. A. Żebrowski, W. Kwiatkowski, *Bezpieczeństwo informacji III Rzeczypospolitej,* Kraków 2000 , s. 65.

- tradycyjne zagrożenia informacyjne – szpiegostwo, działalność dywersyjna lub sabotażowa (ukierunkowane na zdobycie informacji lub ofensywną dezinformację prowadzoną przez inne osoby, podmioty i organizacje),
- zagrożenia technologiczne – zagrożenia związane z gromadzeniem, przechowywaniem i przetwarzaniem informacji w sieciach teleinformatycznych (np. przestępstwa komputerowe, cyberterroryzm, walka informacyjna),
- zagrożenia odnoszące się do praw obywatelskich osób lub grup społecznych (np. sprzedaż informacji, przekazywanie informacji podmiotom nieuprawnionym, naruszanie przez władze prywatności, bezprawne ingerencje służb specjalnych, ograniczenie jawności życia publicznego)[12].

Inne podejście zmierzające do określenia źródeł zagrożenia bezpieczeństwa informacji reprezentują J. i M. Kowalewscy. Autorzy, powołując się na prowadzone prace w zakresie identyfikacji zagrożeń bezpieczeństwa informacji i systemów teleinformatycznych organizacji, wskazują na następujące zagrożenia bezpieczeństwa informacji i systemów teleinformatycznych organizacji:

- siły wyższe,
- uchybienia organizacyjne,
- błędy ludzkie,
- błędy techniczne,
- działania rozmyślne[13].

Określenie „siły wyższe" zawiera w sobie zbiór zagrożeń bezpieczeństwa informacji i systemów teleinformatycznych organizacji o charakterze obiektywnym, na które użytkownik systemów przetwarzających informacje nie ma większego i bezpośredniego wpływu. „Uchybienia organizacyjne" to zbiór zagrożeń bezpieczeństwa informacji i systemów teleinformatycznych organizacji, jakie zostały wygenerowane – szczególnie w procesie przetwarzania informacji – przez źle zorganizowaną i funkcjonującą instytucję. „Błędy ludzkie" to zagrożenia wynikające z niecelowej działalności człowieka. „Błędy techniczne" to zagrożenia związane z urządzeniami technicznymi i niewłaściwym ich eksploatowaniem. „Działania rozmyślne" to celowa działalność człowieka zmierzająca do przechwycenia i modyfikowania informacji lub danych, a także do utrudnienia lub uniemożliwienia ich przesyłania[14].

Cennym uzupełnieniem powyższych rozważań wydaje się być stanowisko A. Żebrowskiego, który wskazuje, iż największe zagrożenie bezpieczeństwa informacyjnego stanowi działalność człowieka. Celowe zagrażanie systemowi bezpieczeństwa informacyjnego jest wynikiem kumulacji trzech elementów: motywu, środka realizacji włamania do owego systemu oraz okazji, czyli uzyskania dostępu do dysku komputerowego lub sieci. Człowiek może wykorzystywać różnorakie sposoby włamań do systemów informacyjnych, jak np.:

[12] P. Bączek, *Zagrożenia informacyjne…*, s. 72-73.
[13] J. Kowalewski, M. Kowalewski, *Polityka bezpieczeństwa…*, s. 27-28.
[14] Ibidem, s. 28-30.

- zmowę kilku sprawców,
- celowe inicjowanie awarii,
- wywoływanie fałszywych alarmów (uśpienie czujności),
- szantaż, korupcję,
- rozsyłanie do firm ankiet, zapytań, propozycji,
- rozkodowywanie hasła dostępu,
- atak słownikowy,
- podsłuch sieciowy,
- wirusy, bakterie, robaki, konie trojańskie, bomby logiczne oraz inne groźne aplikacje destabilizujące sprawność systemu,
- wykorzystywanie luk w zabezpieczeniach dostępu do poczty elektronicznej i serwisu informacyjnego,
- techniki obchodzenia zabezpieczeń, np. programy wykorzystujące błędy w systemach operacyjnych i oprogramowaniu użytkowym,
- przechwytywanie otwartych połączeń sieciowych[15].

