Zeszyty Naukowe AON nr 4 (105) 2016
ISSN 0867–2245

BEZPIECZEŃSTWO INFORMACYJNE ORGANIZACJI

dr Joanna WERNER
Akademia Sztuki Wojennej

dr inż. Edyta SZCZEPANIUK
Akademia Sztuki Wojennej

Abstrakt

W artykule zostały przedstawione rekomendowane metody projektowania systemu zarządzania bezpieczeństwem informacji w organizacji. W analizie uwzględniono istotę i elementy bezpieczeństwa informacji oraz relacje między nimi. Systemowe podejście do badanego obszaru wymagało charakterystyki podstaw prawnych oraz modeli bezpieczeństwa informacji (ISO/IEC oraz TISM). Ponadto przedstawione zostały metody wdrożenia i eksploatacji oraz monitorowania systemu bezpieczeństwa informacji w organizacji. Artykuł zamyka prezentacja wyników badań empirycznych przeprowadzonych przez autorki w jednostkach sektora publicznego i prywatnego oraz wnioski i rekomendacje w przedmiotowym zakresie.

Słowa kluczowe: bezpieczeństwo informacyjne, system zarządzania bezpieczeństwem informacji, modele zarządzania bezpieczeństwem informacji, ochrona informacji

Wprowadzenie

Powszechna informatyzacja wielu procesów związanych z funkcjonowaniem instytucji publicznych i prywatnych przynosi niewątpliwie wiele korzyści zarówno dla obywatela, organizacji, jak i państwa. Z drugiej zaś strony, pojawia się problem zapewnienia bezpieczeństwa informacyjnego, które ma współcześnie fundamentalne znaczenie zarówno dla realizacji procesów biznesowych organizacji, jak i dla bezpieczeństwa narodowego[1].

1 Zob. E. Szczepaniuk, *Wybrane problemy bezpieczeństwa informacyjnego państwa* [w:] *Bezpieczeństwo narodowe i międzynarodowe wobec wyzwań współczesnego świata*, red. W. Kitler, M. Marszałek, Warszawa 2014, s. 68–83.

Wzrost zagrożeń cyberprzestrzeni państwa, a także stopnia ich zaawansowania prowadzi do powstawania różnego rodzaju zabezpieczeń technicznych. Należy jednak mieć na uwadze, że omawiana problematyka wykracza poza obszar bezpieczeństwa sieci i systemów komputerowych. Ryzyko związane z zagrożeniami informacyjnymi obejmuje także aspekty prawne, organizacyjne oraz zarządzanie zasobami ludzkimi[2]. Stąd też dążenie do zapewnienia bezpieczeństwa informacyjnego w organizacji wymaga podejścia interdyscyplinarnego.

Badania prowadzone przez różne ośrodki krajowe i zagraniczne dowodzą, że w wielu instytucjach istnieją problemy związane z bezpieczeństwem informacyjnym. Często zastosowane rozwiązania mają charakter fragmentaryczny i obejmują jedynie niektóre elementy bezpieczeństwa. Wprowadzenie skutecznych zasad ochrony zasobów informacyjnych powinno prowadzić do zmian w zarządzaniu całością organizacji. Na tym tle ważnym aspektem jest systemowe zarządzanie bezpieczeństwem informacji.

Celem artykułu jest wskazanie rekomendowanych metod tworzenia i wdrażania systemu zarządzania bezpieczeństwem informacji. Przywołane metody obejmują podejście eksperckie opierające się na przepisach prawa, normach międzynarodowych oraz dobrych praktykach. Skuteczność zaproponowanych rozwiązań determinowana jest poziomem dojrzałości biznesowej organizacji oraz stosowanych systemów informatycznych. Struktura organizacyjna bezpieczeństwa informacji już na poziomie projektu powinna uwzględniać identyfikację elementów bezpieczeństwa oraz wymagania prawne, stąd też w artykule odniesiono się również do wspomnianych zagadnień. Poruszane zagadnienia obejmują także polecane metody zabezpieczeń oraz wyniki badań diagnozujących obszary problemowe.

Istota i elementy bezpieczeństwa informacyjnego organizacji

W literaturze przedmiotu oraz przepisach prawa bezpieczeństwo informacyjne jest różnie definiowane i nie posiada powszechnie przyjętej definicji. Wiele opracowań stanowi niewątpliwie cenne i wartościowe dzieła, niemniej często pojęcia takie jak bezpieczeństwo teleinformatyczne, bezpieczeństwo informacyjne i bezpieczeństwo informatyczne są traktowane zamiennie. Wobec powyższego istotne jest rozróżnienie tych kategorii oraz zaproponowanie definicji na potrzeby systemowego zarządzania bezpieczeństwem informacji.

Traktując postać informacji jako kryterium rozróżnienia przywołanych kategorii, należy zauważyć, że bezpieczeństwo informacyjne jest pojęciem najszerszym. Obejmuje ono ochronę informacji niezależnie od jej formy, np. informacji cyfrowych, dokumentów papierowych, komunikatów wypowiedzianych w rozmowie. Natomiast

2 Zob. koncepcja ludzkiego firewalla – M.E. Whitman, H.J. Mattord, *Management of Information Security,* Boston 2008, s. 299–300.

bezpieczeństwo informatyczne i teleinformatyczne odnosi się do cyfrowej postaci informacji. Niezależnie od formy, bezpieczeństwo informacji powinno spełniać tzw. atrybuty bezpieczeństwa (tab. 1).

Tabela 1

Atrybuty bezpieczeństwa informacji

Atrybut	Charakterystyka
poufność	dostęp do informacji musi być ograniczony tylko do kręgu użytkowników autoryzowanych
integralność	informacja musi być zachowana w swej oryginalnej postaci, za wyjątkiem sytuacji, gdy jest aktualizowana lub usuwana przez osoby do tego uprawnione
dostępność	informacja musi być dostępna dla osób upoważnionych na ich żądanie w każdej chwili
rozliczalność	dotyczy możliwości identyfikacji użytkowników informacji i systemu teleinformatycznego oraz wykorzystywanych przez niego usług
niezawodność	właściwość oznaczająca spójne zamierzone zachowania i skutki
autentyczność	oznacza możliwość jednoznacznego stwierdzenia tożsamości podmiotu przesyłającego dane

Opracowanie własne na podstawie: A. Barczak, T. Sydoruk, *Bezpieczeństwo systemów informatycznych zarządzania*, Warszawa 2003, s. 246; K. Lidermann, *Bezpieczeństwo informacyjne,* Warszawa 2012, s. 19.

Pierwsze trzy z przywołanych atrybutów, tj. poufność, integralność, dostępność – odnoszone są do informacji w każdej postaci. Natomiast rozliczalność, niezawodność i autentyczność dotyczą ochrony informacji w systemach teleinformatycznych, czyli informacji cyfrowej.

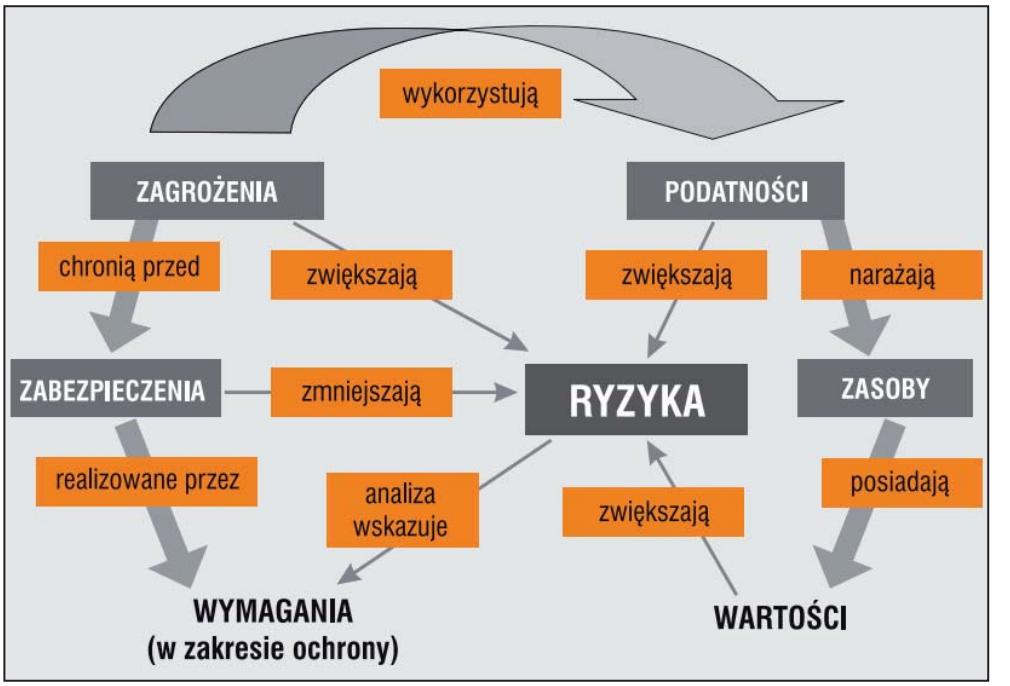
Jak słusznie zauważa Andrzej Białas, w instytucji nie są chronione wszystkie informacje i usługi. Ochroną są objęte tzw. informacje wrażliwe, czyli takie, które mają znaczenie dla zadań stawianych przed instytucją. Wrażliwość informacji jest „pewną miarą ważności przypisaną informacji przez jej autora lub dysponenta w celu konieczności jej ochrony”[3]. Podobnie jest z usługami realizowanymi w organizacjach, w których wyodrębnia się grupę tzw. usług krytycznych.

