Kancelaria Prezesa
Rady Ministrów

NARODOWY STANDARD CYBERBEZPIECZEŃSTWA
NSC 199 wer. 1.1

10 marca 2023

Standardy kategoryzacji bezpieczeństwa

Publikacja dostępna pod adresem:

Narodowe Standardy Cyberbezpieczeństwa

PREAMBUŁA

Szanowni Państwo,

oddajemy w Państwa ręce zestaw publikacji specjalnych - Narodowe Standardy Cyberbezpieczeństwa, o których mowa w interwencji 2.1 celu szczegółowego 2 Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019 – 2024, *Opracowanie i wdrożenie Narodowych Standardów Cyberbezpieczeństwa oraz promowanie dobrych praktyk i zaleceń*. Standardy zostały opracowane na podstawie publikacji amerykańskiego National Institute of Science and Technology (NIST) i posiadają mapowanie na obowiązujące w polskim systemie prawnym Polskie Normy, na których oparte jest zarządzanie bezpieczeństwem informacji w podmiotach krajowego systemu cyberbezpieczeństwa.

Standardy stanowią przewodniki metodyczne, które ułatwiają zbudowanie efektywnego systemu zarządzania bezpieczeństwem informacji w oparciu o praktykę stosowaną w tym zakresie w administracji federalnej USA.

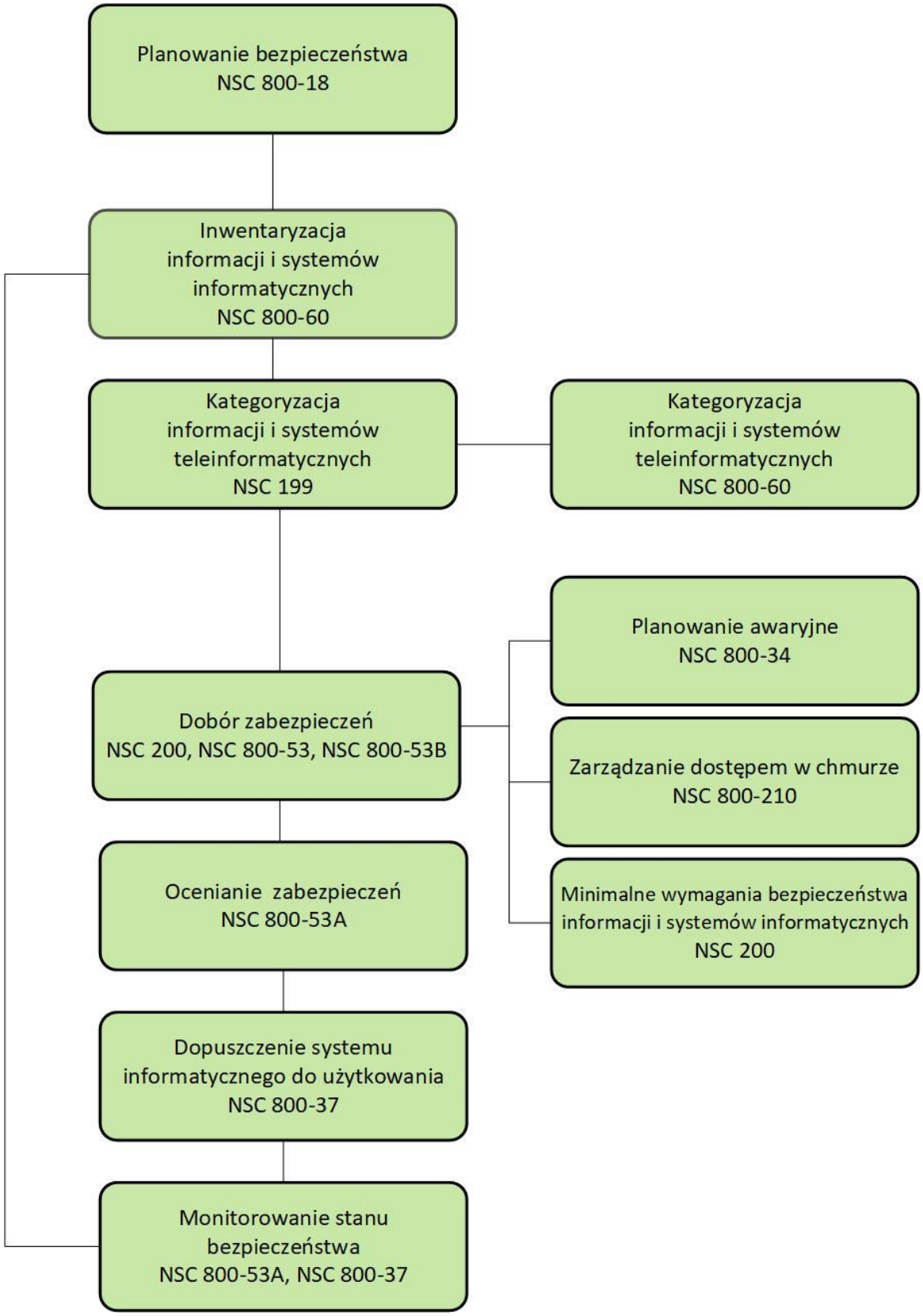
Zestaw publikacji specjalnych obejmuje następujące pozycje:

