

Nazwa standardu	Symbol	Wersja	Data wydania
<b>Przewodnik do opracowywania planów bezpieczeństwa systemów informatycznych w podmiotach publicznych</b>	NSC 800-18	1.0	15/02/2022

# Przewodnik do opracowywania planów bezpieczeństwa systemów informatycznych w podmiotach publicznych



**Szanowni Państwo,**

Departament Cyberbezpieczeństwa Kancelarii Prezesa Rady Ministrów udostępnia do wykorzystania w Państwa działalności zestaw publikacji specjalnych. Stanowią one rekomendację w postaci Narodowych Standardów Cyberbezpieczeństwa, o których mowa w kierunku interwencji 6.1 celu szczegółowego 2 Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019 – 2024, *Opracowanie i wdrożenie Narodowych Standardów Cyberbezpieczeństwa oraz promowanie dobrych praktyk i zaleceń*. Mimo, że prezentowane standardy zostały opracowane na podstawie publikacji amerykańskiego National Institute of Science and Technology (NIST), to posiadają one mapowanie na obowiązujące w polskim systemie prawnym Polskie Normy, stosowane w zarządzaniu bezpieczeństwem informacji przez podmioty krajowego systemu cyberbezpieczeństwa, w tym podmioty realizujące zadania publiczne, operatorów usług kluczowych i dostawców usług cyfrowych.

Zaprezentowane publikacje stanowią przewodniki metodyczne, które ułatwiają zbudowanie efektywnego systemu zarządzania bezpieczeństwem informacji w oparciu o praktykę, jaka w tym zakresie stosowana jest w administracji federalnej USA.

Na prezentowany zestaw publikacji składają się następujące pozycje<sup>1</sup>:

- NSC<sup>2</sup> 199, *Standardy kategoryzacji bezpieczeństwa* – na podstawie FIPS 199;
- NSC 200, *Minimalne wymagania bezpieczeństwa informacji i systemów informatycznych podmiotów publicznych* – na podstawie FIPS 200;
- NSC 500-92, *Architektura referencyjna chmury obliczeniowej – rekomendacje* – na podstawie NIST SP 500-292;
- NSC 800-18, *Przewodnik do opracowywania planów bezpieczeństwa systemów informatycznych w podmiotach publicznych* – na podstawie NIST SP 800-18;

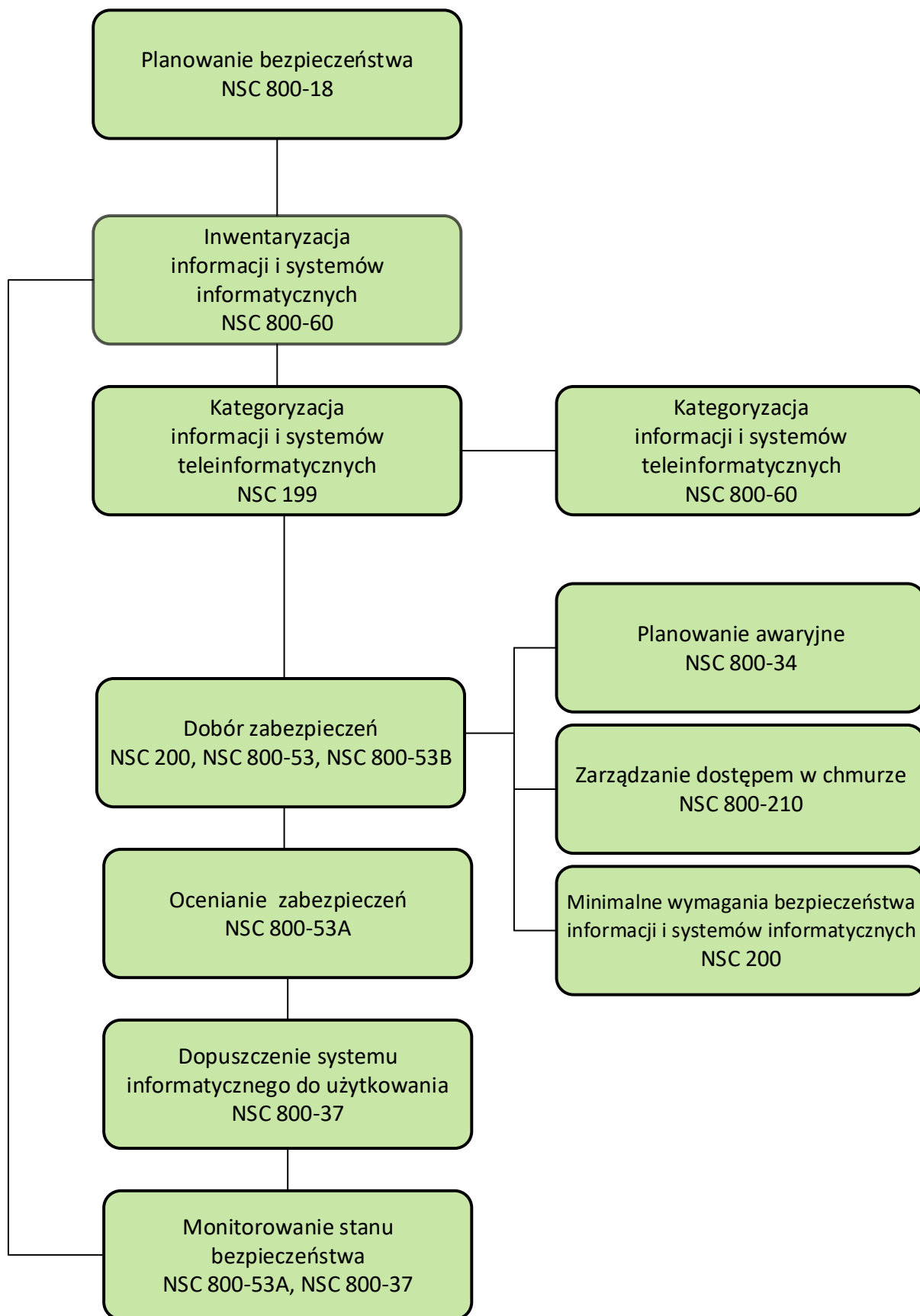
<sup>1</sup> Wymienione są podstawowe dokumenty. Każdy z nich może się odwoływać w rozdziale *Referencje* do szeregu powiązanych publikacji, które składają się na całościowy proces osiągnięcia cyberbezpieczeństwa.

<sup>2</sup> NSC – Narodowy Standard Cyberbezpieczeństwa.

- NSC 800-30, *Przewodnik dotyczący postępowania w zakresie szacowania ryzyka w podmiotach realizujących zadania publiczne* – na podstawie NIST SP 800-30;
- NSC 800-34, *Poradnik planowania awaryjnego* – na podstawie NIST SP 800-34;
- NSC 800-37, *Ramy zarządzania ryzykiem w organizacjach i systemach informatycznych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu* – na podstawie NIST SP 800-37;
- NSC 800-53, *Zabezpieczenia i ochrona prywatności systemów informatycznych oraz organizacji* – na podstawie NIST SP 800-53;
- NSC 800-53A, *Ocenianie środków bezpieczeństwa i ochrony prywatności systemów informatycznych oraz organizacji. Tworzenie skutecznych planów oceny* – na podstawie NIST SP 800-53A;
- NSC 800-53B, *Zabezpieczenia bazowe systemów informatycznych oraz organizacji* – na podstawie NIST SP 800-53B;
- NSC 800-60, *Wytyczne w zakresie określania kategorii bezpieczeństwa informacji i kategorii bezpieczeństwa systemu informatycznego* – na podstawie NIST SP 800-60;
- NSC 800-61, *Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego* – na podstawie NIST SP 800-61;
- NSC 800-210, *Ogólne wytyczne dotyczące kontroli dostępu do systemów chmury obliczeniowej* – na podstawie NIST SP 800-210.

Korzystając z tych publikacji można stosunkowo łatwo zbudować system zarządzania bezpieczeństwem informacji i sprawować nad nim niezbędną kontrolę.

Cykl zarządzania bezpieczeństwem bazujący na publikacjach NIST wykorzystuje następujące dokumenty:



## WSPÓLNE FUNDAMENTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI

National Institute of Standards and Technology (NIST) opracował wiele standardów i wytycznych w celu zapewnienia wspólnego podejścia do problematyki bezpieczeństwa informacji i systemów teleinformatycznych administracji federalnej USA. Podstawową rolę w podejściu do zagadnień związanych z zapewnieniem bezpieczeństwa informacji, bezpieczeństwa systemów teleinformatycznych oraz ochrony prywatności odgrywa elastyczny i spójny sposób zarządzania ryzykiem związanym z bezpieczeństwem i prywatnością operacji organizacyjnych i majątku, osób fizycznych, innych organizacji i Państwa. Zarządzanie ryzykiem stanowi podstawę do wdrożenia stosownych zabezpieczeń w systemach informatycznych, ocenę tych zabezpieczeń, wzajemną akceptację dowodów oceny bezpieczeństwa i ochrony prywatności oraz decyzji autoryzacyjnych, a także dzięki jednolitemu podejściu, ułatwia wymianę informacji i współpracę pomiędzy różnymi podmiotami.

NIST kontynuuje współpracę z sektorem publicznymi i prywatnym w celu stworzenia map i relacji pomiędzy opracowanymi przez siebie standardami i wytycznymi, a tymi, które zostały opracowane przez inne organizacje (np. ISO), co zapewnia zgodność w przypadku, gdy regulacje wymagają stosowania innych standardów.

Publikacje NIST, co do zasady, nie są objęte restrykcjami wynikającymi z autorskich praw majątkowych. Są powszechnie dostępne oraz dozwolone do użytku poza administracją federalną USA. Charakteryzują się pragmatycznym podejściem do zagadnień związanych z bezpieczeństwem informacji, systemów teleinformatycznych oraz ochrony prywatności, przez co ułatwiają podmiotom opracowanie i eksploatację systemu zarządzania tym bezpieczeństwem.

Biorąc pod uwagę wszystkie powyższe aspekty, autorzy niniejszej publikacji polecają opracowania NIST, jako godne zaufania i rekomendują stosowanie ich przez polskie podmioty w opracowywaniu systemów zarządzania bezpieczeństwem informacji, wdrażaniu zabezpieczeń i ocenie ich działania.

Podmioty, urządzenia lub materiały prezentowane są w niniejszym dokumencie w celu odpowiedniego opisanie procedury lub koncepcji eksperymentalnej. Identyfikacja taka nie ma na celu nakłaniania do nich lub ich poparcia, nie ma też na celu sugerowania, że te podmioty, materiały lub sprzęt są najlepsze z dostępnych w tym obszarze.

W niniejszym Narodowym Standardzie Cyberbezpieczeństwa mogą znajdować się odniesienia do innych publikacji opracowywanych obecnie przez Pełnomocnika Rządu ds. Cyberbezpieczeństwa zgodnie z przypisanymi mu obowiązkami ustawowymi. Informacje zawarte w tej publikacji, w tym koncepcje, praktyki i metodologie, mogą być wykorzystywane przez organizacje jeszcze przed ukończeniem innych towarzyszących temu standardowi publikacji. W związku z tym, do czasu ukończenia każdej publikacji, obowiązują aktualne wymagania, wytyczne i procedury, jeśli takie istnieją. W celach planistycznych i wprowadzania zmian, organizacje będą mogły uważnie śledzić rozwój tych nowych publikacji opracowywanych przez Pełnomocnika Rządu ds. Cyberbezpieczeństwa.

Niniejsza publikacja, *Przewodnik do opracowywania planów bezpieczeństwa systemów informatycznych w podmiotach publicznych*, opracowana została za zgodą National Institute of Science and Technology (NIST) na podstawie specjalnej publikacji NIST SP 800-18 rev. 1.

Tam, gdzie to było możliwe i nie budziło kontrowersji, nazwy ról i kluczowych uczestników procesu zarządzania ryzykiem zostały podane w języku polskim. Pozostałe role i funkcje zostały przedstawione w języku angielskim. Do wszystkich tych ról/funkcji zastosowano akronimy terminologii angielskiej.

Terminologia angielska i akronimy występujące w publikacji zdefiniowane są w dokumencie NSC 7298, *Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa*.