W procesie zarządzania bezpieczeństwem informacyjnym istotne znaczenie mają elementy bezpieczeństwa informacji, czyli „wszystko to, na czym opiera się system zarządzania bezpieczeństwem informacji”[4]. Głównym celem systemu zarządzania bezpieczeństwem informacji (SZBI) jest zarządzania ryzykiem zagrożeń informacyjnych w sposób, który będzie minimalizował prawdopodobieństwo ich

3 A. Białas, *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie,* Warszawa 2006, s. 35

4 J. Łuczak, M. Tyburski, *Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC 27001*, Poznań 2010, s. 33.

wystąpienia za pomocą implementacji zabezpieczeń technicznych, organizacyjnych, proceduralnych i prawnych. Normy ISO/IEC[5] wprowadziły nomenklaturę w zakresie elementów bezpieczeństwa oraz ich wzajemnych relacji (rys 1.).



Źródło: M. Blim, *Teoria ochrony informacji (część 1)*, „Zabezpieczenia" nr 3/2007, s. 60.

Rys. 1. Relacje pomiędzy elementami bezpieczeństwa

Zgodnie z rysunkiem zagrożenie jest potencjalną przyczyną niepożądanego incydentu dla bezpieczeństwa systemu, np. ataku DDOS. Wystąpieniu zagrożenia sprzyja tzw. podatność, która jest słabością lub luką w systemie, np. brak stosowania zabezpieczeń technicznych. Podatność naraża zasoby instytucji na utratę określonych wartości. Wystąpienie incydentu bezpieczeństwa stwarza konsekwencje (skutki) dla instytucji, np. pozyskanie informacji poufnych przez podmiot nieuprawniony. Relacja między zagrożeniem a podatnością, a w szczególności prawdopodobieństwo, że zagrożenie wykorzysta podatność systemu, określana jest mianem ryzyka. W celu minimalizacji ryzyka wprowadza się różnego rodzaju zabezpieczenia, np. szkolenia pracowników, kopie bezpieczeństwa[6]. Organizacje powinny zatem uwzględniać powyższe elementy w projektowaniu, tworzeniu, utrzymywaniu i doskonaleniu syste-

5 Normy powstałe w wyniku współpracy Międzynarodowej Organizacji Normalizacyjnej (ISO) i Międzynarodowej Komisji Elektrotechnicznej (IEC).

6 E. Szczepaniuk, *Bezpieczeństwo struktur administracyjnych w warunkach zagrożeń cyberprzestrzeni państwa*, rozprawa doktorska, AON, Warszawa 2015.

mu bezpieczeństwa. Identyfikacja zagrożeń i podatności, zarządzanie ryzykiem oraz implementacja zabezpieczeń są kluczowymi elementami systemu bezpieczeństwa informacyjnego organizacji.

Należy przy tym zauważyć, że każda organizacja jest inna – wykorzystuje różne systemy teleinformatyczne, posiada inne zasoby, zagrożenia, podatności oraz wynikające z nich ryzyko. Dlatego też w celu zapewnienia bezpieczeństwa informacji w organizacji elementy bezpieczeństwa powinny być stale monitorowane i doskonalone. Omawiane zagadnienie jest kategorią interdyscyplinarną, stąd utrzymanie bezpieczeństwa informacji wymaga podejścia systemowego. Implementacja w organizacji systemowego zarządzania bezpieczeństwem informacji zwiększa skuteczność działania, pozwala na rozpatrywanie wszystkich elementów bezpieczeństwa wspólnie, co jest szczególnie istotne w kontekście zachodzących związków przyczynowo-skutkowych oraz umożliwia cykliczne powtarzanie procesu zarządzania ryzykiem.

Na potrzeby systemowego zarządzania bezpieczeństwem informacji proponujemy definiowanie bezpieczeństwa informacyjnego organizacji jako stan, w którym[7]:

- elementy tworzące system bezpieczeństwa cechuje zdolność do ochrony przed obecnymi i przyszłymi zakłóceniami (zagrożeniami) funkcjonowania lub utraty określonych wartości – system jest odporny na zagrożenia (wewnętrzne, zewnętrzne, przypadkowe, celowe);
- bezpieczeństwo informacji jest osiągnięte i utrzymywane na założonym poziomie poufności, integralności i dostępności;
- bezpieczeństwo świadczonych usług jest osiągnięte i utrzymywane na założonym poziomie niezawodności, dostępności i integralności usług;
- zapewniona jest autentyczność i rozliczalność podmiotów związana z autoryzacją użytkowników korzystających z określonych informacji i usług;
- użytkownicy informacji i usług (pracownicy organizacji) oraz odbiorcy informacji i usług (obywatele, przedsiębiorcy, pracownicy zatrudnieni w innych organizacjach) mają świadomość i nie są podatni na zagrożenia bezpieczeństwa informacyjnego;
- aktorzy zagrożeń (także napastnicy wewnętrzni) mają małe możliwości wykorzystania systemów teleinformatycznych do generowania zagrożeń przez wykorzystanie słabości, podatności i luk w systemie zabezpieczeń.

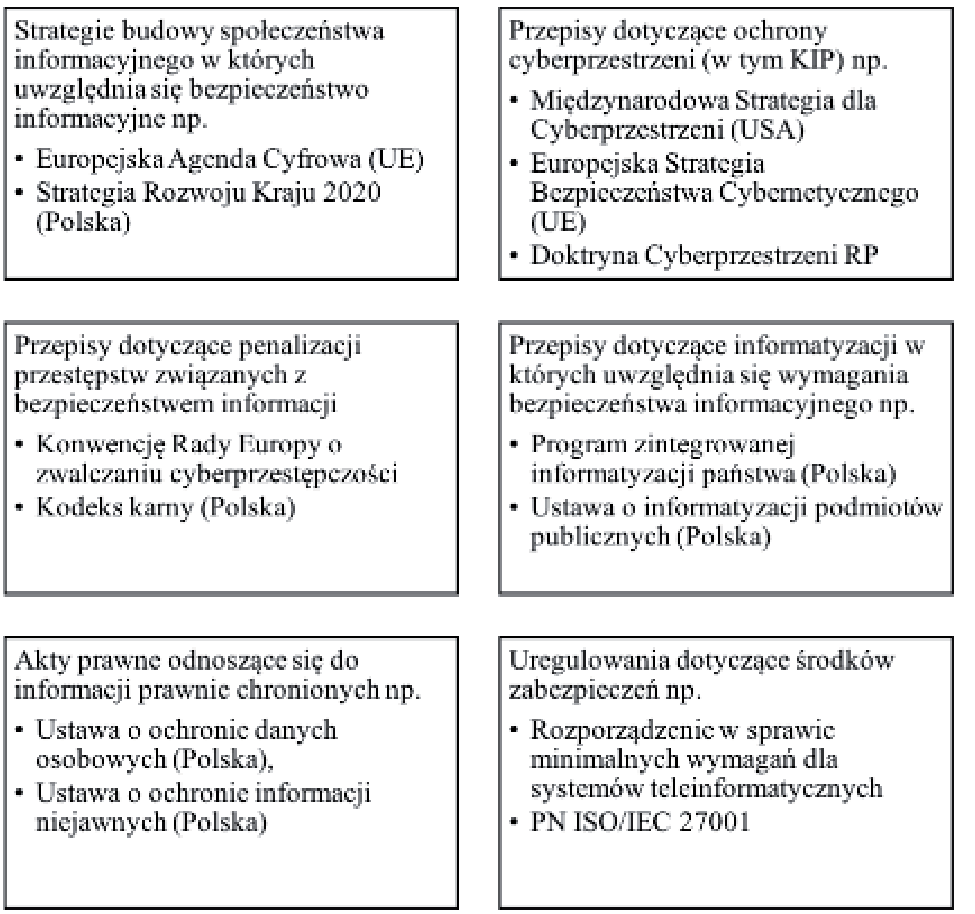
Wymagania prawne dotyczące bezpieczeństwa informacyjnego