- NSC 199, Standardy kategoryzacji bezpieczeństwa – na podstawie FIPS 199.
- NSC 200, Minimalne wymagania bezpieczeństwa informacji i systemów informacyjnych podmiotów publicznych – na podstawie FIPS 200.
- NSC 800-18, Przewodnik do opracowywania planów bezpieczeństwa systemów informacyjnych w podmiotach publicznych – na podstawie NIST SP 800-18.
- 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 informacyjnych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu – na podstawie NIST SP 800-37.

- NSC 800-39, Zarządzanie ryzykiem bezpieczeństwa informacji. Przegląd struktury organizacyjnej, misji i systemu informacyjnego – na podstawie NIST SP 800-39.
- NSC 800-53, Zabezpieczenia i ochrona prywatności systemów informacyjnych oraz organizacji – na podstawie NIST SP 800-53.
- NSC 800-53A, Ocenianie środków bezpieczeństwa i ochrony prywatności systemów informacyjnych oraz organizacji. Tworzenie skutecznych planów oceny – na podstawie NIST SP 800-53A.
- NSC 800-53B, Zabezpieczenia bazowe systemów informacyjnych oraz organizacji – na podstawie NIST SP 800-53B.
- NSC 800-60, Wytyczne w zakresie określania kategorii bezpieczeństwa informacji i kategorii bezpieczeństwa systemu informacyjnego – 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.

W oparciu o te publikacje można stosunkowo łatwo zbudować system zarządzania bezpieczeństwem informacji i sprawować nad nim niezbędną kontrolę.

Cykl zarządzania bezpieczeństwem informacji bazujący na publikacjach NIST wykorzystuje następujące dokumenty:



Cykl zarządzania bezpieczeństwem informacji

WSPÓLNE FUNDAMENTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI

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

NIST kontynuuje współpracę z sektorem publicznym i prywatnym w celu stworzenia map i relacji pomiędzy opracowanymi przez siebie standardami i wytycznymi, a tymi, które zostały opracowane przez inne organizacje (m. in. ISO[1]), co zapewnia zgodność w przypadku, gdy regulacje wymagają stosowania tych innych standardów.

Publikacje NIST co do zasady nie są objęte restrykcjami wynikającymi z autorskich praw majątkowych. Są powszechnie dostępne oraz dopuszczone do użytku poza administracją federalną USA. Charakteryzują się pragmatycznym podejściem do zagadnień związanych z bezpieczeństwem informacji i systemów informacyjnych 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

[1] International Organization for Standardization (ISO) - Międzynarodowa Organizacja Normalizacyjna– organizacja pozarządowa zrzeszająca krajowe organizacje normalizacyjne.

podmioty przy opracowywaniu systemów zarządzania bezpieczeństwem informacji, wdrażaniu zabezpieczeń i ocenie ich działania.

Podmioty, urządzenia lub materiały prezentowane są w niniejszym dokumencie w celu odpowiedniego opisania procedury lub koncepcji eksperymentalnej. Celem ich wskazania nie jest nakłanianie do korzystania z ww. podmiotów, urządzeń lub materiałów lub ich poparcie. Wskazanie ich nie ma również na celu sugerowania, że te podmioty, materiały lub sprzęt są najlepsze z dostępnych w danej dziedzinie.