Szerokie podejście do specyfikacji zagrożeń dla bezpieczeństwa informacji reprezentuje E. Pietras (por. tabela 1). Ujmuje w niej nie tylko zagrożenia wynikające z przetwarzania informacji w systemie informatycznym (choć je wyraźnie wyróżnia), ale także te wynikające z niewłaściwego postępowania z danymi przez personel (pracowników) jednostki organizacyjnej, w której przetwarzane są dane osobowe.

Tabela 1. Identyfikacja zagrożeń bezpieczeństwa informacji

Zagrożenie			
Lp.	**Nazwa zagrożenia**	**Przyczyna**	**Skutek**
1.	Kradzież danych	Brak zabezpieczeń	Wydostanie się danych do konkurencji. Utrata konkurencyjności
2.	Włamania do systemu komputerowego	Ignorowanie zasady korzystania z poczty elektronicznej. Instalowanie nielegalnego oprogramowania	Brak zaufania kontrahentów. Kradzież danych
3.	Nieprzestrzeganie regulaminu obowiązującego w firmie	Brak zrozumienia przepisów. Nieprzestrzeganie regulaminów	Narażenie danych na utratę, zmodyfikowanie
4.	Przekroczenie uprawnień	Pochopne wydawanie uprawnień w systemach informatycznych. Brak wyciągania konsekwencji za przekroczenie uprawnień	Nieuprawniony dostęp do informacji, w wyniku tego straty finansowe firmy

[15] A. Żebrowski, M. Kwiatkowski, *Bezpieczeństwo informacji…*, s. 63-64, 73.

5.	Awaria sprzętu	Kupno uszkodzonego sprzętu. Nieumiejętne użytkowanie	Ograniczony dostęp do danych organizacji. Zakłócenia w procesie realizacji procesów
6.	Złamanie haseł	Nieprzestrzeganie zasad czystego biurka i pulpitu. Niewłaściwe tworzenie zasad	Upowszechnianie haseł. Kradzież danych
7.	Kradzież nośników danych, dokumentów	Wynoszenie danych, nośników poza siedzibę firmy. Kontrahenci pozostawieni bez opieki	Wyciek informacji do firm konkurencyjnych, w wyniku tego straty finansowe
8.	Awaria łączności systemu komputerowego	Nieodpowiednie użytkowanie systemu. Brak legalnego oprogramowania. Uszkodzenie podzespołów.	Zakłócenia związane z komunikacją. Brak możliwości poprawnej realizacji procesów
9.	Nieprawidłowe działania oprogramowania	Brak odpowiedniego nadzoru nad oprogramowaniem. Nieumiejętne korzystanie z oprogramowania	Przekłamanie w działaniu, zapisywaniu i przetwarzaniu informacji
10.	Odtworzenie danych z odnalezionych nośników danych	Zagubienie, zniszczenie, nośników informacji	Modyfikacja, niekontrolowane rozpowszechnienie danych
11.	Nieodpowiednie przygotowanie umowy z personelem i kontrahentami firmy i dostawcami	Brak świadomości zarządu	Wykorzystanie informacji, w wyniku tego utrata pozycji na rynku
12.	Brak zapewnienia bezpieczeństwa informacji w przedsiębiorstwie	Niedobór informacji w świadomości opracowania planu bezpieczeństwa informacji	Wyciek i kradzież informacji. Narażenie aktywów informatycznych na ich utratę
13.	Brak szkoleń dla kadry pracowników z zakresu bezpieczeństwa informacji	Brak świadomości kierownictwa. Brak środków finansowych	Nieświadome narażenie danych na ich utratę
14.	Wykorzystanie informacji udostępnionych w firmie	Brak świadomości kierownictwa. Brak środków finansowych	Utrata pozycji na rynku, w wyniku czego utrata części klientów