## SPIS TREŚCI

<b>PODSUMOWANIE ZARZĄDCZE .....</b>	<b>10</b>
<b>1. WPROWADZENIE .....</b>	<b>12</b>
1.1. TŁO.....	12
1.2. GRUPA DOCELOWA .....	13
1.3. STRUKTURA DOKUMENTU .....	13
1.4. INWENTARYZACJA SYSTEMÓW I STANDARDY PRZETWARZANIA INFORMACJI (NSC 199).....	14
1.5. GŁÓWNE APLIKACJE, OGÓLNE SYSTEMY WSPARCIA I DROBNE APLIKACJE.....	14
1.6. INNE POWIĄZANE PUBLIKACJE NSC.....	15
1.7. ROLE I OBOWIĄZKI W PLANIE BEZPIECZEŃSTWA SYSTEMU .....	15
1.7.1. <i>Chief Information Officer – CIO .....</i>	<i>16</i>
1.7.2. <i>Właściciel systemu informatycznego - ISO .....</i>	<i>17</i>
1.7.3. <i>Właściciel informacji - IO.....</i>	<i>17</i>
1.7.4. <i>Senior Agency Information Security Officer - SAISO .....</i>	<i>18</i>
1.7.5. <i>Information System Security Officer – ISSO.....</i>	<i>18</i>
1.7.6. <i>Authorizing Official – AO .....</i>	<i>19</i>
1.8. ZASADY ZACHOWANIA.....	20
1.9. ZATWIERDZENIE PLANU BEZPIECZEŃSTWA SYSTEMU .....	21
<b>2. ANALIZA GRANIC SYSTEMU I DOBÓR ZABEZPIECZEŃ .....</b>	<b>22</b>
2.1. GRANICE SYSTEMU .....	22
2.2. GŁÓWNE APLIKACJE .....	25
2.3. SYSTEMY OGÓLNEGO WSPARCIA.....	26
2.4. APLIKACJE O MNIEJSZYM ZNACZENIU .....	27
2.5. ZABEZPIECZENIA .....	27
2.5.1. <i>Wskazówki dotyczące ustalania zakresu systemu.....</i>	<i>28</i>
2.5.2. <i>Zabezpieczenia kompensacyjne.....</i>	<i>31</i>
2.5.3. <i>Zabezpieczenia wspólne .....</i>	<i>31</i>
<b>3. BUDOWA PLANU .....</b>	<b>35</b>
3.1. NAZWA I IDENTYFIKATOR SYSTEMU .....	35
3.2. KATEGORYZACJA SYSTEMU .....	35
3.3. WŁAŚCICIEL SYSTEMU .....	37



---

3.4.	ORGAN ZATWIERDZAJĄCY .....	38
3.5.	WYZNACZANIE INNYCH KONTAKTÓW.....	38
3.6.	PRZYPISANIE ODPOWIEDZIALNOŚCI ZA BEZPIECZEŃSTWO .....	38
3.7.	STATUS OPERACYJNY SYSTEMU.....	39
3.8.	TYP SYSTEMU INFORMATYCZNEGO .....	39
3.9.	OGÓLNY OPIS/CEL.....	39
3.10.	ŚRODOWISKO SYSTEMOWE.....	40
3.11.	POŁĄCZENIA SYSTEMU / WYMIANA INFORMACJI .....	41
3.12.	PRZEPISY, REGULACJE I ZASADY DOTYCZĄCE SYSTEMU.....	42
3.13.	DOBÓR ZABEZPIECZEŃ .....	42
3.14.	ZABEZPIECZENIA MINIMALNE .....	43
3.15.	TERMINY UKOŃCZENIA I ZATWIERDZENIA.....	46
3.16.	BIEŻĄCA KONSERWACJA PLANU BEZPIECZEŃSTWA SYSTEMU .....	46
<b>ZAŁĄCZNIK A PRZYKŁADOWY WZÓR PLANU BEZPIECZEŃSTWA SYSTEMU INFORMATYCZNEGO .....</b>		<b>48</b>
<b>ZAŁĄCZNIK B SŁOWNIK I AKRONIMY .....</b>		<b>53</b>

---

## PODSUMOWANIE ZARZĄDCZE

Celem planowania bezpieczeństwa systemu teleinformatycznego jest poprawa ochrony zasobów tego systemu. Wszystkie systemy podmiotów publicznych mają pewien poziom wrażliwości i wymagają ochrony w ramach dobrej praktyki zarządzania. Ochrona systemu musi być udokumentowana w planie bezpieczeństwa systemu. Opracowanie planów bezpieczeństwa systemu jest wymagana przepisem § 20 *rozporządzenia 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*.

Celem planu bezpieczeństwa systemu jest przedstawienie przeglądu wymagań bezpieczeństwa systemu i opisanie zabezpieczeń, które zostały wprowadzone lub zaplanowane do wprowadzenia w celu spełnienia tych wymagań. Plan bezpieczeństwa systemu określa również obowiązki i oczekiwane zachowanie wszystkich osób uzyskujących dostęp do systemu. Plan bezpieczeństwa systemu powinien być postrzegany jako dokumentacja ustrukturyzowanego procesu planowania odpowiedniej, kosztowo racjonalnej, ochrony bezpieczeństwa systemu. Powinien odzwierciedlać wkład różnych menedżerów odpowiedzialnych za system, w tym właścicieli informacji, właściciela systemu oraz *Senior Agency Information Security Officer - SAISO*<sup>3</sup>. Dodatkowe informacje mogą być zawarte w ogólnym planie bezpieczeństwa organizacji, w strukturze i formie przyjętymi zgodnie z potrzebami organizacji, o ile główne sekcje opisane w niniejszym dokumencie są odpowiednio ujęte i łatwe do zidentyfikowania.

W celu odpowiedniego odzwierciedlenia przez plany ochrony zasobów, właściwy członek kierownictwa organizacji musi upoważnić system do działania (*ang. authorize a system to operate*). Upoważnienie systemu do przetwarzania informacji, udzielona przez członka kierownictwa, zapewnia istotne zabezpieczenie organizacyjne. Autoryzując przetwarzanie w systemie, menedżer akceptuje związane z tym ryzyko.

---

<sup>3</sup> Terminologia angielska i akronimy występujące w publikacji zdefiniowane są w dokumencie NSC 7298, Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa.

Autoryzacja przez członka kierownictwa powinna opierać się na ocenie zabezpieczeń zarządczych, operacyjnych i technicznych. Ponieważ plan bezpieczeństwa systemu ustanawia i dokumentuje zabezpieczenia, powinien stanowić podstawę autoryzacji, uzupełniony raportem z oceny (audytu) bezpieczeństwa. Ponadto niezbędny jest okresowy przegląd zabezpieczeń na potrzeby przyszłych autoryzacji. Ponowna autoryzacja powinna nastąpić za każdym razem, gdy nastąpi znacząca zmiana w przetwarzaniu, ale nie rzadziej niż co trzy lata.

## 1. WPROWADZENIE

Dzisiejsze szybko zmieniające się środowisko techniczne wymaga od podmiotów publicznych przyjęcia minimalnego zestawu zabezpieczeń w celu ochrony swoich informacji i systemów informatycznych. Narodowy standard przetwarzania informacji NSC 200, określa minimalne wymagania bezpieczeństwa w siedemnastu obszarach związanych z bezpieczeństwem. Podmioty publiczne powinny spełniać minimalne wymagania bezpieczeństwa określone w NSC 200 poprzez zastosowanie zabezpieczeń znajdujących się w publikacji NSC 800-53. NSC 800-53 zawiera zabezpieczenia zarządcze, operacyjne i techniczne lub środki zaradcze przewidziane dla systemu informatycznego. Wybrane lub zaplanowane zabezpieczenia muszą być udokumentowane w planie bezpieczeństwa systemu. Niniejszy dokument zawiera wytyczne dla podmiotów publicznych dotyczące opracowywania planów bezpieczeństwa systemu dla publicznych systemów informatycznych.

### 1.1. TŁO

Przepis § 20 rozporządzenia 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 (dalej KRI) wymaga aby każdy podmiot publiczny opracował i ustanowił, wdrożył i eksploatował, monitorował i przeglądał oraz utrzymywał i doskonalił system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność. Planowanie bezpieczeństwa systemu jest ważnym działaniem wspierającym cykl życia systemu (*ang. System Development Life Cycle - SDLC*) i należy je ponawiać, ponieważ zdarzenia systemowe powodują konieczność rewizji planu w celu dokładnego odzwierciedlenia aktualnego stanu systemu. Plan bezpieczeństwa systemu zawiera podsumowanie wymagań bezpieczeństwa dla systemu informatycznego i opisuje zabezpieczenia wprowadzone lub planowane do wprowadzenia w celu spełnienia tych wymagań.

Plan może również odnosić się do innych kluczowych dokumentów związanych z bezpieczeństwem dla systemu informatycznego, takich jak ocena ryzyka, decyzja o akredytacji, ocena wpływu na prywatność, plan awaryjny, plan zarządzania konfiguracją, listy kontrolne konfiguracji bezpieczeństwa i umowy o połączeniu systemu stosownie do przypadku.

## 1.2. GRUPA DOCELOWA

Menedżerowie programów, właściciele systemów i personel ochrony w organizacji muszą zrozumieć proces planowania bezpieczeństwa systemu. Ponadto użytkownicy systemu informatycznego i osoby odpowiedzialne za określenie wymagań systemowych powinny zapoznać się z procesem planowania bezpieczeństwa systemu. Osoby odpowiedzialne za wdrażanie systemów informatycznych i zarządzanie nimi muszą brać udział w podejmowaniu decyzji o ustanowieniu zabezpieczeń, które mają być stosowane w ich systemach. Poradnik ten zawiera podstawowe informacje na temat przygotowania planu bezpieczeństwa systemu i został zaprojektowany w taki sposób, aby można go było zastosowywać w różnych strukturach organizacyjnych i był wykorzystywany jako odniesienie przez osoby odpowiedzialne za działania związane z planowaniem bezpieczeństwa.

## 1.3. STRUKTURA DOKUMENTU

Niniejsza publikacja przedstawia zestaw działań i koncepcji mających na celu opracowanie planu bezpieczeństwa systemu informatycznego. Oto krótki opis jej zawartości:

- **Rozdział 1** zawiera podstawowe informacje dotyczące procesu planowania bezpieczeństwa systemu, odbiorców docelowych, informacje na temat NSC 199, omówienie różnych kategorii systemów informatycznych, identyfikację powiązanych publikacji NSC oraz opis ról i obowiązków związanych z opracowywaniem planów bezpieczeństwa systemu.
- **Rozdział 2** omawia, w jaki sposób organizacje powinny analizować swoje wykazy systemów informatycznych w procesie ustalania granic systemu. Omówiono także identyfikację typowych zabezpieczeń i wskazówki dotyczące określania zakresu.

- **Rozdział 3** prowadzi czytelnika przez etapy opracowywania planu bezpieczeństwa systemu.
- **Załącznik A** zawiera szablon planu bezpieczeństwa systemu.
- **Załącznik B** zawiera słownik terminów i akronimów.

#### **1.4. INWENTARYZACJA SYSTEMÓW I STANDARDY PRZETWARZANIA INFORMACJI (NSC 199)**

KRI wymaga, aby podmioty publiczne posiadały inwentaryzację swoich systemów informatycznych. Wszystkie zainwentaryzowane systemy informacyjne powinny zostać skategoryzowane przy użyciu NSC 199 jako pierwszy krok w planowaniu bezpieczeństwa systemu.

NSC 199 jest zalecanym standardem do stosowania przez wszystkie podmioty publiczne w celu kategoryzacji wszystkich informacji i systemów informatycznych gromadzonych lub utrzymywanych przez każdy z tych podmiotów lub w jej imieniu, w oparciu o cele polegające na zapewnieniu odpowiedniego poziomu bezpieczeństwa informacji zgodnie z wpływem zakłócenia. Standardy kategoryzacji bezpieczeństwa systemów informatycznych zapewniają wspólne ramy i zrozumienie dla wyrażania bezpieczeństwa, które promują: (i) skuteczne zarządzanie bezpieczeństwem informacji i nadzór nad nim, w tym koordynację wysiłków w zakresie bezpieczeństwa informacji w całej sferze cywilnej, gotowości na wypadek awarii oraz (ii) spójne raportowanie do właściwych organów w sprawie adekwatności i skuteczności polityk, procedur i praktyk bezpieczeństwa informacji.

#### **1.5. GŁÓWNE APLIKACJE, OGÓLNE SYSTEMY WSPARCIA I DROBNE APLIKACJE**

Wszystkie systemy informatyczne muszą być objęte planem bezpieczeństwa systemu i skategoryzowane jako główna aplikacja lub ogólny system wsparcia. Szczegółowe plany bezpieczeństwa systemu dla mniejszych aplikacji nie są wymagane, ponieważ zabezpieczenia dla tych aplikacji są zazwyczaj zapewniane przez ogólny system wsparcia lub główną aplikację, w której działają. W przypadkach, gdy mniejsza aplikacja nie jest połączona

z główną aplikacją lub ogólnym systemem wsparcia, mniejsza aplikacja powinna zostać krótko opisana w ogólnym planie systemu wsparcia, który ma wspólną lokalizację fizyczną lub jest obsługiwany przez tę samą organizację. Dodatkowe informacje znajdują się w rozdziale 2.

