Jerzy Stanik[1], Jarosław Napiórkowski[2], Maciej Kiedrowicz[3]

Standardy bezpieczeństwa w cyklu życia systemu zabezpieczeń systemu informacyjnego organizacji

1. Wstęp

Podstawą bezpieczeństwa systemu informacyjnego organizacji jest dobrze opracowany projekt systemu zabezpieczeń, wdrożony z użyciem właściwie dobranych technologii renomowanych producentów i zarządzany przez wykwalifikowaną służbę informatyczną i bezpieczeństwa. Projektowane zabezpieczenia powinny być oparte w znacznej mierze na wynikach analizy ryzyka, specyfikacji wymagań bezpieczeństwa, a także ogólnej teorii zabezpieczeń (m.in. wymagane jest dokonanie weryfikacji odporności systemu na strategię różnego typu ataków i włamań)[4]. Wypracowany na podstawie standardów bezpieczeństwa lub dobrych praktyk system zabezpieczeń w znacznym stopniu decyduje o skuteczności działania całości rozwiązań w zakresie ochrony informacji w organizacji.

Celem pracy jest przegląd norm i standardów z zakresu bezpieczeństwa informacyjnego, a następnie zaproponowanie sposobu ich wykorzystania w procesie ustalania, budowy, wdrażania i eksploatacji systemu zabezpieczeń systemu informacyjnego. Poprawny systemu zabezpieczeń systemu informacyjnego powinien charakteryzować się między innymi następującymi własnościami:

- opracowany zgodnie ze sprawdzoną metodyką,
- zawiera etapy analizy, projektowania i wdrożenia,
- przejrzysty i zrozumiały model bezpieczeństwa organizacji,
- opis infrastruktury technicznej (narzędzia informatyczne, platforma sprzętowa, wymagania lokalizacyjne),

[1] Wojskowa Akademia Techniczna, Wydział Cybernetyki.
[2] Wojskowa Akademia Techniczna, Wydział Cybernetyki.
[3] Wojskowa Akademia Techniczna, Wydział Cybernetyki.
[4] PN ISO/IEC 15408–3: 2002 Kryteria oceny zabezpieczenia systemów. Wymagania uzasadnienia pewności.

- opis infrastruktury organizacyjnej (określenie kompetencji i kwalifikacji personelu, opracowanie procedur działań w przypadku obsługi codziennej oraz sytuacji alarmowych).

Spełnienie wszystkich tych wymagań względem systemu zabezpieczeń wymaga opracowania odpowiedniej architektury zabezpieczeń. Tworzenie zabezpieczeń systemu informatycznego powinno odbywać się w przemyślany, wcześniej szczegółowo zaplanowany sposób, zgodnie ze sprawdzoną metodyką.

Problematyka artykułu została podzielona na trzy części.

W pierwszej części przedstawiono model systemu zarządzania bezpieczeństwem informacji w organizacji na potrzeby budowy systemu zabezpieczeń.

Druga część opisuje:

- model cyklu życia systemu zabezpieczeń odzwierciedlający koncepcję rozłożenia w czasie głównych etapów/czynności podczas pracy nad opracowaniem i wyprodukowaniem systemu określonego typu oraz podczas jego eksploatacji;
- oraz podejście ukazujące zbiory norm i standardów z zakresu bezpieczeństwa informacyjnego, które należy wziąć pod uwagę podczas realizacji poszczególnych etapów cyklu życia systemu zabezpieczeń.

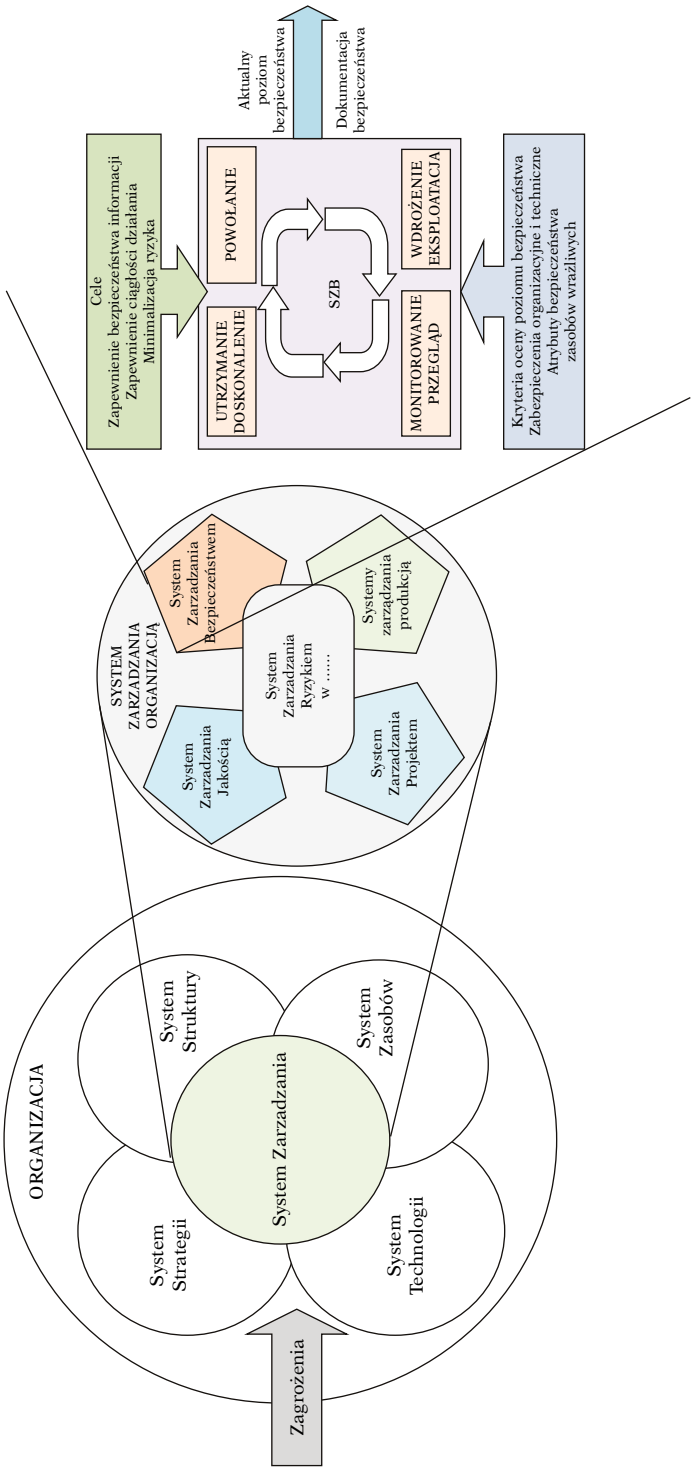
Podsumowanie zawiera wnioski z przeprowadzonych badań, rekomendacje stosowania standardów oraz przykładowy dobór mechanizmów bezpieczeństwa do procesów ochronnych.