W niniejszej publikacji mogą znajdować się odniesienia do innych opracowywanych przez nas publikacji. Informacje tu zawarte, 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 powinny obowiązywać dotychczasowe wymagania, wytyczne i procedury, jeśli takie istnieją. W ramach planowanych przez Państwa prac zalecamy śledzenie naszych prac publikacyjnych.

Aktualne informacje o prowadzonych przez nas pracach dostępne są pod adresem:

 Narodowe Standardy Cyberbezpieczeństwa

Jesteśmy również otwarci na wszelkie Państwa sugestie, które pomogą nam w dalszych pracach nad standardami cyberbezpieczeństwa i zachęcamy do kontaktu.

 +48222455922

 sekretariat.dc@kprm.gov.pl

Niniejszy publikacja NSC 199, ***Standardy Kategoryzacji Bezpieczeństwa***, opracowana została za zgodą National Institute of Science and Technology (NIST) na podstawie specjalnej publikacji FIPS PUB 199, *Standards for Security Categorization of Federal Information and Information Systems*.

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

SPIS TREŚCI

SPIS TABEL

1. CEL

Kompleksowe podejście do spraw związanych z cyberbezpieczeństwem opiera się na trzech fundamentach:

- Standardach, które wykorzystywane będą przez podmioty publiczne w celu kategoryzacji wszelkich informacji i systemów informacyjnych[2] (*ang. information system*) będących w posiadaniu lub utrzymywanych przez lub w imieniu każdego z tych podmiotów, na podstawie celów zapewniania stosownych poziomów bezpieczeństwa zgodnie z oszacowanym zakresem poziomów ryzyka.
- Wytycznych zawierających rekomendacje, co do rodzajów informacji i systemów informacyjnych mających zostać uwzględnionymi w każdej z kategorii.
- Minimalnych wymaganiach bezpieczeństwa informacji (tj. zarządczych, operacyjnych i technicznych mechanizmów zabezpieczeń) odnoszących się do informacji i systemów informacyjnych w każdej z tych kategorii.

Publikacja NSC 199 odnosi się do pierwszego z powyższych zadań – wypracowania standardów kategoryzacji informacji i systemów informacyjnych. Standardy kategoryzacji bezpieczeństwa dotyczące informacji i systemów informacyjnych dostarczają wspólne ramy dla wyrażenia bezpieczeństwa, które promują: (I) skuteczne zarządzanie i nadzór nad programami bezpieczeństwa informacji, w tym koordynację działań w zakresie bezpieczeństwa informacji podejmowanych na poziomie obywateli, bezpieczeństwa narodowego, gotowości na sytuacje awaryjne, bezpieczeństwa wewnętrznego oraz organów ścigania; oraz (II) spójne działania w zakresie adekwatności i skuteczności polityk, procedur i praktyk bezpieczeństwa informacji.

Kolejne standardy i wytyczne publikowane przez Pełnomocnika Rządu ds. Cyberbezpieczeństwa będą wypełniały drugie i trzecie z wymienionych tu zadań.

[2] System informacyjny – patrz: ustawa z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz. U. z 2018 r. poz. 1560 ze zm.

2. ZAKRES STOSOWANIA

Niniejsze standardy mają zastosowanie do: (I) wszelkich informacji, które organizacja uzna za informacje wrażliwe, wymagających ochrony przed nieupoważnionym; oraz (II) wszelkich systemów informacyjnych przetwarzających informacje jawne na szczeblu państwowym, samorządowym i przez przedsiębiorców będących Operatorami Usług Kluczowych lub Operatorami Infrastruktury Krytycznej. Osoby odpowiedzialne w każdej z jednostce organizacyjne są zobowiązane do wykorzystywania kategoryzacji bezpieczeństwa opisanych w publikacji NSC 199 zawsze, gdy występuje wymóg zapewnienia takiej kategoryzacji informacji lub systemów informacyjnych. Dopuszczalne jest opracowanie i wykorzystywanie dodatkowych oznaczeń bezpieczeństwa według uznania właściciela systemu informacyjnego. Instytucje państwowe, a także organizacje sektora prywatnego, obejmujące infrastrukturę krytyczną Rzeczpospolitej Polskiej mogą rozważyć stosowanie tych standardów.

