Krzysztof Bobkowski*

Zarządzanie bezpieczeństwem informacji w ujęciu wybranych aktów normatywnych w zakresie Systemu Zarządzania Bezpieczeństwem Informacji

Wstęp

Funkcjonowanie państwa oraz gospodarki w sferze informacyjnej wymaga odpowiedniego podejścia do zarządzania informacją, a także jej bezpieczeństwem. Rozwój technologii informatycznych jest jednym z istotnych czynników dynamizujących proces rozwoju globalnego społeczeństwa informacyjnego, wpływając jednocześnie na sposób postrzegania informacji, które zyskują coraz większą wartość w ujęciu strategicznym i ekonomicznym [Oleksiewicz, 2017, s. 99].

Wobec istotnego wzrostu znaczenia informacji w organizacjach, która odgrywa kluczową rolę w coraz bardziej złożonych procesach gospodarczych, wymagane jest zastosowanie odpowiedniego podejścia do zarządzania aktywami, jakimi są informacje [Dziekański, 2012, s. 391]. Świadczy o tym chociażby fakt wyodrębnienia zarządzania informacją jako oddzielnej dziedziny nauk o zarządzaniu [Cisek, 2002, s. 45–56].

Straty, jakie mogą wiązać się z naruszeniem bezpieczeństwa informacji, jak na przykład naruszenie ciągłości działania organizacji, utrata zaufania społecznego w zakresie powierzanych danych, poniesienie kosztów z tytułu usunięcia szkód powstałych w wyniku incydentu bezpieczeństwa, wpływ na przyszłą działalność organizacji i tym podobne, mogą być znaczące.

Zapewnienie odpowiedniego poziomu bezpieczeństwa dla informacji w organizacji jest niemałym wyzwaniem, a ocena ryzyka naruszenia bezpieczeństwa informacji i wpływu na relacje pomiędzy partnerami biznesowymi wymusza stworzenie odpowiedniego ekosystemu biznesowego [Stańczyk-Hugiet, Stańczyk, 2013].

* Mgr, Wydział Zarządzania, Uniwersytet Gdański, ul. Armii Krajowej 101, 81-824 Sopot, krzysztof.bobkowski@ug.edu.pl

Zarządzanie bezpieczeństwem informacji jest procesem bardzo złożonym, gdyż w zależności od profilu działalności organizacji informacje będą zróżnicowane pod względem istotności, wartości i przydatności. Wpisanie konieczności zapewnienia bezpieczeństwa informacyjnego do strategii organizacji odgrywa istotną rolę dla pomyślnej realizacji jego celów.

Zapewnienie bezpieczeństwa informacji staje się warunkiem koniecznym, wpisującym się w zakresy obowiązków kadry zarządzającej. Wyzwania stojące przed najwyższym kierownictwem związane z wdrożeniem odpowiedniego modelu bezpieczeństwa informacji w celu utrzymania ładu organizacyjnego stają się niejednokrotnie zadaniem przerastającym organizację. W związku z powyższym konieczne jest wdrożenie sprawdzonych standardów zarówno w aspekcie technicznym, jak i organizacyjnym.

Niejednokrotnie w aktach prawnych pojawiają się odwołania do Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) opartym o normy z serii ISO / IEC 27000, które stanowią obecnie najbardziej rozpowszechniony, znormalizowany model w dziedzinie ochrony informacji [rozporządzenie 2012, s. 8].

Mając na uwadze kwestie wizerunkowe, konieczność zapewnienia ciągłości działania organizacji oraz prawne wymagania, odpowiedni model zarządzania bezpieczeństwem staje się jednym z głównych celów strategicznych, dlatego powinien stanowić nieodłączny element całościowego podejścia do zarządzania.

Celem artykułu jest przedstawienie i przeanalizowanie dostępnych aktów normatywnych w kontekście Systemu Zarządzania Bezpieczeństwem Informacji w zakresie umożliwiającym jego implementację w organizacji. W wyniku kwerendy aktów normatywnych wykazane zostaną korelacje pomiędzy nimi.

1. Zarządzanie bezpieczeństwem informacji

Mechanizmy zapewniające bezpieczeństwo informacji powinny stanowić integralną część systemu zarządzania informacją w organizacji. Wymaga to kompleksowego podejścia do zagadnienia, w związku z czym nie można przeprowadzić wdrożenia cząstkowo, wyłącznie w pewnych aspektach, a także w węższym zakresie, np. obejmującym wyłącznie kluczowe działy w organizacjach (np. księgowość, płace, dział kadr czy IT). Wydzielenie wąskiego obszaru (zakresu) implementacji normy, tak jak ma to miejsce w przypadku Systemu Zarządzania Usługami, opartego o normę ISO / IEC 20000, nie znajduje tutaj zastosowania z uwagi na konieczność całościowego podejścia do zarządzania bezpieczeństwem informacji.