2. Model systemu zarządzania bezpieczeństwem w organizacji

Pojawianie się nowych technologii, a wraz z nimi nowych rodzajów zagrożeń implikuje konieczność tworzenia elastycznych systemów zarządzania bezpieczeństwem (rysunek 1), umożliwiających ich modyfikację w przypadku zmiany środowiska lub otoczenia działania organizacji.

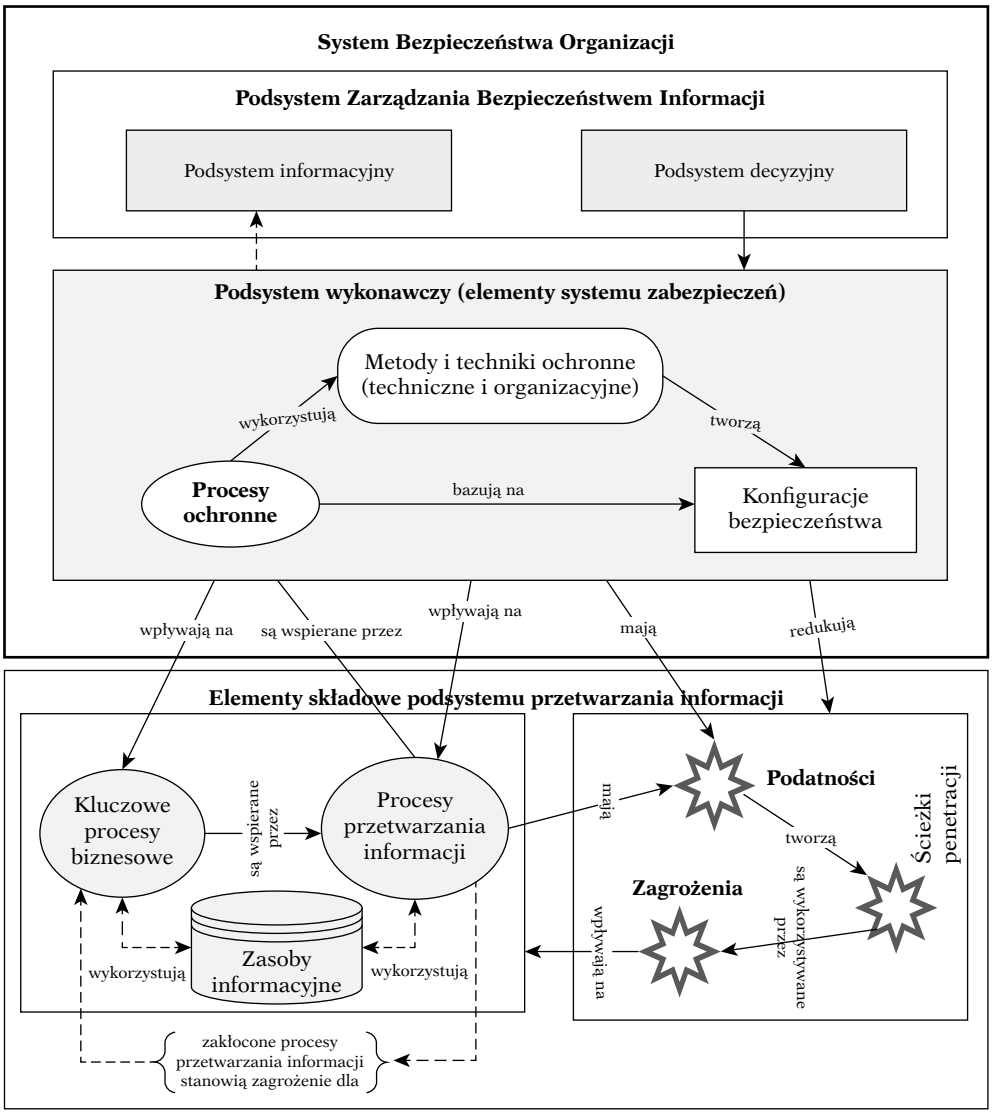
Dlatego w tym modelu zaleca się ciągłe doskonalenie zgodnie z koncepcją PDCA. Stąd szczególna rola ewidencjonowania i dokumentowania w ramach systemu, w tym również w aspekcie ochrony i nadzoru sporządzanych zapisów i dokumentacji[5].

[5] G. Stoneburner, C. Hayden, A. Feringa, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A*, Series/Number: NIST Special Publication 800–27 Rev A (2004).



Rysunek 1. Model systemu zarządzania bezpieczeństwem informacji w organizacji

Źródło: opracowanie własne.



Rysunek 2. System zabezpieczeń na tle modelu systemu bezpieczeństwa organizacji
Źródło: opracowanie własne.

Utrzymanie wysokiego/wymaganego poziomu bezpieczeństwa organizacji wymaga skutecznej ochrony przed zagrożeniami napływającymi zarówno z zewnątrz, jak i wewnątrz organizacji. Skuteczna obrona przed takimi atakami może wymuszać zastosowanie kosztownych produktów lub usług w zakresie zabezpieczeń, lecz to rozwiązanie nie gwarantuje skuteczności. Właściwe obrona/ochrona opiera się na opracowaniu skutecznego systemu zabezpieczeń

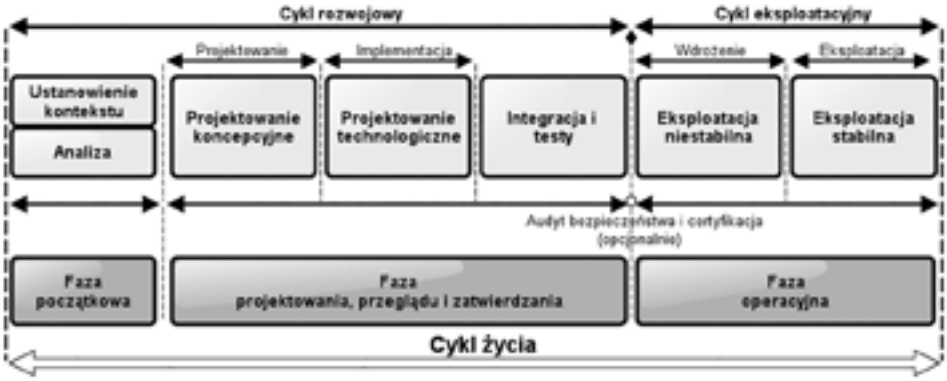
zgodnie z optymalną metodyką, a także wdrożenie przez profesjonalistów oraz odpowiednie technologie wraz z poprawną eksploatacją. Skuteczny system zabezpieczeń powinien wyeliminować lub zredukować zagrożenia do poziomu akceptowalnego. Miejsce i rolę systemu zabezpieczeń w systemie bezpieczeństwa organizacji ilustruje rysunek 2.