Przepisy prawne odnoszące się do bezpieczeństwa informacyjnego są rozproszone w wielu aktach prawnych[8]. Taki stan rzeczy powoduje, że wdrażając system zarządzania bezpieczeństwem informacji, najpierw należy przeanalizować podstawy

7 Tamże, s. 160.

8 W Polsce funkcjonuje ponad 200 aktów prawnych odnoszących się do problematyki bezpieczeństwa informacji.

prawne, na podstawie których dana organizacja funkcjonuje[9]. Na system prawny RP wpływają także akty prawne ustanowione przez organizacje międzynarodowe[10]. Niektóre przepisy są obligatoryjne, czyli organizacja musi je respektować, np. ustawa o ochronie danych osobowych[11]. Inne natomiast są fakultatywne, zatem ich stosowanie jest dobrowolne, np. normy ISO/IEC, metodyka TISM. Z uwagi na to, że przepisy prawne obejmują różne dziedziny i gałęzie prawa, w artykule przyjęto taksonomię według kryterium obszaru uregulowań (rys. 2).



Rys. 2. Klasyfikacja aktów prawnych dotyczących bezpieczeństwa informacji według kryterium obszaru uregulowań

9 J. Łuczak, M. Tyburski, *Systemowe zarządzanie bezpieczeństwem*…, op. cit., s. 43.
10 Zob. analizę przepisów prawnych w obszarze bezpieczeństwa informacyjnego, np. A. Suchorzewska, *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*, Warszawa 2010.
11 *Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych*, Dz.U. 1997 nr 133, poz. 883 ze zm.

Z punktu widzenia omawianej problematyki, szczególnie istotne znaczenie ma standaryzacja i normalizacja bezpieczeństwa informacji. Normy i standardy – podobnie jak zagrożenia informacyjne – podlegają ciągłej ewolucji. Wśród najwcześniejszych standardów wymienia się:

- kryteria techniczno-technologiczne – skierowane na produkt – wywodzą się z USA i prac nad TCSEC (lata 1945–1983) dla potrzeb systemów informatycznych wojska i rządu;
- kryteria organizacyjno-zarządcze – skierowane na system i zarządzanie systemem – wywodzą się z Wielkiej Brytanii i prac nad BS 7799 (lata 1993–1999) dla potrzeb środowiska biznesowego[12].

W literaturze spotykane są różne klasyfikacje norm i standardów. Krzysztof Liderman wyróżnia dwie podstawowe grupy[13]:

- standardy, na podstawie których można przeprowadzać certyfikacje systemów i produktów teleinformatycznych, np. ISO 15408 (*Common Criteria*), ITSEC, TCSEC;
- standardy opisujące tzw. dobre praktyki, np. BS 77991.

Inną klasyfikację proponuje Białas, który wyróżnia standardy[14]:

- de iure – opracowane przez instytucje standaryzacyjne, np. ISO, IEC;
- de facto – obejmują zalecenia firm, organizacji i stowarzyszeń branżowych, np. ISACA.

W Polsce wiodącą rolę przypisuje się osiągnięciom powstałym w wyniku współpracy organizacji – ISO i IEC. W wyniku działalności instytucji powstały standardy dotyczące[15]:

- zarządzania bezpieczeństwem informacji i systemów teleinformatycznych;
- stosowania kryptografii i bezpieczeństwa sieciowego;
- oceny zabezpieczeń teleinformatycznych.

Procesy biznesowe/statutowe realizowane w organizacji wymagają przetwarzania różnego rodzaju grup informacji. Zasoby informacyjne zależą od specyfiki danej organizacji oraz wymagań prawnych, na podstawie których ona funkcjonuje. W odniesieniu do atrybutów bezpieczeństwa informacji polskie prawodawstwo określa kilka podstawowych informacji prawnie chronionych (tab. 2).

12 A. Wójcik, *System Zarządzania Bezpieczeństwem Informacji zgodny z ISO/IEC 27001. Część 1*, „Zabezpieczenia" nr 2/2008, s. 72.

13 K. Liderman, *Standardy w ocenie bezpieczeństwa teleinformatycznego*, „Biuletyn Instytutu Automatyki i Robotyki" nr 17/2002, s. 99–100.

14 Zob. A. Białas, *Bezpieczeństwo informacji i usług*…, op. cit., s. 45–73.

15 E. Szczepaniuk, *Bezpieczeństwo struktur administracyjnych*…, op. cit., s. 170.

Tabela 2

Wybrane rodzaje informacji prawnie chronionych a wymagania ich ochrony

Podstawa prawna	Wymogi określone w przepisach prawa		
	Zachowanie atrybutów bezpieczeństwa	Zabezpieczenie systemu teleinformatycznego	Dostęp osób do informacji
	Dane osobowe		
Ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych	• poufność • integralność • dostępność	Trzy poziomy bezpieczeństwa: podstawowy, podwyższony i wysoki	Upoważnienie do przetwarzania danych: prowadzenie ewidencji osób upoważnionych, obowiązek zachowania tajemnicy danych i sposobów ich zabezpieczenia
	Informacje niejawne		
Ustawa z 5 sierpnia 2010 r. o ochronie informacji niejawnych	• poufność (klauzule: zastrzeżone, poufne, tajne i ściśle tajne) • integralność • dostępność	Wymagania w zależności od klauzuli niejawności	Poświadczenie bezpieczeństwa osobowego do dostępu do informacji o określonej klauzuli naiwności
	Informacje rachunkowe		
Ustawa z 29 września 1994 r. o rachunkowości	• integralność • dostępność	Zabezpieczenie kopii danych przetwarzanych w systemie	Brak
	Informacje giełdowe		
Ustawa z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi	• poufność (klauzula: informacje poufne) • integralność • dostępność	Brak	Prowadzenie wykazu osób dopuszczonych do informacji poufnych, obowiązek zachowania poufności
	Informacje publiczne		
Ustawa z dnia 8 września 2001 r. o dostępie do informacji publicznej	• integralność • dostępność	Wdrożenie modułu bezpieczeństwa – uniemożliwienie zniszczenia lub modyfikacji informacji oraz zablokowania dostępu	Uprawnienia dostępu do modułu administracyjnego BIP
	Tajemnica przedsiębiorstwa		
Ustawa z 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji	• poufność (warunek wskazania informacji) • integralność • dostępność	Podjęcie działań zabezpieczających wybrane informacje	Dopuszczenie osób do wybranych informacji, zobowiązanie do zachowania poufności
	Tajemnica pracodawcy		
Ustawa z 26 czerwca 1974 r. Kodeks pracy	• poufność (wskazanie informacji, których ujawnienie może narażać pracodawcę na szkodę) • integralność • dostępność	Podjęcie działań zabezpieczających wybrane informacje	Zobowiązanie do zachowania poufności

Opracowanie własne na podstawie: M. Byczkowski, *Zarządzanie bezpieczeństwem informacji i systemów* [w:] *Informatyka gospodarcza*, t. 4, red. J. Zawiła-Niedźwiecki, K. Rostek, A. Gąsiorkiewicz, Warszawa 2010, s. 378.

Podsumowując, przepisy prawne pełnią różnorodne funkcje zarówno w stosunku do obywatela, jak i organizacji. Artykuł 7 Konstytucji RP stanowi, że „Organy władzy publicznej działają na podstawie i w granicach prawa”[16], stąd też prawo oprócz problemów dogmatycznych reguluje funkcjonowanie instytucji. W procesie zarządzania bezpieczeństwem informacyjnym istotne jest dostosowywanie przepisów prawnych do zmieniającego się środowiska bezpieczeństwa, procesów informatyzacji państwa oraz tworzenie reguł umożliwiających implementację efektywnych procedur bezpieczeństwa. Skuteczność systemu bezpieczeństwa informacyjnego organizacji jest zatem determinowana opracowaniem odpowiednich przepisów prawnych, które powinny optymalizować przedsięwzięcia w omawianym obszarze.

