mgr Jarosław Jan Feliński
Akademia Marynarki Wojennej
jaroslaw.felinski@gazeta.pl

MENEDŻER BEZPIECZEŃSTWA INFORMACJI (MBI) – INTERDYSCYPLINARNE WYZWANIE EDUKACYJNE ADMINISTRATORÓW INFORMACJI

INFORMATION SAFETY MANAGER – AN INTERDISCIPLINARY EDUCATIONAL CHALLENGE OF INFORMATION ADMINISTRATORS

Streszczenie: Sprawność zastosowania wiedzy w procesach analizy i oceny zagrożeń, wprowadzanie praktycznych rozwiązań zabezpieczenia gromadzonych zasobów informacji w przedsiębiorstwach i administracji, stały się pożądanymi i poszukiwanymi w potrzebach rynku pracy. Wyrazem tego zainteresowania są liczne ogłoszenia prasowe i internetowe zapraszające potencjalnych kandydatów do współpracy. Dynamicznie rozwijający się system usług elektronicznych powiększył ilość specjalistów branży informatycznej, lecz powstała luka w istotnym czynniku systemu informatycznego – zarządca / administrator. Przewodnią myślą administratorów na różnych płaszczyznach kierowania powinno być pytanie, jak zdefiniować potencjalne zagrożenia oraz w jaki sposób przeciwdziałać tym zagrożeniom. Koncepcja przedstawionego problemu jest materiałem do dyskusji, czy i jak środowisko naukowe oraz szkoły wyższe powinny wspierać kształcenie osób zarządzających systemem zarządzania bezpieczeństwem informacji w kontekście zmian prawa krajowego lat 2014–2016 i do 2018.

Słowa kluczowe: administrator, audytor, bezpieczeństwo, edukacja, inspektor, bazy danych.

Summary: The efficiency of the use of knowledge in the processes of analysis and evaluation of risks, the introduction of practical solutions to secure collected information resources in enterprises and administration have become a desired and sought-after skill in the needs of the labour market. What proves that this is of great interest are numerous press and internet releases, inviting potential candidates for cooperation. Dynamically developing electronic services system increased the number of IT professionals, but there appeared a flaw in an important factor of the information system of MANAGER / ADMINISTRATOR. The keynote for administrators in various areas of targeting should be the question of how to define potential threats and how to counter them. The concept of the presented problem is to discuss whether and how the scientific and higher education institutions should promote the training of managers of information security management system, in the context of the changes to the national law of the years 2014–2016/2018.

Keywords: the administrator, auditor, security, education, the Inspector, the database.

Wstęp

Powstające dzięki technikom teleinformatycznym nowe formy aktywności ludzkiej w efekcie prowadzą do powstawania nowych rodzajów komunikacji społecznej, nowych miejsc pracy, kolejnych przestrzeni wolnego rynku, a także tworzenia się nowych wartości – ale i zupełnie nowych zagrożeń. Obecna rzeczywistość to *e ~ rzeczywistość (*Feliński, 2014) zdominowana przez powszechnie stosowane techniki informatyczne umożliwiające niemal nieograniczony dostęp do informacji osobowej lub instytucjonalnej. W kontekście tak istotnego zagadnienia jak zagrożenia integralności i wiarygodności informacji, kilkanaście ostatnich lat przyniosło wiele zmian w podejściu do identyfikacji źródeł zagrożeń. Ostatecznie doprowadziły one do sformalizowania i ukonstytuowania nauk o bezpieczeństwie – dyscypliny naukowej umiejscowionej w dziedzinie nauk społecznych w obszarze nauk społecznych[1]. Określenie bezpieczeństwa wewnętrznego jako dyscypliny naukowej wytworzyło przestrzeń do prowadzenia dyskusji na tematy bieżących potrzeb obszaru jakim jest zarządzanie bezpieczeństwem informacji. Tym samym bezpieczeństwo informacyjne stało się trwałym elementem bezpieczeństwa narodowego. Zdefiniowane w wymiarze cyberprzestrzeni[2] aktywności społeczne, tak w wymiarze państwowym jak również każdego obywatela, wymagają nowego naukowego spojrzenia na zakres powstających zagrożeń. Cyberterroryzm[3] został utrwalony jako zjawisko oddziaływania o zasięgu globalnym, lokalnym, krajowym a także indywidualnym.

Rozwój techniki przynoszący oprócz oczywistych szans i korzyści płynących z wykorzystywania nowych technologii oraz sprawności działania teleinformatycznych systemów przesyłania informacji, komunikacji i transferów danych wprowadza zagrożenie integralności i poufności przetwarzanych informacji. Stąd też bieżącą i przyszłą potrzebą stało się prognozowanie skali zagrożeń, skutków utraty informacji a także potencjalnych szkód i ponoszonych strat. Wraz z katalogiem prawdopodobnych zdarzeń powodowanych świadomym działaniem przestępców, nieodpowiedzialnością wykonawców, losowymi przypadkami utraty sprawności systemów, powinno pojawić się odpowiednie reagowanie na wszystkie niebezpieczne zjawiska. Analiza i ocena źródeł, a także ryzyka wystąpienia zagrożeń bezpieczeństwa, stanowi w chwili obecnej przedsięwzięcie planistyczno – kontrolne i weryfikacyjne zmierzające do minimalizacji niepożądanych zjawisk i odpowiedniej wewnętrznej reakcji na zewnętrzne zagrożenia w oparciu o przepisy prawa o ochronie informacji.

Czynnikiem istotnie wpływającym na funkcjonalność systemów informa-

[1] Zob. poz. 2 załącznika do Rozporządzenia Ministra Nauki i Szkolnictwa Wyższego z dnia 8 sierpnia 2011r. w sprawie obszarów wiedzy, nauki i sztuki oraz dyscyplin naukowych i artystycznych (Dz.U. 2011 nr 179 poz. 1065),

[2] Cyberprzestrzeń – «przestrzeń wirtualna, w której odbywa się komunikacja między komputerami połączonymi siecią internetową» Pobrano 17 lutego 2017, z: http://sjp.pwn.pl/sjp/cyberprzestrze%C5%84;2553915,

[3] Cyberterroryzm – neologizm opisujący dokonywanie aktów terroru przy pomocy zdobyczy technologii informacyjnej. Pobrano 17 lutego 2017, z: https://pl.wikipedia.org/wiki/Cyberterroryzm.