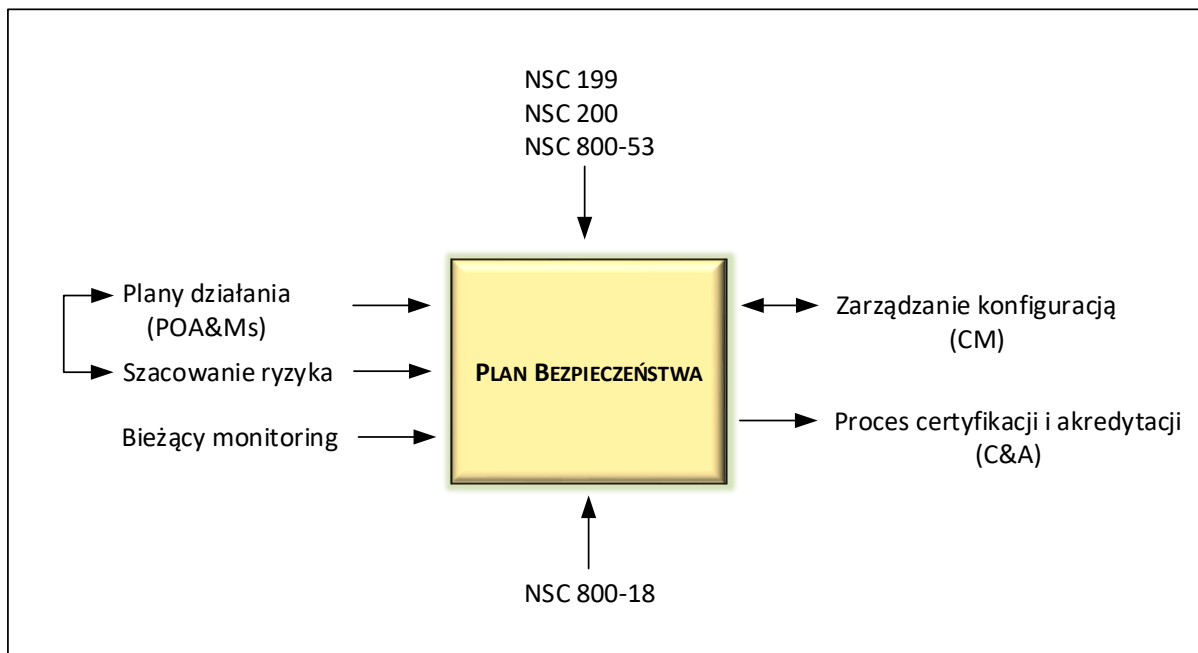
## **1.6. INNE POWIĄZANE PUBLIKACJE NSC**

W celu opracowania planu bezpieczeństwa systemu, należy zapoznać się ze standardami i wytycznymi bezpieczeństwa NSC. Niezbędne jest, aby użytkownicy niniejszej publikacji rozumieli wymagania i metodologię kategoryzacji systemu informatycznego opisane w NSC 199, a także wymagania dotyczące uwzględnienia minimalnych zabezpieczeń dla danego systemu, jak opisano w NSC 800-53 i NSC 200.

## **1.7. ROLE I OBOWIĄZKI W PLANIE BEZPIECZEŃSTWA SYSTEMU**

Podmioty publiczne powinny opracować zasady dotyczące procesu planowania bezpieczeństwa systemu. Plany bezpieczeństwa systemu to żywe dokumenty, które wymagają okresowego przeglądu, modyfikacji oraz planów działania w celu wdrożenia zabezpieczeń. Powinny istnieć procedury określające, kto dokonuje przeglądu planów, utrzymuje plan na bieżąco i monitoruje zaplanowane zabezpieczenia. Ponadto procedury powinny wymagać opracowania i przeglądu planów bezpieczeństwa systemu przed przystąpieniem do procesu certyfikacji bezpieczeństwa i akredytacji systemu.

Podczas procesu certyfikacji i akredytacji bezpieczeństwa plan bezpieczeństwa systemu jest analizowany, aktualizowany i akceptowany. Organ certyfikacji potwierdza, że zabezpieczenia opisane w planie bezpieczeństwa systemu są zgodne z kategorią bezpieczeństwa NSC 199, określoną dla systemu informatycznego oraz że identyfikacja zagrożeń i podatności oraz wstępne określenie ryzyka są zidentyfikowane i udokumentowane w planie bezpieczeństwa systemu, ocenie ryzyka lub równoważnym dokumencie. Wyniki certyfikacji bezpieczeństwa są wykorzystywane do ponownej oceny ryzyka, opracowania planu i etapów działania (POA&M), które są wymagane do śledzenia działań zaradczych i aktualizacji planu bezpieczeństwa systemu, zapewniając tym samym podstawę merytoryczną dla osoby autoryzującej do wydania decyzji o akredytacji bezpieczeństwa.



Rysunek 1. Proces planowania.

Role i obowiązki w tej sekcji dotyczą planowania bezpieczeństwa systemu informatycznego. Uznając, że podmioty publiczne mają bardzo różne misje i struktury organizacyjne, mogą występować różnice w konwencjach nazewnictwa dla ról związanych z planowaniem bezpieczeństwa oraz w sposobie podziału powiązanych obowiązków między personelem podmiotu (np. wiele osób pełniących jedną rolę lub jedna osoba pełniąc wiele ról<sup>4</sup>).

### 1.7.1. CHIEF INFORMATION OFFICER – CIO

**CIO** to kluczowa osoba w jednostce organizacyjnej odpowiedzialna za technologie informacyjne (z wyłączeniem informacji niejawnych w rozumieniu ustawy o ochronie informacji niejawnych), zwykle członek kierownictwa jednostki organizacyjnej i odpowiada za planowanie bezpieczeństwa systemu:

- wyznacza SAISO (*ang. senior agency information security officer*), który będzie realizował zadania CIO w zakresie planowania bezpieczeństwa systemu;

<sup>4</sup> Podmiot publiczny powinien zapewnić opisane role w ramach swojego regulaminu organizacyjnego, zapewniając rozdzielanie obowiązków pomiędzy stanowiskami pełniącymi role mogące być w konflikcie interesów.



- opracowuje i utrzymuje zasady bezpieczeństwa informacji, procedury i techniki zabezpieczeń w celu uwzględnienia planowania bezpieczeństwa systemu;
- zarządza identyfikacją, wdrażaniem i oceną ogólnych zabezpieczeń;
- zapewnia przeszkolenie personelu odpowiedzialnego za plany bezpieczeństwa systemu;
- pomaga kierownikom komórek organizacyjnych w organizacji w wypełnianiu ich planów bezpieczeństwa systemu;
- identyfikuje i koordynuje zabezpieczenia ogólne w organizacji.

### 1.7.2. WŁAŚCICIEL SYSTEMU INFORMATYCZNEGO - ISO

**Właściciel systemu informatycznego** (*ang. Information System Owner – ISO*) jest osobą w organizacji odpowiedzialną za zamówienia, rozwój, integrację, modyfikację lub obsługę i utrzymanie systemu informatycznego. Właściciel systemu informatycznego ma następujące obowiązki związane z planami bezpieczeństwa systemu:

- opracowuje plan bezpieczeństwa systemu w koordynacji z właścicielami informacji, administratorem systemu, ISSO, SAISO oraz użytkownikami końcowymi;
- utrzymuje plan bezpieczeństwa systemu i zapewnia, że system jest wdrażany i obsługiwany zgodnie z uzgodnionymi wymogami bezpieczeństwa;
- zapewnia, że użytkownicy systemu i personel pomocniczy zostaną odpowiednio przeszkoleni w zakresie bezpieczeństwa (np. zgodnie z instrukcją dotyczącą zasad zachowania);
- aktualizuje plan bezpieczeństwa systemu za każdym razem, gdy nastąpi znacząca zmiana;
- pomaga w identyfikacji, wdrażaniu i ocenie ogólnych zabezpieczeń.

### 1.7.3. WŁAŚCICIEL INFORMACJI - IO

**Właściciel informacji** (*ang. Information Owner - IO*) jest osobą w organizacji posiadającą uprawnienia ustawowe, zarządcze lub operacyjne w zakresie określonych informacji oraz jest

odpowiedzialny za ustanowienie polityki i procedur regulujących ich wytwarzanie, gromadzenie, przetwarzanie, rozpowszechnianie i usuwanie. Właściciel informacji ma następujące obowiązki związane z planami bezpieczeństwa systemu:

- ustanawia zasady właściwego wykorzystania i ochrony danych/informacji organizacji (zasady zachowania);
- dostarcza informacje właścicielom systemów informatycznych dotyczących wymagań bezpieczeństwa i zabezpieczeń systemów informatycznych, w których przetwarzane są informacje;
- decyduje, kto ma dostęp do systemu informatycznego oraz z jakiego rodzaju przywilejami lub prawami dostępu;
- pomaga w identyfikacji i ocenie ogólnych zabezpieczeń systemów, w których znajdują się informacje.

#### 1.7.4. SENIOR AGENCY INFORMATION SECURITY OFFICER - SAISO

**SAISO** jest osobą w organizacji odpowiedzialną za wspomaganie CIO w wykonywaniu jego obowiązków i pełniącym funkcję głównego łącznika CIO z osobami autoryzującymi, właścicielami systemów, dostawcami zabezpieczeń wspólnych i SSO.

SAISO ma następujące obowiązki związane z planami bezpieczeństwa systemu:

- realizuje zadania CIO w zakresie planowania bezpieczeństwa systemu;
- koordynuje opracowywanie, przegląd i akceptację planów bezpieczeństwa systemu z właścicielami systemów informatycznych, ISSO i AO;
- koordynuje identyfikację, wdrażanie i ocenę zabezpieczeń wspólnych.

SAISO posiada kwalifikacje zawodowe, w tym szkolenie i doświadczenie, wymagane do opracowania i przeglądu planów bezpieczeństwa systemu.

#### 1.7.5. INFORMATION SYSTEM SECURITY OFFICER – ISSO

**ISSO** to osoba w organizacji, której przypisano odpowiedzialność za zapewnienie utrzymania odpowiedniego poziomu bezpieczeństwa operacyjnego dla systemu informatycznego.

ISSO ma następujące obowiązki związane z planami bezpieczeństwa systemu:

- pomaga SAISO w identyfikacji, wdrażaniu i ocenie ogólnych zabezpieczeń;
- odgrywa aktywną rolę w opracowywaniu i aktualizowaniu planu bezpieczeństwa systemu, a także koordynowaniu z właścicielem systemu informatycznego wszelkich zmian w systemie i ocenie wpływu tych zmian na bezpieczeństwo.

#### 1.7.6. AUTHORIZING OFFICIAL – AO

**AO** to osoba lub komórka organizacyjna dokonująca autoryzacji (dalej: *osoba autoryzująca*) polegającej na dopuszczeniu systemu informatycznego do eksploatacji w jednostce organizacyjnej, w tym za dopuszczenie do stosowania zabezpieczeń wspólnych dla wielu systemów.

**AO** jest członkiem kierownictwa organizacji upoważnionym do formalnego przyjęcia odpowiedzialności za prowadzenie systemu informatycznego na akceptowalnym poziomie ryzyka w zakresie działalności organizacji, aktywów organizacji lub osób fizycznych. Osoba autoryzująca ma następujące obowiązki związane z planami bezpieczeństwa systemu:

- zatwierdza plany bezpieczeństwa systemu;
- autoryzuje działanie systemu informatycznego;
- wydaje tymczasowe upoważnienie do działania systemu informatycznego na określonych warunkach;
- odmawia wydania upoważnienia do działania systemu informatycznego (lub jeśli system już działa, przerywa działanie), jeśli istnieją niedopuszczalne ryzyka.

## 1.8. ZASADY ZACHOWANIA

Zasady zachowania stanowiące zabezpieczenia zawarte w NSC 800-53 powinny jasno określać obowiązki i oczekiwane zachowanie wszystkich osób mających dostęp do systemu. Reguły powinny określać konsekwencje niespójnego zachowania lub niezgodności i być udostępniane każdemu użytkownikowi przed otrzymaniem autoryzacji na dostęp do systemu. Wymagane jest, aby reguły zawierały stronę podpisu dla każdego użytkownika potwierdzającą otrzymanie, wskazującą, że przeczytał, zrozumiał i zgodził się przestrzegać zasad zachowania. Podpisy elektroniczne są dopuszczalne do stosowania w uznaniu zasad zachowania.