Ochrona informacji stanowiących podstawę funkcjonowania, a zarazem zapewniających przewagę rynkową na tle konkurencji, wymaga

zastosowania całościowego podejścia do zagadnienia [ISO / IEC 27000, 2018, s. 26]. W innym przypadku zapewnienie odpowiedniego poziomu bezpieczeństwa informacyjnego w organizacji nie będzie możliwe, chociażby z uwagi na brak możliwości oceny wartości i istotności posiadanych i przetwarzanych aktywów informacyjnych, w obszarach znajdujących się poza zakresem stosowania polityki bezpieczeństwa informacji stanowiącej podstawę SZBI.

Na bezpieczeństwo informacyjne w organizacji składa się wiele czynników. Począwszy od aspektów związanych z ochroną fizyczną, bezpieczeństwem osobowym, a skończywszy na bezpieczeństwie infrastruktury i usług informatycznych. Możliwość doboru właściwych środków organizacyjnych i technicznych jest zapewniona poprzez analizę ryzyka dla poszczególnych zinwentaryzowanych aktywów informacyjnych [Szlachcic, 2014, s. 231]. Właściwie dobrane środki mają na celu zapewnienie, że ryzyko wystąpienia incydentu jest jak najniższe.

Wybór metodyki zarządzania bezpieczeństwem informacji nie jest trywialnym zadaniem. Literatura obfituje w opisy wielu modeli bezpieczeństwa informacji. Jednakże tylko znormalizowany model bezpieczeństwa informacji odzwierciedla kompletne ujęcie problematyki w zakresie bezpieczeństwa informacyjnego. Podjęcie decyzji o wdrożeniu SZBI, który spełni swoje zadanie, a także będzie wspomagał procesy realizowane w ramach istniejącego już systemu zarządzania informacją w organizacji, wiąże się z poważnymi konsekwencjami.

W tym miejscu najczęściej pojawia się pytanie, czy System Zarządzania Bezpieczeństwem Informacji musi być oparty o akty normatywne, czy może być budowany w oparciu o dostępne standardy, które nie wymagają certyfikacji? Otóż wdrożenie SZBI zgodnego z normą ISO / IEC nie musi wiązać się z deklaracją certyfikacji, niemniej jednak niekiedy certyfikat jest wartością dodaną dla organizacji (np. ułatwiającą współpracę z innymi podmiotami). Liczba wydanych certyfikatów zgodności z normą ISO / IEC 27001 co roku powiększa się. Tylko na koniec roku 2017 było wydanych 39501 certyfikatów. Stanowi to wzrost o 19% w stosunku do roku poprzedzającego [The ISO Survey, 2017].

Organizacje, które decydują się na wdrożenie SZBI opartego o akty normatywne, posiadają pewność korzystania z normy opracowanej na zasadzie konsensusu przez upoważnione jednostki organizacyjne [Krawiec, Ożarek, 2014, s. 8].

Korzyścią tworzenia SZBI opartego o zapisy ISO / IEC 27001 jest fakt, iż norma ta przejęła zapisy zamieszczone we wcześniej publikowanych i rozwijanych przez lata normach. Zagadnienie bezpieczeństwa informacji

nie jest nowe, jednak próby standaryzacji metod zarządzania nim trwają od początku lat 90. XX wieku [Łuczak, Tyburski, 2010, s. 5].

Historia norm z rodziny ISO / IEC 27000 sięga roku 1993, w którym to opublikowany został dokument BS PD0003 – A code of practice for information security management, który dał podstawy do utworzenia normy BS 7799, opracowanej dwa lata później. Na przełomie lat normy te były rozwijane zarówno przez Brytyjski Instytut Normalizacyjny, jak i Międzynarodową Organizację Normalizacyjną (ISO) przy współpracy z Międzynarodową Komisją Elektrotechniczną (IEC) aż do momentu powstania w 2005 r. pierwszej normy ISO / IEC 27001, która zapoczątkowała serię standardów ISO / IEC 27000 [Łuczak, Tyburski, 2010, s. 55–56].

Do dnia dzisiejszego akty normatywne z rodziny ISO / IEC 27000 są rozwijane, a seria zyskuje aktualizacje obecnych zapisów, a także kolejne normy. Poszczególne normy doczekały się również publikacji polskojęzycznych wydanych przez Polski Komitet Normalizacyjny, co w znacznym stopniu ułatwia korzystanie z jej zapisów w rodzimym języku.