tycznych w kontekście zapewnienia stabilności pracy, warunków organizacyjnych i sprawności zarządzania wykonawcami będzie systematyczna i powszechna edukacja odpowiednich specjalistów. Typowanie podmiotu organizacyjno- technicznego zabezpieczenia danych, administratorów – *specjalistów Systemu Zarządzania Bezpieczeństwem Informacji (dalej jako:* ***SZBI****)*[4] *określanych także mianem – Menedżer Bezpieczeństwa Informacji (dalej jako:* ***MBI****)*[5] jest trudnym zadaniem wielu kierowników instytucji i organizacji biznesowych. Dotychczasowe doświadczenia audytowe i kontrolne wykazują, iż instytucje i firmy mają w tym zakresie poważny problem. Wyznaczanie lub powołanie MBI powinno cechować się kryteriami kwalifikacji opartych na ocenie stanu wiedzy kandydata, a także na umiejętnościach dostosowania wewnętrznych rozwiązań do zmian prawa i warunków środowiska systemów informatycznych. W praktyce losowo wyznaczone osoby do pełnienia funkcji, z nieformalnym przygotowaniem merytorycznym lub jego brakiem, nie spełniają wymagań skutecznego realizowania procesów zarządzania bezpieczeństwem informacji. Ilość specjalistów szeroko rozumianej branży informatycznej, cyberprzestrzeni6 w ostatniej dekadzie znacznie wzrosła, powstała jednak luka w istotnym czynniku systemu informatycznego – zarządców / administratorów potrafiących skutecznie połączyć ustawowe delegacje ustawowe (granice dopuszczalności gromadzenia danych) przetwarzania informacji z programami i aplikacjami. Zadaniem specjalistów SZBI/MBI, jest umiejętność połączenia specjalistycznych pojęć prawa i informatyki w przejrzystą formę zadań przekazywaną użytkownikom realizującym czynności zgodnie z przyjętymi politykami bezpieczeństwa informacji. Kierowanie, nadzorowanie i weryfikacja działań użytkowników w praktyce działania specjalisty SZBI, oznacza pracę z najsłabszym ogniwem systemu ochrony informacji – człowiekiem. Użytkownicy stanowią tym samym stały element zagrożenia bezpieczeństwa informacji, na które zgodnie z zasadami przetwarzania i zabezpieczania informacji powinien mieć wpływ interdyscyplinarny specjalista – Menedżer Bezpieczeństwa Informacji. Skuteczność i efektywność oddziaływania MBI związana będzie zatem z poziomem jego praktycznych umiejętności, wiedzy i ciągłego doskonalenia w poznawaniu nowych zagrożeń. W związku z zapowiadanymi zmianami przepisów prawa koniecznością staje się kształcenie specjalistów SZBI w celu wypełnienia nowych wymagań i przywrócenia równowagi w organizacyjno -personalnym zarządzaniu bezpieczeństwem informacji. Jednocześnie można założyć, iż działania edukacyjne prowadzone przez MBI w ramach określonych przepisami prawa form kształcenia wykonawców i użytkowników, podwyższą poziom ogólnej wiedzy i przyczynią się do minimalizowania błędów. Określając potencjalne potrzeby bezpieczeństwa informacji, w niniejszym opracowaniu przedstawiono usprawiedliwione przypuszczenie:

---

[4] System Zarządzania Bezpieczeństwem Informacji – (ang. Information Security Management System – ISMS) PN – ISO/IEC 27001:2014 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Przegląd i terminologia

[5] Menedżer Bezpieczeństwa Informacji – (MBI) Menedżer, menadżer, zarządca (ang. manager Pobrano 17 lutego 2017, z: https://pl.wikipedia.org/wiki/Mened%C5%BCer,

[6] Cyberterroryzm. Pobrano 17 lutego 2017, z: https://pl.wikipedia.org/wiki/Cyberterroryzm.

- Czy na poziomie kierownictwa instytucji lub firmy spełnione są warunki organizacyjne i techniczne przygotowania systemu zarządzania bezpieczeństwem informacji?
- Jaki poziom wiedzy reprezentują wykonawcy procedur zabezpieczenia informacji w organizacji?
- Jakie działania podjęto w zakresie opracowania Specyfikacji Istotnych Warunków Bezpieczeństwa Informacji (dalej jako: **SIWBI**[7])
- Czy należy ustawicznie kształcić specjalistów SZBI/MBI?
- Jaki model interoperacyjnych zadań powinien określać – Menedżera Bezpieczeństwa Informacji?
- Jak szeroki zakres wiedzy powinien posiadać MBI – wariant:
  - zarządzanie i organizacja,
  - elementy prawa w zarysie,
  - informatyka stosowana,
  - zarys pedagogiki i zarządzanie zasobami ludzkimi,
  - metody kontroli i oceny (audyt bezpieczeństwa informacji).
- Czy MBI powinien znać metodologię audytu bezpieczeństwa informacji?
- Jakie procesowe narzędzia analizy i oceny zagrożeń powinien stosować w ocenie Systemu Zarządzania Bezpieczeństwem Informacji menedżer bezpieczeństwa informacji (MBI)?

W odpowiedzi na zróżnicowane formy i treści zagrożeń określenie charakterystyki obszarów bezpieczeństwa informacji, ustawowych obowiązków, zadań i profilu MBI a także ewentualne (formalne i kwalifikowane) unormowanie standardów kształcenia, jest przedmiotem niniejszego opracowania.

System Zarządzania Bezpieczeństwem Informacji

Hipoteza robocza problemu zarządzania bezpieczeństwem informacji koncentruje się na określeniu siły oddziaływania osoby odpowiedzialnej za funkcjonalność i skuteczność systemu zarządzania bezpieczeństwem informacji (jako pożądanych efektów organizacyjno edukacyjnych). Powiązanie rozproszonych przepisów prawa o ochronie informacji połączone z umiejętnościami korzystania z technologii informatycznych, a także znormalizowane standardy zarządzania bezpieczeństwem informacji, są naturalnym warsztatem menedżera bezpieczeństwa informacji – MBI. Opracowania specjalistyczne na temat diagnostyki zagrożeń i skutków ich oddziaływania na SZBI w obecnym stanie wiedzy koncentrują się w większości na techniczno- mechanicznym zabezpieczeniu informacji. Pomijanie człowieka / użytkownika jest działaniem o wysokim stopniu w określonej skali ryzyka.

Z punktu widzenia podatności informacji na zagrożenie związane z integralnością dokonywanych zapisów, takie ujęcie problemu zabezpieczeń jest błędem. Stąd też pier-

[7] Specyfikacja Istotnych Warunków Bezpieczeństwa Informacji (SIWBI) – źródło Feliński J. konstrukcja własna.

wotnym działaniem administratorów powinno być spotkanie w ramach forum bezpieczeństwa informacji[8] (FBI) w celu określenia warunków koordynacji bezpieczeństwa informacji. Uczestnikami forum co do zasady powinny być osoby odpowiedzialne za przetwarzanie i zabezpieczanie informacji w określonych obszarach lub komórkach organizacyjnych. Standardową grupę uczestników forum stanowią – kierownictwo, administratorzy i projektanci aplikacji, audytorzy jakości oraz pracownicy działów związanych z takimi dziedzinami jak prawo, a także zarządzania zasobami ludzkimi. Efektem działań forum pod kierownictwem MBI, powinien być spis potrzeb organizacji i wstępna ocena stanu faktycznego (*audyt zerowy*) w podziale na aktywa, obszary nadzoru i zakresy realizacji zadań. Umiejętności i wiedza użytkowników o zasadach bezpieczeństwa uznawana jest mylnie za wiedzę przypisaną do zakresu obowiązków pracowniczych, naturalną, powszechną i w zasadzie intuicyjną (wszystkich szczebli organizacji).

