NSC NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA	Narodowy Standard Cyberbezpieczeństwa		
Nazwa standardu	Symbol	Wersja	Data wydania
Minimalne wymagania bezpieczeństwa informacji i systemów informatycznych podmiotów publicznych	**NSC 200**	2.0	01/09/2021

Minimalne wymagania bezpieczeństwa informacji i systemów informatycznych podmiotów publicznych

PEŁNOMOCNIK RZĄDU DS. CYBERBEZPIECZEŃSTWA
Warszawa 2021

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:[1]

- NSC[2] 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;

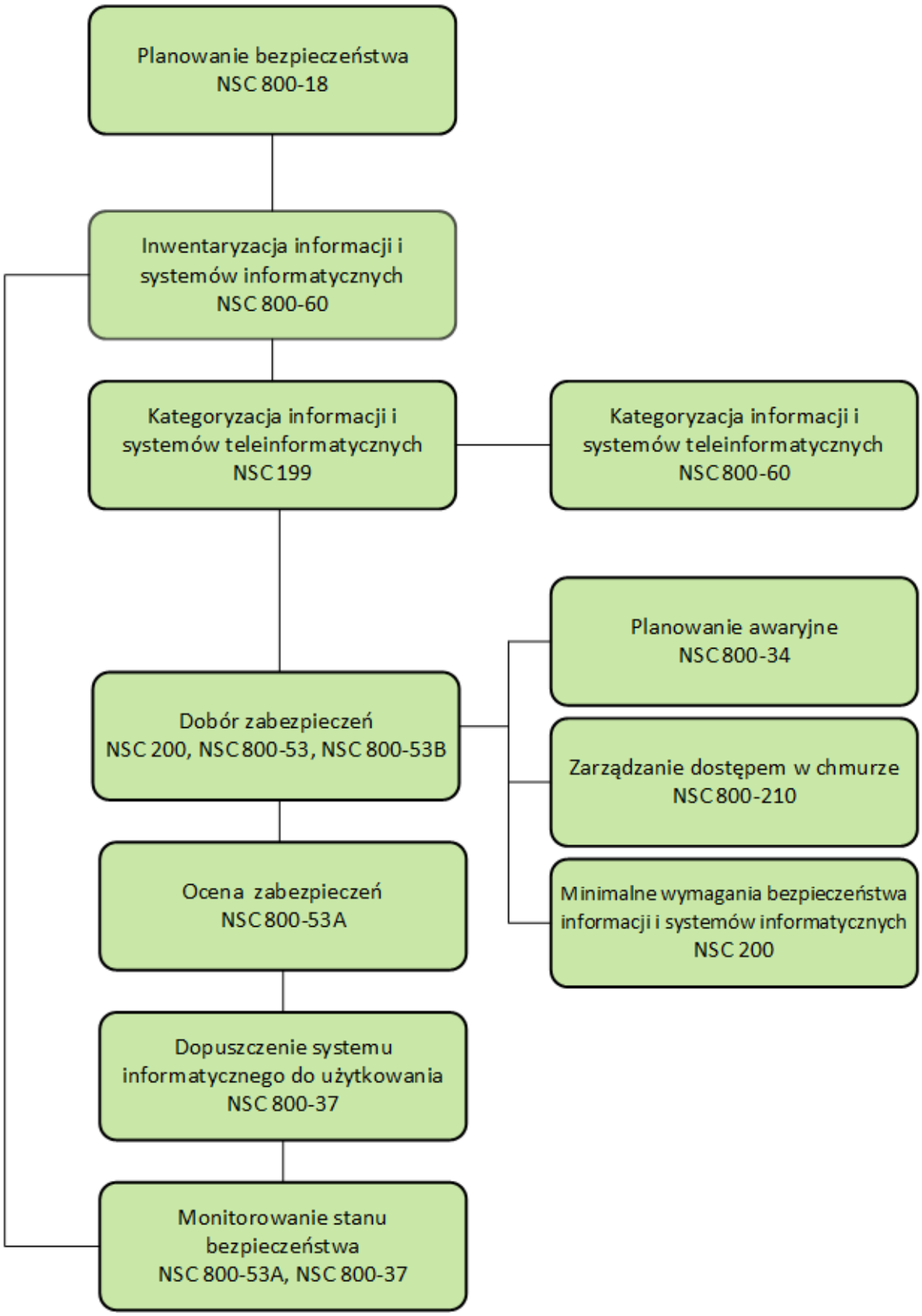
[1] Wymienione są podstawowe dokumenty. Każdy z nich może się odwoływać w rozdziale *Referencje* do szeregu powiązanych publikacji, które składają się na całościowy proces osiągania cyberbezpieczeństwa.