Argumentem przemawiającym za wdrożeniem SZBI dla organizacji z sektora publicznego są również przepisy prawa polskiego wskazujące bezpośrednio na zastosowanie norm ISO / IEC w celu spełnienia zapisów ustawy [rozporządzenie, 2012]. Ustawodawca w sposób bezpośredni odwołuje się do norm:

- PN-ISO / IEC 27001 – w odniesieniu do ustanowienia Systemu Zarządzania Bezpieczeństwem Informacji,
- PN-ISO / IEC 17799 – w odniesieniu do ustanawiania zabezpieczeń,
- PN-ISO / IEC 27005 – w odniesieniu do zarządzania ryzykiem,
- PN-ISO / IEC 24762 – w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania [rozporządzenie, 2012].

System Zarządzania Bezpieczeństwa Informacji oparty o normę ISO / IEC 27001 jest dojrzałym i dopracowanym dokumentem, a zasadność zastosowania tego modelu w organizacji, w szczególności sektora publicznego, nie powinna budzić wątpliwości.

2. Wybrane akty normatywne w zakresie zarządzania bezpieczeństwem informacji

Wdrażając System Zarządzania Bezpieczeństwem Informacji, organizacje nie zdają sobie zazwyczaj sprawy z mnogości aktów normatywnych w tej dziedzinie. W związku z istnieniem szerokiego wachlarza aktów normatywnych w zakresie bezpieczeństwa informacji można dokonać ich podziału w następujący sposób:

1) Normy słownikowe:
   – ISO / IEC 27000:2018 – System Zarządzania Bezpieczeństwem Informacji – Przegląd i terminologia [ISO / IEC 27000, 2018, s. 19].
2) Normy zawierające wymagania:
   – ISO / IEC 27001:2013 – System Zarządzania Bezpieczeństwem Informacji – Wymagania,
   – ISO / IEC 27006:2015 – Wymagania dla jednostek prowadzących audyt i certyfikację Systemów Zarządzania Bezpieczeństwem Informacji,
   – ISO / IEC 27009:2016 – Zastosowania sektorowe ISO / IEC 27001 – Wymagania [ISO / IEC 27000, 2018, s. 19–20].
3) Normy zawierające wytyczne:
   – ISO / IEC 27002:2013 – Praktyczne zasady zabezpieczenia informacji,
   – ISO / IEC 27003:2017 – Systemy zarządzania bezpieczeństwem informacji – Wytyczne,
   – ISO / IEC 27004:2016 – Zarządzanie bezpieczeństwem informacji – Monitorowanie, pomiar, analiza i ocena,
   – ISO / IEC 27005:2018 – Zarządzanie ryzykiem w zakresie bezpieczeństwa informacji,
   – ISO / IEC 27007:2017 – Wytyczne dotyczące audytu Systemów Zarządzania Bezpieczeństwem Informacji,
   – ISO / IEC TR 27008:2011 – Wytyczne dla audytorów dotyczące zarządzania bezpieczeństwa informacji,
   – ISO / IEC 27013:2015 – Wytyczne do zintegrowanego wdrożenia ISO / IEC 27001 oraz ISO / IEC 20000-1,
   – ISO / IEC 27014:2013 –Zarządzanie bezpieczeństwem informacji – ład organizacyjny,
   – ISO / IEC TR 27016:2014 – Zarządzanie bezpieczeństwem informacji – Ekonomika organizacji,
   – ISO / IEC 27021: 2017 – Wymagania kompetencyjne dla specjalistów Systemów Zarządzania Bezpieczeństwem Informacji [ISO / IEC 27000, 2018, s. 20–23].
4) Normy zawierające wytyczne dla specyficznych, określonych sektorów:
   – ISO / IEC 27010:2015 – Zarządzanie bezpieczeństwem informacji w komunikacji międzysektorowej i międzyorganizacyjnej,
   – ISO / IEC 27011:2016 – Zasady postępowania w zakresie zarządzania bezpieczeństwem informacji w oparciu o ISO / IEC 27002 dla organizacji telekomunikacyjnych,

- ISO / IEC 27017:2015 – Praktyczne zasady zabezpieczenia informacji na podstawie ISO / IEC 27002 dla usług w chmurze,
- ISO / IEC 27018:2014 – Praktyczne zasady ochrony danych identyfikujących osobę (PII) w chmurach publicznych działających jako przetwarzający PII,
- ISO / IEC 27019:2017 – Zarządzanie bezpieczeństwem informacji w przemyśle energetycznym,
- ISO 27799:2016 – Zarządzanie bezpieczeństwem informacji w ochronie zdrowia z wykorzystaniem ISO / IEC 27002 [ISO / IEC 27000, 2018, s. 23–25].