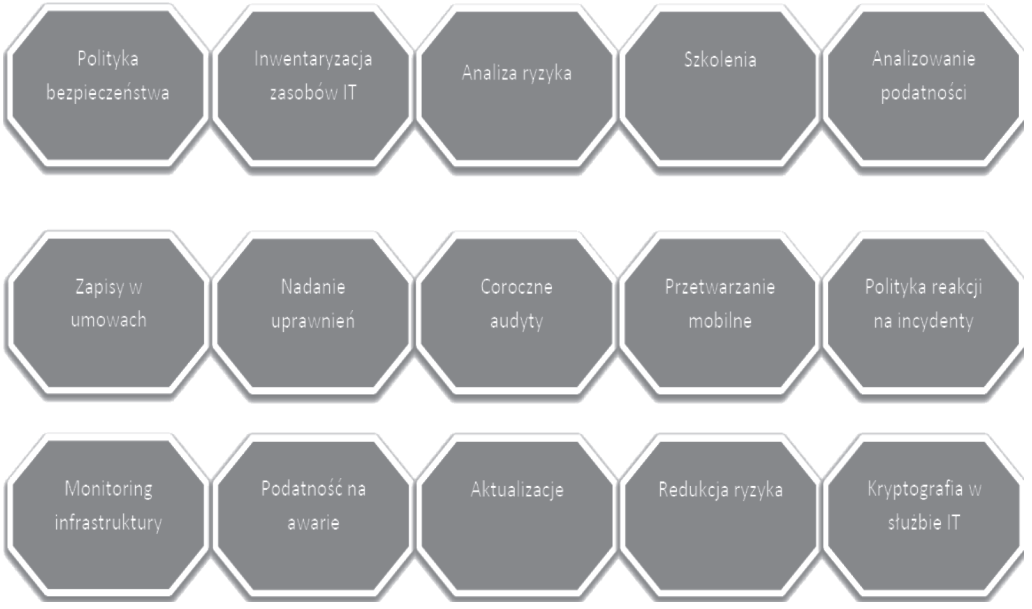
Z tego też względu nie należy bagatelizować, upraszczać lub unikać tematu edukacyjnych aspektów bezpieczeństwa informacji. W środowisku zmiennych zagrożeń szkolenia użytkowników i kształtowanie właściwych działań i nawyków, powinny stać się priorytetowym zadaniem MBI organizacji. Objaśnienie kontekstu bezpieczeństwa w szerokim zakresie przepisów krajowych, poprzez procedury wewnętrzne i czynności na stanowiskach pozwoli personelowi zrozumieć cel, sens i zadania polityki bezpieczeństwa informacji.

W zgodności z art. 51 ust. 5 Konstytucji Rzeczpospolitej (Dz.U. z 1997 nr 78 poz. 483) (dalej jako: Konstytucja) – *zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa (*Dz.U. z 1997 nr 78 poz. 483), ten stosunkowo ogólny zapis powoduje szczególną staranność działania i konieczność poznania wielu przepisów prawa ogólnego i resortowego. Cel działania, charakter działalności instytucji, a także rachunek ekonomiczny, umożliwia określenie wartości przetwarzanych informacji, określanych jako zasoby aktywów. Specyfikacja Istotnych Warunków Bezpieczeństwa Informacji (SIWBI), może wspierać procesy osiągnięcia odpowiedzi na pytania: co chronimy? Z kim chronimy? Jak chronimy (procesy)? Jakimi narzędziami chronimy? Przed czym chronimy? Jakie szkody ponosimy? Ile to kosztuje? Co dalej? Kto odpowiada?

Identyfikacja obszarów bezpieczeństwa, pozwala dokonać klasyfikacji organizacyjnych i technicznych potrzeb organizacji, określić szczegółowe zakresy zadań, opracować procedury wewnętrznej wymiany informacji, a także odpowiedzialność uczestników. Elementem integralnym systemu zarządzania bezpieczeństwem informacji jest procedura weryfikacji i aktualizacji przyjętych rozwiązań, w wymiarze kompleksowym lub zgodnie z podziałem obszarów zarządzania. Przykład podziału obszarów nadzoru ilustruje rysunek 1.

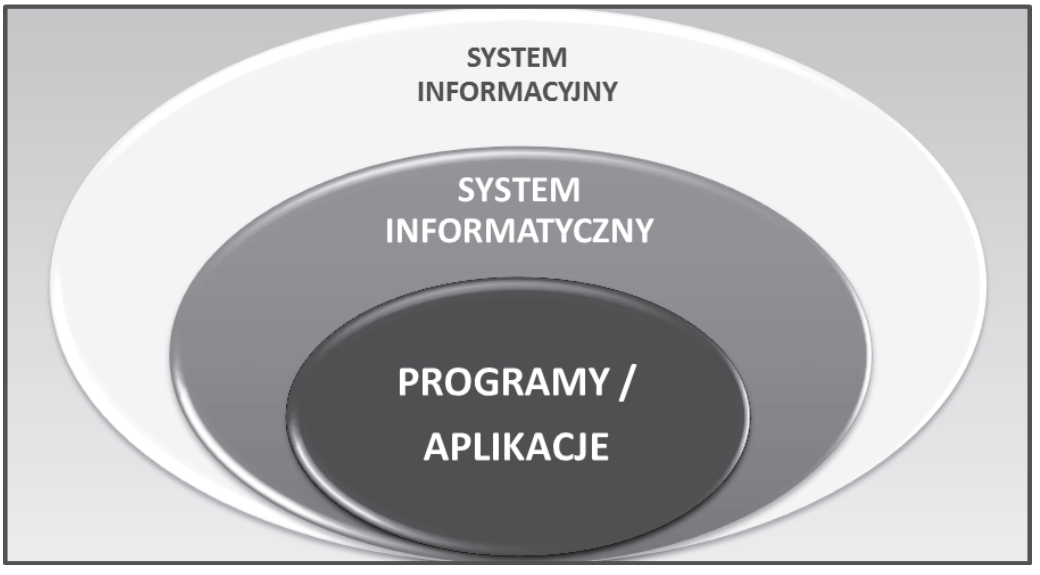
Każda organizacja jako określona struktura korelacji elementów systemu, dąży do osiągnięcia optymalnej funkcjonalności i efektów podjętych działań. Rolę systemu informacyjnego z punktu widzenia skuteczności zarządzania określił W. Kieżun (SGH, 1997), który formułuje tezę, że stopień sprawności komunikacji między częściami organizacji, między częściami a otoczeniem oraz całością organizacji a otoczeniem, jest w bezpośrednim związku przyczynowym ze sprawnością całej organizacji (Kieżun,

[8] Forum Bezpieczeństwa Informacji (FBI) – opracowanie własne.