3. KATEGORYZACJA INFORMACJI I SYSTEMÓW INFORMACYJNYCH

Niniejsza publikacja ustanawia kategorie bezpieczeństwa zarówno dla informacji[3], jak i systemów informacyjnych. Kategorie bezpieczeństwa oparte zostały na potencjalnym wpływie na organizację. Wpływ ten mógłby zostać wywarty przez określone zdarzenia zagrażające informacjom i systemom informacyjnym, wykorzystywanym przez tę organizację do wykonywania powierzonej jej misji, ochrony jej zasobów, wywiązania się z obowiązków prawnych, bieżącego funkcjonowania i ochrony osób. Kategorie bezpieczeństwa w ocenie ryzyka dla organizacji należy stosować w połączeniu z informacjami dotyczącymi podatności i zagrożeń.

3.1. ATRYBUTY BEZPIECZEŃSTWA

Określa się trzy główne atrybuty bezpieczeństwa informacji i systemów informacyjnych:

Poufność

Zapewnienie stosowania zatwierdzonych ograniczeń w zakresie ujawniania i dostępu do informacji, w tym środków ochrony prywatności i informacji osobistych. Utrata *poufności* oznacza nieuprawnione ujawnienie informacji.

Integralność

Ochrona przed niewłaściwą modyfikacją lub zniszczeniem informacji, w tym zapewnienie niezaprzeczalności i autentyczności informacji. Utrata *integralności* oznacza nieuprawnioną modyfikację lub zniszczenie informacji.

[3] Informacje są dzielone na kategorie według rodzaju informacji. Rodzaj informacji to kategoria informacji (np. informacje dotyczące prywatności, informacje medyczne, informacje zastrzeżone, informacje finansowe, informacje śledcze, informacje wrażliwe dot. kontrahentów, informacje w zakresie zarządzania bezpieczeństwem) określona przez organizację lub – w niektórych przypadkach – przez szczególny przepis prawa, zarządzenie wykonawcze, dyrektywę, politykę lub regulację.

Dostępność

Zapewnienie terminowego i niezawodnego dostępu i możliwości wykorzystania informacji. Utrata *dostępności* oznacza zaburzenie dostępu lub możliwości wykorzystania informacji lub systemu informacyjnego.

3.2. POTENCJALNY WPŁYW NA ORGANIZACJE I OSOBY FIZYCZNE

Publikacja NSC 199 definiuje trzy poziomy potencjalnego wpływu na organizacje i osoby fizyczne w przypadkach wystąpienia naruszenia bezpieczeństwa (tj. utraty poufności, integralności lub dostępności). Stosowanie tych definicji musi być dokonywane w kontekście danej organizacji.

Potencjalny wpływ jest **NISKI**, jeżeli można oczekiwać **ograniczonego** negatywnego wpływu utraty poufności, integralności lub dostępności na działalność organizacji, jej zasoby lub osoby fizyczne.[4]

*Wyjaśnienie: **Ograniczony** negatywny wpływ oznacza np. taką utratę poufności, integralności lub dostępności, która może: (I) spowodować nieznaczne pogorszenie zdolności organizacji w takim stopniu i przez taki okres, że wprawdzie jest ona w stanie wykonywać swoje podstawowe funkcje, jednak ich skuteczność jest znacząco ograniczona; (II) skutkować nieznacznym uszkodzeniem aktywów organizacji; (III) skutkować nieznaczną stratą finansową; lub (IV) skutkować nieznaczną szkodą dla osób fizycznych.*

Potencjalny wpływ jest **UMIARKOWANY**, jeżeli można oczekiwać **poważnego** negatywnego wpływu utraty poufności, integralności lub dostępności na działalność organizacji, jej zasoby lub osoby fizyczne.

*Wyjaśnienie: **Poważny** negatywny wpływ oznacza np. taką utratę poufności, integralności lub dostępności, która może: (I) spowodować znaczne pogorszenie zdolności organizacji w takim stopniu i przez taki okres, że wprawdzie jest ona w stanie wykonywać swoje podstawowe funkcje, jednak ich skuteczność jest znacząco ograniczona; (II) skutkować znacznym uszkodzeniem aktywów organizacji; (III) skutkować znaczną stratą finansową; lub (IV)*

[4] Niekorzystne skutki dla osób fizycznych mogą obejmować m.in. utratę określonej przepisami prawa do prywatności.

skutkować znaczną szkodą dla osób fizycznych, jednak z wyłączeniem utraty życia i urazów zagrażających życiu.