5) Normy zawierające specyficzne zabezpieczenia:
   - ISO / IEC 27031:2011 – zawiera wytyczne w zakresie gotowości technologii informacyjnej i komunikacyjnej do zapewnienia ciągłości działania [ISO / IEC 27031, 2011, s. 1],
   - ISO / IEC 27032:2012 – zawiera wytyczne w zakresie poprawy stanu cyberbezpieczeństwa [ISO / IEC 27032, 2012, s. 1],
   - ISO / IEC 27033 – (od 1 do 6) – zawiera wytyczne w zakresie bezpieczeństwa sieci [ISO / IEC 27033-1, 2015, s. 1],
   - ISO / IEC 27034 – (od 1 do 7) – zawiera wytyczne w zakresie bezpieczeństwa aplikacji [ISO / IEC 27034-1, 2011, s. 1],
   - ISO / IEC 27035 – (od 1 do 2) – zawiera wytyczne w zakresie postępowania z incydentem bezpieczeństwa informacji [ISO / IEC 27035-1, 2016, s. 1],
   - ISO / IEC 27036 – (od 1 do 4) – zawiera wytyczne w zakresie bezpieczeństwa informacji w relacjach z dostawcami [ISO / IEC 27036-1, 2014, s. 1],
   - ISO / IEC 27037:2012 – zawiera wytyczne dotyczące identyfikacji, gromadzenia, nabywania i przechowywania dowodów cyfrowych [ISO / IEC 27037, 2012, s. 1],
   - ISO / IEC 27038:2014 – określa cechy technik wykonywania cyfrowej redakcji na dokumentach cyfrowych [ISO / IEC 27038, 2014, s. 1],
   - ISO / IEC 27039:2015 – zawiera wytyczne pomagające organizacjom przygotować się do wdrożenia systemów wykrywania i zapobiegania włamaniom (IDPS) [ISO / IEC 27039, 2015, s. 1],
   - ISO / IEC 27040:2015 – dostarcza szczegółowych wskazówek technicznych, w jaki sposób organizacje mogą zdefiniować odpowiedni poziom ograniczenia ryzyka, stosując sprawdzone i spójne podejście do planowania, projektowania, dokumentacji i wdrażania zabezpieczeń przechowywania danych [ISO / IEC 27040, 2015, s. 1],

- ISO / IEC 27041:2015 – zawiera wytyczne w zakresie mechanizmów zapewniających, że metody i procesy stosowane w dochodzeniach dotyczących incydentów związanych z bezpieczeństwem informacji są „odpowiednie do celu" [ISO / IEC 27041, 2015, s. 1],
- ISO / IEC 27042:2015 – zawiera wytyczne dotyczące analizy i interpretacji dowodów cyfrowych w sposób odnoszący się do kwestii ciągłości, ważności, odtwarzalności i powtarzalności [ISO / IEC 27042, 2015, s. 1],
- ISO / IEC 27043:2015 – zawiera wytyczne oparte na wyidealizowanych modelach dla wspólnych procesów dochodzeniowych incydentów w różnych scenariuszach dochodzeniowych, w których biorą udział dowody cyfrowe [ISO / IEC 27043, 2015, s. 1],
- ISO / IEC 27050 – (od 1 do 3) – zawiera wytyczne i wskazówki dotyczące działań związanych z elektronicznym wykrywaniem, w tym między innymi identyfikację, przechowywanie, gromadzenie, przetwarzanie, przegląd, analizę i produkcję informacji przechowywanych elektronicznie (electronically stored information – ESI) [ISO / IEC 27050-1, 2016, s. 1],
- ISO / IEC 29101:2013 – zawiera wytyczne architektury prywatności, która określa podatności dotyczące systemów technologii informacyjnych i komunikacyjnych (TIK), które przetwarzają informacje umożliwiające identyfikację osób (PII) [ISO / IEC 29101, 2013, s. 1].