Na rysunku 2 przedstawiono przykłady, co należy objąć typowymi zasadami postępowania. Organizacje mają elastyczność w zakresie szczegółów i treści zasad zachowania. Opracowując reguły zachowania, należy pamiętać, że celem jest uczynienie wszystkich użytkowników odpowiedzialnymi za swoje działania, potwierdzając, że przeczytali, rozumieli i zgadzają się przestrzegać zasad zachowania. Reguły nie powinny być kompletną kopią przewodnika dotyczącego polityki bezpieczeństwa lub procedur, ale powinny obejmować, na wysokim poziomie, niektóre elementy zabezpieczeń opisane na poniższym przykładzie.

### Przykłady zabezpieczeń zawartych w zasadach zachowania

- Określ obowiązki, oczekiwane sposoby wykorzystanie systemu i zachowanie wszystkich użytkowników.
- Opisz odpowiednie limity połączeń wzajemnych.
- Zdefiniuj świadczone usługi i priorytety ich przywracania.
- Opisz konsekwencje zachowania niezgodnego z zasadami.
- Obejmij zasadami następujące zagadnienia:
  - praca w domu;
  - dostęp telefoniczny;
  - połączenie z Internetem;
  - wykorzystanie dzieła chronionego prawem autorskim;
  - nieoficjalne użycie sprzętu służbowego;
  - przypisanie i ograniczenia uprawnień systemowych oraz indywidualnej odpowiedzialności;
  - użycie hasła;
  - przeszukiwanie baz danych i ujawnianie informacji.

*Rysunek 2. Przykład zasad zachowania.*

## 1.9. ZATWIERDZENIE PLANU BEZPIECZEŃSTWA SYSTEMU

Zasady organizacyjne powinny jasno określać, kto jest odpowiedzialny za zatwierdzenie planu bezpieczeństwa systemu i opracowane procedury przedkładane wraz z planem lub inną dokumentacją wymaganą przez organizację. Przed procesem certyfikacji i akredytacji plan zatwierdza wyznaczona osoba autoryzująca, niezależna od właściciela systemu.

## 2. ANALIZA GRANIC SYSTEMU I DOBÓR ZABEZPIECZEŃ

Przed opracowaniem planu bezpieczeństwa systemu, system informatyczny i informacje znajdujące się w tym systemie muszą zostać skategoryzowane na podstawie analizy wpływu zakłócenia zgodnie z NSC 199. Następnie można ustalić, które systemy w inwentarzu można logicznie pogrupować w główne aplikacje lub ogólne systemy wsparcia. Poziomy wpływ NSC 199 należy wziąć pod uwagę podczas określania granic systemu i przy wyborze początkowego zestawu zabezpieczeń. Wyjściowe zabezpieczenia można następnie dostosować na podstawie oceny ryzyka i warunków lokalnych, w tym wymagań bezpieczeństwa specyficznych dla organizacji, szczegółowych informacji o zagrożeniach, analiz kosztów i korzyści, dostępności zabezpieczeń kompensacyjnych lub szczególnych okoliczności. Przed opracowaniem planu bezpieczeństwa systemu należy zidentyfikować zabezpieczenia wspólne, które są jednym z aspektów dostosowywania, aby zidentyfikować i uwzględnić zabezpieczenia poczynione na poziomie organizacji (np. zabezpieczenia fizyczne i środowiskowe), które nie są specyficzne dla systemu. Zabezpieczenia wspólne można następnie włączyć do planu bezpieczeństwa systemu przez odniesienie się do nich.

### 2.1. GRANICE SYSTEMU

Proces jednoznacznego przypisywania zasobów informatycznych do systemu informatycznego określa granicę bezpieczeństwa dla tego systemu. Organizacje mają dużą elastyczność w określaniu, co stanowi system informatyczny (tj. główne zastosowanie lub ogólny system wsparcia). Jeżeli zbiór zasobów informatycznych zostanie zidentyfikowany jako system informatyczny, zasoby powinny zasadniczo podlegać temu samemu zarządzaniu<sup>5</sup>. Zarządzanie takie niekoniecznie oznacza, że nie ma interweniowania w tak rozumiane zarządzanie.

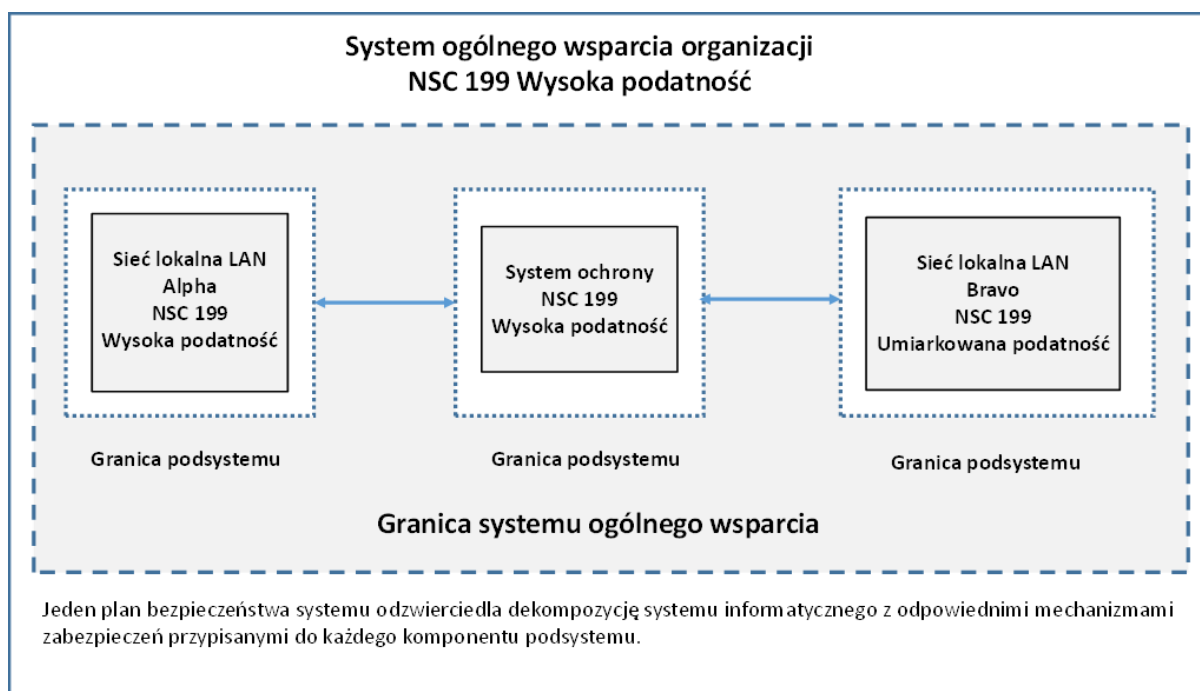
---

<sup>5</sup> Bezpośrednie zarządzanie zwykle obejmuje władzę budżetową, programową lub operacyjną oraz związaną z tym odpowiedzialność. W przypadku nowych systemów informatycznych zarządzanie można interpretować jako posiadanie władzy budżetowej / programowej i odpowiedzialności za rozwój i wdrażanie systemów informatycznych. W przypadku systemów informatycznych znajdujących się obecnie w eksploatacji zarządzanie można interpretować jako posiadanie uprawnień budżetowych / operacyjnych do codziennych operacji i utrzymania systemów informatycznych.

Możliwe jest również, że system informatyczny zawiera wiele podsystemów. Podsystem jest głównym podziałem lub komponentem systemu informatycznego składającym się z informacji, technologii informatycznej i personelu wykonującego jedną lub więcej określonych funkcji. Podsystemy zazwyczaj podlegają temu samemu organowi zarządzającemu i są objęte jednym planem bezpieczeństwa systemu. Rysunek 3 przedstawia przykład ogólnego systemu wsparcia z trzema podsystemami.

Oprócz rozważania bezpośredniego zarządzania pomocne może być rozważenie przez organizację, czy zasoby informacyjne zostały określone jako system informatyczny:

- mają ten sam cel funkcji lub misji i zasadniczo te same cechy operacyjne i potrzeby w zakresie bezpieczeństwa;
- funkcjonują w tym samym ogólnym środowisku operacyjnym (lub w przypadku rozproszonego systemu informacyjnego, funkcjonują w różnych lokalizacjach o podobnych środowiskach operacyjnych).



Rysunek 3. Dekompozycja dużych i złożonych systemów informatycznych (przykład).

Chociaż powyższe rozważania mogą być przydatne dla organizacji przy ustalaniu granic systemu informatycznego do celów akredytacji bezpieczeństwa, nie należy ich postrzegać

jako ograniczających elastyczność organizacji w ustalaniu granic promujących skuteczne bezpieczeństwo informacji w ramach dostępnych zasobów. Osoby autoryzujące i SAISO powinni konsultować się z potencjalnymi właścicielami systemów informatycznych przy ustalaniu granic systemu informatycznego. Proces ustanawiania granic dla systemów informatycznych organizacji i związanych z tym konsekwencji dla bezpieczeństwa jest działaniem na poziomie organizacji, które powinno obejmować staranne negocjacje między wszystkimi kluczowymi uczestnikami - biorąc pod uwagę wymagania biznesowe organizacji, względy techniczne w odniesieniu do bezpieczeństwa informacji i koszty wdrożenia.

NSC 199 definiuje kategorie bezpieczeństwa dla systemów informatycznych w oparciu o potencjalny wpływ na organizację, aktywa lub osoby w przypadku naruszenia bezpieczeństwa - to znaczy utraty poufności, integralności lub dostępności. Kategorie bezpieczeństwa NSC 199 odgrywają ważną rolę w określaniu granic systemów informatycznych poprzez podział systemów informatycznych organizacji w zależności od ich krytyczności lub wrażliwości oraz znaczenia tych systemów w realizacji celu działania organizacji. Jest to szczególnie ważne, gdy w jednym systemie informatycznym występują różne poziomy wpływu NSC 199. Wymóg NSC 199 dotyczący zabezpieczenia systemu informatycznego do najwyższego poziomu wpływu i musi być zastosowany podczas grupowania mniejszych aplikacji/podsystemów o różnych poziomach oddziaływania NSC 199 w jednym ogólnym systemie wsparcia lub dużej aplikacji, chyba że istnieje odpowiednia ochrona granic, np. zapory sieciowe i szyfrowanie wokół podsystemów lub aplikacji o najwyższym poziomie wpływu. Ponadto należy zapewnić, że zasoby współdzielone, tj. sieci, komunikacja i fizyczny dostęp w ramach całego ogólnego systemu wsparcia lub głównej aplikacji, są odpowiednio chronione, aby zapewnić ochronę dla najwyższego poziomu wpływu. Możliwość izolowania systemów o dużym wpływie nie tylko zapewni bardziej bezpieczne systemy, ale także zmniejszy ilość zasobów wymaganych do zabezpieczenia wielu aplikacji/systemów, które nie wymagają takiego poziomu bezpieczeństwa. NSC 800-53 zapewnia trzy podstawowe poziomy zabezpieczeń, tj. niski, umiarkowany i wysoki, które są powiązane z trzema poziomami wpływu NSC 199; wraz ze wzrostem poziomu wpływu zwiększają się również minimalne wymagania w zakresie zaufania do zabezpieczenia.



W sytuacji, gdy w systemie informatycznym występują różne poziomy wpływu NSC 199, system ten jest klasyfikowany według najwyższego poziomu wpływu.

## 2.2. GŁÓWNE APLIKACJE

Wszystkie aplikacje podmiotów realizujących zadania publiczne mają wartość i wymagają określonego poziomu ochrony. Niektóre aplikacje, ze względu na informacje, które przetwarzają, przechowują lub przekazują lub ze względu na ich krytyczność dla celu działania podmiotu, wymagają specjalnego nadzoru ze strony kierownictwa. Takie aplikacje są określane jako aplikacje główne. Oczekuje się, że wobec takich aplikacji będzie miał zastosowanie poziom wpływu NSC 199 umiarkowany lub wysoki. Jako „główny system informatyczny” uznaje się taki system, który wymaga szczególnej uwagi kierownictwa ze względu na jego znaczenie dla celu działania organizacji, wysokie koszty rozwoju, eksploatacji lub utrzymania lub jego znaczącą rolę w administrowaniu zadaniami organizacji, finansami, nieruchomościami lub innymi zasobami. Główne zastosowania to z definicji główne systemy informatyczne.