Modele systemowego zarządzania bezpieczeństwem informacyjnym

Ochrona zasobów informacyjnych wymaga koordynacji w wielu obszarach organizacji. Rozwiązania powinny implementować zagadnienia związane z zarządzaniem całością procesów informacyjnych i ich wykorzystaniem na różnych poziomach decyzyjnych. Skuteczność tych rozwiązań wydaje się możliwa przy implementacji systemowego zarządzania bezpieczeństwem informacji uwzględniającego związki przyczynowo-skutkowe oraz wszystkie zasoby instytucji. Wdrożenie takich rozwiązań pozwala na doskonalenie wszystkich elementów systemu. Współcześnie funkcjonuje wiele modeli systemowego zarządzania bezpieczeństwem informacji. W artykule odwołano się do rekomendowanych rozwiązań, które z powodzeniem mogą zostać wdrożone w instytucjach sektora publicznego i prywatnego. Wśród omawianych modeli znalazły się:

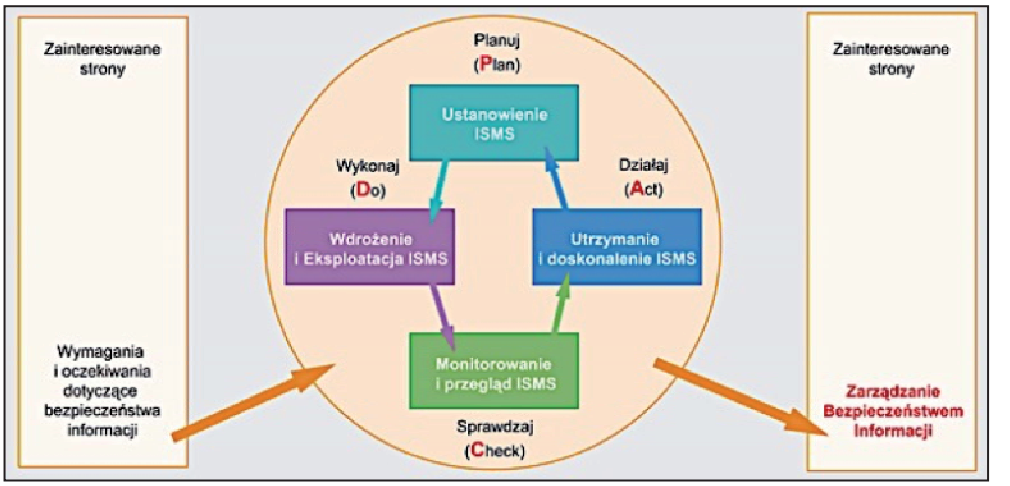
- model ISO/IEC 27001,
- model TISM.

Model ISO/IEC 27001 opracowany przez organizacje ISO i IEC stanowi propozycję praktycznej implementacji systemu zarządzania bezpieczeństwem informacji, który może być zastosowany przez każdą organizację. Model ten podporządkowany jest podejściu procesowemu, które umożliwia ustanowienie, wdrożenie, eksploatację, monitorowanie, przegląd i doskonalenie systemu. W normie podkreśla się, że wdrożenie systemu powinno być wynikiem decyzji strategicznej wypływającej z potrzeb biznesowych organizacji.

Decyzja o wdrożeniu modelu nie pozwala na dokonywanie wyłączeń jakiegokolwiek wymagania standardu ISO/IEC. Możliwe są natomiast ograniczenia w stosowaniu niektórych zabezpieczeń pod warunkiem spełnienia kryteriów akceptacji ryzyka – co powinno być uzasadnione, udokumentowane oraz zatwierdzone. Taka sytuacja nie może wpływać na obniżenie poziomu bezpieczeństwa organizacji oraz spełnienie wymagań wynikających z szacowania ryzyka, wymagań prawnych oraz

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

omawianego standardu[17]. Jak już wcześniej wspomniano, model podporządkowany jest podejściu procesowemu, które opiera się na cyklu Deminga (PDCA). Model ten składa się z czterech etapów przedstawionych na rys. 3.



Źródło: A. Wójcik, *System Zarządzania Bezpieczeństwem Informacji zgodny z ISO/IEC 27001. Część 4*, „Zabezpieczenia" nr 6/2008, cyt. za: E. Szczepaniuk, *Zarządzanie bezpieczeństwem informacji w urzędach administracji publicznej* [w:] *Inżynieria systemów bezpieczeństwa*, red. P. Sienkiewicz, Warszawa 2015, s. 91.

Rys. 3. Model PDCA stosowany w procesach systemu zarządzania bezpieczeństwem informacji (SZBI)

Przedstawione na rys. 3 etapy obejmują następujące przedsięwzięcia:

- planuj – ustalenie i zaplanowanie działań mających doprowadzić do osiągnięcia założonego celu, takich jak ustanowienie polityki SZBI, celów, procedur i strategii;
- wykonuj – wdrożenie i eksploatacja opracowanej polityki SZBI, zabezpieczeń i procedur;
- sprawdzaj – sprawdzenie poprawności i skuteczności realizowanych procesów przez przeglądy, kontrole i audyty;
- działaj – ciągłe doskonalenie procesów, które są skuteczne, oraz zastosowanie działań korygujących w stosunku do zdiagnozowanych obszarów problemowych.

Model ISO/IEC 27001 oprócz wymagań związanych z ustanowieniem, funkcjonowaniem i utrzymywaniem SZBI określa także zabezpieczenia. Lista konkretnych wymagań w tym zakresie znajduje się w załączniku A, który składa się z 11 rozdziałów obejmujących różnego rodzaju zabezpieczenia w powiązaniu z celami ich implementacji. Norma określa następujące rodzaje zabezpieczeń: 1) polityka bezpieczeństwa, 2) organizacja bezpieczeństwa informacji, 3) zarządzanie aktywami, 4) bezpieczeństwo zasobów ludzkich, 5) bezpieczeństwo fizyczne i środowiskowe, 6) zarządzanie systemami i sieciami, 7) kontrola dostępu, 8) pozyskiwanie, rozwój

17 J. Łuczak, M. Tyburski, *Systemowe zarządzanie bezpieczeństwem*…, op. cit., s. 118.

i utrzymywanie systemów informatycznych, 9) zarządzanie incydentami związanymi z bezpieczeństwem informacji, 10) zarządzanie ciągłością działania, 11) zgodność[18]. Rekomendowane typy zabezpieczeń określone w standardzie, odnoszą się nie tylko do rozwiązań technicznych, ale także proceduralnych, technicznych oraz do zasobów ludzkich.

Wdrażanie omawianego modelu musi opierać się na procesie zarządzania ryzykiem zagrożeń informacyjnych. Wybór odpowiednich zabezpieczeń w organizacji powinien być determinowany wynikami i wnioskami płynącymi z procesu szacowania ryzyka. Celem jest zapewnienie ochrony adekwatnej do prawdopodobnych zagrożeń oraz możliwych strat powstałych w wyniku incydentu bezpieczeństwa.

Model TISM jest metodyką zarządzania bezpieczeństwem informacji opracowaną przez ENSI[19]. Zastosowanie tego modelu w organizacji umożliwia wprowadzenie ochrony informacji w sposób planowy, z uwzględnieniem procesów dotyczących analizy ryzyka, konstrukcji wymaganej dokumentacji, opracowania polityki audytów i testów oraz odpowiednich procedur postępowania przy zachowaniu kultury ochrony informacji właściwej dla danej instytucji.