Potencjalny wpływ jest **WYSOKI**, jeżeli można oczekiwać **drastycznie lub katastrofalnie** negatywnego wpływu utraty poufności, integralności lub dostępności na działalność organizacji, jej zasoby lub osoby fizyczne.

*Wyjaśnienie: **Drastyczny lub katastrofalny**, negatywny wpływ oznacza np. taką utratę poufności, integralności lub dostępności, która może: (I) spowodować drastyczne pogorszenie lub utratę zdolności organizacji w takim stopniu i przez taki okres, że nie jest ona w stanie wykonywać swoich podstawowych funkcji; (II) skutkować poważnym uszkodzeniem aktywów organizacji; (III) skutkować poważną stratą finansową; lub (IV) skutkować drastyczną lub katastrofalną szkodą dla osób fizycznych, w tym utraty życia i urazów zagrażających życiu.*

3.3. KATEGORYZACJA BEZPIECZEŃSTWA W ODNIESIENIU DO RODZAJÓW INFORMACJI

Kategoria bezpieczeństwa rodzaju informacji może być powiązana zarówno z informacjami użytkownika, jak i informacjami na poziomie systemu[5] i może mieć zastosowanie do informacji w formie elektronicznej oraz nieelektronicznej. Można jej również używać, jako danych wejściowych na potrzeby ustalenia odpowiedniej kategorii bezpieczeństwa systemu informacyjnego (patrz: określanie kategorii bezpieczeństwa systemów informacyjnych). Ustanowienie właściwej kategorii bezpieczeństwa dla rodzaju informacji wymaga określenia *potencjalnego wpływu* dla każdego atrybutu bezpieczeństwa związanego z danym rodzajem informacji.

Uogólniona formuła wyrażania kategorii bezpieczeństwa (**KB**) dla rodzaju informacji przedstawiona została poniżej:

[5] Informacje o systemie (np. tabele routingu sieciowego, pliki haseł i informacje dotyczące zarządzania kluczami kryptograficznymi) muszą być chronione na poziomie współmiernym do najbardziej krytycznych lub wrażliwych informacji użytkownika przetwarzanych, przechowywanych lub przesyłanych przez system informacyjny, tak, aby zapewnić ich poufność, integralność, i dostępność.

KB rodzaju informacji = {(**poufność**, *wpływ*), (**integralność**, *wpływ*), (**dostępność**, *wpływ*)}, gdzie dopuszczalne wartości potencjalnego wpływu to NISKI, UMIARKOWANY, WYSOKI, oraz NIE DOTYCZY[6].

PRZYKŁAD 1: Organizacja zarządzająca informacją publiczną na swoim serwerze www określa, iż nie występuje potencjalny wpływ utraty poufności (tj. wymagania na poufność nie mają zastosowania), umiarkowany potencjalny wpływ utraty integralności, oraz umiarkowany potencjalny wpływ utraty dostępności. Wynikowa kategoria bezpieczeństwa (KB) tego rodzaju informacji wyrażona jest, jako:

KB informacji publicznej = {(**poufność**, ND), (**integralność**, UMIARKOWANY), (**dostępność**, UMIARKOWANY)}.

PRZYKŁAD 2: Organ ścigania, zarządzający wysoce wrażliwą informacją śledczą określa, iż potencjalny wpływ utraty poufności jest wysoki. Natomiast potencjalny wpływ utraty integralności jest umiarkowany a potencjalny wpływ utraty dostępności jest umiarkowany. Wynikowa kategoria bezpieczeństwa (KB) tego rodzaju informacji wyrażona jest, jako:

KB informacji śledczej = {(**poufność**, WYSOKI), (**integralność**, UMIARKOWANY), (**dostępność**, UMIARKOWANY)}.