W celu zapewnienia bezpieczeństwa funkcjonowania „Systemu Informacyjnego Organizacji" powinien być stworzony SBSIO – System Bezpieczeństwa „Systemu Informacyjnego Organizacji", rozumiany jako zespół sił i środków oraz powiązań pomiędzy nimi zapewniających pożądany poziom bezpieczeństwa organizacji. Projektowanie systemu zabezpieczeń (mechanizmów bezpieczeństwa) dla systemu informacyjnego organizacji to bardzo ważny etap w cyklu życia systemu bezpieczeństwa. Celem projektowania jest zaprojektowanie procesów ochronnych dla procesów przetwarzania informacji wspierającej krytyczne procesy biznesowe organizacji. Podstawowym zadaniem systemu zabezpieczeń jest zapewnienie (podstawowych atrybutów bezpieczeństwa) tajności, integralności, niezaprzeczalności i dostępności przetwarzanej w chronionych systemach informacyjnych informacji, ponieważ ma ona wpływ na przebieg procesów biznesowych[6].

3. Cykl życia systemu zabezpieczeń

Termin „cykl życia" systemu określa koncepcję rozłożenia w czasie głównych etapów/czynności podczas pracy nad opracowaniem i wyprodukowaniem systemu określonego typu oraz podczas jego eksploatacji. Podstawowe elementy składowe cyklu życia systemu to trzy fazy (rysunek 3): Faza początkowa, Faza projektowania, przeglądu i zatwierdzania, Faza operacyjna (eksploatacji).

[6] ISO / IEC 27002: 2013 Technika informatyczna – Techniki bezpieczeństwa – Kodeks postępowania w zakresie kontroli bezpieczeństwa informacji.

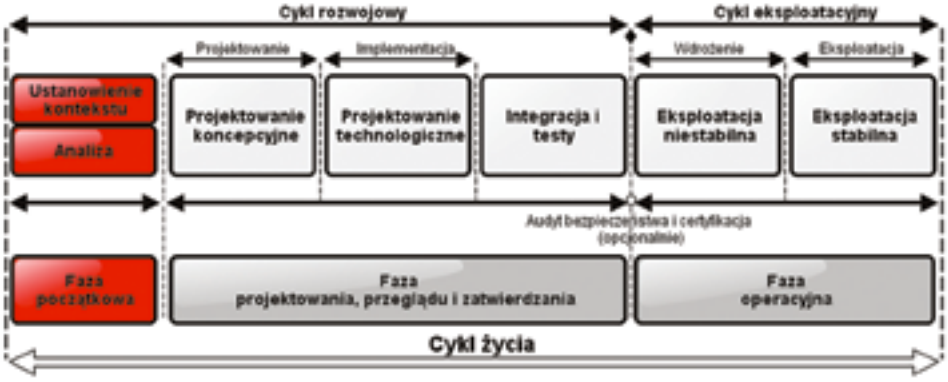


Rysunek 3. Model cyklu życia systemu zabezpieczeń

Źródło: opracowanie własne.

3.1. Faza początkowa – ustanowienie kontekstu

Umiejscowienie fazy początkowej w modelu cyklu życia systemu zabezpieczeń ilustruje rysunek 4.



Rysunek 4. Umiejscowienie fazy początkowej w modelu cyklu życia systemu zabezpieczeń

Źródło: opracowanie własne.

Zakres wykonywanych czynności oraz w ramach tej fazy oraz zbiór możliwych do wykorzystania standardów zawiera tabela 1.

Tabela 1. Zakres wykonywanych czynności na etapie prac przedprojektowych oraz zbiór możliwych do wykorzystania standardów

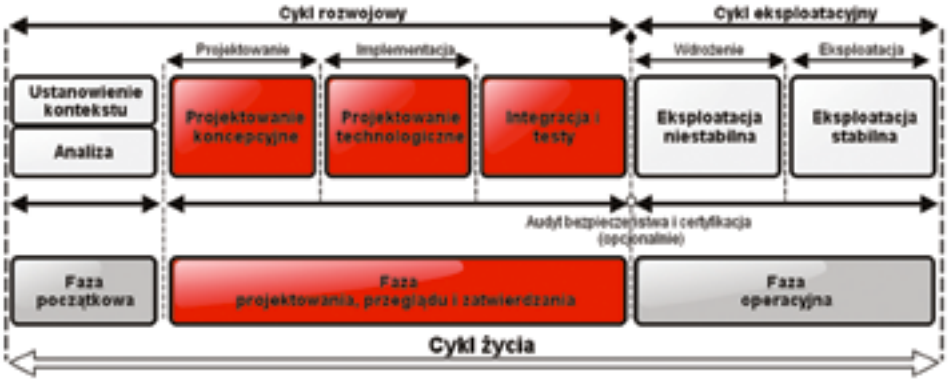
Etap	Zakres czynności	Wykorzystywane standardy
Ustanowienie kontekstu	1. Wyłania się interdyscyplinarną grupę ekspertów (rzeczywisty przekrój wszystkich stron) sterującą całym procesem: analizy, projektowania, realizacji i obsługi zabezpieczeń w obszarze chronionym (np. w obszarze ochrony danych statystycznych). 2. Określenia się zakres procesu zarządzania bezpieczeństwem informacji, tak aby zapewnić, że przy szacowaniu ryzyka uwzględniono wszystkie odnośne aktywa. 3. Wyznacza się podstawowe kryteria (kryteria oceny ryzyka, kryteria skutków, kryteria akceptowania ryzyka) potrzebne do procesu zarządzania: • bezpieczeństwem w obszarze ochrony danych, informacji i wiedzy, • przedsięwzięciem projektowania i budowy systemu mechanizmów bezpieczeństwa w celu zapewnienia tajności, integralności, niezaprzeczalności i dostępności przetwarzanej w chronionych systemach informacyjnych (np. baz danych systemów informatycznych).	• Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach. • Ustawa z dnia 23 czerwca 1995 r. o statystyce publicznej. • Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych • Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych. • Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne • Ustawa z dnia 05 sierpnia 2010 r. o ochronie informacji niejawnych • ISO 22301 Bezpieczeństwo społeczne – Systemy zarządzania ciągłością działania – Wymagania • ISO / IEC 27001:2013 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania • ISO / IEC 27005:2011 Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie Bezpieczeństwem Informacji – Analiza ryzyka
Analiza	1. Identyfikowanie procesów kluczowych (krytycznych). 2. Określenie dla zidentyfikowanych procesów ich wrażliwości na zakłócenia we wspierających je procesach przetwarzania informacji. 3. Dla procesów krytycznych zidentyfikowanie wspierających je procesów przetwarzania informacji w systemach teleinformatycznych.	• PN-ISO/IEC 15408–3:2002: Technika informatyczna – Techniki zabezpieczeń – Kryteria oceny zabezpieczeń informatycznych – Część 3: Wymagania uzasadnienia zaufania do zabezpieczeń • PN-IEC 62198:2005: Zarzadzanie ryzykiem przedsięwzięcia – Wytyczne stosowania • IEC/ISO 31010 Risk management – Risk assessment techniques (2009)