Głównymi aplikacjami są systemy, które wykonują jasno określone funkcje, dla których istnieją łatwe do zidentyfikowania względy bezpieczeństwa i potrzeby (np. elektroniczny system transferu środków). Główna aplikacja może obejmować wiele pojedynczych programów i sprzętu, oprogramowania i komponentów telekomunikacyjnych. Komponenty te mogą być pojedynczą aplikacją lub kombinacją sprzętu/oprogramowania ukierunkowaną na wspieranie określonej funkcji związanej z działalnością. Główna aplikacja może również składać się z wielu pojedynczych aplikacji, jeśli wszystkie dotyczą jednej funkcji z zakresu działalności (np. listy płac personelu). Jeśli system jest zdefiniowany jako główna aplikacja, a aplikacja działa w systemie ogólnego wsparcia innej organizacji, główny właściciel aplikacji jest odpowiedzialny za przyjęcie ryzyka, a ponadto:

- powiadamia właściciela ogólnego systemu wsparcia, że aplikacja jest krytyczna i zapewnia określone wymagania bezpieczeństwa;
- dostarcza kopię planu bezpieczeństwa systemu głównej aplikacji operatorowi ogólnego systemu wsparcia;

- żąda kopii planu bezpieczeństwa systemu ogólnego wsparcia i zapewnia, że zastosowana będzie odpowiednia ochrona aplikacji i informacji;
- zawiera odniesienie do ogólnego planu bezpieczeństwa systemu wsparcia w głównym planie bezpieczeństwa systemu aplikacji.

### 2.3. SYSTEMY OGÓLNEGO WSPARCIA

Ogólny system wsparcia to połączony zestaw zasobów informatycznych pod tym samym bezpośrednim zarządzaniem, który ma wspólną funkcjonalność. Ogólny system wsparcia zwykle obejmuje sprzęt, oprogramowanie, informacje, dane, aplikacje, komunikację, udogodnienia i ludzi oraz zapewnia wsparcie dla różnych użytkowników i/lub aplikacji.

Ogólnym systemem wsparcia, może być na przykład:

- LAN, w tym inteligentne terminale obsługujące oddział;
- sieć szkieletowa (np. w całej organizacji);
- sieć komunikacyjna;
- centrum przetwarzania danych organizacji;
- organizacyjna sieć radiowa;
- wspólna usługa przetwarzania informacji (prywatna chmura obliczeniowa).

Ogólny system wsparcia może mieć poziom wpływu NSC 199 niski, umiarkowany lub wysoki pod względem kategoryzacji bezpieczeństwa, w zależności od krytyczności lub wrażliwości systemu i głównych aplikacji obsługiwanych przez ogólny system wsparcia. Ogólny system wsparcia jest uważany za główny system informatyczny, gdy wymagana jest szczególna uwaga kierownictwa, wysokie koszty rozwoju, eksploatacji lub utrzymania, a system/informacja odgrywa znaczącą rolę w administrowaniu działalnością organizacji. Gdy ogólny system wsparcia jest ważnym systemem informatycznym, poziom wpływu NSC 199 w systemie jest umiarkowany lub wysoki.

Główna aplikacja może być hostowana w ogólnym systemie wsparcia. Ogólny plan bezpieczeństwa systemu wsparcia powinien odnosić się do głównego planu bezpieczeństwa systemu aplikacji.

## 2.4. APLIKACJE O MNIEJSZYM ZNACZENIU

Oczekuje się, że kierownictwa organizacji ustalą, które z ich aplikacji są aplikacjami o mniejszym znaczeniu i zapewnią, że wymogi bezpieczeństwa dotyczące tych aplikacji zostaną uwzględnione w ramach planu bezpieczeństwa systemu dla właściwych dla ogólnych systemów wsparcia lub w niektórych przypadkach w planach bezpieczeństwa aplikacji głównych. Często zdarza się, że niewielka aplikacja może mieć większość zabezpieczeń zapewnianych przez ogólny system wsparcia lub główną aplikację, z którymi współdziela. W takim przypadku właściciel systemu informatycznego ogólnego systemu wsparcia lub głównej aplikacji jest właścicielem systemu informatycznego dla aplikacji o mniejszym znaczeniu i jest odpowiedzialny za opracowanie planu bezpieczeństwa systemu z uwzględnieniem tych aplikacji. Dodatkowe zabezpieczenia specyficzne dla aplikacji o mniejszym znaczeniu powinny być udokumentowane w planie bezpieczeństwa systemu jako załącznik lub oddzielny rozdział. Właściciel aplikacji o mniejszym znaczeniu (często ten sam co właściciel informacji) może opracować załącznik lub rozdział opisujący dodatkowe elementy zabezpieczające. Kompletny plan bezpieczeństwa ogólnego systemu wsparcia lub plan bezpieczeństwa systemu głównej aplikacji powinien zostać udostępniony właścicielowi informacji w aplikacji o mniejszym znaczeniu.

Aplikacja o mniejszym znaczeniu może mieć niską lub umiarkowaną kategorię bezpieczeństwa NSC 199. Jeśli jednak aplikacja o mniejszym znaczeniu znajduje się w systemie, który nie ma odpowiedniej ochrony granic, aplikacja ta musi wdrożyć minimalne zabezpieczenia podstawowe wymagane przez system, w którym funkcjonuje lub system, z którym się łączy.

## 2.5. ZABEZPIECZENIA

NSC 200 zapewnia siedemnaście **minimalnych** wymagań bezpieczeństwa dla informacji i systemów informatycznych podmiotów publicznych. Wymagania stanowią szeroko

zakrojony, zrównoważony program bezpieczeństwa informacji, który dotyczy zarządzania oraz działań operacyjnych i technicznych w zakresie ochrony poufności, integralności i dostępności informacji i systemów informatycznych. Organizacja musi spełniać minimalne wymagania bezpieczeństwa określone w tym standardzie, stosując środki zabezpieczeń wybrane zgodnie z NSC 800-53 i wyznaczonymi poziomami wpływu zakłócenia na systemy informatyczne. Organizacja ma swobodę dostosowywania podstawowych zabezpieczeń zgodnie z warunkami określonymi w tym standardzie. Działania w tym zakresie obejmują: (i) stosowanie wskazówek dotyczących zakresu; (ii) specyfikację zabezpieczeń kompensujących; oraz (iii) specyfikację parametrów określonych przez organizację w środkach zabezpieczeń, o ile jest to dozwolone. Plan bezpieczeństwa systemu powinien dokumentować wszystkie działania dostosowawcze.

### **2.5.1. WSKAZÓWKI DOTYCZĄCE USTALANIA ZAKRESU SYSTEMU**

Wskazówki dotyczące ustalania zakresu systemu zapewniają organizacji wsparcie w zakresie stosowania i wdrażania podstawowych zabezpieczeń określonych w NSC 800-53. Opisane poniżej uwagi mogą potencjalnie wpłynąć na sposób, w jaki organizacja zastosuje podstawowe zabezpieczenia. Plany bezpieczeństwa systemu powinny jasno określać, które zabezpieczenia wynikają z wytycznych dotyczących określania zakresu systemu oraz zawierać opis rodzaju podjętych przedsięwzięć. Zastosowanie wytycznych dotyczących zakresu musi zostać sprawdzone i zatwierdzone przez osobę autoryzującą plan.

#### **Uwagi dotyczące technologii**

- Zabezpieczenia odnoszące się do określonych technologii (np. sieci bezprzewodowych, kryptograficznych, infrastruktury klucza publicznego) będą miały zastosowanie tylko wtedy, gdy technologie te zostaną zastosowane lub będą wymagane w systemie informatycznym.
- Zabezpieczenia będą miały zastosowanie tylko do tych elementów systemu informatycznego, które zazwyczaj zapewniają funkcje bezpieczeństwa określone przez minimalne wymagania bezpieczeństwa.

- Zabezpieczenia, które mogą być bezpośrednio lub pośrednio wspierane przez zautomatyzowane mechanizmy, nie będą wymagać opracowania takich mechanizmów, jeżeli mechanizmy te już istnieją lub są łatwo dostępne w gotowych produktach. W sytuacjach, w których zautomatyzowane mechanizmy nie są łatwo dostępne lub technicznie wykonalne, w celu spełnienia minimalnych wymagań bezpieczeństwa zostaną zastosowane zabezpieczenia kompensacyjne, wdrożone za pomocą mechanizmów niezautomatyzowanych lub określonych procedur.

### Ogóle kwestie związane z zabezpieczeniami

- Zabezpieczeniami przyjętymi przez organizację jako zabezpieczenia wspólne w większości przypadków będzie zarządzać jednostka organizacyjna inna niż właściciel systemu informatycznego. Każde zabezpieczenie podstawowe musi zostać zastosowane przez agencję jako zabezpieczenie wspólne lub zabezpieczenie przyjęte przez konkretnego właściciela systemu informatycznego. Decyzje w sprawie zabezpieczeń wspólnych nie mogą jednak wpływać na odpowiedzialność organizacji za zapewnienie niezbędnych zabezpieczeń wymaganych w celu spełnienia minimalnych wymagań bezpieczeństwa dla systemu informatycznego. (Dodatkowe informacje na temat zabezpieczeń wspólnych podano w sekcji 2.5.3.).

### Uwagi dotyczące systemów informatycznych z dostępem publicznym

- Zabezpieczenia związane z systemami informacji z dostępem publicznym muszą być starannie rozważone i stosowane z zachowaniem dyskrecji, ponieważ niektóre zabezpieczenia podstawowe (np. zabezpieczenia dotyczące bezpieczeństwa personelu, zabezpieczenia dotyczące identyfikacji i uwierzytelnienia) mogą nie mieć zastosowania do użytkowników uzyskujących dostęp do systemów informatycznych poprzez interfejsy publiczne<sup>6</sup>.

---

<sup>6</sup> Na przykład, podczas gdy zabezpieczenia podstawowe wymagają identyfikacji i uwierzytelnienia personelu organizacyjnego, który utrzymuje i wspiera systemy informatyczne zapewniające usługi dostępu publicznego, te same zabezpieczenia mogą nie być wymagane dla użytkowników uzyskujących dostęp do tych systemów za pośrednictwem interfejsów publicznych, w celu uzyskania publicznie dostępnych informacji. Z drugiej strony identyfikacja i uwierzytelnienie muszą być wymagane, aby użytkownicy uzyskujący dostęp do systemów informatycznych za pośrednictwem publicznych interfejsów mieli dostęp do swoich danych prywatnych / osobistych.

### Uwagi dotyczące infrastruktury

- Zabezpieczenia odnoszące się do obiektów organizacji (np. zabezpieczenia w zakresie dostępu fizycznego, takie jak zamki i osłony, zabezpieczenia środowiskowe dotyczące temperatury, wilgotności, oświetlenia, zasilania, przeciwpożarowe) będą miały zastosowanie tylko do tych części obiektów, które bezpośrednio zapewniają ochronę, wsparcie dla systemu informatycznego lub są z nim związane (w tym jego zasoby informatyczne, takie jak poczta elektroniczna lub serwery sieciowe, farmy serwerów, centra danych, węzły sieciowe, sprzęt komunikacyjny).

### Uwagi dotyczące skalowalności

- Zabezpieczenia powinny być dopasowane co do skali z uwzględnieniem wielkości i złożoności konkretnej organizacji wdrażającej zabezpieczenie oraz poziomu wpływu zakłócenia na system informatyczny. Skalowalność dotyczy zakresu i głębokości implementacji zabezpieczenia. Konieczna jest indywidualizacja zastosowania konkretnego zabezpieczenia z uwzględnieniem środowiska użytkowania, tak aby zapewnić podejście do wdrażania zabezpieczenia oparte na ryzyku, uwzględniające jego opłacalność<sup>7</sup>.

### Uwagi dotyczące ryzyka

- Zabezpieczenia, które dotyczą atrybutów bezpieczeństwa w zakresie poufności, integralności lub dostępności, mogą zostać obniżone do odpowiednio niższej kategorii zabezpieczeń podstawowych (lub odpowiednio zmodyfikowane lub wyeliminowane, o ile nie zostały zdefiniowane jako absolutnie wymagane zabezpieczenia minimalne) tylko wtedy, gdy działanie obniżające: (i) jest zgodne z kategoryzacją bezpieczeństwa NSC 199 dla odpowiednich atrybutów bezpieczeństwa, takich jak poufność, integralność lub dostępność przed przejściem

---

<sup>7</sup> Na przykład plan awaryjny dla dużej i złożonej organizacji z systemem informacyjnym o umiarkowanym lub dużym wpływie zakłócenia może być dość długi i zawierać znaczną ilość szczegółów dotyczących wdrożenia. Natomiast plan awaryjny dla mniejszej organizacji z systemem informacyjnym o niskim wpływie może być znacznie krótszy i zawierać znacznie mniej szczegółów dotyczących wdrożenia.

do ostatecznego odcenienia kategorii wpływu<sup>8</sup>; (ii) jest poparte przeprowadzoną przez organizację oceną ryzyka; oraz (iii) nie wpływa na informacje dotyczące bezpieczeństwa w systemie informatycznym.