Zgodnie z modelem ustalane są zasady na trzech poziomach[20]:

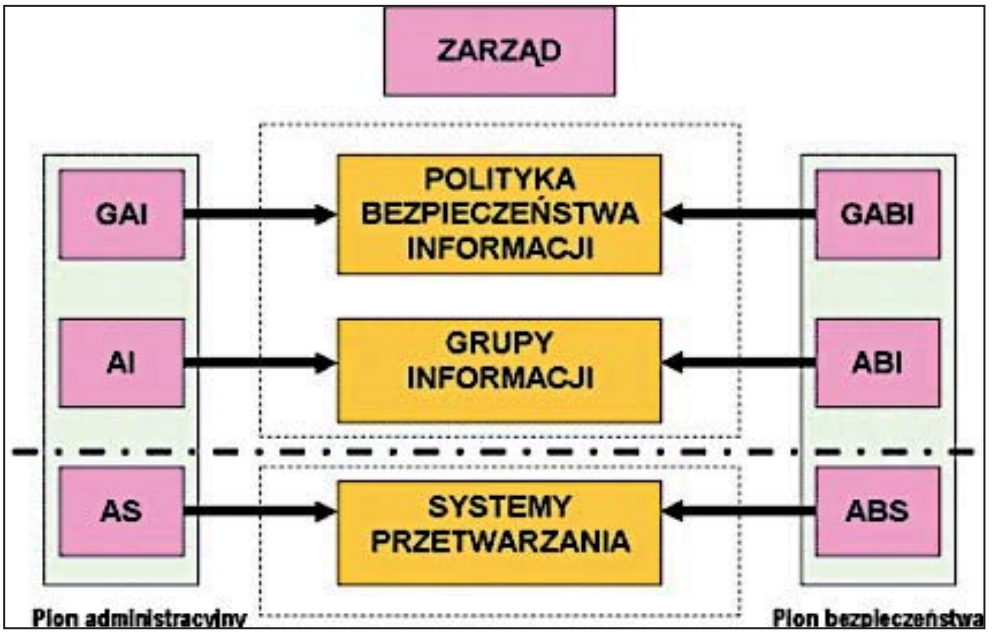
- poziom polityki bezpieczeństwa informacji (PBI), w którym ustalane są podstawowe zasady ochrony informacji w instytucji,
- poziom grup informacji (GI), definiujący specyficzne wymagania ochrony dla danej grupy informacji,
- poziom systemów przetwarzania (SP), określający spełnienie wymagań wyższych poziomów przez system przetwarzania, w którym znajdują się informacje z danej grupy.

W modelu TISM wymienione poziomy opierają się na trzech elementach: strukturze organizacyjnej dotyczącej zarządzania bezpieczeństwem informacji, dokumentacji PBI oraz określeniu miejsc przetwarzania i agregowania informacji.

Struktura zarządzania bezpieczeństwem informacyjnym polega na określeniu ról zarządczych (administracyjnych) oraz kontrolnych (bezpieczeństwa) odnoszących się do trzech wyżej wymienionych poziomów bezpieczeństwa (rys. 4).

Zgodnie z rys. 4. na poziomie PBI określa się role głównego administratora informacji (GAI) oraz głównego administratora bezpieczeństwa informacji (GABI). Natomiast na poziomie grupy informacji tworzone jest stanowisko: administratora grupy informacji (AI) oraz administratora bezpieczeństwa grupy informacji (ABI). Na ostatnim poziomie systemu przetwarzania występuje administrator systemu (AS) oraz administrator bezpieczeństwa systemu (ABS)[21]. W praktyce w poszczególnych pionach często występuje łączenie ról. Przykładowo zarząd może pełnić funkcje GAI. Funkcje nie są jednak łączone między różnymi pionami.

18 J. Łuczak, M. Tyburski, *Systemowe zarządzanie bezpieczeństwem*…, op. cit., s. 139–140.
19 ENSI – ang. European Network Security Institute.
20 M. Byczkowski, *Zarządzanie bezpieczeństwem informacji i systemów*…, op. cit., s. 379.
21 M. Zarzycki, *Audyty systemów informatycznych*…, op. cit., s. 5.



Źródło: M. Zarzycki, *Audyty systemów informatycznych*, http://www.forge154.forgehost.pl/notatki/ASI-temat_3.pdf, s. 4 [dostęp 18.03.2016].

Rys. 4. Metodyka TISM – struktura zarządzania informacją i jej bezpieczeństwem

W modelu TISM istotną rolę ma klasyfikacja informacji, ponieważ określa dobór odpowiednich zabezpieczeń. Jak już wcześniej wspomniano, ochrona określonych grup informacji może wynikać z przepisów prawa (np. dane osobowe) lub może być elementem przyjętej strategii w danej instytucji (np. tajemnica przedsiębiorstwa).

W omawianym modelu zaproponowano trójstopniową klasyfikację informacji[22]:

- informacje chronione drugiego stopnia – limitowane do grupy odbiorców,
- informacje chronione pierwszego stopnia – do użytku wewnętrznego (służbowe),
- informacje chronione poziomu podstawowego – jawne.

TISM umożliwia hierarchiczne porządkowanie zależności między procesami biznesowymi w instytucji a funkcjonowaniem systemów teleinformatycznych. Metodyka jest jak dotąd z powodzeniem stosowana w instytucjach prywatnych, natomiast znacznie rzadziej wykorzystuje się ją sektorze publicznym.

22 M. Byczkowski, *Zarządzanie bezpieczeństwem informacji i systemów*…, op. cit., s. 385.

Wdrożenie, eksploatacja i monitorowanie systemu zarządzania bezpieczeństwem informacji

Decyzja kierownictwa instytucji związana z ustanowieniem SZBI wiąże się z koniecznością wdrożenia w praktyce przyjętych założeń. Opracowane procedury i polityki powinny precyzyjnie określać zasady bezpieczeństwa, które będą umożliwiały powtarzalność czynności wykonywanych przez personel, w tym rozwiązywały problemy związane z bezpieczeństwem. Charakteryzowane czynności powinny zapewniać wykrywanie i reakcję na incydenty przez opracowanie procedur zgłaszania incydentów, sposobów reagowania na nie, usuwania skutków oraz przywrócenia systemu do stanu sprzed wystąpienia incydentu. W procesie wdrażania systemu zarządzania bezpieczeństwem informacji dominują dwa zasadnicze podejścia:

- podejście normatywne,
- podejście eksperckie.

Podejście normatywne opiera się na implementacji norm dotyczących bezpieczeństwa informacji. W odniesieniu do norm ISO/IEC są to w szczególności normy 17799 i 27001. Pierwsza z nich zawiera zbiór wytycznych dotyczących zarządzania bezpieczeństwem, które można zastosować całościowo lub wybiórczo. Druga natomiast odnoszona jest do całościowego SZBI i zawiera wymagania do wdrożenia systemu, który może podlegać certyfikacji[23]. Zasadniczą różnicą w implementacji przywołanych norm jest uwzględnienie procesu zarządzania ryzykiem. W celu wdrożenia SZBI opartego na PN-ISO/IEC wymagane jest stosowanie metod zarządzania ryzykiem związanych z bezpieczeństwem aktywów informacyjnych organizacji.

W literaturze można odnaleźć wiele metodyk szacowania ryzyka[24]. Istotą problemu zarządzania ryzykiem w kontekście ochrony zasobów informacyjnych jest tworzenie map zagrożeń dotyczących[25]:

- przetwarzania informacji (np. gromadzenie, udostępnianie, archiwizowanie),
- miejsc agregowania informacji (np. nośniki, systemy informatyczne),
- nadawania uprawnień dostępu do informacji i wykonywania operacji na nich.

Opracowanie mapy zagrożeń powinno skutkować stworzeniem planu postępowania z ryzykiem, zakładającego określoną strategię postępowania. Podejście normatywne w implementacji SZBI z uwzględnieniem zarządzania ryzykiem można odnieść do kilku etapów. Decyzji o ustanowieniu SZBI powinno towarzyszyć przeprowadzenie pierwszej analizy ryzyka, polegającej na identyfikacji aktywów instytucji oraz rozpatrzeniu zagrożeń i podatności mogących wpływać na bezpieczeństwo informacyjne.

Na etapie wdrożenia i eksploatacji SZBI na podstawie danych z analizy ryzyka zostaje stworzony plan postępowania z ryzykiem. Istotne jest także wdrożenie planów uświadamiających i szkoleń dla pracowników. Po wdrożeniu systemu nie-

23 M. Byczkowski, *Zarządzanie bezpieczeństwem informacji i systemów…*, op. cit., s. 391.

24 Zob. W. Skomra (red.), *Metodyka oceny ryzyka na potrzeby systemu zarządzania kryzysowego RP*, Warszawa 2015.

25 M. Byczkowski, *Zarządzanie bezpieczeństwem informacji i systemów…*, op. cit., s. 393.

zbędne jest monitorowanie jego działania i dokonywanie okresowych przeglądów. Monitorowanie ma na celu wykrywanie nieprawidłowości, błędów i incydentów bezpieczeństwa[26]. Informacje pochodzące z monitorowania pozwalają określić, czy zabezpieczenia funkcjonują zgodnie z przeznaczeniem. Natomiast przeglądy służą pomiarowi skuteczności zabezpieczeń, okresowemu szacowaniu ryzyka, audytom oraz zadaniom kontrolnym realizowanym przez kierownictwo.