PRZYKŁAD 3: Organizacja finansowa zarządzająca informacją administracyjną (niezwiązaną z prywatnością) określa, iż potencjalny wpływ utraty poufności jest niski. Także potencjalny wpływ utraty integralności i utraty dostępności jest niski. Wynikowa kategoria bezpieczeństwa (KB) tego rodzaju informacji wyrażona jest, jako:

KB informacji administracyjnej = {(**poufność**, NISKI), (**integralność**, NISKI), (**dostępność**, NISKI)}.

3.4. KATEGORYZACJA BEZPIECZEŃSTWA W ODNIESIENIU DO SYSTEMÓW INFORMACYJNYCH

Określenie kategorii bezpieczeństwa systemu informacyjnego wymaga pogłębionej analizy, jak również musi uwzględniać kategorie bezpieczeństwa wszystkich rodzajów

[6] Potencjalna wartość wpływu *NIE DOTYCZY* ma zastosowanie wyłącznie w odniesieniu do atrybutu bezpieczeństwa: zachowanie poufności.

informacji przetwarzanych w systemie informacyjnym. W przypadku systemu informacyjnego, potencjalne wartości wpływu przypisane do stosownych atrybutów bezpieczeństwa (poufności, integralności, dostępności) są to najwyższe wartości (koncepcja najwyższej wartości – *ang. high water mark*)[7] spośród tych kategorii bezpieczeństwa, które zostały określone dla poszczególnych rodzajów informacji przetwarzanych w tym systemie informacyjnym[8].

Uogólniona formuła wyrażania kategorii bezpieczeństwa (KB) dla systemu informacyjnego przedstawiona została poniżej:

KB systemu informacyjnego = {(**poufność**, *wpływ*), (**integralność**, *wpływ*), (**dostępność**, *wpływ*)}, gdzie dopuszczalne wartości potencjalnego wpływu to NISKI, UMIARKOWANY, oraz WYSOKI.

Należy zwrócić uwagę, że **wartość *NIE DOTYCZY* nie może zostać przypisana do żadnego z atrybutów bezpieczeństwa w kontekście ustalania kategorii bezpieczeństwa systemu informacyjnego**. Odzwierciedla to fakt, iż występuje niski minimalny potencjalny wpływ (koncepcja najniższej wartości - *ang. low water mark*) utraty poufności, integralności i dostępności systemu informacyjnego w związku z fundamentalnym wymaganiem ochrony funkcji przetwarzania na poziomie systemu i informacji krytycznych dla działania systemu informacyjnego.

[7] Stosowana jest koncepcja najwyższej wartości, ponieważ istnieją znaczące zależności pomiędzy atrybutami bezpieczeństwa, takimi jak poufność, integralność i dostępność. W większości przypadków naruszenie jednego z atrybutów bezpieczeństwa ostatecznie wpływa również na pozostałe atrybuty bezpieczeństwa. W związku z tym środki bezpieczeństwa nie są kategoryzowane według atrybutów bezpieczeństwa. Natomiast są grupowane w zabezpieczenia bazowe mające na celu zapewnienia ogólnej zdolności ochrony poszczególnych klas systemów w oparciu o poziom wpływu na te systemy.

[8] Uznaje się, że systemy informacyjne składają się zarówno z programów, jak i informacji oraz infrastruktury IT zapewniającej ich funkcjonowanie. Programy w trakcie ich wykonywania w systemie informacyjnym (tj. procesy systemowe) ułatwiają przetwarzanie, przechowywanie i przesyłanie informacji i są niezbędne organizacjom do wykonywania ich podstawowych funkcji i operacji związanych z ich misją. Funkcje przetwarzania systemu również wymagają ochrony i mogą również podlegać kategoryzacji bezpieczeństwa. Jednak w celu uproszczenia zakłada się, że kategoryzacja wszystkich rodzajów informacji związanych z systemem informacyjnym pod względem bezpieczeństwa zapewnia odpowiedni najgorszy możliwy potencjalny wpływ na cały system informacyjny – eliminując w ten sposób potrzebę uwzględnienia procesów systemowych w kategoryzacji bezpieczeństwa systemu informacyjnego.