3. System Zarządzania Bezpieczeństwem Informacji w ujęciu aktów normatywnych

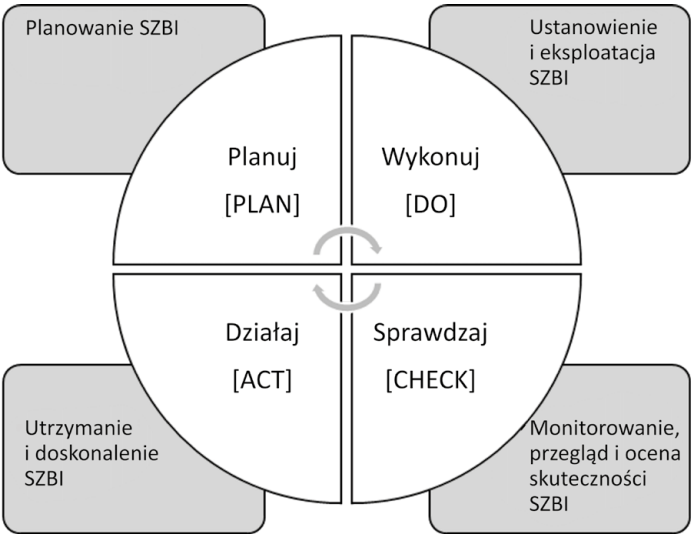
Zarządzanie bezpieczeństwem informacji w organizacji bazuje na szacowaniu ryzyka, a także poziomach jego akceptacji, sformułowanych w taki sposób, aby skutecznie z nim postępować, zarządzać i mitygować. Zdaniem J. Pera „Prawidłowo przeprowadzona mitygacja ryzyka to taka, w wyniku której zmitygowane ryzyko jest jak najmniejsze lub w całości wygaszone, a jego wpływ na wyniki finansowe przedsiębiorstwa jest minimalne" [Pera, 2012, s. 100].

Właściwie opracowane procedury i mechanizmy w organizacji umożliwią zapewnienie bezpieczeństwa informacyjnego na pożądanym poziomie. Skoordynowanie działań w zakresie bezpieczeństwa informacji możliwe jest poprzez określenie polityki oraz celów do osiągnięcia poprzez stosowanie systemu zarządzania. Na System Zarządzania Bezpieczeństwem Informacji składają się:

- polityka,
- procedury,
- wytyczne [Łuczak, Tyburski, 2010, s. 71–73].

Analiza wymagań dla ochrony informacji oraz stosowanie właściwych zabezpieczeń i zasad zawartych w aktach normatywnych przyczynia się do udanego wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji. Procesy zachodzące w systemie zarządzania, tj. opracowanie, ustanowienie, monitorowanie i utrzymanie, odbywają się w oparciu o cykl Deminga, zaprezentowany na rysunku 1, który jest podstawą wszystkich aktów normatywnych w zakresie bezpieczeństwa informacji.

Rysunek 1. Implementacja cyklu Deminga do Systemu Zarządzania Bezpieczeństwem Informacji



Źródło: Opracowanie własne na podstawie [Pelnekar, 2011].

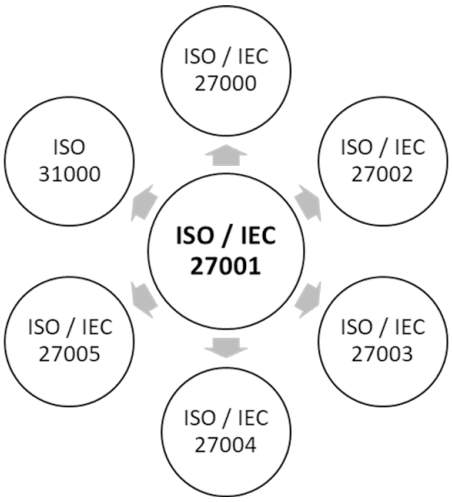
Rodzina norm w zakresie SZBI zawiera wzajemnie uzupełniające się dokumenty, w których opisane zostały wymagania dla ustanowienia, wdrożenia, przeglądu, a także utrzymania i doskonalenia systemu zarządzania.

Terminy i definicje powszechnie stosowane w rodzinie standardów, a także przegląd SZBI zawarte zostały w normie ISO / IEC 27000. Dokument zawiera prezentację poszczególnych norm tworzących rodzinę aktów normatywnych w zakresie SZBI.

Wymagania w zakresie SZBI podane zostały w normie ISO / IEC 27001. Dokument określa wymagania dotyczące ustanawiania, wdrażania, utrzymywania i ciągłego doskonalenia tego systemu w organizacji. Wymagania w nim określone, poprzez ogólny charakter, mają zastosowanie we wszystkich organizacjach, niezależnie od ich rodzaju. Liczne odniesienia do norm zawierających wytyczne, które zostały zobrazowane na rysunku 2, uławiają

korzystanie z zapisów pozostałych aktów normatywnych [ISO / IEC 27001, 2013, s. 1].