Etap	Zakres czynności	Wykorzystywane standardy
Analiza	4. Dla każdego z procesów zidentyfikowanych jako krytyczne ustalić zbiór zagrożeń, które mogą doprowadzić do utraty tajności, integralności, niezaprzeczalności i dostępności przetwarzanych w nich informacjach. 5. Dla zidentyfikowanych procesów zidentyfikować zasoby w nich wykorzystywane. 6. Dla każdego zasobu z każdego procesu zidentyfikować podatności, które mogą być wykorzystane przez zagrożenia. 7. Na podstawie zbioru zasobów i zbioru podatności wyznaczyć ścieżki penetracji dla procesów wspierających.	• IEC Guide 73:2009 Risk Management –Vocabulary – Guidelines for use in standards (Wielka Brytania 2009) • Standard Zarządzania Ryzykiem FERMA (Federation of European Risk Management Associations – Wielka Brytania 2003) • AS/NZS 4360:2004 Risk Management (Australia, Nowa Zelandia 2004) • CAN/CSA Q850 Risk Management: Guideline for Decision-Makers (Kanada 1997) • COSO II – ERM Enterprise Risk Management – Integrated Framework (USA 2004)

Źródło: opracowanie własne.

3.2. Faza projektowania

Celem etapu projektowania jest zaprojektowanie procesów ochronnych dla procesów przetwarzania informacji wspierającej krytyczne procesy biznesowe. Umiejscowienie fazy początkowej w modelu cyklu życia systemu zabezpieczeń ilustruje rysunek 5.



Rysunek 5. Umiejscowienie fazy początkowej w modelu cyklu życia systemu zabezpieczeń

Źródło: opracowanie własne.

Podstawowe czynności procesu projektowania procesów ochronnych obejmują[7]:

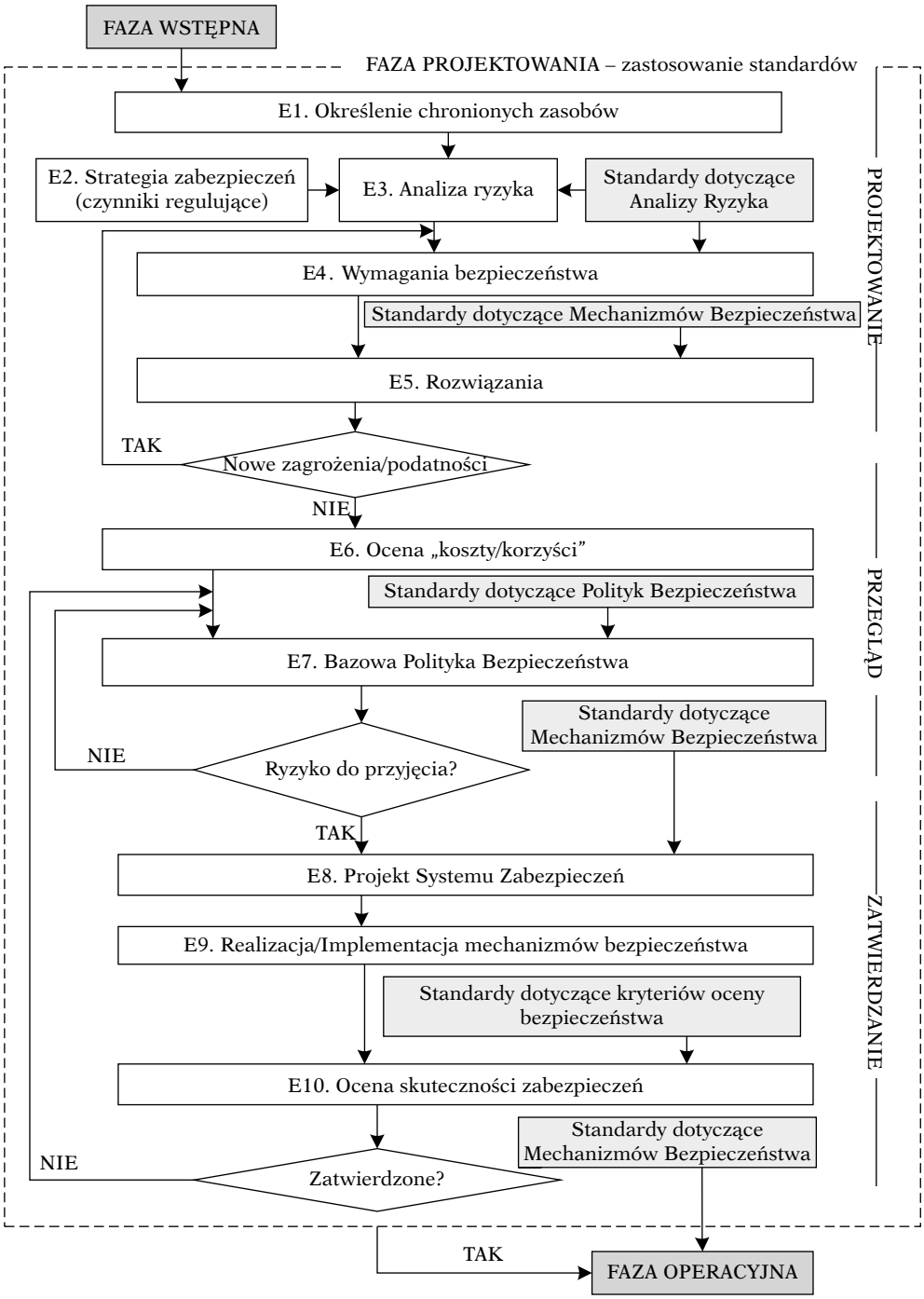
- Zaprojektowanie środków zarządzania bezpieczeństwem (struktur, dokumentów i procedur) – rozwiązania organizacyjne.
- Dobór technicznych i programowych środków ochronnych do podatności.
- Dobór zabezpieczeń sieciowych.
- Zaprojektowanie sposobu zastosowania mechanizmów bezpieczeństwa (architektury rozwiązań).
- Ocena ryzyka szczątkowego.
- Przeprojektowanie systemu zabezpieczeń lub przejście do realizacji/implementacji mechanizmów bezpieczeństwa.

Podstawowe czynności fazy projektowania, przeglądu i akredytacji obejmują (rysunek 6):

- Określenie zasobów chronionych.
- Ustalenie Strategii Zabezpieczeń (USZ).
- Przeprowadzenie Uszczegółowionej Analizy Ryzyka (UAR), na podstawie której określa się Wymagania Bezpieczeństwa.
- Opracowanie specyfikacji wymagań bezpieczeństwa (SWB).
- Zaproponowanie wariantów rozwiązań spełniających wymagania (WR).
- Przeprowadzenie oceny „koszty/zyski" dla zaproponowanych rozwiązań (OW).
- Wybór rozwiązania i opracowanie Bazowej Polityki Bezpieczeństwa (BPB).
- Opracowanie projektu zabezpieczeń (PZ).
- Formalna akceptacja dokumentów wynikowych.