Rysunek 1. SIWBI – podział obszarów

Źródło: opracowanie własne w oparciu o wybrane elementy tabeli A – PN ISO/IEC 27001.



Rysunek 2. System Informacyjny (SI) A System Informatyczny (SIT)

Źródło: opracowanie własne w oparciu o System informacyjny. Pobrano 17 lutego 2017, z: https://pl.wikipedia.org/wiki/System_informacyjny.

1997), co oznacza iż, istotnym elementem sprawnego działania systemu jest osoba nadzorcy, administratora zarządzającego. W związku z tak ujętym istotnym elementem zarządzania, specjalista MBI w zakresie działania organizacji powinien rozpoznawać dwie istotne składowe z punktu widzenia wartości informacyjnych: **System Informacyjny – *(SI)*** i **System Informatyczny – *(SIT) (***https://pl.wikipedia.org/wiki/System_informacyjny).

Szerokie określenie systemu informacyjnego w opracowaniu ujęto jako: zasoby ludzkie, cele i zadania, procedury wewnętrzne, urządzenia, nośniki i technologie organizacji, zewnętrzne usługi wsparcia informatycznego oraz procesy weryfikacji rozwiązań i działań użytkowników.

Prawne aspekty SZBI

Absolutnie bezpieczny system informatyczny z punktu widzenia techniki nie istnieje, co oznacza konieczność jasnego zdefiniowania ról, zadań i czynności wszystkich użytkowników wypełniających ustalone wewnętrznie procedury organizacji. Zadania zarządcy – specjalisty SZBI, określają nowe przepisy ustawy z dnia 17 lutego 2005r o informatyzacji podmiotów realizujących zadania publiczne (Dz.U. Nr 45, poz.565 z późn. zm.). Istotna zmiana podejścia do zarządzania systemami informatycznymi wprowadzona została w postaci Rozporządzenia Rady Ministrów dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności (Dz.U. 2016 poz. 113) (*dalej jako:* Rozporządzenie KRI). Zakres nowych przepisów i standardów jakościowego zarządzania bezpieczeństwem informacji ilustruje tabela porównawcza – tabela 1:

W świecie technologii informatycznej od wielu lat stosowane są normy, standardy, wytyczne i zalecenia. Szczególnie istotny okres zmian obejmujący wiele nowelizacji istniejących przepisów i wprowadzonych nowych rozwiązań prawnych, wymogów organizacyjnych i technicznych, a także standardy PN – ISO /IEC rodziny norm 27001[9] i norm związanych, przypada na lata 2012–2014. Obszerny zakres specjalistycznych zmian, wymaga odpowiednich kwalifikacji, wiedzy i merytorycznego przygotowania osób funkcyjnych do realizacji w praktyce ustanowionych zasad. Ustawodawca trafnie w przepisach, po nowelizacji prawa, wyróżnia kryteria bezpieczeństwa informacji jako:

- obowiązek zastosowania środków organizacyjnych (art. 36 ust. 1. Dz.U 2016 poz. 922),
- konieczność wprowadzania środków technicznych (art. 36 ust. 1. Dz.U 2016 poz. 922),
- ochronę zasobów odpowiednią do kategorii zagrożeń,
- ograniczenia dostępu do treści zasobów informacyjnych,
- Rozliczalność uczestników procesu przetwarzania i zabezpieczania informacji.

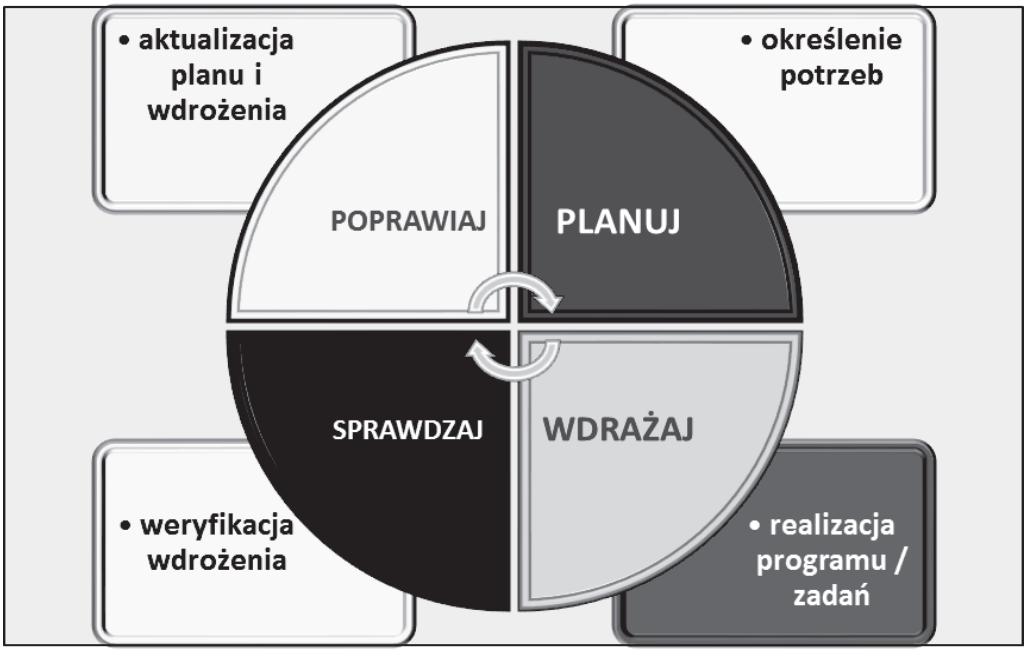
[9] PN ISO/IEC 27001 - norma międzynarodowa standaryzująca systemy zarządzania bezpieczeństwem informacji.

Tabela 1. Zmiany przepisów prawa w obszarach zarządzania bezpieczeństwem informacji

Zmiany przepisów prawa w latach: • 2005 • 2012 • 2015 • ~ 2018
Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. Nr 64, poz. 565, ze zm.)
ROZPORZĄDZENIE RADY MINISTRÓW z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.
PN ISO/IEC 27001:2014 Systemy zarządzania bezpieczeństwem informacji PN ISO/IEC 17799:2014 Praktyczne zasady zarządzania bezpieczeństwem informacji PN ISO/IEC 27005:2014 Zarządzanie ryzykiem w bezpieczeństwie informacji PN ISO/IEC 24762:2010 Wytyczne dla usług odtwarzania techniki teleinformatycznej po katastrofie
ROZPORZĄDZENIE 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) (Tekst mający znaczenie dla EOG) [procedowany od 2012] – ***obowiązuje w pełnym zakresie od 25 maja 2018r (dalej: RODO)***
Krajowe przepisy Ustaw o ochronie informacji niejawnych, danych osobowych, ochronie osób i mienia, wraz z aktami wykonawczymi.