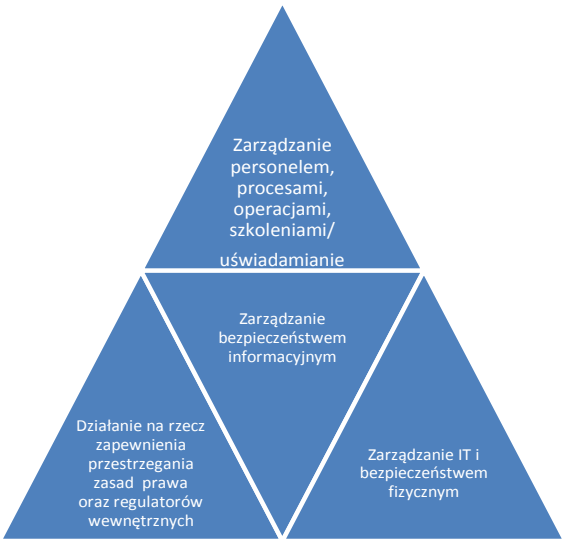
Źródło: E. Pietras, *Szacowanie ryzyka utraty bezpieczeństwa informacji na przykładzie wybranej jednostki gospodarczej*, www.ptzp.org.pl/files/konferencje/kzz/artyk_pdf_2017/T1/t1_088.pdf [dostęp: 14.02.2018].

ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACJI

Zarządzanie bezpieczeństwem informacji to nowa dziedzina z pogranicza informatyki, prawa, organizacji i zarządzania, zajmująca się definiowaniem aspektów bezpieczeństwa dla instytucji i jej systemów teleinformatycznych, jego osiąganiem i utrzymywaniem. Podlega ona takim samym regułom ogólnym jak każda inna dziedzina zarządzania – ma swój cel, plany, polityki, instrumenty kontroli i oceny, rachunek kosztów i ryzyka, programy utrzymania dotychczasowych wyników oraz ciągłej poprawy[16].

Na uwagę zasługuje stanowisko G. Ożarek, w którym Autorka podnosi, że System Zarządzania Bezpieczeństwem Informacyjnym (SZBI) jest jednym z wielu podsystemów zarządzania funkcjonujących we współczesnych, dobrze zarządzanych organizacjach[17]. Przychylam się do tego stanowiska. Ujmowanie zarządzania daną jednostką organizacyjną tylko przez pryzmat bezpieczeństwa informacji, bez uwzględnienia procesów zarządczych odbywających się w pozostałych sferach jej działalności, jest nie tylko niemożliwe, ale również niecelowe. Systemy te są nawzajem komplementarne i tylko taki sposób ich traktowania zapewnia ich efektywność i skuteczność. W tym miejscu zauważyć trzeba, że takie również podejście do SZBI preferują procedury wyznaczone normą PN-ISO/IEC 27001.

Rysunek 1. Obszary zarządzania bezpieczeństwem informacji



Źródło: ISO/EIC 27001 *for small businesses*, s. 16.

[16] Szerzej: A. Suchorzewska, *Rozdział V. Przestępstwo cyberterroryzmu w polskim systemie prawnym 4. Ochrona informacji utrzymywanych w systemach informatycznych a bezpieczeństwo informacyjne państwa 4.3. Zarządzanie bezpieczeństwem informacji*, [w:] A. Suchorzewska, *Ochrona prawna systemów informatycznych wobec zagrożeń cyberterroryzmem,* Oficyna 2010, LEX

[17] G. Ożarek, *System Zarządzania Bezpieczeństwem Informacji – budowa i wdrożenie*, [w:] *Ochrona danych osobowych w praktyce*, Polski Komitet Normalizacyjny, Warszawa 2013, s. 52.