Zakres wykonywanych czynności fazy projektowania, przeglądu i akredytacji oraz zbiór możliwych do wykorzystania standardów przedstawiają poniższe tabele.

[7] ISO / IEC 27004: 2009 Technika informatyczna – Techniki zabezpieczeń – Zarządzanie bezpieczeństwem informacji – pomiary.



Rysunek 6. Podstawowe czynności fazy projektowania, przeglądu i akredytacji

Źródło: opracowanie własne.

Tabela 2. Zakres wykonywanych czynności oraz zbiór możliwych do wykorzystania standardów na etapie projektowania – faza identyfikacji aktywów

Etap	Zakres czynności	Wykorzystywane standardy
E1. Określenie chronionych zasobów	Określenie zasobów (aktywów), które podlegają ochronie i określenie poziomu zabezpieczeń jest niezbędnym i nie podlegającym dyskusji krokiem przy projektowaniu mechanizmów bezpieczeństwa. Można wyróżnić dwa rodzaje aktywów: 1. Aktywa podstawowe: • Procesy i działania biznesowe • Informacje 2. Aktywa wspierające (na których opierają się podstawowe elementy z zakresu) wszystkich rodzajów: • Sprzęt • Oprogramowanie • Sieć • Personel • Siedziba • Struktura organizacyjna	• Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. • Ustawa z dnia 05 sierpnia 2010 r. o ochronie informacji niejawnych. • Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych. • Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (podstawowe zasady odnośnie klasyfikacji dokumentacji, jej zabezpieczenia w archiwach oraz postępowania z materiałami archiwalnymi). • Ustawa z dnia 23 czerwca 1995 r. o statystyce publicznej (definiuje, iż zbierane i gromadzone w badaniach statystycznych statystyki publicznej dane indywidualne i dane osobowe są poufne i podlegają szczególnej ochronie). • PN-ISO/IEC 27001:2007. Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania • ISO/IEC 27005:2008 zawiera wytyczne w zakresie zarządzania ryzykiem na potrzeby systemów bezpieczeństwa informacji zgodnych z ISO/IEC 27001:2005 – Załączniki A i B • Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach.

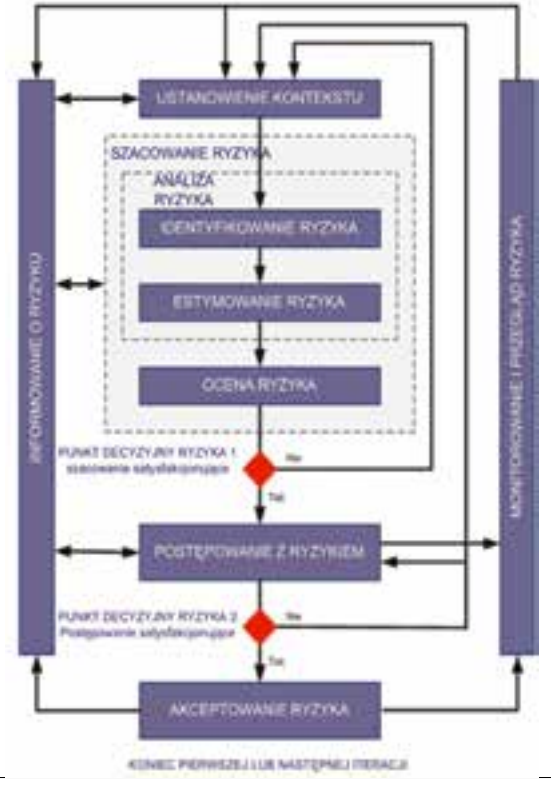
Źródło: opracowanie własne.

Tabela 3. Zakres wykonywanych czynności oraz zbiór możliwych do wykorzystania standardów na etapie projektowania – faza strategia zabezpieczeń

Etap	Zakres czynności	Wykorzystywane standardy
E2. Strategia zabezpieczeń	1. Nakreślenie obszarów i celów zabezpieczeń. 2. Zdefiniowanie zakresu zabezpieczeń. 3. Utworzenie oficjalnego słownika pojęć dotyczących bezpieczeństwa.	Podstawowym czynnikiem kształtującym strategię zabezpieczeń są przepisy prawne, m.in.: • Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. • Ustawa z dnia 05 sierpnia 2010 r. o ochronie informacji niejawnych. • Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych. • Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne. Pomocniczymi elementami są normy: • PN-ISO/IEC-17799:2003 Technika informatyczna – Praktyczne zasady zarządzania bezpieczeństwem informacji zawiera ogólne wytyczne, które powinny zostać uwzględnione w trakcie projektowania i wdrażania zabezpieczeń. • ISO / IEC 27001:2013 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania – Załącznik A PN-ISO/IEC 15408–1:2002: Technika informatyczna – Techniki zabezpieczeń – Kryteria oceny zabezpieczeń informatycznych – Część 1: Wprowadzenie i model ogólny. • PN-ISO/IEC 15408–3:2002: Technika informatyczna – Techniki zabezpieczeń – Kryteria oceny zabezpieczeń informatycznych – Część 3: Wymagania uzasadnienia zaufania do zabezpieczeń.

Źródło: opracowanie własne.

Tabela 4. Zakres wykonywanych czynności oraz zbiór możliwych do wykorzystania standardów na etapie projektowania – faza analiza ryzyka

	Zakres czynności[8]	Wykorzystywane standardy
E3. Analiza ryzyka		• Zalecenia ABW „Szczegółowe zalecenia dotyczące analizy oraz zarządzania ryzykiem w systemach i sieciach teleinformatycznych”. • ISO / IEC 27005:2011 Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie Bezpieczeństwem Informacji – Analiza ryzyka • PN-IEC 62198:2005: *Zarzadzanie ryzykiem przedsięwzięcia – Wytyczne stosowania.* • IEC/ISO 31010 Risk management – Risk assessment techniques (2009). • ISO 31000 Risk Management – Guidelines for principles and implementation of risk management (2009). • IEC Guide 73:2009 Risk Management – Vocabulary – Guidelines for use in standards (Wielka Brytania 2009). • BS-6079-3:2000 Project management. Guide to the management of business related project risk (Wielka Brytania 2000). • Standard Zarządzania Ryzykiem FERMA (Federation of European Risk Management Associations – Wielka Brytania 2003). • AS/NZS 4360:2004 Risk Management (Australia, Nowa Zelandia 2004). • CAN/CSA Q850 Risk Management: Guideline for Decision-Makers (Kanada 1997). • COSO II-ERM Enterprise Risk Management – Integrated Framework (USA 2004).

Źródło: opracowanie własne.

[8] http://www.iso27000.pl/ (dostęp: 23.06.2016).