### 2.5.2. ZABEZPIECZENIA KOMPENSACYJNE

Zabezpieczenia kompensacyjne to zabezpieczenia, operacyjne lub techniczne stosowane przez organizację zamiast zalecanych zabezpieczeń podstawowych dla niskich, umiarkowanych lub wysokich poziomów wpływu zakłócenia, które zapewniają równoważną lub porównywalną ochronę systemu informatycznego co te zabezpieczenia podstawowe. Zabezpieczenia kompensacyjne dla systemu informatycznego będą stosowane przez organizację tylko pod następującymi warunkami: (i) organizacja wybiera zabezpieczenia kompensacyjne z katalogu zabezpieczeń znajdujących się w NSC 800-53; (ii) organizacja przedstawia kompletne i przekonujące uzasadnienie, w jaki sposób zabezpieczenia kompensacyjne zapewniają równoważne bezpieczeństwo lub poziom ochrony systemu informatycznego; oraz (iii) organizacja ocenia i formalnie akceptuje ryzyko związane z zastosowaniem zabezpieczeń kompensacyjnych w systemie informatycznym. Zastosowanie zabezpieczeń kompensacyjnych musi zostać przejrzane, udokumentowane w planie bezpieczeństwa systemu i zatwierdzone przez osobę autoryzującą.

### 2.5.3. ZABEZPIECZENIA WSPÓLNE

Ogólne spojrzenie organizacji na bezpieczeństwa informacji ułatwia identyfikację wspólnych zabezpieczeń, które można zastosować do jednego lub więcej systemów informatycznych organizacji. Zabezpieczenia wspólne mogą mieć zastosowanie do: (i) wszystkich systemów informatycznych organizacji; (ii) grupy systemów informatycznych w określonej lokalizacji (czasami w związku z terminami certyfikacji/akredytacji lokalizacji); lub (iii) wspólnych systemów informatycznych, podsystemów lub aplikacji (tj. wspólny sprzęt, oprogramowanie

---

<sup>8</sup> Stosując koncepcję końcowego odcenienia niektóre atrybuty bezpieczeństwa (tj. poufność, integralność lub dostępność) mogły zostać zwiększone do wyższego poziomu wpływu. W związku z tym zabezpieczenia, które wspierają te atrybuty bezpieczeństwa, zostaną również zaktualizowane. W związku z tym organizacje muszą rozważyć odpowiednie i dopuszczalne działania obniżające, aby zapewnić opłacalne stosowanie zabezpieczeń, oparte na ryzyku.

i/lub oprogramowanie układowe) wdrożone w wielu lokalizacjach operacyjnych (czasami związane z terminami certyfikacji/akredytacji). Zabezpieczenia wspólne, zwykle identyfikowane podczas procesu obejmującego całą organizację, z udziałem CIO, SAISO, AO, właścicieli systemów informatycznych i ISSO (oraz przez kierowników programów rozwojowych w przypadku zabezpieczeń wspólnych dla wspólnego sprzętu, aplikacji i/lub oprogramowania układowego), mają następujące właściwości:

- opracowanie, wdrożenie i ocena zabezpieczeń wspólnych może być przypisane do upoważnionego personelu organizacji lub komórek organizacyjnych (innych niż właściciele systemów informatycznych, których systemy będą wdrażać lub wykorzystywać te wspólne środki bezpieczeństwa);
- wyniki oceny zabezpieczeń wspólnych można wykorzystać do wsparcia procesów certyfikacji bezpieczeństwa i akredytacji systemów informatycznych organizacji, w których zastosowano te zabezpieczenia.

Wiele spośród zabezpieczeń zarządczych i operacyjnych (np. zabezpieczenia planowania awaryjnego, zabezpieczenia w zakresie reagowania na incydenty, zabezpieczeń z zakresu uświadamiania i szkolenia, zabezpieczeń w zakresie bezpieczeństwa personelu i zabezpieczenia fizycznego) potrzebnych do ochrony systemu informatycznego może być doskonałymi przykładami na status zabezpieczeń wspólnych. Celem jest obniżenie kosztów bezpieczeństwa poprzez centralne zarządzanie opracowywaniem, wdrażaniem i oceną zabezpieczeń wspólnych wymaganych przez organizację, a następnie udostępnianie wyników oceny właścicielom systemów informatycznych, w których stosowane są te zabezpieczenia wspólne. Zabezpieczenia nie stanowiące zabezpieczeń wspólnych są uważane za zabezpieczenia specyficzne dla systemu i ich ustanowienie jest obowiązkiem właściciela systemu informatycznego. Plany bezpieczeństwa systemu powinny wyraźnie określać, które zabezpieczenia zostały określone jako zabezpieczenia wspólne, a które zabezpieczenia zostały określone jako zabezpieczenia specyficzne dla systemu.

W celu zwiększenia skuteczności opracowywania planów bezpieczeństwa systemu należy udokumentować zabezpieczenia wspólne, a następnie wprowadzić do każdego planu bezpieczeństwa systemu informatycznych. Osoba odpowiedzialna za wdrożenie



zabezpieczeń wspólnych powinna zostać wymieniona w planie bezpieczeństwa. Skuteczne maksymalizowanie zastosowania zabezpieczeń wspólnych w procesie planowania bezpieczeństwa systemu zależy od następujących czynników:

- organizacja opracowała, udokumentowała i przekazała szczegółowe wytyczne dotyczące identyfikacji zabezpieczeń wspólnych;
- organizacja przypisała odpowiedzialność za koordynację identyfikacji i przeglądu zabezpieczeń wspólnych oraz uzyskanie konsensusu w sprawie tych zabezpieczeń osobie zarządzającej, której obowiązki dotyczą programu bezpieczeństwa, takiemu jak CIO lub SAISO;
- właściciele systemów zostali poinformowani o procesie planowania bezpieczeństwa systemu, w tym o stosowaniu zabezpieczeń wspólnych;
- w ramach tego procesu skonsultowano się z ekspertami organizacji z określonych wspólnych obszarów zabezpieczeń.

Organizacja może również przypisać do zabezpieczenia status hybrydowy w sytuacjach, w których jedna część zabezpieczenia jest uważana za wspólną, podczas gdy inna jego część jest uważana za specyficzną dla systemu. Na przykład organizacja może postrzegać zabezpieczenie IR-1 (polityka i procedury reagowania na incydenty) jako zabezpieczenie hybrydowe z częścią zasad dotyczących uznawanych za zabezpieczenie wspólne, a część procedury dotyczącą zabezpieczenia za specyficzną dla systemu. Hybrydowe mechanizmy zabezpieczeń mogą również służyć jako szablony do dalszego udoskonalania zabezpieczeń. Organizacja może na przykład zdecydować się na wdrożenie zabezpieczenia CP-2 (Plan awaryjny) jako wzorzec uogólnionego planu awaryjnego dla wszystkich systemów informatycznych agencji z indywidualnymi właścicielami systemów informatycznych dostosowującymi plan, w stosownych przypadkach, do problemów konkretnego systemu. Właściciele systemów informatycznych są odpowiedzialni za wszelkie problemy systemowe związane z wdrażaniem zabezpieczeń wspólnych. Problemy powinny zostać zidentyfikowane i opisane w planach bezpieczeństwa systemu dla poszczególnych systemów informatycznych. SAISO, działając w imieniu CIO, powinien koordynować z personelem

organizacji (np. kierownikami obiektów, kierownikami placówek, kierownikami personelu) odpowiedzialnym za opracowanie i wdrożenie wyznaczonych zabezpieczeń wspólnych, tak aby zapewnić wprowadzenie wymaganych zabezpieczeń. Zabezpieczenia powinny być oceniane, a wyniki oceny są udostępniane odpowiednim właścicielom systemów informatycznych.

Podział zabezpieczeń na zabezpieczenia wspólne i zabezpieczenia specyficzne dla systemu mogą przynieść organizacji znaczne oszczędności w zakresie ich kosztów wdrożenia. Może to również skutkować bardziej spójnym stosowaniem zabezpieczeń w całej organizacji. Ponadto również znaczące oszczędności można uzyskać w procesie certyfikacji bezpieczeństwa i akredytacji. Zamiast oceniać zabezpieczenia w każdym systemie informatycznym, proces certyfikacji opierać się będzie na wynikach aktualnej oceny wszelkich mających zastosowanie zabezpieczeniach wspólnych, przeprowadzanych na poziomie organizacji. Całościowe podejście do ponownego wykorzystywania i dzielenia się wynikami oceny może znacznie poprawić efektywność przeprowadzanych przez organizację certyfikacji bezpieczeństwa i akredytacji systemów oraz znacznie obniżyć koszty programu ochrony.

Chociaż koncepcja podziału zabezpieczeń na zabezpieczenia wspólne i zabezpieczenia specyficzne dla systemu jest prosta i intuicyjna, zastosowanie tej zasady w organizacji wymaga planowania, koordynacji i wytrwałości. Jeśli organizacja dopiero zaczyna wdrażać to podejście lub tylko częściowo wdrożyła to podejście, uzyskanie maksymalnych korzyści z podziału zabezpieczeń i związanego z nim ponownego wykorzystania dowodów oceny może zająć trochę czasu. Ze względu na potencjalną zależność od zabezpieczeń wspólnych w wielu systemach informatycznych organizacji, nieprawidłowe zastosowanie takich zabezpieczeń wspólnych może spowodować znaczny wzrost ryzyka na poziomie organizacji – pojawia się ryzyko dla każdego systemu zależnego od takich zabezpieczeń.

### 3. BUDOWA PLANU

Pozostała część tego dokumentu prowadzi czytelnika w zakresie opracowania planu bezpieczeństwa systemu, w tym logicznych kroków, które należy wykonać przy jego opracowaniu, zalecanej struktury i treści, a także w jaki sposób zmaksymalizować wykorzystanie bieżących publikacji NSC do skutecznego wspierania działań związanych z planowaniem bezpieczeństwa systemu. Należy ustanowić w organizacji zasady dotyczące tego, w jaki sposób plany bezpieczeństwa systemu informatycznego powinny być kontrolowane i dostępne przed rozpoczęciem działalności.

#### 3.1. NAZWA I IDENTYFIKATOR SYSTEMU

Pierwszą pozycją wymienioną w planie bezpieczeństwa systemu jest nazwa i identyfikator systemu. Do każdego systemu należy przypisać nazwę i unikatowy identyfikator. Przypisanie unikatowego identyfikatora wspiera zdolność organizacji do łatwego zbierania w organizacji informacji i wskaźników bezpieczeństwa specyficznych dla systemu, a także ułatwia pełną identyfikowalność wszystkich wymagań związanych z wdrożeniem i wydajnością systemu. Taki identyfikator powinien pozostać taki sam przez cały okres eksploatacji systemu i powinien być przechowywany w dziennikach kontroli związanych z użytkowaniem systemu.

#### 3.2. KATEGORYZACJA SYSTEMU

Każdy system zidentyfikowany z systemów organizacji musi zostać skategoryzowany za pomocą NSC199. Podsumowanie kategorii NSC 199 znajduje się w tabeli 1.

ATRYBUT BEZPIECZEŃSTWA	POTENCJALNY WPŁYW		
	NISKI	UMIARKOWANY	WYSOKI
<b><i>POUFNOŚĆ</i></b>			
Zapewnienie stosowania zatwierdzonych	Można oczekiwać <b>ograniczonego</b> negatywnego	Można oczekiwać <b>poważnego</b> negatywnego	Można oczekiwać <b>drastycznie lub katastrofalnie</b>

ATRYBUT BEZPIECZEŃSTWA	POTENCJALNY WPŁYW		
	NISKI	UMIARKOWANY	WYSOKI
ograniczeń w zakresie ujawniania i dostępu do informacji, w tym środków ochrony prywatności i informacji osobistych.	wpływu nieuprawnionego ujawnienia informacji na działalność organizacji, jej zasoby lub osoby fizyczne.	wpływu nieuprawnionego ujawnienia informacji na działalność organizacji, jej zasoby lub osoby fizyczne.	negatywnego wpływu nieuprawnionego ujawnienia informacji na działalność organizacji, jej zasoby lub osoby fizyczne.
<b>INTEGRALNOŚĆ</b> Ochrona przed niewłaściwą modyfikacją lub zniszczeniem informacji, w tym zapewnienie niezaprzeczalności i autentyczności informacji.	Można oczekiwać <b>ograniczonego</b> negatywnego wpływu nieuprawnionej modyfikacji lub zniszczenia informacji na działalność organizacji, jej zasoby lub osoby fizyczne.	Można oczekiwać <b>poważnego</b> negatywnego wpływu nieuprawnionej modyfikacji lub zniszczenia informacji na działalność organizacji, jej zasoby lub osoby fizyczne.	Można oczekiwać <b>drastycznie lub katastrofalnie</b> negatywnego wpływu nieuprawnionej modyfikacji lub zniszczenia informacji na działalność organizacji, jej zasoby lub osoby fizyczne.