Zgodzić się należy z tezą postawioną przez A. Suchorzewską, według której zarządzanie bezpieczeństwem to ciągły i złożony proces umożliwiający bezpieczną realizację misji, do której instytucję powołano. Proces ten zachodzi w stale zmieniającym się środowisku, przy występowaniu coraz to nowych form zagrożeń i wyzwań dla instytucji, a także przy niebywałym postępie technologicznym[18]. Uwzględniając powyższe, wydaje się, że „wybór właściwego modelu zarządzania bezpieczeństwem informacyjnym, obejmującego aktywa informacyjne całej jednostki, gwarantuje pełną ich ochronę oraz ekonomiczną efektywność podjętej decyzji. Dobry model zarządzania bezpieczeństwem informacyjnym uwzględnia wszystkie formy danych i informacji, takie jak wydruk, zapisy odręczne na papierze, informację przechowywaną elektronicznie, przesyłaną pocztą lub za pomocą urządzeń elektronicznych, wyświetlaną na ekranie monitora lub w formie filmów, zdjęć, ale także tę, która wypowiadana jest w trakcie rozmowy. Takim sprawdzonym empirycznie, uznanym za najlepsze rozwiązanie Systemem zarządzania bezpieczeństwem informacyjnym jest model opisany w normie PN-ISO/IEC 27001. W tym modelu zrządzanie bezpieczeństwem informacyjnym obejmuje trzy rozległe obszary zarządzania organizacją. Sprawne funkcjonowanie tych obszarów umożliwia osiąganie celów biznesowych. Jakiekolwiek zakłócenia (w jakimkolwiek z tych obszarów) stanowią zagrożenie dla realizacji tych celów, bowiem każdy z tych obszarów połączony jest różnymi relacjami z pozostałymi"[19]. Dlatego też „zidentyfikowanie mechanizmów zarządzania bezpieczeństwem danych wymaga starannego i szczegółowego planowania przy zaangażowaniu wszystkich pracowników danej instytucji. Wybór zabezpieczeń powinien być poprzedzony określeniem wymagań bezpieczeństwa, zidentyfikowaniem ryzyka, ustaleniem poziomu akceptacji sposobu postępowania z ryzykiem oraz wytycznych w zakresie zarządzania ryzykiem w instytucji. Skuteczna ochrona danych zależy od następujących czynników:

- polityki bezpieczeństwa informacji i celów biznesowych,
- zaangażowania kierownictwa,
- zrozumienia wymagań bezpieczeństwa danych, szacowania ryzyka i zarządzania ryzykiem,
- kultury instytucji przy wdrażaniu, utrzymaniu, monitorowaniu i doskonaleniu bezpieczeństwa danych,
- skutecznego propagowania wymagań i zaleceń bezpieczeństwa danych wśród pracowników i instytucji współpracujących,
- finansowania działań związanych z zarządzaniem bezpieczeństwem,
- zapewnienia odpowiedniej świadomości, kształcenia i szkoleń,
- ustanowienia skutecznego procesu zarządzania incydentami związanymi z bezpieczeństwem danych,

[18] Szerzej A. Suchorzewska, *Rozdział V. Przestępstwo cyberterroryzmu w polskim systemie prawnym 4..Ochrona informacji utrzymywanych w systemach informatycznych a bezpieczeństwo informacyjne państwa 4.3..Zarządzanie bezpieczeństwem informacji*, [w:] A. Suchorzewska, *Ochrona prawna…*
[19] G. Ożarek, *System Zarządzania...* s. 52.

- wdrożenia mierników efektywności systemu zarządzania bezpieczeństwem informacji oraz mechanizmów sprzężenia zwrotnego służących jego doskonaleniu"[20].

Tabela 2. Zasady OECD – wskazówki wspomagające tworzenie kultury bezpieczeństwa w organizacji i społeczeństwie