Tabela 5. Zakres wykonywanych czynności oraz zbiór możliwych do wykorzystania standardów na etapie przeglądu – faza przeglądu specyfikacji wymagań oraz proponowanego rozwiązania

Et.	Zakres czynności	Wykorzystywane standardy
E4. Wymagania bezpieczeństwa i E5. Proponowane rozwiązania	1. Wymagania bezpieczeństwa są określane po wykonaniu analizy ryzyka i przeanalizowaniu problemów natury prawnej. 2. Proponowane rozwiązania mają na celu spełnienie określonych wcześniej wymagań bezpieczeństwa. 3. Usługi i mechanizmy bezpieczeństwa mogą być wybrane z biblioteki technik ochrony informacji.	Podstawowym czynnikiem kształtującym strategię zabezpieczeń są przepisy prawne, m.in.: • Rozporządzenie Prezesa Rady Ministrów z 25 lutego 1999 r. w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformacyjnych (Dz.U.18/99 poz. 162). • Rozporządzenie Prezesa Rady Ministrów z 25 sierpnia 2005 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego. • Ustawa o podpisie elektronicznym z 18 września 2001 r. • Dokumenty wydawnictwa Urzędu Ochrony Państwa dotyczące bezpieczeństwa teleinformatycznego, wersja1.1. • Dokumenty wydawnictwa ABW dotyczące „Metodyki opracowywania szczególnych wymagań bezpieczeństwa dla systemów lub sieci teleinformatycznych". • Dokumenty wydawnictwa ABW dotyczące „Szczegółowych zaleceń dotyczących opracowywania dokumentów szczegółowych wymagań bezpieczeństwa dla systemów i sieci teleinformatycznych". • Dokumenty wydawnictwa RFC dotyczące opracowań specyfikacji.

Źródło: opracowanie własne.

Tabela 6. Zakres wykonywanych czynności oraz zbiór możliwych do wykorzystania standardów na etapie przeglądu – faza oceny kosztów i korzyści

Et.	Zakres czynności	Wykorzystywane standardy
E6. Ocena „koszty i korzyści" E7. Bazowa Polityka Bezpieczeństwa	1. Opracowanie Rozwiązań – Zaproponowane rozwiązania są oceniane pod kątem kosztów i korzyści. 2. Opracowanie Bazowej Polityki Bezpieczeństwa – opracowanie aktualnego zbioru praw, zasad, reguł i sposobów, które regulują zarządzanie, przetwarzanie, użycie, zabezpieczenie rozpowszechnienie informacji i zasobów systemu informacyjnego. 3. Określenie Budżetu – Koszty określające wymagany/pożądany poziom bezpieczeństwa nie powinny przekraczać zysków z zastosowanych usług bezpieczeństwa.	• Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004 r. w sprawie **dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych**, jakim powinny odpowiadać urządzenia i systemy informatyczne służce do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024), zwanego dalej rozporządzeniem, wydane zostało na podstawie delegacji ustawowej art. 39a ustawy o ochronie danych osobowych i jego zakres na podstawie art. 36 ust. 2 tejże ustawy ograniczony jest do przetwarzania danych osobowych. • **PN-ISO/IEC 27001:2007**. Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania. • **TISM** (***Total Information Security Management***) Metodyka opracowana przez firmę ENSI – European Network Security Institute. Metodyka TISM pozwala zbudować modułową i hierarchiczną Politykę Bezpieczeństwa Informacji. Wiodącym celem metodyki jest stworzenie konkretnej struktury zarządzania, czyli określenie ról zarządzających i kontrolnych, niezbędnych dla podtrzymania procesów ochrony informacji. • **Rekomendacja D** wydana przez GINB.

Źródło: opracowanie własne.

Tabela 7. Zakres wykonywanych czynności oraz zbiór możliwych do wykorzystania standardów na etapie zatwierdzania – faza zatwierdzania projektu zabezpieczeń

Etap	Zakres czynności	Wykorzystywane standardy
E8. Projekt zabezpieczeń	Projekt zabezpieczeń jest ostatecznym wynikiem działań przeprowadzanych w fazie projektowania, przeglądu i zatwierdzania. Zawiera: 1. Bazową Politykę Bezpieczeństwa (BPB), 2. Wyniki analizy ryzyka (Raport Analizy Ryzyka), 3. Listę procesów ochronnych dla procesów przetwarzania informacji wspierających krytyczne procesy biznesowe, 4. Dobór środków ochronnych (zwanych również mechanizmów bezpieczeństwa, zabezpieczeń) do procesów ochronnych.	• ISO/IEC-27002:2007: Technika informatyczna – Praktyczne zasady zarządzania bezpieczeństwem informacji. • PN-I-02000:2002 – Technika informatyczna – Zabezpieczenia w systemach informatycznych. • **Publikacje specjalne NIST** (National Institute of Standards and Technology) **serial SP-800-53:** Recommended Security Controls for Federal Information System. • **ISO/IEC 21827:2008,** Information technology – Security techniques -- Systems Security Engineering – Capability Maturity Model® (SSE-CMM®). • **ISO/IEC 18028–2:2006,** Information technology – Security techniques – IT network security – Part 2: Network security architecture. • **ISO/IEC 18028–3:2005,** Information technology – Security techniques -IT network security – Part 3: Securing communications between networks using security gateways. • **ISO/IEC 18028–5:2006,** Information technology – Security techniques – IT network security – Part 5: Securing communications across networks using virtual private networks. • **ISO/IEC 19772:2009,** Information technology – Security techniques – Authenticated encryption. • **ISO/IEC 24759:2008,** Information technology – Security techniques -- Test requirements for cryptographic modules. • **ISO/IEC TR 19791:2010,** Information technology – Security techniques – Security assessment of operational systems.

Źródło: opracowanie własne.

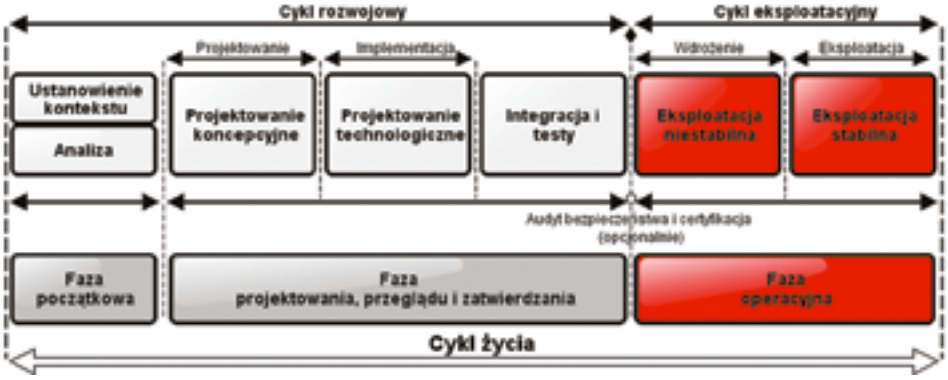
Tabela 8. Zakres wykonywanych czynności oraz zbiór możliwych do wykorzystania standardów na etapie zatwierdzania – faza zatwierdzania projektu zabezpieczeń