ATRYBUT BEZPIECZEŃSTWA	POTENCJALNY WPŁYW		
	NISKI	UMIARKOWANY	WYSOKI
<b>DOSTĘPNOŚĆ</b>			
Zapewnienie terminowego i niezawodnego dostępu i możliwości wykorzystania informacji.	Można oczekiwać <b>ograniczonego</b> negatywnego wpływu zaburzenia dostępu lub możliwości wykorzystania informacji na działalność organizacji, jej zasoby lub osoby fizyczne.	Można oczekiwać <b>poważnego</b> negatywnego wpływu zaburzenia dostępu lub możliwości wykorzystania informacji na działalność organizacji, jej zasoby lub osoby fizyczne.	Można oczekiwać <b>drastycznie lub katastrofalnie</b> negatywnego wpływu zaburzenia dostępu lub możliwości wykorzystania informacji na działalność organizacji, jej zasoby lub osoby fizyczne.

Tabela 1. Kategoryzacja systemów wg NSC 199.

### 3.3. WŁAŚCICIEL SYSTEMU

Dla każdego systemu wyznaczony właściciel systemu musi zostać zidentyfikowany w planie bezpieczeństwa systemu. Osoba ta jest kluczowym punktem kontaktowym (PoC) dla systemu i odpowiada za koordynację działań związanych z cyklem życia systemu (SDLC), specyficznych dla tego systemu. Ważne jest, aby osoba taka miała specjalistyczną wiedzę na temat możliwości i funkcjonalności systemu. Przypisanie właściciela systemu powinno być udokumentowane na piśmie, a plan powinien zawierać następujące dane kontaktowe:

- imię i nazwisko;
- stanowisko;

- nazwa organizacji;
- adres;
- numer telefonu;
- adres e-mail.

### **3.4. ORGAN ZATWIERDZAJĄCY**

Dla każdego systemu w planie bezpieczeństwa musi zostać określona osoba autoryzująca. Osoba ta jest członkiem kierownictwa organizacji, który jest upoważniony do autoryzacji (akredytacji) systemu informatycznego (głównej aplikacji lub ogólnego systemu wsparcia) i do zaakceptowania ryzyka szacunkowego związanego z tym systemem. Ustanowienie osoby autoryzującej powinno mieć formę pisemną, a plan musi zawierać te same informacje kontaktowe co wymienione w sekcji 3.3.

### **3.5. WYZNACZANIE INNYCH KONTAKTÓW**

W tej sekcji należy podać dane innego kluczowego personelu kontaktowego, który może odpowiedzieć na pytania dotyczące charakterystyki i działania systemu. Dla każdej osoby wymienionej w tej sekcji należy podać te same informacje wymienione w sekcji 3.3.

### **3.6. PRZYPISANIE ODPOWIEDZIALNOŚCI ZA BEZPIECZEŃSTWO**

W ramach organizacji należy przypisać odpowiedzialność za każdy system. Można to osiągnąć na wiele sposobów. W niektórych organizacjach ogólna odpowiedzialność może zostać przekazana SAISO. Często SAISO jest obsługiwany przez personel ds. bezpieczeństwa przypisany do każdego głównego komponentu. Personel ds. bezpieczeństwa może zostać upoważniony do zapewnienia spełnienia wymagań bezpieczeństwa dla wszystkich systemów w swojej dziedzinie uprawnień. Inne modele mogą podzielić tę odpowiedzialność na inne sposoby w oparciu o strukturę organizacji. Dla tych osób należy podać te same dane kontaktowe, które wymieniono w sekcji 3.3. Najważniejsze jest, aby odpowiedzialność tę sformalizować na piśmie w opisie stanowisk personelu.

### 3.7. STATUS OPERACYJNY SYSTEMU

Wskaż jedną lub więcej z poniższych informacji o stanie operacyjnym systemu. Jeśli wybrano więcej niż jeden status, należy wymienić, która część systemu są objęte każdym ze statusów.

- **Operacyjny** - system jest w produkcji.
- **W fazie rozwoju** - system jest projektowany, rozwijany lub wdrażany.
- **Przeszedł poważną modyfikację** - system przechodzi poważną konwersję lub przejście.

Jeśli system jest opracowywany lub przechodzi poważną modyfikację, należy podać informacje o metodach zastosowanych w celu zapewnienia, że z góry uwzględniono wymagania bezpieczeństwa. Uwzględnij określone zabezpieczenia w odpowiednich sekcjach planu, w zależności od tego, w której fazie cyklu życia znajduje się system.

### 3.8. TYP SYSTEMU INFORMATYCZNEGO

W tej części planu wskaż, czy system jest główną aplikacją, czy ogólnym systemem wsparcia. Jeśli system zawiera aplikacje o mniejszym znaczeniu, opisz je w części Opis ogólny/Cel planu. Jeśli organizacja ma dodatkowe kategorie typów systemów informatycznych, zmodyfikuj szablon, aby uwzględnić inne kategorie.

### 3.9. OGÓLNY OPIS/CEL

Przygotuj krótki opis (od jednego do trzech akapitów) funkcji i celu systemu (np. wskaźnik ekonomiczny, wsparcie sieciowe dla organizacji, analiza danych biznesowych, obsługa raportowania).

Jeśli system jest systemem ogólnym wsparcia, należy wymienić wszystkie aplikacje obsługiwane przez ogólny system wsparcia. Określ, czy aplikacja jest aplikacją główną, czy nie, i podaj, w stosownych przypadkach, unikatową nazwę/identyfikator. Opisz funkcję każdej aplikacji i przetwarzane informacje. Dołącz listę organizacji użytkowników, niezależnie od tego, czy są one wewnętrzne, czy zewnętrzne w stosunku do organizacji właściciela systemu.

### 3.10. ŚRODOWISKO SYSTEMOWE

Podaj krótki (jeden do trzech akapitów) ogólny opis techniczny systemu.

Uwzględnij wszelkie czynniki środowiskowe lub techniczne, które budzą szczególne obawy dotyczące bezpieczeństwa, takie jak korzystanie z osobistych asystentów cyfrowych, technologii bezprzewodowej itp. Zazwyczaj środowiska operacyjne są następujące:

- autonomiczne lub małe biuro/biuro domowe (SOHO) opisuje małe, nieformalne instalacje komputerowe, które są używane do celów domowych lub biznesowych, obejmuje wiele małych środowisk i urządzeń, od laptopów, urządzeń mobilnych lub komputerów domowych, po systemy telepracy, małe firmy i małe oddziały firmy;
- centralnie zarządzane to zazwyczaj duże systemy organizacji ze zdefiniowanymi, zorganizowanymi pakietami konfiguracji sprzętu i oprogramowania, zwykle składającymi się z centralnie zarządzanych stacji roboczych i serwerów chronionych przed atakiem z Internetu przez zapory sieciowe i inne urządzenia bezpieczeństwa sieciowego;
- środowiska niestandardowe zawierają systemy, w których funkcjonalność i stopień bezpieczeństwa nie pasują do innych środowisk. Dwa typowe środowiska niestandardowe to:
  - Specjalizowane środowisko o ograniczonej funkcjonalności zawierające systemy i sieci o wysokim ryzyku ataku lub ujawnienia danych, przy czym bezpieczeństwo ma pierwszeństwo przed funkcjonalnością. Zakłada się, że systemy mają ograniczoną lub wyspecjalizowaną (nie ogólną stację roboczą lub system) funkcjonalność w wysoce zagrożonym środowisku, takim jak zewnętrzna zaporę sieciową lub publiczny serwer sieciowy, lub których zawartość danych lub cel misji ma taką wartość, że priorytet bezpieczeństwa przeważa nad potencjalnymi negatywnymi konsekwencjami wynikającymi ze stosowania starszych aplikacji lub braku interoperacyjności z innymi systemami. Specjalizowane środowisko o ograniczonej funkcjonalności może stanowić podzbiór innego środowiska.



- Starsze środowisko zawierające starsze systemy lub aplikacje, które mogą korzystać ze starszych, mniej bezpiecznych mechanizmów komunikacji. Komputery działające w tym środowisku mogą wymagać mniej restrykcyjnych ustawień bezpieczeństwa, aby mogły komunikować się ze starszymi systemami i aplikacjami. Starsze środowisko może być podzbiorem środowiska autonomicznego lub centralnie zarządzanego.

### 3.11. POŁĄCZENIA SYSTEMU / WYMIANA INFORMACJI

Połączenie systemowe to bezpośrednie połączenie dwóch lub więcej systemów informatycznych w celu współdzielenia zasobów informatycznych. Połączenie systemu, jeśli nie jest odpowiednio chronione, może doprowadzić do naruszenia bezpieczeństwa wszystkich podłączonych systemów oraz danych, które przechowują, przetwarzają lub przesyłają. Ważne jest, aby właściciele systemu, właściciele informacji i kierownictwo uzyskali jak najwięcej informacji na temat podatności związanych z połączeniami systemowymi i udostępnianiem informacji. Jest to niezbędne do wyboru odpowiednich mechanizmów zabezpieczeń wymaganych w celu ograniczenia tych podatności. Między systemami (nie między stacjami roboczymi lub publicznie dostępnymi systemami), które współużytkują dane należące do różnych organizacji lub zarządzane przez różne organizacje, potrzebna jest umowa o bezpieczeństwie połączeń międzysieciowych (ISA), protokół uzgodnień (MoU) lub porozumienie o współpracy (MoA). ISA nie jest potrzebne w przypadku wewnętrznych systemów organizacji, jeśli organizacja zarządza i egzekwuje rygorystyczny cykl życia systemu, który wymaga zatwierdzeń zapewniających zgodność z wymogami bezpieczeństwa.

W tej sekcji, dla każdego połączenia między systemami będącymi własnością lub obsługiwanych przez różne organizacje, podaj następujące informacje dotyczące autoryzacji połączenia z innymi systemami lub udostępniania informacji:

- nazwa systemu;
- nazwa organizacji;
- rodzaj połączenia (Internet, połączenie telefoniczne itp.);

- zezwolenia na wzajemne połączenia (MOU / MOA, ISA);
- data umowy;
- kategoria NSC 199;
- status certyfikacji i akredytacji systemu;
- nazwisko i stanowisko osoby autoryzującej.

W przypadku organizacji z licznymi połączeniami wzajemnymi dobrym sposobem prezentacji informacji może być format tabeli zawierający powyższe informacje.

### **3.12. PRZEPISY, REGULACJE I ZASADY DOTYCZĄCE SYSTEMU**

Wymień wszelkie przepisy ustawowe, wykonawcze lub zasady, które ustanawiają szczegółowe wymagania dotyczące poufności, integralności lub dostępności systemu oraz informacji przechowywane przez system, przekazywane przez niego lub przetwarzane przez ten system. Ogólne wymagania bezpieczeństwa organizacji nie muszą być wymienione, ponieważ dotyczą one zabezpieczenia wszystkich systemów. Każda organizacja powinna decydować o poziomie przepisów ustawowych, wykonawczych i zasad, które należy uwzględnić w planie bezpieczeństwa systemu. Przykładami mogą być przepisy o ochronie danych osobowych lub szczególna ustawa lub rozporządzenie dotyczące przetwarzanych informacji (np. informacje podatkowe lub statystyczne). Jeśli system przetwarza dane podlegające ustawie o ochronie danych osobowych, należy podać odwołania do konkretnych jednostek redakcyjnych odpowiednich aktów prawa.