Lp.	Zasada	Treść zasady	Uwagi
1.	Świadomość	Uczestnicy powinni być świadomi potrzeby bezpieczeństwa systemów i sieci informatycznych oraz kroków, jakie mogą podjąć w celu poprawy bezpieczeństwa	Świadomość zagrożeń i potrzeby bezpieczeństwa jest jednym z najważniejszych elementów obrony. Uczestnicy powinni wiedzieć, że zagrożenia mogą pochodzić z wnętrza i z zewnątrz organizacji. Powinni znać dobre praktyki podnoszące bezpieczeństwo w sieci
2.	Odpowiedzialność	Wszyscy uczestnicy są odpowiedzialni za bezpieczeństwo systemów i sieci.	Każdy uczestnik jest zależny od lokalnych oraz globalnych systemów i sieci informacyjnych, które są ze sobą połączone, zatem powinien mieć świadomość swojej odpowiedzialności za ich bezpieczeństwo. Odpowiedzialność ta musi wynikać z zadań mu przydzielonych
3.	Reakcja	Uczestnicy powinni działać bez zwłoki i współpracować ze sobą w celu zapobiegania, wykrywania i reagowania na naruszenia bezpieczeństwa.	Uczestnicy powinni bezzwłocznie reagować na incydenty bezpieczeństwa. Dzielić się wiedzą na temat zagrożeń i luk w zabezpieczeniach. Wdrożyć procedury mające na celu zapobieganie, wykrywanie i reagowanie na naruszenie bezpieczeństwa
4.	Etyka	Uczestnicy powinni szanować uzasadnione dobra innych	Postępowanie etyczne to rozwijanie i wdrażanie najlepszych praktyk postępowania oraz promowanie zachowań, w których nie tylko unika się działania na szkodę innych, ale także respektuje się ich prawa
5.	Demokracja	Bezpieczeństwo systemów i sieci informatycznych powinno być zgodne z podstawowymi wartościami społeczeństwa demokratycznego	Wdrażanie rozwiązań z zakresu bezpieczeństwa musi korespondować z wartościami takimi jak: swobodny przepływ informacji, poufność informacji i komunikacji, odpowiednia ochrona danych osobowych

[20] J. Krawiec, *Bezpieczeństwo danych – podejście systemowe*, [w:] *Ochrona danych osobowych w praktyce*, Polski Komitet Normalizacyjny, Warszawa 2013, s. 31.

6.	Ocena ryzyka	Uczestnicy powinni przeprowadzać oceny ryzyka	Ocena ryzyka powinna obejmować czynniki wewnętrzne i zewnętrzne, np. technologię, czynniki fizyczne, ludzi, zasady postępowania, usługi świadczone przez jednostki zewnętrzne. Ocena ryzyka ma na celu identyfikację zagrożeń oraz luk w zabezpieczeniach
7.	Projektowanie i wdrażanie rozwiązań zakresu bezpieczeństwa	Uczestnicy powinni włączać rozwiązania z zakresu bezpieczeństwa do systemów i sieci informatycznych jako elementy kluczowe	Wymaga się wdrożenia zabezpieczeń technicznych i organizacyjnych, które powinny być dostosowane do wartości danych i informacji przetwarzanych w systemach i sieciach jednostki
8.	Zarządzanie bezpieczeństwem	Uczestnicy powinni przyjąć całościowe podejście do zarządzania bezpieczeństwem	Podstawą zarządzania powinna być ocena ryzyka. Zarządzanie powinno: przewidywać zagrożenia, zapobiegać, wykrywać i reagować na zagrożenia, planować i wykonywać konserwację, aktualizację i audyty, być przygotowanym do przywracania systemów do pracy po awarii. Wszystkie dokumenty, tj. polityki bezpieczeństwa, zasady, procedury, powinny stanowić spójny system bezpieczeństwa
9.	Przegląd	Użytkownicy powinni dokonywać przeglądów i ocen bezpieczeństwa systemów i sieci informatycznych oraz wprowadzać niezbędne zmiany do polityk, praktyk, środków i procedur dotyczących bezpieczeństwa	Dynamika zmian powoduje powstawanie nowych zagrożeń lub w zabezpieczeniach. Należy nieustannie badać, oceniać i modyfikować wszystkie elementy wdrożonego systemu bezpieczeństwa, aby przeciwdziałać nowym zagrożeniom

Źródło: G. Ożarek, *System Zarządzania Bezpieczeństwem Informacji – budowa i wdrożenie*, [w:] *Ochrona danych osobowych w praktyce*, Warszawa 2013, s. 53-54 i podana tam literatura.