Etap	Zakres czynności	Wykorzystywane standardy
E8. Projekt zabezpieczeń	Projekt zabezpieczeń jest ostatecznym wynikiem działań przeprowadzanych w fazie projektowania, przeglądu i zatwierdzania. Zawiera: 5. Bazową Politykę Bezpieczeństwa (BPB), 6. Wyniki analizy ryzyka (Raport Analizy Ryzyka), 7. Listę procesów ochronnych dla procesów przetwarzania informacji wspierających krytyczne procesy biznesowe, 8. Dobór środków ochronnych (zwanych również mechanizmów bezpieczeństwa, zabezpieczeń) do procesów ochronnych.	• ISO/IEC-27002:2007: Technika informatyczna – Praktyczne zasady zarządzania bezpieczeństwem informacji. • PN-I-02000:2002 – Technika informatyczna – Zabezpieczenia w systemach informatycznych. • **Publikacje specjalne NIST (***National Institute of Standards and Technology)* **serii 800** – Zalecenia zawarte **w SP-800-53:** Recommended Security Controls for Federal Information System. • **ISO/IEC 21827:2008,** Information technology – Security techniques – Systems Security Engineering – Capability Maturity Model® (SSE-CMM®). • **ISO/IEC 18028–2:2006,** Information technology – Security techniques – IT network security – Part 2: Network security architecture. • **ISO/IEC 18028–3:2005,** Information technology – Security techniques – IT network security – Part 3: Securing communications between networks using security gateways. • **ISO/IEC 18028–5:2006,** Information technology – Security techniques – IT network security – Part 5: Securing communications across networks using virtual private networks. • **ISO/IEC 19772:2009,** Information technology – Security techniques -- Authenticated encryption. • **ISO/IEC 24759:2008,** Information technology – Security techniques -- Test requirements for cryptographic modules. • **ISO/IEC TR 19791:2010,** Information technology – Security techniques – Security assessment of operational systems.

Źródło: opracowanie własne.

3.5. Faza operacyjna – eksploatacji

Umiejscowienie fazy eksploatacji w modelu cyklu życia systemu zabezpieczeń ilustruje rysunek 7.



Rysunek 7. Umiejscowienie fazy początkowej w modelu cyklu życia systemu zabezpieczeń

Źródło: opracowanie własne.

Tabela 9. Zakres wykonywanych czynności oraz zbiór możliwych do wykorzystania standardów na etapie eksploatacji – faza operacyjna

Etap	Zakres czynności	Wykorzystywane standardy
Faza operacyjna – eksploatacji	**I. Wytwarzanie**: 1. Instalacja sprzętu i oprogramowania w systemie informacyjnym oraz systemów ochrony fizycznej i technicznej 2. Rekonfiguracja sieci/ systemów na potrzeby systemu zabezpieczeń 3. Spisanie polityki, planu i procedur bezpieczeństwa teleinformatycznego 4. Opracowanie planów **zapewniania ciągłości działania** 5. Wdrożenie SZ i szkolenia	• **PN-EN ISO 22301:2014–11** Bezpieczeństwo społeczne – Systemy zarządzania ciągłością działania – Wymagania (określa wymogi wobec systemu zarządzania w celu zapobiegania incydentom zakłócającym pracę). • **ISO/IEC 27031** – międzynarodowa norma opisująca koncepcje i zasady gotowości teleinformatyki (Information and Communication Technology, ICT) do zapewnienia ciągłości biznesu. Zapewnia ramy metod i procesów do zidentyfikowania i określenia wszystkich aspektów udoskonalania gotowości ICT organizacji do zapewnienia ciągłości biznesowej. Zakres ISO/IEC 27031:2011 obejmuje wszystkie zdarzenia i incydenty (łącznie z tymi, które są związane z bezpieczeństwem), które mogłyby mieć wpływ na infrastrukturę i systemy ICT.

Etap	Zakres czynności	Wykorzystywane standardy
Faza operacyjna – eksploatacji	**II. Testowanie:** 1. **Audyt** bezpieczeństwa lub 2. Ocena na zgodność z ustalonym standardem lub 3. Testy penetracyjne **III. Eksploatacja:** 1. Nadzór i kontrola w zakresie bezpieczeństwa (w tym audyty wewnętrzne i różnicowa analiza ryzyka) 2. Likwidacja lub bezpieczeństwa 3. Szkolenie podstawowe 4. Przeglądy i aktualizacje dokumentacji bezpieczeństwa 5. Testowanie planów zapewniania ciągłości działania.	• **Inne** normy związane z zarządzaniem ciągłością działania to **ISO/IEC 24762, ISO 22313 i załącznik A do ISO/ IEC 27002** oraz standardy **i przepisy dotyczące zarządzania kryzysowego**. • **Audyt zgodności z wymogami prawa**: (Ustawa o Ochronie Danych Osobowych oraz Ustawa o Ochronie Informacji Niejawnych, Sarbanes-Oxley Act (w zakresie mającym odniesienie do bezpieczeństwa systemów IT)). • **Audyt informatyczny** zgodności z zewnętrznymi lub wewnętrznymi regulacjami: • normy dotyczące zarządzania procesami IT (ISO/IEC 20000, COBIT), • bezpieczeństwem informatycznym (ISO/IEC 27001, PCI DSS, FIPS. • 6**. ISO / IEC TR 27008:2011** Technika informatyczna – Techniki bezpieczeństwa – Wytyczne dla audytorów informatycznych systemów zarządzania kontroli bezpieczeństwa

Źródło: opracowanie własne.

5. Podsumowanie

Podsumowując przedstawione rozważania z zakresu standardów możliwych do wykorzystania w procesie projektowania mechanizmów bezpieczeństwa, można stwierdzić, co następuje:

1. Standard należy rozumieć różnie, jako: „wzorzec prawidłowego wykonania jakiejś czynności", „określone wymagania stawiane obiektowi procesowi, systemowi", „reguły, zasady, praktyki postępowania" w celu zwiększenia bezpieczeństwa informacji".
2. Projektowanie mechanizmów bezpieczeństwa jest szczególnym rodzajem przedsięwzięcia i oznacza złożone działanie, wielopodmiotowe, przeprowadzone na podstawie: Wyników analizy ryzyka i planu postępowania z ryzykiem, Zatwierdzonej specyfikacji wymagań bezpieczeństwa, Bazowej polityki bezpieczeństwa.

Przykładowy dobór mechanizmów bezpieczeństwa do procesów ochronnych przedstawiono w tabeli 10, zaś skład dokumentacji w tabeli 11.