PRZYKŁAD 4: System informacyjny stosowany przy dużych akwizycjach przetwarza zarówno wrażliwe informacje o umowach na etapie poprzedzającym ich zawieranie, jak i informacje administracyjne. Kierownictwo organizacji ustala, że: (I) w przypadku wrażliwych informacji o umowie potencjalny wpływ utraty poufności jest umiarkowany, potencjalny wpływ utraty integralności jest umiarkowany, oraz potencjalny wpływ utraty dostępności jest niski; oraz (II) w przypadku informacji administracyjnych (niezwiązanych z prywatnością) potencjalny wpływ utraty poufności jest niski, potencjalny wpływ utraty integralności jest niski, oraz potencjalny wpływ utraty dostępności jest niski. Wynikowe kategorie bezpieczeństwa (KB) tych rodzajów informacji są wyrażone, jako:

KB informacji o umowach = {(**poufność**, UMIARKOWANY), (**integralność**, UMIARKOWANY), (**dostępność**, NISKI)},

oraz

KB informacji administracyjnej = {(**poufność**, NISKI), (**integralność**, NISKI), (**dostępność**, NISKI)}.

Wynikowa kategoria bezpieczeństwa systemu informacyjnego wyrażona jest, jako:

KB systemu wykorzystywanego przy akwizycji = {(**poufność**, UMIARKOWANY), (**integralność**, UMIARKOWANY), (**dostępność**, NISKI)},

przedstawiając najwyższy wpływ lub potencjalnie maksymalne wartości wpływu poszczególnych atrybutów bezpieczeństwa dla rodzajów informacji przetwarzanych w systemie wykorzystywanym przy akwizycji.

PRZYKŁAD 5: Elektrownia posiada system kontroli nadzorczej i pozyskiwania danych *(ang. Supervisory Control and Data Acquisition – SCADA) kontrolujący rozdział energii elektrycznej w dużej instalacji wojskowej. System SCADA przetwarza zarówno dane czasu rzeczywistego z czujników, jak i informacje administracyjne. Kierownictwo w elektrowni ustala, że: (i) w przypadku danych z czujników pozyskiwanych przez system SCADA nie występuje potencjalny wpływ utraty poufności, natomiast potencjalny wpływ utraty integralności i dostępności jest wysoki; oraz (ii) w przypadku informacji administracyjnych*

przetwarzanych przez system występuje niewielki potencjalny wpływ utraty poufności, niski potencjalny wpływ utraty integralności oraz niski potencjalny wpływ utraty dostępności. Wynikowe kategorie bezpieczeństwa (KB) tych rodzajów informacji wyrażane są, jako:

KB danych z czujników = {(**poufność**, NIE DOTYCZY), (**integralność**, WYSOKI), (**dostępność**, WYSOKI)},

oraz

KB informacji administracyjnej = {(**poufność**, NISKI), (**integralność**, NISKI), (**dostępność**, NISKI)}.

Wynikowa kategoria bezpieczeństwa systemu informacyjnego wyrażona jest, jako:

KB systemu SCADA = {(**poufność**, NISKI), (**integralność**, WYSOKI), (**dostępność**, WYSOKI)},

przedstawiając najwyższy wpływ lub potencjalnie maksymalne wartości wpływu poszczególnych atrybutów bezpieczeństwa dla rodzajów informacji przetwarzanych w systemie SCADA. Zarząd elektrowni wybiera podniesienie potencjalnego wpływu utraty poufności z niskiego do umiarkowanego w celu odzwierciedlenia bardziej realistycznego obrazu potencjalnego wpływu na system informacyjny w sytuacji, w której wystąpiłoby naruszenie bezpieczeństwa związane z nieuprawnionym ujawnieniem informacji na poziomie systemu lub funkcji przetwarzania. Ostateczna kategoria bezpieczeństwa systemu informacyjnego wyrażana jest, jako:

KB systemu SCADA = {(**poufność**, UMIARKOWANY), (**integralność**, WYSOKI), (**dostępność**, WYSOKI)},

Tabela 1 zawiera podsumowanie definicji potencjalnego wpływu dla poszczególnych atrybutów bezpieczeństwa – poufności, integralności i dostępności.

Tabela 1. Definicje potencjalnego wpływu na atrybuty bezpieczeństwa.