Podejście eksperckie charakteryzuje się tym, że przed rozpoczęciem wdrożenia systemu zarządzania bezpieczeństwem informacji dokonuje się oceny poziomu dojrzałości biznesowej oraz na tej podstawie wybiera się plan i zakres wdrożenia.

Ocena poziomu dojrzałości biznesowej ma na celu określenie stanu wejściowego wdrażanych regulacji w zakresie zarządzania aktywami informacyjnymi i ich bezpieczeństwem. W literaturze przedmiotu spotykana jest najczęściej metodyka oceny według TISM-ISMS oraz według ISACA[27]. Pierwsza z przywołanych metodyk obejmuje trzy poziomy zaawansowania, gdzie pierwszy poziom oznacza brak regulacji w zakresie ochrony informacji, a trzeci – najbardziej zaawansowane struktury w omawianym obszarze. Druga z koncepcji jest bardziej szczegółowa, w związku z tym częściej rekomendowana do stosowania w praktyce. Tabela 3 prezentuje poziomy dojrzałości zarządzania bezpieczeństwem informacji według ISACA.

Tabela 3

Poziomy dojrzałości zarządzania bezpieczeństwem informacji według ISACA

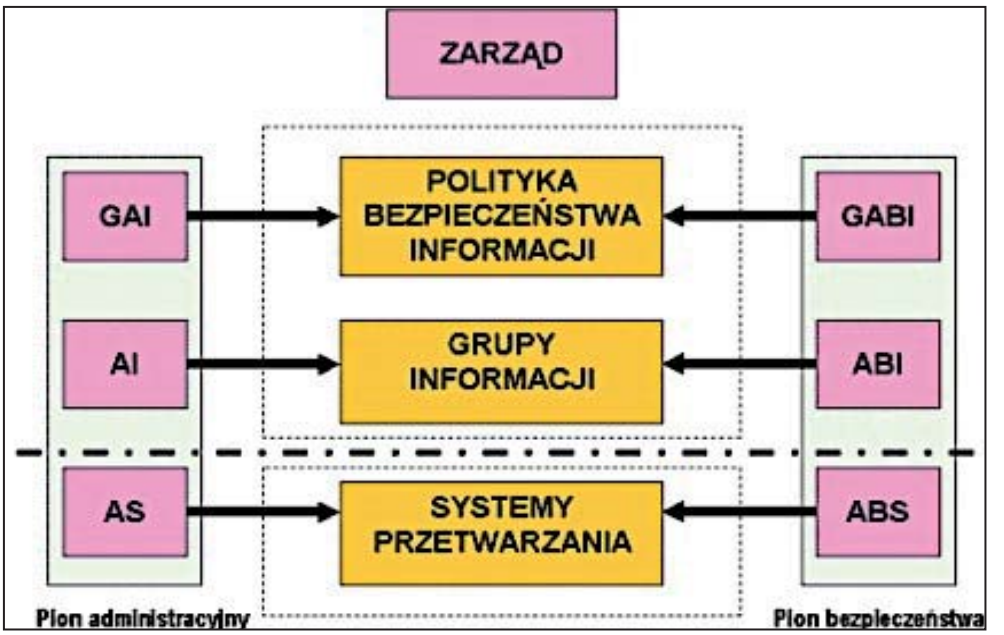
Poziom	Charakterystyka
Poziom 0 Brak świadomości	• brak definiowanych wymagań bezpieczeństwa • bezpieczeństwo traktowane jako problem poszczególnych użytkowników
Poziom I Początkowy	• świadomość potrzeby • kierownictwo uważa to za problem służb IT
Poziom II Intuicyjny	• próby tworzenia zabezpieczeń • brak jednolitego podejścia • efekty zależne od zaangażowania osób zainteresowanych
Poziom III Zdefiniowany	• zdefiniowane zasady w całej organizacji • procedury bezpieczeństwa są utrzymywane i komunikowane • brak kontroli stosowania
Poziom IV Zarządzany	• jednolite podejście dla wszystkich komórek i wszystkich rozwiązań • obowiązuje perspektywa biznesu • funkcjonuje mechanizm kontroli stosowania
Poziom V Optymalizowany	• świadomość zarządzania ryzykiem • zgodność strategii bezpieczeństwa ze strategią biznesową • zapewnienie bezpieczeństwa jako proces (wiedza, doskonalenie)

Opracowanie własne na podstawie: M. Forystek, *Audyt informatyczny*, Zgierz 2005, cyt. za: M. Byczkowski, *Zarządzanie bezpieczeństwem informacji i systemów*…, op. cit., s. 395.

26 Solecki A., Solecki P., *Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie* [w:] *Zarządzanie bezpieczeństwem informacji i programami antykorupcyjnymi*, Bielsko-Biała 2007, s. 132.

27 ISACA – ang. Information Security Audit and Control Association.

Przywołane poziomy dojrzałości zarządzania bezpieczeństwem informacji są pomocne w określeniu czasu wdrożenia, zakresu działań oraz kosztów. Wobec powyższego zasadne jest, aby wdrożenie systemu bezpieczeństwa informacji przebiegało w kilku fazach, przedstawionych na rys. 5.



Opracowanie własne.

Rys. 5. Podejście eksperckie w implementacji SZBI

Zarówno podejście normatywne, jak i eksperckie pozwala w końcowym etapie na osiągnięcie certyfikowanego SZBI. W tym celu niezbędne jest skorzystanie z usług organizacji certyfikującej, która wykonuje audyt certyfikacyjny. Audytorzy oceniają adekwatność SZBI do wymagań organizacji oraz czy jest on stosowany w praktyce.

Po wdrożeniu SZBI organizacja powinna monitorować działanie sytemu pod kątem skuteczności wprowadzonych rozwiązań. Standardy wskazują na konieczność określenia i ustanowienia procedur monitorowania i dokonywania przeglądów systemu i wprowadzonych zabezpieczeń przede wszystkim pod kątem kryterium efektywnościowego. Zgodnie z normą ISO/IEC 27001 efektywność jest rozumiana jako relacja między osiągniętymi wynikami a wykorzystanymi zasobami[28]. Celem tych procedur jest opracowanie mechanizmów służących wykrywaniu nieprawidłowości we wdrożonym systemie. Ponadto rozwiązania te powinny umożliwiać kierownictwu stwierdzenie, czy pracownicy wykonują prawidłowo swoje obowiązki

28 J. Łuczak, M. Tyburski, *Systemowe zarządzanie bezpieczeństwem*…, op. cit., s. 223–224.

oraz czy środki informatyczne są wykorzystywane zgodnie z oczekiwaniami. Potrzeba monitorowania wynika także z faktu, że elementy bezpieczeństwa, tzn. zasoby, podatności i zagrożenia podlegają permanentnym zmianom[29]. Pożądane jest, aby organizacja stale doskonaliła wdrożony SZBI i utrzymywała zakładany poziom bezpieczeństwa.

Dla skuteczności wdrożonego systemu konieczne jest także wykonywanie przeglądów zgodności z polityką i celami, stosowanych zabezpieczeń, wyników audytu, incydentów, rezultatów pomiarów efektywności, sugestii oraz informacji zwrotnych od zainteresowanych stron. W zaplanowanych odstępach czasu powinny być wykonywane przeglądy ryzyka szczątkowego oraz poziomów ryzyka akceptowalnego, z uwzględnieniem zmian w organizacji, technologii, celów biznesowych i procesów, zidentyfikowanych zagrożeń, efektywności wdrażanych zabezpieczeń, zewnętrznych zdarzeń, np. zmiany przepisów prawnych[30]. Dane z monitorowania i przeglądów pozwalają na działania korygujące i zapobiegawcze, służą zatem doskonaleniu systemu i dostosowaniu go do zmieniającego się środowiska bezpieczeństwa i potrzeb instytucji.