[2] 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, *Ocena 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:


Planowanie bezpieczeństwa
NSC 800-18
Inwentaryzacja informacji i systemów informatycznych
NSC 800-60
Kategoryzacja informacji i systemów teleinformatycznych
NSC 199
Kategoryzacja informacji i systemów teleinformatycznych
NSC 800-60
Planowanie awaryjne
NSC 800-34
Dobór zabezpieczeń
NSC 200, NSC 800-53, NSC 800-53B
Zarządzanie dostępem w chmurze
NSC 800-210
Ocena zabezpieczeń
NSC 800-53A
Minimalne wymagania bezpieczeństwa informacji i systemów informatycznych
NSC 200
Dopuszczenie systemu informatycznego do użytkowania
NSC 800-37
Monitorowanie stanu bezpieczeństwa
NSC 800-53A, NSC 800-37

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 informacyjnych, 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 tych 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 podejście 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 opisania 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 (NSC) 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.

Niniejszy publikacja, ***Minimalne wymagania bezpieczeństwa informacji i systemów informatycznych podmiotów publicznych***, opracowana została za zgodą National Institute of Science and Technology (NIST) na podstawie publikacji FIPS PUB 200.

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***.

Uwaga:

W standardzie NSC 200 wer. 2.0 przywoływany jest standard NSC 800-53 wer. 2.0 (bazujący na publikacji NIST SP 800-53 rev. 5) oraz standard NSC 800-53B (bazujący na publikacji NIST SP 800-53B).

SPIS TREŚCI

1. WPROWADZENIE

Opracowane zostały standardy w zakresie: (i) kategoryzacji bezpieczeństwa informacji i systemów informatycznych w oparciu o cele zapewnienia odpowiedniego poziomu bezpieczeństwa informacji w zależności od zakresu poziomów ryzyka; oraz (ii) minimalnych wymagań bezpieczeństwa dla informacji i systemów informatycznych w każdej z tych kategorii.[3]

Niniejszy standard dotyczy specyfikacji minimalnych wymagań bezpieczeństwa informacji i systemów informatycznych w sektorze publicznym. Określa minimalne wymagania bezpieczeństwa systemów informatycznych w siedemnastu obszarach związanych z bezpieczeństwem. Organizacje powinny spełniać minimalne wymagania bezpieczeństwa określone w niniejszym dokumencie poprzez stosowanie środków bezpieczeństwa zgodnie ze standardem NSC 800-53.

Stosowanie środków bezpieczeństwa określonych w standardzie NSC 800-53 i wymaganych przez ten standard stanowi aktualny stan praktycznych zabezpieczeń i środków zaradczych dla systemów informatycznych. Zabezpieczenia te będą poddawane przeglądowi przez Kolegium ds. Cyberbezpieczeństwa co najmniej raz w roku, oraz w razie potrzeby zmieniane i rozszerzane w celu odzwierciedlenia: (i) doświadczenia zdobytego podczas korzystania z zabezpieczeń; (ii) zmieniających się wymagań w zakresie bezpieczeństwa informacji; oraz (iii) nowych, dostępnych technologii bezpieczeństwa. Oczekuje się również, że minimalne mechanizmy zabezpieczeń określone dla systemów informatycznych podlegających niskim, umiarkowanym i wysokim wpływom zakłócenia, również będą się zmieniać w miarę zmian w czasie, a poziom bezpieczeństwa i należytej staranności w zakresie ograniczania ryzyka w organizacjach będzie wzrastał.

[3] Zdefiniowany zgodnie ze standardem NSC 800-53B zestaw minimalnych zabezpieczeń / zabezpieczeń bazowych (*ang. Security control baselines)* systemu informatycznego o niskim, umiarkowanym lub o dużym wpływie zakłócenia na atrybuty bezpieczeństwa informacji (poufność, integralność, dostępność). Ustanowiony w wyniku podjętych działań planowania strategicznego bezpieczeństwa informacji w celu określenia jednej lub kilku kategoryzacji zabezpieczeń (określanych zgodnie ze standardem NSC 199). Ten zestaw zabezpieczeń jest początkowym zbiorem środków bezpieczeństwa wybranym dla określonego systemu informatycznego po określeniu kategoryzacji zabezpieczeń systemu.