Tabela 10. Przykładowy dobór mechanizmów bezpieczeństwa do procesów ochronnych

Rodzaj zabezpieczenia (jest to minimum etapu projektowania) Procesy ochronne	Organizacyjne	Programowe	Sieciowe	Techniczne	Fizyczne
Uwierzytelniania: • w systemach dostępu logicznego do systemu informatycznego • w systemach dostępu fizycznego do obiektów systemu informacyjnego • danych	X[9] X X	X X		X	X
Autoryzacji: • Osób • Procesów	X X	X X	X	X X	X X
Zapewniania integralności: • Systemu • Informacji	X X	X X	X		
Wykrywania: • Zagrożeń • Podatności • Nieuprawnionych działań	X X X		X X X		X X X
Utajniania informacji	X	X	X	X	X

Źródło: opracowanie własne.

3. Ze względu na specyficzny sposób realizacji fazy początkowej i fazy projektowania, można zaryzykować stwierdzenie, że są one sterowane analizą ryzyka. Implikuje to między innymi posiadanie odpowiednich kwalifikacji przez zespół projektujący system zabezpieczeń – wiedza i doświadczenie z zakresu inżynierii bezpieczeństwa, oprogramowania i/lub inżynierii systemów mogą być w takim przedsięwzięciu niewystarczające.
4. Wybór konkretnego standardu zależy od poziomu dojrzałości Zespołu Projektującego i służb bezpieczeństwa.
5. Stosowanie standardów w całym cyklu życia systemu zabezpieczeń zdecydowanie podnosi jakość procesów i ich rezultatów wchodzących w skład cyklu rozwojowego (analiza, projektowanie, scalanie i testowanie) systemu zabezpieczeń, lecz nie gwarantuje wytworzenia kompleksowego i skutecznego systemu bezpieczeństwa informacji.

[9] X – liczba mechanizmów bezpieczeństwa danego rodzaju dla danego procesu ochronnego lub atrybutu bezpieczeństwa, np. 3.

Tabela 11. Przykładowy wykaz elementów dokumentacji bezpieczeństwa na tle wyróżnionych etapów cyklu życia systemu zabezpieczeń

Etap	Podstawowe czynności	Wytwarzane dokumenty – minimum
Etap Analizy	1. Inwentaryzacja zasobów 2. Identyfikacja kluczowych procesów biznesowych 3. Identyfikacja zagrożeń 4. Identyfikacja podatności 5. Określenie wymaganego poziomu ochrony dla każdego podstawowego atrybutu bezpieczeństwa informacji 6. Identyfikacja ograniczeń	1. Lista kluczowych procesów biznesowych i wspierających je procesów przetwarzania informacji 2. Spis inwentaryzacyjny zasobów informacyjnych 3. Lista zagrożeń wraz z identyfikacją ich typów i źródeł 4. Lista podatności w odniesieniu do aktywów, zagrożeń i zabezpieczeń; lista podatności, które nie odnoszą się do żadnego zidentyfikowanego zagrożenia, dla celów przeglądu 5. Lista ryzyk z priorytetami zgodnymi z kryteriami oceny ryzyka, w odniesieniu do scenariuszy incydentów, powodujących te ryzyka
Etap Projektowania	1. Projektowanie struktur i procedur organizacyjnych 2. Opracowanie strategii zabezpieczeń 3. Analiza ryzyka 4. Dobór technicznych, programowych i sieciowych środków ochronnych (mechanizmów bezpieczeństwa) 5. Projektowanie sposobu zastosowania zabezpieczeń (projekt architektury systemu zabezpieczeń) 6. Ocena ryzyka szczątkowego	1. Wyniki analizy ryzyka 2. Plan postępowania z ryzykiem i ryzyka szczątkowe będące przedmiotem decyzji kierownictwa organizacji o akceptacji 3. Wymagania bezpieczeństwa 4. Lista zaakceptowanych ryzyk wraz z uzasadnieniem dla tych, które nie spełniają normalnych dla organizacji kryteriów akceptowania ryzyka 5. Projekty rozwiązań 6. Bazowa Polityka Bezpieczeństwa 7. Projekt systemu zabezpieczeń
Etapy Zapewniania Jakości	**REZULTATY** 1. Uzgodnione kryteria oceny 2. Formalna akceptacja wyników 3. Formalna akceptacja ryzyka szczątkowego 4. Formalna akceptacja wyników i dokumentów fazy projektowania	**STANDARDY** 1. ISO/IEC 9001:2010 System zarządzania jakością, TQM. 2. Deklaracja w sprawie etyki zawodowej statystyków przyjęta przez Międzynarodowy Instytut Statystyczny 3. Podstawowe zasady statystyki oficjalnej przyjęte przez Komisję Statystyczną ONZ 4. Deklaracja Jakości Europejskiego Systemu Statystycznego 5. Europejski Kodeks Praktyk Statystycznych

Źródło: opracowanie własne.

6. Liczba przydatnych standardów: Faza początkowa – ponad 20, Faza projektowania, przeglądu zatwierdzania – ponad 30, Faza operacyjna (wdrażania i eksploatacji) – 10.
7. Standardy umożliwiają: kontrole zgodności z obowiązującymi przepisami prawa, zwiększenie wiarygodności oraz zaufania klientów, których dane są przetwarzane, „lepszą" identyfikację zagrożeń i ocenienie podatności w celu zminimalizowania strat i realizacji celów biznesowych, poprawę konkurencyjności i wizerunku, skuteczniejszą ochronę przed wyciekiem informacji.

Bibliografia

Brookshire D., *AV Diversification, Next Generation Network Defense*, SANS Institute 2004.

DISA, Infrastructure Security Technical Implementation Guide, stig PDF, ePub eBook, 10 May 2016.

ISO / IEC 27002: 2013 Technika informatyczna – Techniki bezpieczeństwa – Kodeks postępowania w zakresie kontroli bezpieczeństwa informacji.

ISO / IEC 27004: 2009 Technika informatyczna – Techniki zabezpieczeń – Zarządzanie bezpieczeństwem informacji – Pomiary.

NSA, *Defense in Depth – A practical strategy for achieving Information Assurance in today'shighly networked environments*, NSA 2000.

PN ISO/IEC 15408–3: 2002 Kryteria oceny zabezpieczenia systemów. Wymagania uzasadnienia pewności.

Stoneburner G., Hayden C., Feringa A., *Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A*, Series/Number: NIST Special Publication 800–27 Rev A (2004).

Źródła sieciowe

http://www.iso27000.pl/ (dostęp: 23.06.2016).

http://www.immusec.com/ (dostęp: 23.06.2016).

https://www.nist.gov/publications (dostęp: 23.06.2016).

* * *

Safety Standards in the Life Cycle of the Security System Concerning the Information System in an Organization

Summary

This paper presents the principles and good practice of the system design concerning the security of the information system in an organization. For this purpose, a review was conducted concerning the guidelines, norms and standards of the system design safeguards against the model of the life cycle of the system security. It was stressed that the design standards of security organizations are clearly defined milestones, fixing the next steps of the process of preparation, planning, analysis, design, implementation and monitoring. In addition, the article stressed that maintaining a high level of security and the proper functioning of the enterprise information system requires the creation of appropriate organizational infrastructure and substantive preparation of the management team.

Keywords: safety, security standards, security mechanism, security.