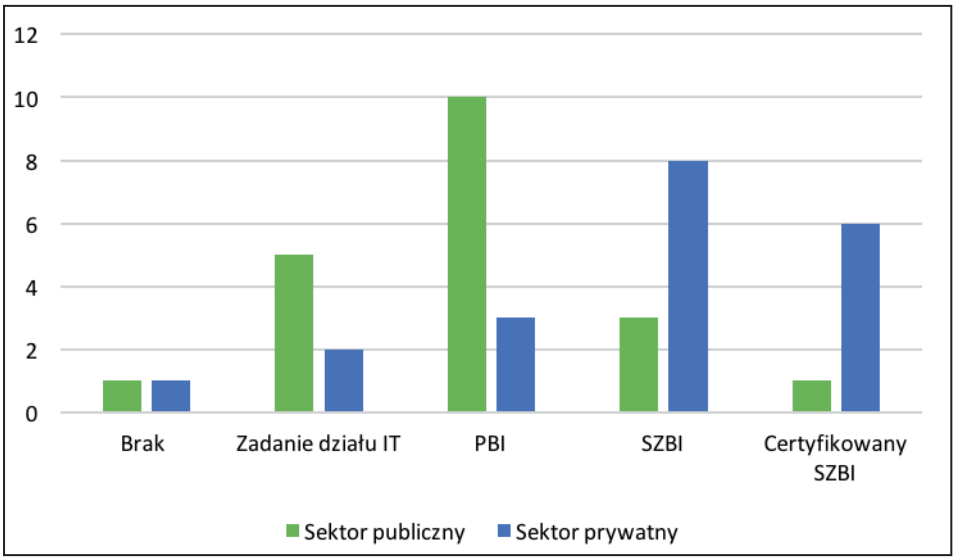
Problemy bezpieczeństwa informacyjnego w organizacji – wyniki badań

Diagnoza obszarów problemowych w aspekcie bezpieczeństwa informacyjnego wymagała przeprowadzenia badań ankietowych w jednostkach sektora publicznego i prywatnego. W badaniu łącznie wzięło udział 40 osób. W celu możliwości zastosowania analizy porównawczej wybrano 20 ankietowanych zatrudnionych w sektorze publicznym oraz 20 w sektorze prywatnym. Kwestionariusz ankiety składał się z 10 pytań dotyczących informacji ogólnych na temat ankietowanych (wiek, wykształcenie, stanowisko, zatrudnienie w sektorze publicznym lub prywatnym), struktur organizacyjnych związanych z bezpieczeństwem informacyjnym, stosowanych rozwiązań proceduralnych i organizacyjnych oraz świadomości ankietowanych na temat zagrożeń informacyjnych. W niniejszym artykule, ze względu na ograniczone możliwości szczegółowej analizy prowadzonych badań, odniesiono się jedynie do wybranych wyników.

Jedno z pytań w kwestionariuszu ankiety dotyczyło wdrożonych struktur systemu bezpieczeństwa informacyjnego. Odpowiedzi udzielane przez ankietowanych w powiązaniu z jednostką sektora publicznego i prywatnego przedstawia rys. 6.

29 Szarzej na temat monitorowania elementów bezpieczeństwa: A. Białas, *Bezpieczeństwo informacji i usług*…, op. cit., s. 394–398.

30 J. Łuczak, M. Tyburski, *Systemowe zarządzanie bezpieczeństwem*…, op. cit., s. 224.

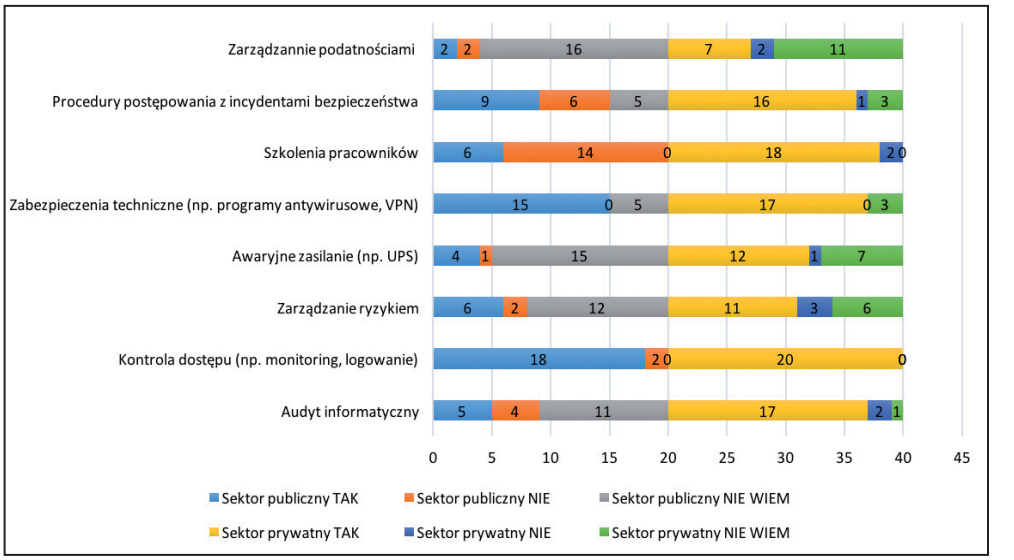


Rys. 6. Rozwiązania organizacyjne wdrożone w badanych jednostkach

Zgodnie z prezentowanymi wynikami tylko w jednej jednostce z sektora publicznego i prywatnego nie istnieją żadne struktury związane z organizacją bezpieczeństwa informacji. Należy zauważyć, że możliwe odpowiedzi zawarte w kwestionariuszu ankiety odpowiadają poziomom dojrzałości biznesowej instytucji – od braku struktur do najbardziej zaawansowanej formy, czyli certyfikowanego systemu zarządzania bezpieczeństwem informacji (SZBI). W miarę zaawansowania stopnia organizacji systemu wyraźnie spada implementacja takich rozwiązań w sektorze publicznym. Jedynie trzech ankietowanych przyznało, że w instytucji istnieje SZBI. Natomiast certyfikowany SZBI funkcjonuje w jednej z badanych jednostek sektora publicznego. W sektorze prywatnym można natomiast zaobserwować odwrotną tendencję. W większości instytucji wdrożono SZBI lub certyfikowany SZBI.

Następne pytanie odnosiło się do rozwiązań proceduralnych stosowanych w badanych jednostkach. W kwestionariuszu określono osiem różnych rozwiązań odnoszących się zarówno do aspektów technicznych, np. wydzielone sieci wirtualne (VPN), jak organizacyjnych, np. szkolenia, kontrola dostępu. Do każdej z przywołanych procedur określono trzy możliwe odpowiedzi – tak, nie i nie wiem. Wyniki badania uwzględniające porównanie sektora publicznego i prywatnego prezentuje rys. 7.

Analiza odpowiedzi udzielanych przez respondentów wskazuje na różnicę w odpowiedziach osób zatrudnionych w sektorze publicznym i prywatnym. W pierwszym z wymienionych ankietowani znacznie częściej odpowiadali „nie wiem" lub „nie" w porównaniu do zatrudnionych w drugim sektorze. Może to świadczyć o zależnościach między szkoleniami a wiedzą ankietowanych oraz zaimplementowanych strukturach organizacyjnych ds. bezpieczeństwa informacji. Dla przypomnienia warto wskazać, że zgodnie z danymi przedstawionymi na poprzednim wykresie (rys. 7.) struktury te były rozwinięte w sektorze publicznym znacznie słabiej.



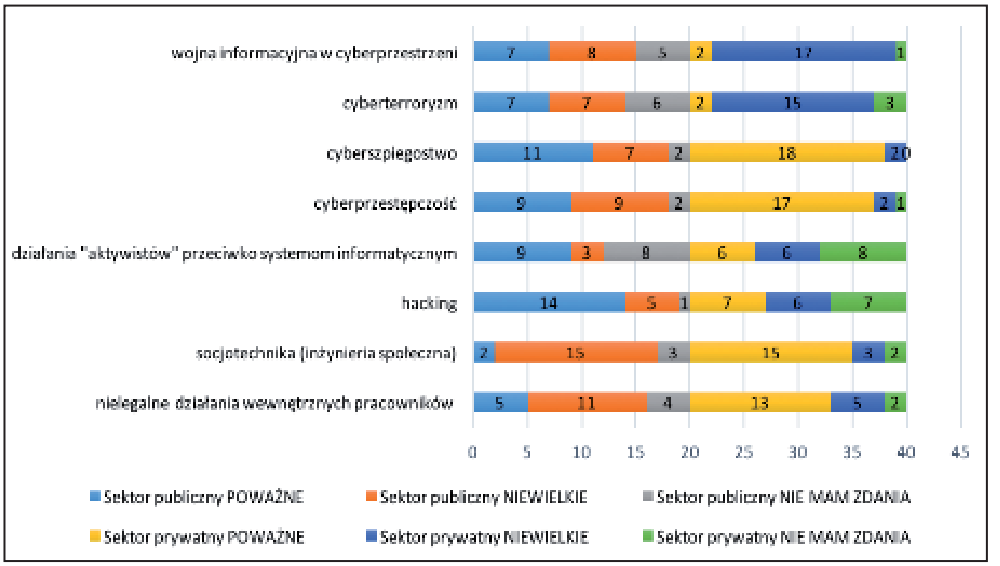
Rys. 7. Rozwiązania proceduralne stosowane w badanych jednostkach