Rysunek 2. Odniesienia normy ISO / IEC 27001:2013 do pozostałych aktów normatywnych

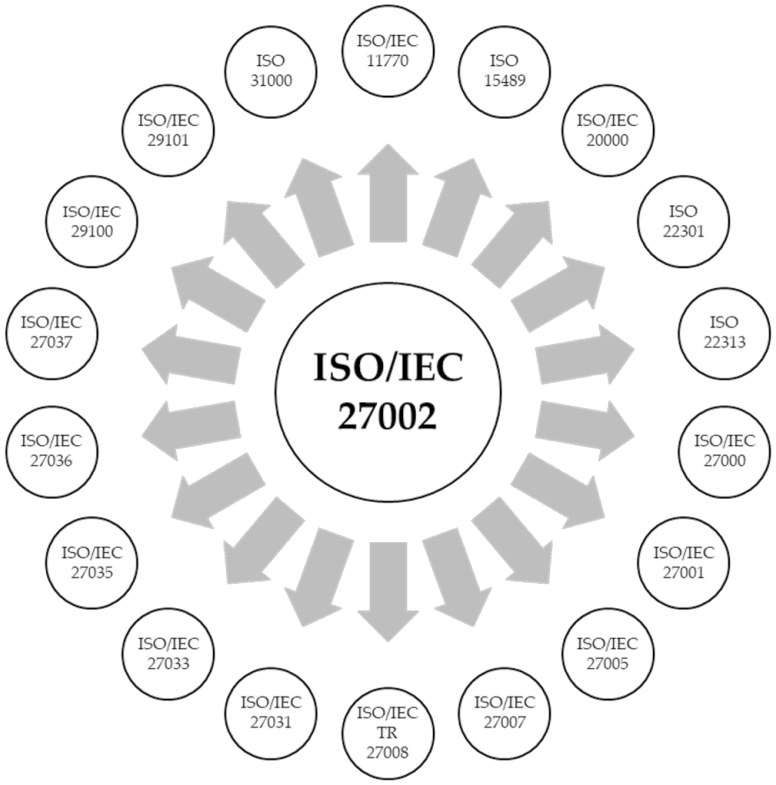


Źródło: Opracowanie własne na podstawie [ISO / IEC 27001:2013].

W normie ISO / IEC 27000:2018 zostało wyszczególnionych dziesięć norm zawierających szczegółowe wytyczne organizacji bezpieczeństwa informacji. Jedną z nich jest norma ISO / IEC 27002:2013, która zawiera opis najlepszych praktyk zarządzania bezpieczeństwem, stanowiąc kodeks postępowania w zakresie zarządzania bezpieczeństwem informacji. Opracowanie indywidualnych wytycznych zarządzania bezpieczeństwem informacji możliwe jest poprzez liczne odniesienia do pozostałych aktów normatywnych, które zostały zaprezentowane na rysunku 3.

Widoczna korelacja normy ISO / IEC 27001 z normą ISO / IEC 27002, a także wspólne odniesienia do norm z zakresu zarządzania ryzykiem (norma ISO / IEC 27005 oraz ISO 31000) świadczą o spójności i dojrzałości aktów normatywnych w dziedzinie bezpieczeństwa informacji. Zgodnie z zapisami normy ISO / IEC 27013 każde aktywo informatyczne jest aktywem informacyjnym, natomiast nie każde aktywo informacyjne jest aktywem informatycznym [ISO / IEC 27013, 2015, s. 7]. Odwołania do innych dokumentów normatywnych, jak chociażby ISO / IEC 20000, świadczą o całościowym podejściu do zarządzania bezpieczeństwem, w tym konkretnym przypadku odnoszącym się do Systemu Zarządzania Usługami, definiując mechanizmy bezpieczeństwa w usługach informatycznych.

Rysunek 3. Odniesienia normy ISO / IEC 27002:2013 do pozostałych aktów normatywnych



Źródło: Opracowanie własne na podstawie [ISO / IEC 27002:2013].

W przypadku niewystarczającej ilości informacji związanych z wyspecjalizowanym obszarem działalności organizacji powstały normy sektorowe, które odnoszą się bezpośrednio do normy ISO / IEC 27002. Zawierają one zalecenia w zakresie stosowania standardów i praktyk zarządzania bezpieczeństwem informacji w poszczególnych sektorach. W szczególności wyboru wdrażania i zarządzania zabezpieczeniami uwzględniającymi specyfikę ryzyk występujących w poszczególnych sektorach [ISO / IEC 27002, 2013, s. 1]. Wszystkie poniżej wymienione akty normatywne dla poszczególnych sektorów zawierają wytyczne w zakresie bezpieczeństwa informacji adekwatnie do specyfiki branży, lecz nie określają, w jaki sposób mają zostać spełnione.