Proponowane uzupełnienia, usunięcia lub modyfikacje zabezpieczeń oraz zmiany minimalnych środków bezpieczeństwa określonych w standardzie NSC 800-53 przejdą rygorystyczny, publiczny proces przeglądu w celu uzyskania informacji zwrotnych dla sektora podmiotów publicznych oraz do wypracowania konsensusu w sprawie zmian

2. CEL

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

1) Standardach, które wykorzystywane będą przez podmioty publiczne w celu kategoryzacji wszelkich informacji i systemów informatycznych 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;

2) Wytycznych zawierających rekomendacje, co do rodzajów informacji i systemów informatycznych, mających zostać uwzględnionymi w każdej z kategorii; oraz

3) Minimalnych wymaganiach bezpieczeństwa informacji (tj. zarządczych, operacyjnych i technicznych mechanizmów zabezpieczeń) odnoszących się do informacji i systemów informatycznych w każdej z tych kategorii.

Standard NSC 199, Standardy kategoryzacji bezpieczeństwa, jest jednym ze standardów odnoszących się do pierwszego z powyższych fundamentów – wypracowania standardów kategoryzacji informacji i systemów informatycznych. Standard NSC 200, drugi ze standardów bezpieczeństwa odnoszących się do pierwszego z powyższych fundamentów, określa minimalne wymagania bezpieczeństwa informacji i systemów informatycznych oraz proces wyboru środków bezpieczeństwa niezbędny do zapewnienia minimalnych wymogów bezpieczeństwa zgodnie z oszacowanym zakresem poziomów ryzyka. Standard ten będzie wspierać rozwój, wdrażanie i funkcjonowanie bezpieczniejszych systemów informatycznych poprzez ustanowienie minimalnych poziomów należytej staranności w zakresie bezpieczeństwa informacji i ułatwienie bardziej spójnego, porównywalnego i powtarzalnego podejścia do wyboru i określania zabezpieczeń systemów informatycznych spełniających minimalne wymagania bezpieczeństwa.

3. POZIOMY WPŁYWU ZAKŁÓCENIA NA SYSTEM INFORMATYCZNY

Standard NSC 199 definiuje trzy poziomy potencjalnego wpływu zakłócenia na organizacje i osoby fizyczne powodującego naruszenie bezpieczeństwa (tj. utratę 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.

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

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.

Określenie kategorii bezpieczeństwa systemu informatycznego wymaga pogłębionej analizy, jak również musi uwzględniać kategorie bezpieczeństwa wszystkich rodzajów informacji przetwarzanych w systemie informatycznym. W przypadku systemu informatycznego, potencjalne wartości wpływu przypisane do stosownych atrybutów bezpieczeństwa (poufności, integralności, dostępności) są to najwyższe wartości[4] (*ang. high water mark*) spośród tych atrybutów, które zostały określone dla poszczególnych rodzajów informacji przetwarzanych w danym systemie informatycznym.

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

[4] 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.

KB system informatycznego = {(**poufność**, *wpływ*), (**integralność**, *wpływ*), (**dostępność**, *wpływ*)},

gdzie dopuszczalne wartości potencjalnego wpływu to NISKI, UMIARKOWANY, oraz WYSOKI.

Ponieważ potencjalne wartości wpływu na atrybuty bezpieczeństwa (poufność, integralność i dostępność) mogą nie zawsze być takie same dla danego systemu informatycznego, do określenia ogólnego poziomu oddziaływania na system informatyczny należy zastosować koncepcję najwyższej wartości spośród tych kategorii bezpieczeństwa, które zostały określone dla poszczególnych rodzajów informacji przetwarzanych w tym systemie informatycznym.

W związku z tym, system o ***niskim*** wpływie jest systemem informatycznym, w którym wpływ na wszystkie trzy atrybuty bezpieczeństwa jest ***niski***.

System o ***umiarkowanym*** wpływie jest systemem informatyczny, w którym wpływ, na co najmniej jeden z atrybutów bezpieczeństwa jest ***umiarkowany*** i żaden atrybut bezpieczeństwa nie podlega wpływowi większemu niż ***umiarkowany***.

System o ***wysokim*** wpływie jest systemem informatycznym, w którym wpływ, na co najmniej jeden atrybut bezpieczeństwa, jest **wysoki**.

Określenie poziomów oddziaływania systemu informatycznego musi zostać osiągnięte przed określeniem minimalnych wymogów bezpieczeństwa i wyborem odpowiednich środków bezpieczeństwa systemów informatycznych.