Kolejne z pytań zawartych w ankiecie dotyczyło wiedzy i świadomości zagrożeń dla bezpieczeństwa informacyjnego organizacji. Na potrzeby badań ankietowych wyróżniono osiem grup zagrożeń. Wśród możliwych odpowiedzi znalazły się: poważne, niewielkie oraz nie mam zdania. Odpowiedzi udzielane przez badanych przedstawia rys. 8. Zgodnie z prezentowanymi danymi osoby zatrudnione w sektorze publicznym znacznie częściej udzielały odpowiedzi „nie mam zdania". Warto wspomnieć, że statystyki dotyczące incydentów bezpieczeństwa publikowane przykładowo przez CERT.gov wskazują, jak znacznym zagrożeniem dla zasobów informacyjnych jest zjawisko inżynierii społecznej. Wśród osób zatrudnionych w administracji publicznej, w przeciwieństwie do osób zatrudnionych w sektorze prywatnym, istnieje przekonanie o znikomym zagrożeniu tym zjawiskiem. Świadczy to o braku świadomości zagrożeń wśród badanych.

Jak już wcześniej wspomniano, w artykule zaprezentowane zostały jedynie wybrane wyniki badań ankietowych. Prezentowana analiza miała na celu przedstawienie obszarów problemowych w zakresie bezpieczeństwa informacyjnego. Do głównych nieprawidłowości można zaliczyć następujące:

- W większości jednostek sektora publicznego brakuje certyfikowanego SZBI, a wprowadzone rozwiązania mają charakter fragmentaryczny. W jednostkach sektora prywatnego znacznie częściej spotyka się sformalizowany i faktycznie wdrożony SZBI. Dodatkowo przeprowadza się także audyty certyfikujące przez jednostki zewnętrzne (certyfikowany SZBI).
- W administracji publicznej istnieje problem ze stosowaniem zabezpieczeń, np. w zarządzaniu podatnościami. Wiele z obligatoryjnych rozwiązań nie jest implementowanych lub pracownicy nie mają świadomości ich stosowania. W sektorze prywatnym znacznie powszechniej wykorzystywane są tego typu mechanizmy.

• Wśród ankietowanych ogólnie brakuje świadomości na temat zagrożeń informacyjnych. Sytuacja wygląda znacznie lepiej w sektorze prywatnym. W obu badanych grupach istnieje zbyt duży – w naszym przekonaniu – odsetek osób udzielających odpowiedzi „nie mam zdania", co może świadczyć o braku odpowiednich szkoleń, kompetencji lub wiedzy.



Rys. 8. Świadomość zagrożeń dla bezpieczeństwa informacyjnego organizacji

Podsumowanie

Celem artykułu było zaprezentowanie rekomendowanych rozwiązań dotyczących wdrożenia systemu zarządzania bezpieczeństwem informacji. Omawiana problematyka stanowi współcześnie istotne wyzwanie zarówno dla sektora publicznego, jak i prywatnego. Publikowane incydenty bezpieczeństwa w Polsce i na świecie świadczą niewątpliwie o skali poruszanego problemu. Wiele państw dąży do implementacji skutecznego systemu bezpieczeństwa informacji. Opracowywane są także strategie sektorowe dotyczące cybernetycznego wymiaru bezpieczeństwa narodowego, które najogólniej można odnieść do bezpieczeństwa informacji cyfrowej.

Jeżeli traktujemy system bezpieczeństwa narodowego jako „całość tworzoną przez zbiór obiektów elementarnych (elementów) i powiązań (relacji) pomiędzy nimi"[31], to organizacje sektora publicznego i prywatnego są jednymi z elementów sieci połączeń. Ma to szczególnie istotne znaczenie w przypadku rozprzestrzeniania się zagrożenia (efekt domino), które jest wysoce prawdopodobne w środowisku

31 P. Sienkiewicz, *Inżynieria systemów*, Warszawa 1983, s. 27.

elektronicznym. Stąd też podjęta przez nas problematyka stanowi aktualny problem wymagający kontynuowania badań w przedmiotowym obszarze.

Przyszłość problematyki powinna uwzględniać integrację systemów zarządzania bezpieczeństwem z systemem zarządzania jakością, który jest szczególnie istotny w organizacjach ukierunkowanych na efektywność ekonomiczną (sektor prywatny). Ponadto rola i znaczenie administracji publicznej w społeczeństwie uległo zmianie w kierunku potrzeby zapewnienia jakości świadczonych usług (koncepcja New Public Governance[32]). Obszar badań, dotyczy wielu dziedzin wiedzy (m.in. nauk społecznych, technicznych, prawnych), dlatego wymaga prac w wielu ośrodkach naukowych i interdyscyplinarnych analiz.

Bibliografia

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

Białas A., *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, Warszawa 2006.

Blim M., *Teoria ochrony informacji (część 1)*, „Zabezpieczenia" nr 3/2007.

Byczkowski M., *Zarządzanie bezpieczeństwem informacji i systemów* [w:] *Informatyka gospodarcza*, t. 4, red. J. Zawiła-Niedźwiecki, K. Rostek, A. Gąsiorkiewicz, Warszawa 2010.

Forystek, M., *Audyt informatyczny*, Zgierz 2005.

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

Liderman K., *Bezpieczeństwo informacyjne*, Warszawa 2012.

Liderman K., *Standardy w ocenie bezpieczeństwa teleinformatycznego*, „Biuletyn Instytutu Automatyki i Robotyki" nr 17/2002.

Łuczak J., Tyburski M., *Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC 27001*, Poznań 2010.

Promoting good governance. European Social Fund thematic paper, European Commission, January 2014.

Sienkiewicz P., *Inżynieria systemów*, Warszawa 1983.

Skomra W. (red.), *Metodyka oceny ryzyka na potrzeby systemu zarządzania kryzysowego RP*, Warszawa 2015.

Solecki A., Solecki P., *Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie* [w:] *Zarządzanie bezpieczeństwem informacji i programami antykorupcyjnymi*, Bielsko-Biała 2007.

Suchorzewska A., *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*, Warszawa 2010.

Szczepaniuk E., *Bezpieczeństwo struktur administracyjnych w warunkach zagrożeń cyberprzestrzeni państwa*, rozprawa doktorska, AON, Warszawa 2015.

32 Zob. *Promoting good governance. European Social Fund thematic paper*, European Commission, January 2014.

Szczepaniuk E., *Wybrane problemy bezpieczeństwa informacyjnego państwa* [w:] *Bezpieczeństwo narodowe i międzynarodowe wobec wyzwań współczesnego świata*, red. W. Kitler, M. Marszałek, Warszawa 2014.
Szczepaniuk E., *Zarządzanie bezpieczeństwem informacji w urzędach administracji publicznej* [w:] *Inżynieria systemów bezpieczeństwa*, red. P. Sienkiewicz, Warszawa 2015.
Szomański B., *Systemy zarządzania bezpieczeństwem informacji – założenia i projektowanie*, „Problemy Jakości" nr 4/2004.
Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Dz.U. 1997 nr 133, poz. 883 ze zm.
Whitman M.E., Mattord H.J., *Management of Information Security*, Boston 2008.
Wójcik A., *System Zarządzania Bezpieczeństwem Informacji zgodny z ISO/IEC 27001. Część 1*, „Zabezpieczenia" nr 2/2008.
Wójcik A., *System Zarządzania Bezpieczeństwem Informacji zgodny z ISO/IEC 27001. Część 4*, „Zabezpieczenia" nr 6/2008.
Zarzycki M., *Audyty systemów informatycznych*, http://www.forge154.forgeho st.pl/notatki/ASI-temat_3.pdf [dostęp 18.03.2016].

INFORMATION SECURITY IN ORGANISATIONS

Abstract

The paper presents recommended methods of information security systems designs. The analysis comprises the essence and elements of information security, but also the relations between them. The systemic approach to the studied area required providing characteristics of legal basis and information security models – ISO/IEC and TISM. Also characterised were the implementation, exploitation, and monitoring methods of information systems. The paper concludes with a presentation of results of empirical research conducted in public and private sector entities, as well as conclusions and recommendations.

Key words: information security, management information security models, information protection