Zakres normy ISO / IEC 27011 ma na celu określenie wytycznych wspierających wdrażanie SZBI w organizacjach świadczących usługi telekomunikacyjne [ISO / IEC 27011, 2016, s. 1]. Zastosowanie zapisów normy pozwoli spełnić podstawowe wymagania w zakresie zarządzania bezpieczeństwem informacji.

Norma ISO / IEC 27019:2017 zawiera wytyczne w zakresie systemów zarządzania procesami bezpieczeństwa informacji w przemyśle energetycznym, w szczególności w procesach zabezpieczania i monitorowania produkcji lub wytwarzania, przesyłania, magazynowania i dystrybucji energii elektrycznej, gazu, ropy i ciepła oraz do zabezpieczania powiązanych procesów wspomagających z wyłączeniem sektora energetyki jądrowej, który został objęty normą IEC 62645 [ISO / IEC 27019, 2017, s. 1].

Wytyczne dotyczące standardów w zakresie zarządzania bezpieczeństwem informacji, stanowiące interpretację normy ISO / IEC27002:2013, w organizacjach zajmujących się ochroną zdrowia zostały udokumentowane w normie ISO 27799:2016. Dokument zawiera szczegółowe wytyczne dotyczące zapewnienia bezpieczeństwa informacji o zdrowiu pacjentów we wszystkich jego aspektach, niezależnie od formy przetwarzania (nagrania dźwiękowe, wideo, obrazy medyczne), bez względu na środki używane do ich przechowywania (drukowane, pisanie odręcznie, przechowywanie w formie elektronicznej), niezależnie od wykorzystywanych środków przekazu (faksem, za pośrednictwem sieci komputerowej, pocztą) [ISO 27799, 2016, s. 1].

Zakończenie

Stale rosnąca liczba dostępnych aktów normatywnych z dziedziny bezpieczeństwa informacji, a także ich aktualizacji, umożliwia ciągły rozwój, determinując jednocześnie potrzebę stałej analizy i weryfikacji dostępności i aktualności aktów normatywnych w tym zakresie.

System Zarządzania Bezpieczeństwa Informacji oparty na normie ISO / IEC 27000 jest dojrzałym i sprawdzonym rozwiązaniem, którego konieczność implementacji w organizacji, w szczególności w sektorze publicznym, jest uzasadniona. Wartością dodaną jest fakt możliwości integracji Systemu Zarządzania Bezpieczeństwem Informacji z pozostałymi systemami zarządzania funkcjonującymi lub wdrażanymi w organizacji.

Literatura

Cisek S. (2002), *Filozoficzne aspekty informacji naukowej*, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków.

Dziekański P. (2012), *Informacja jako dobro ekonomiczne będące źródłem przewagi konkurencyjnej*, „Nierówności Społeczne a Wzrost Gospodarczy", z. 24, Wydawnictwo Uniwersytetu Rzeszowskiego, Rzeszów.

ISO / IEC 27000:2018, *Information technology – Security techniques – Information security management systems – Overview and vocabulary* (2018), ISO, Geneva.

ISO / IEC 27001:2013, *Information technology – Security techniques – Information security management systems – Requirements* (2013), ISO, Geneva.

ISO / IEC 27002:2013, *Information technology – Security techniques – Code of practice for information security controls* (2013), ISO, Geneva.

ISO / IEC 27011:2016, *Information technology – Security techniques – Code of practice for Information security controls based on ISO / IEC 27002 for telecommunications organizations* (2016), ISO, Geneva.

ISO / IEC 27013:2015, *Information technology – Security techniques – Guidance on the integrated implementation of ISO / IEC 27001 and ISO / IEC 20000-1* (2015), ISO, Geneva.

ISO / IEC 27019:2017, *Information technology – Security techniques – Information security controls for the energy utility industry* (2017), ISO, Geneva.

ISO / IEC 27031:2011, *Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity* (2011), ISO, Geneva.

ISO / IEC 27032:2012, *Information technology – Security techniques – Guidelines for cybersecurity* (2012), ISO, Geneva.

ISO / IEC 27033-1:2015, *Information technology – Security techniques – Network security – Part 1: Overview and concepts* (2015), ISO, Geneva.

ISO / IEC 27034-1:2011, *Information technology – Security techniques – Application security – Part 1: Overview and concepts* (2011), ISO, Geneva.

ISO / IEC 27035-1:2016, *Information technology – Security techniques – Information security incident management – Part 1: Principles of incident management* (2016), ISO, Geneva.

ISO / IEC 27036-1:2014, *Information technology – Security techniques – Information security for supplier relationships – Part 1: Overview and concepts* (2014), ISO, Geneva.

ISO / IEC 27037:2012, *Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence* (2012), ISO, Geneva.