Źródło: opracowanie własne.

Zdefiniowany katalog norm i standardów zarządzania, umiejętności weryfikacji zagrożeń, metod szacowania ryzyka, wykazania planu ciągłości działania instytucji w sytuacji katastrofy systemu informatycznego (Technika informatyczna Techniki bezpieczeństwa Wytyczne dla usług odtwarzania techniki teleinformatycznej po katastrofie PN – ISO/IEC 24762) nie obejmuje profilowanego kształcenia specjalistów. Zasoby instytucji traktowane jako aktywa podlegające zarządzaniu w zgodności z uniwersalnym procesem / „cyklem Deminga" (Technika informatyczna Techniki bezpieczeństwa Wytyczne dla usług odtwarzania techniki teleinformatycznej po katastrofie PN – ISO/IEC 24762) stanowią materiał poddawany cyklicznemu procesowi sprawdzania skuteczności działań. Planowanie, wdrażanie, sprawdzanie i działania korygujące są narzędziem w zakresie zarządzania organizacją, którym w sposób sprawny, powinien posługiwać się MBI jednostki organizacyjnej. Ilustracją takiego procesu jest rysunek 3.



Rysunek 3. Koło PDCA[10]

Źródło: Opracowanie własne w oparciu o cykl Deminga- https://pl.wikipedia.org/wiki/Cykl_Deminga

Sygnalizowanie potrzeb optymalizacji SZBI

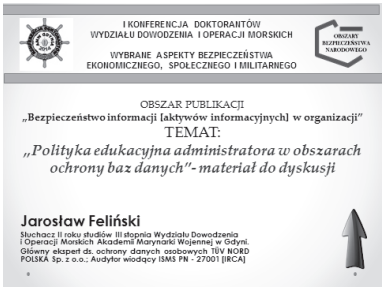
Autor opracowania w licznych wystąpieniach podkreślał od lat potrzebę edukacyjnych aspektów przygotowania profesjonalistów systemu zarządzania bezpieczeństwem informacji, akcentując wpływ zmian przepisów prawa i zjawisk zmieniających skalę i potencjał zagrożeń. Szczególnie intensywny okres nowelizacji przepisów o ochronie informacji nastąpił w latach 2012 – 2016. Z dniem 4 maja 2016 r. weszły w życie regulacje przejściowe, w których określono zadania zarządcze nowego podmiotu nadzoru w zgodności z art. 37 ust. 5[11] w postaci *inspektora ochrony danych* z delegacją wskazującą na konieczność posiadania wiedzy, umiejętności i praktyki zarządzania bezpieczeństwem informacji do czasu wejścia w życie w pełnym zakresie obowiązywania do dnia 25 maja 2018 r. Konieczność wypracowania w powszechnym wymiarze stosowania wy-

[10] Cykl Deminga (określany też jako cykl PDCA z ang. *Plan-Do-Check-Act* lub cykl P-D-S-A z ang. *Plan-Do-Study-Act* lub koło Deminga) – schemat ilustrujący podstawową zasadę ciągłego ulepszania (ciągłego doskonalenia, Kaizen), stworzoną przez Williama Edwardsa Deminga, źródło: https://pl.wikipedia.org/wiki/Cykl_Deminga.

[11] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. – (RODO) – Dziennik Urzędowy UE.

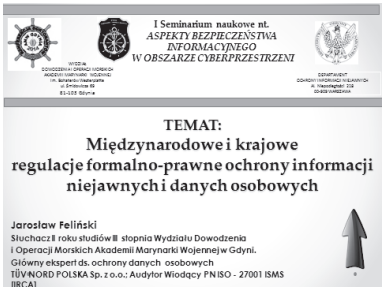
tycznych i programów kształcenia osób zaangażowanych w organizacje bezpieczeństwa informacji wyrażano w trakcie:

1. I Konferencji Doktorantów WDiOM AMW w Gdyni – 2014



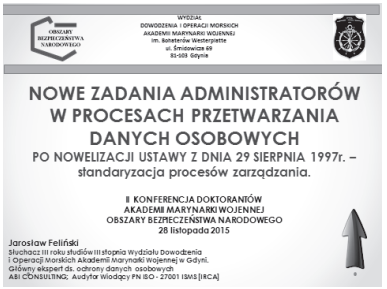
W trakcie wystąpienia przedstawione zostały istotne aspekty edukacji właścicieli, zarządców, a także uczestników procesów przetwarzania informacji, z uwzględnieniem wrażliwości baz danych, w kontekście zagrożeń systemu zarządzania bezpieczeństwem informacji. Treść wystąpienia koncentrowała się na ustawowej terminologii i słownictwie zawartym w przepisach prawa i normach jakościowego zarządzania bezpieczeństwem informacji. Wykazano korelację pomiędzy stanem wiedzy użytkowników a jakością wprowadzonych w organizacji zabezpieczeń na przykładzie zdarzenia utraty dokumentów (nośników). Konkluzja podsumowująca wystąpienie jednoznacznie akcentowała konieczność metodycznego rozpoznania poziomu wiedzy użytkowników w obszarach zastosowanych zabezpieczeń w praktyce administratora baz danych.

2. I Seminarium naukowego nt. *Aspekty bezpieczeństwa informacyjnego w obszarze cyberprzestrzeni* – AMW w Gdyni – 2015



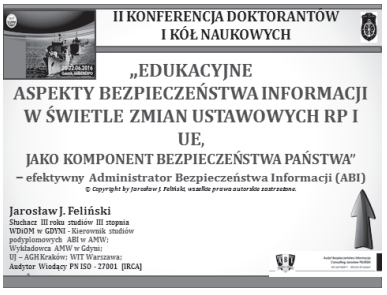
Treścią wystąpienia były zakresy zmian przepisów prawa krajowego i implementacja zmian przepisów Unii Europejskiej w latach 2012 – 2018. Zasadnicza część wystąpienia koncentrowała się na zmianach w podejściu do możliwości wykonywaniu czynności zarządzania przez osoby posiadające WIEDZĘ o Systemie Zarządzania BI.