Atrybut bezpieczeństwa	**Potencjalny wpływ**		
	Niski	**Umiarkowany**	**Wysoki**
Poufność Zapewnienie stosowania zatwierdzonych ograniczeń w zakresie ujawniania i dostępu do informacji, w tym środków ochrony prywatności i informacji osobistych.	Można oczekiwać **ograniczonego** negatywnego wpływu nieuprawnionego ujawnienia informacji na działalność organizacji, jej zasoby lub osoby fizyczne.	Można oczekiwać **poważnego** negatywnego wpływu nieuprawnionego ujawnienia informacji na działalność organizacji, jej zasoby lub osoby fizyczne.	Można oczekiwać **drastycznie lub katastrofalnie** negatywnego wpływu nieuprawnionego ujawnienia informacji na działalność organizacji, jej zasoby lub osoby fizyczne.
Integralność Ochrona przed niewłaściwą modyfikacją lub zniszczeniem informacji, w tym zapewnienie niezaprzeczalności i autentyczności informacji.	Można oczekiwać **ograniczonego** negatywnego wpływu nieuprawnionej modyfikacji lub zniszczenia informacji na działalność organizacji, jej zasoby lub osoby fizyczne.	Można oczekiwać **poważnego** negatywnego wpływu nieuprawnionej modyfikacji lub zniszczenia informacji na działalność organizacji, jej zasoby lub osoby fizyczne.	Można oczekiwać **drastycznie lub katastrofalnie** negatywnego wpływu nieuprawnionej modyfikacji lub zniszczenia informacji na działalność organizacji, jej zasoby lub osoby fizyczne.

Atrybut bezpieczeństwa	**Potencjalny wpływ**		
	Niski	**Umiarkowany**	**Wysoki**
Dostępność Zapewnienie terminowego i niezawodnego dostępu i możliwości wykorzystania informacji.	Można oczekiwać **ograniczonego** negatywnego wpływu zaburzenia dostępu lub możliwości wykorzystania informacji na działalność organizacji, jej zasoby lub osoby fizyczne.	Można oczekiwać **poważnego** negatywnego wpływu zaburzenia dostępu lub możliwości wykorzystania informacji na działalność organizacji, jej zasoby lub osoby fizyczne.	Można oczekiwać **drastycznie lub katastrofalnie** negatywnego wpływu zaburzenia dostępu lub możliwości wykorzystania informacji na działalność organizacji, jej zasoby lub osoby fizyczne.

ZAŁĄCZNIK A SŁOWNIK I AKRONIMY

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

ZAŁĄCZNIK B REFERENCJE

NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA[9]	
NSC 200	Minimalne wymagania bezpieczeństwa informacji i systemów informacyjnych podmiotów publicznych – na podstawie FIPS 200
NSC 800-18	Przewodnik do opracowywania planów bezpieczeństwa systemów informacyjnych w podmiotach publicznych – na podstawie NIST SP 800- 18
NSC 800-37	Ramy zarządzania ryzykiem w organizacjach i systemach informacyjnych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu – na podstawie NIST SP 800-37
NSC 800-53	Zabezpieczenia i ochrona prywatności systemów informacyjnych oraz organizacji – na podstawie NIST SP 800-53
NSC 800-53B	Zabezpieczenia bazowe systemów informacyjnych oraz organizacji – na podstawie NIST SP 800-53B
NSC 800-53 MAP	Mapowanie środków bezpieczeństwa: NSC 800-53 wer. 2 – PN-ISO/IEC 27001:2013; PN-ISO/IEC 27001:2013 – NSC 800-53 wer. 2 Patrz: SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations
NSC 800-60	Wytyczne w zakresie określania kategorii bezpieczeństwa informacji I kategorii bezpieczeństwa systemu informacyjnego – na podstawie NIST SP 800-60

[9] Narodowe Standardy Cyberbezpieczeństwa

PUBLIKACJE ANGLOJĘZYCZNE[10]	
[1]	Privacy Act of 1974 (Public Law 93-579), September 1975.
[2]	Paperwork Reduction Act of 1995 (Public Law 104-13), May 1995.
[3]	OMB Circular A-130, Transmittal Memorandum #4, Management of Federal Information Resources, November 2000.
[4]	Information Technology Management Reform Act of 1996 (Public Law 104-106), August 1996.
[5]	Federal Information Security Management Act of 2002 (Public Law 107-347), December 2002.

[10] Referencje zostały podane w celach uzupełniających dla osób zainteresowanych.