### **3.13. DOBÓR ZABEZPIECZEŃ**

W ramach przygotowań do udokumentowania, w jaki sposób zabezpieczenia NSC 800-53 dla odpowiednich zabezpieczeń podstawowych (systemy informatyczne o niskim, umiarkowanym lub wysokim wpływie zakłócenia) są wdrażane lub planowane do wdrożenia, zabezpieczenia zawarte w tych zasadach powinny zostać przejrzane i ewentualnie dostosowane. Przy określaniu stosowalności lub dostosowywania poszczególnych zabezpieczeń należy stosować wytyczne dotyczące ustalania zakresu wyjaśnione w sekcji 2.5.1. Ponadto zabezpieczenia, które są wspólne dla wielu systemów lub w całej organizacji,

powinny zostać zidentyfikowane, a następnie udokumentowane w planie. Wskazówki dotyczące tego, w jaki sposób należy określać, dokumentować i koordynować zabezpieczenia wspólne, zawiera sekcja 2.5.3. Proces wyboru odpowiednich zabezpieczeń i zastosowania wytycznych dotyczących zakresu w celu osiągnięcia odpowiedniego bezpieczeństwa jest działaniem wieloaspektowym, opartym na szacowaniu ryzyka, w który w ramach organizacji zaangażowani są kierownictwo i personel operacyjny. Proces ten należy przeprowadzić przed napisaniem tej części planu bezpieczeństwa.

- W przypadku systemów informatycznych o niskim wpływie organizacja musi co najmniej stosować zabezpieczenia określone w NSC 800-53 dla poziomu niskiego i musi zapewnić spełnienie minimalnych wymagań w zakresie zapewnienia bezpieczeństwa związanych z tymi zabezpieczeniami.
- W przypadku systemów informatycznych o umiarkowanym wpływie organizacja musi co najmniej stosować zabezpieczenia określone w NSC 800-53 dla poziomu umiarkowanego i musi zapewnić spełnienie minimalnych wymagań w zakresie zapewnienia bezpieczeństwa związanych z tymi zabezpieczeniami.
- W przypadku systemów informatycznych o dużym wpływie organizacja musi co najmniej stosować zabezpieczenia określone w NSC 800-53 dla poziomu wysokiego i musi zapewnić spełnienie minimalnych wymagań w zakresie zapewnienia bezpieczeństwa związanych z tymi zabezpieczeniami.

### **3.14. ZABEZPIECZENIA MINIMALNE**

Teraz, gdy zabezpieczenia zostały wybrane, dostosowane i zidentyfikowano zabezpieczenia wspólne, opisz każdy z nich. Opis powinien zawierać 1) nazwę zabezpieczenia; 2) sposób, w jaki zabezpieczenie jest wdrażane lub planowane do wdrożenia; 3) wszelkie zastosowane wskazówki dotyczące zakresu i rozważania dotyczące zabezpieczenia; oraz 4) wskazania, czy zabezpieczenie jest zabezpieczeniem wspólnym i kto jest odpowiedzialny za jego wdrożenie. Zabezpieczenia w katalogu zabezpieczeń NSC 800-53 mają dobrze zdefiniowaną organizację i funkcje. Dla łatwości użycia w procesie wyboru i konfiguracji zabezpieczenia są podzielone na klasy i kategorie (rodziny).

Obejmują one trzy ogólne klasy zabezpieczeń (tj. zarządzanie, operacje i techniczne). Każda kategoria zawiera mechanizmy zabezpieczeń związane z funkcją bezpieczeństwa danej rodziny. W celu zidentyfikowania każdej kategorii zabezpieczeń, przypisany jest każdej rodzinie jednoznaczny identyfikator dwuznakowy. Tabela 2 podsumowuje klasy i kategorie w katalogu zabezpieczeń oraz dane identyfikacyjne rodziny.

Klasa	Kategoria zabezpieczeń	Identyfikator
Zarządzanie	Zarządzanie ryzykiem	RA
Zarządzanie	Planowanie	PL
Zarządzanie	Nabywanie systemu i usług	SA
Zarządzanie	Ocena bezpieczeństwa i autoryzacja	CA
Operacje	Bezpieczeństwo osobowe	PS
Operacje	Ochrona fizyczna i środowiskowa	PE
Operacje	Planowanie awaryjne/ciągłość działania	CP
Operacje	Zarządzanie konfiguracją	CM
Operacje	Utrzymanie i wsparcie	MA
Operacje	Integralność systemu i informacji	SI
Operacje	Ochrona nośników danych	MP
Operacje	Reagowanie na incydenty	IR
Operacje	Uświadamianie i szkolenia	AT
Techniczne	Identyfikacja i uwierzytelnianie	IA
Techniczne	Kontrola dostępu	AC
Techniczne	Audyt i rozliczalność	AU
Techniczne	Ochrona systemów i sieci telekomunikacyjnych	SC

Tabela 2. Klasy, kategorie i identyfikatory zabezpieczeń.

Oznaczenia klas zabezpieczeń (tj. zarządzanie, operacyjne i techniczne) są zdefiniowane poniżej w celu wyjaśnienia na potrzeby przygotowywania planów bezpieczeństwa systemu.

Zabezpieczenia zarządzania koncentrują się na zarządzaniu systemem informatycznym i zarządzaniu ryzykiem w systemie. Są to zagadnienia, którymi zwykle interesuje się kierownictwo. Zabezpieczenia operacyjne dotyczą metod bezpieczeństwa koncentrujących się na mechanizmach przede wszystkim wdrażanych i wykonywanych przez ludzi (w przeciwieństwie do systemów). Zabezpieczenia te wprowadzono w celu poprawy bezpieczeństwa określonego systemu (lub grupy systemów). Często wymagają wiedzy technicznej lub specjalistycznej i często opierają się na działaniach zarządczych, a także na zabezpieczeniach technicznych. Zabezpieczenia techniczne skupiają się na zabezpieczeniach wykonywanych przez system komputerowy. Elementy sterujące mogą zapewniać automatyczną ochronę przed nieautoryzowanym dostępem lub niewłaściwym użyciem, ułatwiać wykrywanie naruszeń bezpieczeństwa oraz wspierać wymagania bezpieczeństwa dotyczące aplikacji i danych.

### **3.15. TERMINY UKOŃCZENIA I ZATWIERDZENIA**

Należy podać datę zakończenia opracowywania planu bezpieczeństwa systemu. Data zakończenia powinna być aktualizowana za każdym razem, gdy plan jest okresowo sprawdzany i aktualizowany. Po zaktualizowaniu należy dodać numer wersji. Plan bezpieczeństwa systemu powinien również zawierać datę zatwierdzenia planu przez osobę autoryzującą. Dokumentacja zatwierdzenia planu, tj. dokument akredytacyjny, memorandum zatwierdzające powinna znajdować się w aktach lub być dołączona jako część planu.

### **3.16. BIEŻĄCA KONSERWACJA PLANU BEZPIECZEŃSTWA SYSTEMU**

Po opracowaniu planu bezpieczeństwa systemu informatycznego ważne jest, aby okresowo oceniać plan, przeglądać wszelkie zmiany stanu systemu, funkcjonalności, projektu itp. oraz upewnić się, że plan nadal odzwierciedla prawidłowe informacje o systemie. Dokumentacja i jej poprawność są kluczowe dla działalności certyfikacyjnej w odniesieniu do systemu.

Wszystkie plany powinny być przeglądane i aktualizowane co najmniej raz w roku oraz po istotnej zmianie. Niektóre elementy do uwzględnienia w przeglądzie to:

- zmiana właściciela systemu informatycznego;
- zmiana personelu ds. bezpieczeństwa informacji;
- zmiana w architekturze systemu;
- zmiana statusu systemu;
- dodania/usunięcia wzajemnych połączeń systemowych;
- zmiana zakresu systemu;
- zmiana osoby autoryzującej;
- zmiana statusu certyfikacji i akredytacji.

## ZAŁĄCZNIK A PRZYKŁADOWY WZÓR PLANU BEZPIECZEŃSTWA SYSTEMU INFORMATYCZNEGO

Poniższe opracowanie jest **TYLKO** przykładem. Organizacje mogą korzystać z innych formatów i zdecydować się na zmiany, tak aby odzwierciedlić wszelkie zastosowane pominięcia na podstawie niniejszych wskazówek. To nie jest obowiązkowy format; uznaje się, że wiele organizacji i dostawców usług w zakresie bezpieczeństwa informacji mogło opracować i wdrożyć inne podejścia do opracowywania i prezentacji planu bezpieczeństwa systemu informatycznego w celu zaspokojenia własnych potrzeb w zakresie jego opracowania.



---

## SZABLON PLANU BEZPIECZEŃSTWA SYSTEMU INFORMATYCZNEGO

1. Nazwa systemu informacyjnego:

- unikatowy identyfikator i nazwa nadana systemowi.

2. Kategoryzacja systemu informacyjnego:

- zidentyfikuj odpowiednią kategoryzację NSC 199.

Niska	Umiarkowana	Wysoka
-------	-------------	--------

3. Właściciel systemu informatycznego:

- imię i nazwisko, stanowisko, organizacja, adres, adres e-mail i numer telefonu osoby, która jest właścicielem systemu.

4. Osoba autoryzująca:

- imię i nazwisko, stanowisko, organizacja, adres, adres e-mail i numer telefonu wyznaczonej osoby autoryzującej.

5. Inne wyznaczone kontakty:

- wymień inny kluczowy personel, jeśli dotyczy; zawierać ich tytuł, adres, adres e-mail i numer telefonu.

6. Przypisanie odpowiedzialności za bezpieczeństwo:

- nazwisko, tytuł, adres, adres e-mail i numer telefonu osoby odpowiedzialnej za bezpieczeństwo systemu.

7. Status operacyjny systemu informacyjnego:

- wskaż status operacyjny systemu. Jeśli wybrano więcej niż jeden status, należy wymienić, która część systemu jest objęta każdym statusem.

Operacyjny	W fazie rozwoju	Główna modyfikacja
------------	-----------------	--------------------

8. Typ systemu informacyjnego:

- wskaż, czy system jest główną aplikacją, czy ogólnym systemem wsparcia. Jeśli system zawiera aplikacje o mniejszym znaczeniu, wymień je w punkcie 9. Ogólny opis/cel systemu.

<b>Główna aplikacja</b>	<b>Ogólny system wsparcia</b>
-------------------------	-------------------------------

9. Ogólny opis systemu / cel

- opisz funkcję lub cel systemu oraz procesy informacyjne.

10. Środowisko systemowe

- podaj ogólny opis techniczny systemu obejmujący podstawowy sprzęt, oprogramowanie i środki telekomunikacyjne.

11. Połączenia systemowe/wymiana informacji

- wymień połączone systemy i identyfikatory tych systemów (w stosownych przypadkach), podaj system, nazwę, organizację, typ systemu (główna aplikacja

lub ogólny system wsparcia), wskaż, czy w aktach znajduje się dokument ISA/MOU/MOA, data umowy o połączeniu, Kategoria NSC 199, status C&A i nazwisko osoby autoryzującej.

Nazwa systemu	Organizacja	Typ	Porozumienia (ISA/MoU/MoA)	Data	Kategoria NSC 199	Status C&A	Osoba autoryzująca

12. Powiązane przepisy prawne/regulacje/zasady

- wymień wszelkie przepisy ustawowe i wykonawcze, które ustanawiają szczegółowe wymagania dotyczące poufności, integralności lub dostępności danych w systemie.

13. Minimalne środki bezpieczeństwa

- wybierz odpowiednie minimalne zabezpieczenia bazowe uwzględniając kategorię wpływu zakłócenia na system (niski, umiarkowany, wysokim) z NSCP 800-53, a następnie podaj dokładny opis, w jaki sposób zabezpieczenia te są wdrażane lub planowane do wdrożenia. Opis powinien zawierać: 1) nazwę zabezpieczenia;

- 2) sposób, w jaki zabezpieczenie jest wdrażane lub planowane do wdrożenia;
- 3) wszelkie zastosowane wytyczne dotyczące zakresu; oraz 4) wskazanie, czy zabezpieczenie jest zabezpieczeniem wspólnym i kto jest odpowiedzialny za jego wdrożenie.

14. Data zakończenia planu bezpieczeństwa systemu informatycznego:

\_\_\_\_\_

- wprowadź datę zakończenia opracowania planu.

15. Data zatwierdzenia planu bezpieczeństwa systemu informatycznego:

\_\_\_\_\_

- wprowadź datę zatwierdzenia planu bezpieczeństwa systemu i wskaż, czy dokumentacja zatwierdzenia jest dołączona do planu czy zapisana w innej dokumentacji.

## **ZAŁĄCZNIK B SŁOWNIK I AKRONIMY**

**PATRZ: NSC 7298, SŁOWNIK KLUCZOWYCH POJĘĆ Z ZAKRESU CYBERBEZPIECZEŃSTWA**