3. II Konferencji Doktorantów WDiOM AMW w Gdyni – 2015



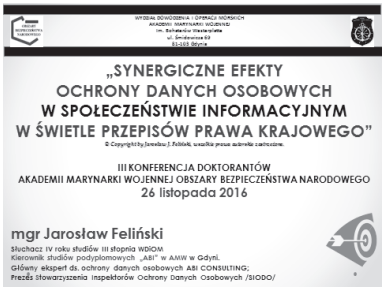
Przedmiotem analizy porównawczej i oceny nowych zadań administratorów baz danych były znowelizowane przepisy prawa ochrony danych osobowych, w świetle których ustawodawca jednoznacznie określił konieczność posiadania WIEDZY, przez osoby zajmujące stanowiska zarządzania bezpieczeństwem informacji. Wskazane zostały nowe rozwiązania, zadania i czynności określone w aktach wykonawczych obowiązujących od 1 stycznia 2015 r. i stan prawny po okresie dostosowania przepisów po 30 czerwca 2015 r. w nowym standardzie zarządzania bezpieczeństwem informacji. Oceniono wstępnie proces standaryzacji zarządzania bezpieczeństwem informacji w oparciu o wprowadzone nowelizacje.

4. II Konferencji Doktorantów i Kół Naukowych – NAT CON Gdańsk, Gdynia – 2016



W treści wystąpienia główny akcent położony został na związek podstawowych zadań administratora każdej organizacji w tworzenie systemu bezpieczeństwa informacji w wymiarze lokalnym i krajowego systemu bezpieczeństwa informacji, po kolejnych zmianach przepisów prawa ochrony informacji. Edukacyjne aspekty bezpieczeństwa informacji jako komponent bezpieczeństwa państwa, określono w oparciu o studium przypadku administratora bezpieczeństwa informacji po rocznych doświadczeniach realizacji ustawy o ochronie danych osobowych.

5. III Konferencji Doktorantów WDiOM AMW w Gdyni – 2016



Szeroki temat społeczeństwa informacyjnego został zaprezentowany w aspekcie zagrożeń prywatności i ich skutków w aktywnościach związanych z siecią publiczną (internet) oraz konieczności kształcenia specjalistów zarządzania bezpieczeństwem informacji w kwalifikowanych formach edukacyjnych. Efekty wartości dodanej jaką mogą stanowić studia specjalistyczne specjalistów SZBI / MBI wykazano w porównaniu z powszechnymi ofertami szkolenia (jednodniowe zajęcia) podmiotów działalności komercyjnej, nie posiadających uprawnień kwalifikowanych form szkolenia.

Menedżer Bezpieczeństwa Informacji – wymagania

Interdyscylinarność menedżerów bezpieczeństwa informacji (MBI), w zakresie posiadanych kompetencji i wiedzy, umożliwia skuteczną realizację przedmiotowych zadań. Wdrożenie skoordynowanych działań, jako zbioru elementów organizacyjnych, sił i środków w optymalizacji procesów kształcenia specjalistów Systemu Zarządzania Bezpieczeństwem Informacji jest potrzebnym przeciwdziałaniem (dającym się przewidzieć) potencjalnym zagrożeniom.

Wariant zróżnicowania profesjonalizacji wybranych funkcji zarządzania zilustrowano w tabeli 2 w podziale na zakres przygotowania merytorycznego:Ochrona Informacji Niejawnych, Bezpieczeństwo i Higiena Pracy, Ochrona Danych Osobowych.

Osiągnięcie zamierzonego celu naukowo dydaktycznego, będzie możliwe poprzez profilowane i zbilansowane kształcenie, określone w ramach projektu badawczego podyplomowych studiów specjalistycznych skierowanego do kandydatów na specjalistów SZBI. Zgodnie z art. 2 pkt 2 (Dz.U. 2016 poz. 64) ustawy z dnia 22 grudnia 2015 r. o Zintegrowanym Systemie Kwalifikacji edukacja formalna oznacza kształcenie realizowane przez publiczne i niepubliczne szkoły oraz inne podmioty systemu oświaty, uczelnie oraz inne podmioty systemu szkolnictwa wyższego w ramach programów, które prowadzą do uzyskania kwalifikacji pełnych, kwalifikacji nadawanych po ukończeniu studiów podyplomowych, o których mowa w art. 2 ust. 1 pkt 11 ustawy z dnia 27 lipca 2005 r. – Prawo o szkolnictwie wyższym (Dz.U. z 2012 r. poz. 572, z późn. zm.) albo kwalifikacji w zawodzie, o której mowa w art. 10 ust. 3 pkt 1 ustawy z dnia 7 września 1991 r. o systemie oświaty (Dz.U. z 2015 r. poz. 2156 oraz z 2016 r. poz. 35). W oparciu

o art. 2 pkt 10 (Dz.U. z 2015 r. poz. 2156 oraz z 2016 r. poz. 35) Dz.U. z 2012 r. poz. 572, z późn. zm.) kwalifikacje pełne uznaje się za jednoznacznie spełnione, które nadawane są wyłącznie w ramach systemu oświaty po ukończeniu określonych etapów kształcenia oraz kwalifikacje pierwszego, drugiego i trzeciego stopnia w rozumieniu ustawy z dnia 27 lipca 2005 r. – Prawo o szkolnictwie wyższym, w zakresie wiedzy, umiejętności i kompetencji społecznych.

Tabela 2. Zakres zmian zarządzania bezpieczeństwem informacji na przykładzie

Źródło: opracowanie własne.

W związku z powyższym, otwarte zostały możliwości do przygotowania modelu kształcenia specjalistów SZBI / MBI obejmującego treści zgodne z efektami kształcenia jak:

- znajomość metod i narzędzi, w tym technik pozyskiwania danych, właściwych dla dziedzin nauki i dyscyplin naukowych, właściwych dla zaliczanego kierunku studiów, pozwalające opisywać struktury i instytucje społeczne oraz procesy w nich i między nimi zachodzące;
- rozszerzona wiedza o charakterze nauk społecznych, ich miejscu w systemie nauk i relacjach do innych nauk;
- umiejętność prognozowania i modelowania złożonych procesów społecznych obejmujących zjawiska z różnych obszarów życia społecznego z wykorzystaniem zaawansowanych metod i narzędzi w zakresie dziedzin nauki i dyscyplin naukowych, w wymiarze interdyscyplinarnym;
- posiadanie umiejętności językowych w zakresie dziedzin nauki i dyscyplin naukowych, właściwych dla kierunku studiów;
- kompetentne, samodzielne i krytyczne uzupełnianie wiedzy i umiejętności, rozszerzone o kompleksowy wymiar interdyscyplinarny.