Niestety – co słusznie zauważa G. Ożarek – SZBI nie jest jeszcze tak powszechnie wdrażany jak np. System Zarządzania Jakością (SZJ). Nie jest także tak powszechnie znany jak SZJ. Ale wiele instytucji jest zobligowanych przepisami prawa do przestrzegania reguł związanych z ochroną danych osobowych. I można powiedzieć, że instytucje te posiadają *sui generis* podsystem SZBI – ochronę danych osobowych zor-

ganizowaną zgodnie z wytycznymi prawa[21]. W sytuacji, kiedy informacja ma coraz większą wartość, gdy dostęp do niej jest gwarantowany autorytetem państwa i od jego skuteczności uzależnione jest powodzenie wielu przedsięwzięć nie tylko publicznych, ale też społecznych, gospodarczych, niezbędne jest podjęcie problematyki ochrony informacji i mechanizmów, jakie z tym procesem mają mieć związek. Kluczowe znaczenie dla budowania systemu zabezpieczeń informacji ma identyfikacja zagrożeń. Aby móc informacje chronić, trzeba wiedzieć przed czym, jakie sytuacje mogą stanowić źródło zagrożenia wymagające usunięcia lub chociażby zminimalizowania do akceptowanego poziomu. Trzeba wziąć pod uwagę także i to, że nie każdą informację chronimy tak samo. Informacje mają bowiem różny charakter, co powoduje konieczność weryfikacji poprawności postępowania z nią na każdym etapie. Wiedza ta powinna być następnie wykorzystywana do podejmowania działań na poziomie zarządczym mającym na celu eliminację lub obniżenie możliwości powstania niepożądanych zjawisk.

Bibliografia

Bączek P., *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Toruń 2006.
Beskosty M., *Zarządzanie bezpieczeństwem informacji*, „Studia nad Bezpieczeństwem" 2017, nr 2.
Kowalewski J., Kowalewski M., *Polityka bezpieczeństwa informacji w praktyce*, Wrocław 2004.
Krawiec J., *Bezpieczeństwo danych – podejście systemowe*, [w:] *Ochrona danych osobowych w praktyce*, Polski Komitet Normalizacyjny, Warszawa 2013.
Liedel K., *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Toruń 2005.
Liderman K., *Bezpieczeństwo informacyjne*, Warszawa 2012.
Nowak E., Nowak M., *Zarys teorii bezpieczeństwa narodowego*, Warszawa 2011.
Ożarek G., *System Zarządzania Bezpieczeństwem Informacji – budowa i wdrożenie*, [w:] *Ochrona danych osobowych w praktyce*, Polski Komitet Normalizacyjny Warszawa 2013.
Polski Komitet Normalizacyjny. „Technika informatyczna. Praktyczne zasady zarządzania bezpieczeństwem informacji". PN-ISO/IEC 17799, Warszawa 2003.
Suchorzewska A., *Ochrona prawna systemów informatycznych wobec zagrożeń cyberterroryzmem*, Oficyna 2010 LEX.
Żebrowski A., Kwiatkowski M., *Bezpieczeństwo informacji III Rzeczypospolitej*, Kraków 2000.

[21] G. Ożarek, *System Zarządzania…*, s. 52.

Streszczenie: Dbałość o posiadane zasoby informacyjne jest przedmiotem nie tylko normatywnie określonych obowiązków organu administracji publicznej. Konieczność zapewnienia bezpieczeństwa gromadzonych informacji wymaga zastosowania właściwych rozwiązań o charakterze organizacyjnym, dlatego też jest jednym z kluczowych elementów zarządzania konkretną jednostką organizacyjną. Zidentyfikowanie zagrożeń bezpieczeństwa informacji i umiejętność skutecznego zarządzania nimi staje się cenioną umiejętnością, bez której funkcjonowanie w dobie społeczeństwa informacyjnego nie jest możliwe.

Słowa kluczowe: informacja, bezpieczeństwo informacji, zagrożenia bezpieczeństwa informacji, zarządzanie bezpieczeństwem informacji

AROUND THE ISSUES OF INFORMATION SECURITY

Summary: It is undeniable that processing of personal data is an inherent element of the relationship between an employer and an employee. The employee cannot maintain information autonomy in this social sphere, however it shall not mean the employer's freedom in obtaining and collecting any information about the employee. Provisions of the Labour Code specify how to protect the employee against excessive requirements made by employers.

Keywords: information, information security, information security threats, information security management