ISO / IEC 27038:2014, *Information technology – Security techniques – Specification for digital redaction* (2014), ISO, Geneva.

ISO / IEC 27039:2015, *Information technology – Security techniques – Selection, deployment and operations of intrusion detection and prevention systems (IDPS)* (2015), ISO, Geneva.

ISO / IEC 27040:2015, *Information technology – Security techniques – Storage security* (2015), ISO, Geneva.

ISO / IEC 27041:2015, *Information technology – Security techniques – Guidance on assuring suitability and adequacy of incident investigative method* (2015), ISO, Geneva.

ISO / IEC 27042:2015, *Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence* (2015) , ISO, Geneva.

ISO / IEC 27043:2015, *Information technology – Security techniques – Incident investigation principles and processes* (2015) , ISO, Geneva.

ISO / IEC 27050-1:2016, *Information technology – Security techniques – Electronic discovery – Part 1: Overview and concepts* (2016) , ISO, Geneva.

ISO / IEC 29101:2013, *Information technology – Security techniques – Privacy architecture framework* (2013) , ISO, Geneva.

ISO 27799:2016, *Health informatics — Information security management in health using ISO/IEC 27002* (2016), ISO, Geneva.

Krawiec J., Ożarek G. (2014), *System Zarządzania Bezpieczeństwem Informacji w praktyce Zabezpieczenia*, Wydawnictwo Polskiego komitetu Normalizacyjnego, Warszawa.

Łuczak J., Tyburski M. (2010), *Systemowe zarządzanie bezpieczeństwem informacji ISO / IEC 27001*, Wydawnictwo Uniwersytetu Ekonomicznego, Poznań.

Oleksiewicz I. (2017), *Bezpieczeństwo informacyjne jako wyzwanie w XXI wieku*, „Zeszyty Naukowe Wyższej Szkoły Informatyki, Zarządzania i Administracji w Warszawie", t. 15, z. 4(41), Wydawnictwo Wyższej Szkoły Informatyki, Zarządzania i Administracji, Warszawa.

Pelnekar C. (2011), *Planning for and implementing ISO 27001*, „ISACA Journal", Vol. 4, ISACA, Minneapolis.

Pera J. (2012), *Niepewność a problem mitygacji ryzyka w przedsiębiorstwie*, „Zarządzanie i Finanse", nr 1, cz. 1.

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, t.j. Dz.U. z 2017 r. poz. 2247.

Stańczyk-Hugiet E., Stańczyk S. (2013), *Kulturowy kontekst relacji międzyorganizacyjnych*, „Zeszyty Naukowe Wyższej Szkoły Bankowej w Poznaniu", t. 49, nr 4, Wydawnictwo Wyższej Szkoły Bankowej, Poznań.

Szlachcic B. (2014), *Analiza ryzyka i zarządzania ryzykiem jako element systemu zarządzania kryzysowego w organizacji*, „Zeszyty Naukowe Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach. Seria: Administracja i Zarządzanie", nr 30(103), Wydawnictwo Uniwersytetu Przyrodniczo-Humanistycznego, Siedlce.

The ISO Survey Of Management System Standard Certifications – 2017 – Explanatory Note, August 2018 https://www.accredia.it/app/uploads/2017/09/ISO_Survey_2016.pdf, dostęp: 28.10.2018.

Streszczenie

W artykule omówiono istotę wyboru właściwego modelu zarządzania bezpieczeństwem informacji. Przedstawiono proces powstawania, standaryzacji, a także rozwoju aktów normatywnych w zakresie zarządzania bezpieczeństwem informacji.

W wyniku przeglądu i analizy dostępnych aktów normatywnych zostały wybrane i przedstawione normy wpływające w sposób bezpośredni na wdrożenie i zarządzanie bezpieczeństwem informacji. Spełnienie zapisów wyszczególnionych norm ma na celu umożliwienie ustanowienia Systemu Zarządzania Bezpieczeństwem Informacji w organizacji.

Słowa kluczowe
System Zarządzania Bezpieczeństwem Informacji, bezpieczeństwo informacji, akty normatywne w zakresie bezpieczeństwa informacji, model zarządzania bezpieczeństwem informacji

Information security management in the recognition of selected normative acts in terms of the Information Security Management System (Summary)

This study discusses the essence of choosing the right model for information security management. The process of creating, standardizing, and the development of normative acts regarding the management of information security was presented.

As a result of the review and analysis of available normative acts, standards that influence directly the implementation and management of information security have been selected and presented. Fulfilling the provisions of the specified standards enables the implementation of the Information Security Management System in the organization.

Keywords
Information Security Management System, information security, normative acts in the field of information security, information security management model