Menedżer Bezpieczeństwa Informacji – nowa edukacja – wariant

Jakościowe ujęcie potrzeb zabezpieczenia informacji, musi iść w parze z jakościowym sposobem kształcenia specjalistów i tym samym potwierdza zasadność podjęcia działań edukacyjnych i wprowadzenia do procesu kształcenia uczelni wyższych podyplomowych studiów specjalistycznych SZBI. Procesowe przygotowanie kandydatów do pełnienia odpowiedzialnych funkcji i stanowisk, w oparciu o zdefiniowane kryteriami - profilowanego, już realizowanego -eksperymentu – w przekazywaniu wiedzy i kształtowaniu umiejętności, umożliwi:

- prawidłowe wypełnianie przepisów obowiązującego prawa,
- sprawne kierowanie użytkownikami w organizacji,
- efektywne opracowanie pism i dokumentacji PBI,
- zarządzanie funkcyjnymi administratorami systemów informatycznych,
- wykonanie czynności audytowych oraz analizy i oceny ryzyka,
- wypracowanie koncepcji działań korygujących i naprawczych,
- przygotowanie i przeprowadzenie zajęć zgodnie z wdrożonymi procedurami SZBI,
- dalsze samodzielne lub kierowane doskonalenie umiejętności zarządzania SZBI,
- ponoszenie odpowiedzialności w obszarze zarządzania.

Wariant profilu kształcenia i dyscyplin naukowych MBI ilustruje rysunek 4

Rysunek 4. Model kształcenia specjalistów SZBI / MBI – wariant

Źródło: opracowanie własne

Program stanowiący eksperyment naukowo dydaktyczny, obejmuje przedmioty kilku dyscyplin naukowych i ich związek (*korelacje*) z systemem zarządzania bezpieczeństwem informacji (SZBI). Analiza możliwości wdrożenia programu studiów w oparciu o kryteria kwalifikowanego kształcenia z uwzględnieniem wytycznych określonych w załączniku 2 Krajowych Ram Kwalifikacji[12], stała się wypadkową realizacji potrzeb. Program studiów przedstawia tabela 3.

[12] Rozporządzenie Ministra Nauki i Szkolnictwa Wyższego z dnia 2 listopada 2011 r. w sprawie Krajowych Ram Kwalifikacji dla Szkolnictwa Wyższego. Dz.U. 2011. nr 253 poz. 1520.

Tabela 3. Nazwa studiów podyplomowych „Administrator Bezpieczeństwa Informacji (ABI) – ABI / IODo – podyplomowe studia zarządzania bezpieczeństwem informacji"

Lp.	Semestr I – Nazwa przedmiotu	Liczba godzin	ECTS
1	2	3	4
1	Krajowe i międzynarodowe regulacje prawne ochrony danych	8/8	2
2	Bezpieczeństwo informacji w świetle normy PN-IS/IEC 27001:2014 cz. I	16/24	4
3	Ochrona państwa i porządku konstytucyjnego	8/32	2
4	Funkcjonalne systemy bezpieczeństwa informacji – warianty, schematy organizacyjne	16/48	4
5	Dobór osób funkcyjnych (ABI/ASI/Manager Bezpieczeństwa Informacji)	8/56	4
6	Zasady oceny efektywności PBI (preaudyt)	16/72	2

Tabela 3. (cd.)

1	2	3	4
7	System zarządzania bezpieczeństwem informacji – nowa jakość ochrony informacji PN -27001 cz.II.	16/88	4
8	Psychologia ludzi w organizacji w zarządzaniu informacją, psychologia tłumu (działania w sytuacjach ekstremalnych)	6/94	2
9	Ochrona osób, instytucji i urządzeń –użytkownicy, systemy i nośniki	16/110	3
10	Ocena zagrożeń, proces decyzyjny i problemy ryzyka	16/126	3
		126	**30**
Lp.	**Semestr II – Nazwa przedmiotu**	**Liczba godzin**	**ECTS**
1	GIODO – krajowy strażnik ochrony danych osobowych: uprawnienia	12/12	3
2	Rola i znaczenie służb specjalnych RP w systemie bezpieczeństwa państwa i ochrony informacji	8/20	3
3	Systemy informatyczne i programy ochrony. Zarządzanie ochroną systemów informatycznych w organizacji	16/36	4
4	Polityka informacyjna administratora	8/44	2
5	Identyfikacja zagrożeń, ocena i zarządzaniem ryzykiem	8/52	3
6	System zarządzania bezpieczeństwem informacji – nowa jakość ochrony informacji PN–27001:2007 cz. II	8/60	3
7	Zarządzanie jakością i bezpieczeństwem informacji	8/68	3
8	Systemy technicznej ochrony informacji – nowe rozwiązania, trendy, *cloud computing*	8/76	3
9	Inżynieria systemów ochrony i bezpieczeństwa informacji	8/84	3
10	Klasyfikacja informacji niejawnych. Organizacja systemu ochrony informacji i urządzeń niejawnych w zarysie	8/92	3
		92	**30**

Źródło: opracowanie własne

Konstrukcja programu studiów stanowiąca połączenie wielu dziedzin nauki, jako modelu kształcenia specjalistów SZBI, zmierza do uzyskania nowej pożądanej wartości naukowej rozwiązywania problemów zarządzania systemami bezpieczeństwa informacji. Jakie korzyści społeczne i jakie efekty skutecznego realizowania polityki bezpieczeń-

stwa państwa można osiągnąć inwestując w proces optymalizacji kształcenia licznych Specjalistów Systemu Zarządzania Bezpieczeństwem Informacji w wymiarze programu studiów podyplomowych, to wiąż otwarte zapytanie.

Zagrożenia bezpieczeństwa informacji

Prezentowane w mediach tradycyjnych i elektronicznych liczne przypadki naruszenia zabezpieczeń informacji, odczytywane są jako cudzy problem z założeniem, iż naszej instytucji ten zakres nie dotyczy. Teza tak wyrażona jest niebezpieczna i nieodpowiedzialna. Ofiarami narażonymi na przełamanie stosowanych zabezpieczeń są w praktyce wszystkie podmioty działalności gospodarczej oraz instytucje publiczne. Skutkami tych działań bywają straty materialne i wizerunkowe, utrata dobrego imienia i w efekcie możliwość wyrządzenia szkody indywidualnej lub spowodowanie straty w wielkiej skali publicznej, a w dalszej konsekwencji zagrożenie stanu bezpieczeństwa państwa. Istotnym mankamentem przekazów medialnych jest „sensacyjność" i niekompletność oraz brak informacji o przyczynach wystąpienia niepożądanego zjawiska[13].

Mark Zuckerberg publikując na Facebooku zdjęcie z zaklejonym obiektywem kamery używanego notebooka, sprawił iż nastąpiło poruszenie wśród użytkowników sieci, co do motywów takiego postępowania. Czyżby producenci urządzeń i dostawcy usług sieciowych, posiadali możliwość korzystania z możliwości monitorowania użytkowników? Wielu użytkowników w ślad za M. Z. zastosowało podobny wariant w swoich urządzeniach. – W komentarzu M. Zuckerberg odniósł się jedynie do przezornego postępowania na wypadek ataku hakerów.

Na potrzeby artykułu dokonano analizy wybranej literatury i piśmiennictwa związanych z zagadnieniami bezpieczeństwa i klasyfikacją zagrożeń. Można je określić w kilku kategoriach, uwzględniając lokalizację ich źródła na:

- wewnętrzne (powstające wewnątrz organizacji), które obejmują: → zagrożenie utratą, uszkodzeniem danych lub brakiem możliwości obsługi z powodu błędu lub przypadku, →→ zagrożenie utratą lub uszkodzeniem poprzez celowe działania 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 (http://www.zabezpieczenia.com.pl/ochrona-informacji/zagro%C5%BCenia-bezpiecze%C5%84stwa-informacji-w-przedsi%C4%99biorstwie-cz-1).

Mając świadomość wielowątkowości zagrożeń bezpieczeństwa informacji, naj-

[13] To także wynik niskiego poziomu wiedzy autorów tekstów, skupionych na efekcie szoku, dystrybucji możliwie największej liczby egzemplarzy pisma lub odsłon internetowych, publikowanych treściach.

istotniejszy w działaniu ograniczającym podatność na utratę danych, dokumentów, nośników będzie świadomy użytkownik – człowiek. Przed specjalistami SZBI trudne zadanie – opracowanie i wdrożenie procedur mających na celu ochronę zdefiniowanych obszarów, selektywny zakres uprawnień użytkowników, nadzór i weryfikacja oraz systematyczne prowadzenie szkoleń.

Wnioski

W świecie określonym *SMS*'em, mailem lub „*ikonką*" bądź „*emotikonem*", niniejsza publikacja powinna przyjąć formę „krótkiej prezentacji – snapchat...". Nadal dla wielu użytkowników sieci publicznej zakres wiedzy i umiejętności korzystania z nowoczesnych technologii społeczeństwa informacyjnego jest częściowo intuicyjny bez głębszego poznania zasad funkcjonowania urządzeń, sieci i potencjalnych zagrożeń. Zachęty dostawców usług ograniczają się wyłącznie do zapewniania sprawności urządzeń i możliwości komunikacji. Problem wynikający z takiej powierzchowności traktowania osobistych urządzeń i aplikacji, wielu użytkowników przenosi na wykonawstwo zadań w działaniach administratorów informacji. Brak staranności w przestrzeganiu ustalonych i wdrożonych procedur, wymaga systematycznego korygowania i reakcji specjalisty Systemu Zarządzania Bezpieczeństwem Informacji. Szkolenia, instruktaże, symulacje z omówieniem skutków będą jednym z procesów zmniejszania, eliminowania poziomu ryzyka utraty informacji.

Bibliografia

Audyt – pobrane z: https://pl.wikipedia.org/wiki/Audyt
Cyberprzestrzeń – pobrane z: http://sjp.pwn.pl/sjp/cyberprzestrze%C5%84;2553915
Cyberterroryzm – pobrane z: https://pl.wikipedia.org/wiki/Cyberterroryzm.
Cykl Deminga – pobrane z: https://pl.wikipedia.org/wiki/Cykl_Deminga.
Feliński J. źródło – opracowanie własne
Forum Bezpieczeństwa Informacji (FBI) – źródło Feliński J. – opracowanie własne.
Michalak J. (red.), Feliński J. (2014) Oblicza bezpieczeństwa narodowego. *Polityka informacyjna administratora w obszarach ochrony baz danych* (s. 81); Gdynia.
Interdyscyplinarność – pobrane z: https://pl.wikipedia.org/wiki/Interdyscyplinarno%C5%9B%C4%87
Kieżun W. (1997) Sprawne zarządzanie organizacją, SGH, Warszawa.
Konstytucja Rzeczypospolitej z dnia 2 kwietnia 1997 r. – (Dz.U. z 1997 nr 78 poz. 483).
Optymalizacja – pobrane z: http://sjp.pwn.pl/sjp/optymalizacja;2569873.html
Menedżer – pobrane z: https://pl.wikipedia.org/wiki/Mened%C5%BCer
PN - ISO/IEC 27001:2014 Technika Informatyczna Techniki Bezpieczeństwa Systemy zarządzania bezpieczeństwem informacji Wymagania.
PN – ISO/IEC 24762 - Technika informatyczna Techniki bezpieczeństwa Wytyczne dla usług odtwarzania techniki teleinformatycznej po katastrofie.
Rozporządzenie Ministra Nauki i Szkolnictwa Wyższego z dnia 8 sierpnia 2011r. w sprawie obszarów wiedzy, nauki i sztuki oraz dyscyplin naukowych i artystycznych (Dz.U. 2011 nr 179 poz. 1065).

Rozporządzenie Ministra Nauki i Szkolnictwa Wyższego z dnia 2 listopada 2011 r. w sprawie Krajowych Ram Kwalifikacji dla Szkolnictwa Wyższego – (Dz.U. 2011. nr 253 poz. 1520).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. – (RODO).

Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2016 poz. 113).

System informacyjny. Pobrane 17 lutego 2017, z: https://pl.wikipedia.org/wiki/System_informacyjny,

System Zarządzania Bezpieczeństwem Informacji - PN - ISO/IEC 27001:2014 Technika Informatyczna Techniki Bezpieczeństwa Systemy zarządzania bezpieczeństwem informacji Wymagania.

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

Ustawa z dnia 17 lutego 2005 r. o informatyzacji podmiotów realizujących zadania publiczne (Dz.U. Nr 45, poz.565 z późn. zm.).

Ustawa z dnia 7 września 1991 r. o systemie oświaty (Dz.U. z 2015 r. poz. 2156 oraz z 2016 r. poz. 35).

Ustawa z dnia 27 lipca 2005 r. Prawo o szkolnictwie wyższym (Dz.U. z 2012 r. poz. 572, z późn. zm.).

Ustawa z dnia 22 grudnia 2015 r. o Zintegrowanym Systemie Kwalifikacji (Dz.U. 2016 poz. 64).

ps (23.06.2016), *Mark Zuckerberg zasłonił kamerę i mikrofon w swoim laptopie. „Wie co robi, to przejaw przezorności" Czytaj więcej na: http://www.wirtualnemedia.pl/artykul/mark-zuckerberg-zaslonil-kamere-i-mikrofon-w-swoim-laptopie-wie-co-robi-to-przejaw-przezornosci*. Pobrane 17 lutego 2017, z: http://www.wirtualnemedia.pl/artykul/mark-zuckerberg-zaslonil-kamere-i-mikrofon-w-swoim-laptopie-wie-co-robi-to-przejaw-przezornosci

Jabłoński M., Mielus M., *Zagrożenia bezpieczeństwa informacji w przedsiębiorstwie (cz. 1)*. Pobrane 17 lutego 2017, z: http://www.zabezpieczenia.com.pl/ochrona-informacji/zagro%C5%BCenia-bezpiecze%C5%84stwa-informacji-w-przedsi%C4%99biorstwie-cz-1