4. MINIMALNE WYMAGANIA BEZPIECZEŃSTWA

Minimalne wymagania bezpieczeństwa obejmują dwadzieścia obszarów związanych z bezpieczeństwem w odniesieniu do ochrony poufności, integralności i dostępności systemów informatycznych oraz informacji przetwarzanych, przechowywanych i przekazywanych przez te systemy. Obszary związane z bezpieczeństwem obejmują: (i) kontrolę dostępu; (ii) uświadamianie i szkolenia; (iii) audyt i rozliczalność; (iv) ocenę, autoryzację i monitorowanie ; (v) zarządzanie konfiguracją; (vi) planowanie awaryjne / ciągłość działania; (vii) identyfikację i uwierzytelnienie; (viii) reagowanie na incydenty; (ix) utrzymanie i wsparcie; (x) ochronę nośników danych; (xi) ochronę fizyczną i środowiskową; (xii) planowanie; (xiii) programy zarządzania; (xiv) bezpieczeństwo osobowe; (xv) przejrzystość przetwarzania danych osobowych; (xvi) ocenę ryzyka; (xvii) nabywanie systemu i usług; (xviii) ochronę systemów i sieci telekomunikacyjnych; (xix) integralność systemu i informacji oraz (xx) zarządzanie ryzykiem w łańcuchu dostaw. Dwadzieścia obszarów reprezentuje szeroko zakrojony, zrównoważony program bezpieczeństwa informacji, który dotyczy zarządzania, operacyjnych i technicznych aspektów ochrony informacji i systemów informatycznych.

Zasady i procedury odgrywają ważną rolę w skutecznym wdrażaniu programów bezpieczeństwa informacji w całej organizacji i stanowią o sukcesie wynikającym ze stosowania środków bezpieczeństwa w celu ochrony informacji i systemów informatycznych. W związku z tym, organizacje powinny opracować i propagować formalne, udokumentowane zasady i procedury regulujące minimalne wymogi bezpieczeństwa określone w niniejszym standardzie i powinny zapewnić ich skuteczne wdrożenie.

SPECYFIKACJE DOTYCZĄCE MINIMALNYCH WYMAGAŃ BEZPIECZEŃSTWA

Kontrola dostępu (*ang. Access Control - AC*): Organizacje powinny ograniczyć dostęp do systemu informatycznego do autoryzowanych użytkowników, procesów działających w imieniu autoryzowanych użytkowników lub urządzeń (w tym innych systemów informatycznych) oraz do typów transakcji i funkcji, które upoważnieni użytkownicy mogą wykonywać.

Uświadamianie i szkolenia (*ang. Awareness and Training - AT*): Organizacje powinny: (i) zapewnić, aby menedżerowie i użytkownicy organizacyjnych systemów informatycznych byli informowani o zagrożeniach bezpieczeństwa związanych z ich działalnością oraz o obowiązujących przepisach prawa, zarządzeniach wykonawczych, dyrektywach, zasadach, standardach, instrukcjach, przepisach lub procedurach związanych z bezpieczeństwem organizacyjnych systemów informatycznych; oraz (ii) zapewnić, aby personel organizacyjny był odpowiednio przeszkolony w zakresie wykonywania powierzonych mu zadań i obowiązków związanych z bezpieczeństwem informacji.

Audyt i rozliczalność (*ang. Audit and Accountability - AU*): Organizacje powinny: (i) tworzyć, chronić i przechowywać rejestry audytu systemu informatycznego w zakresie niezbędnym do umożliwienia monitorowania, analizy, badania i zgłaszania bezprawnych, nieautoryzowanych lub nieodpowiednich działań systemu informatycznego; oraz (ii) zapewnić, aby działania poszczególnych użytkowników systemu informatycznego mogły być jednoznacznie powiązane z tymi użytkownikami, tak, aby mogli oni zostać pociągnięci do odpowiedzialności za swoje działania.

Ocena, autoryzacja i monitorowanie (*ang. Certification, Accreditation, and Security Assessments – CA*): Organizacje powinny: (i) okresowo oceniać środki bezpieczeństwa w systemach informatycznych organizacji, w celu ustalenia, czy zabezpieczenia są skuteczne w ich stosowaniu; (ii) opracowywać i wdrażać plany działania mające na celu wyeliminowanie niedociągnięć oraz zmniejszenie lub wyeliminowanie luk w zabezpieczeniach organizacyjnych systemów informatycznych; (iii) autoryzować działanie organizacyjnych systemów informatycznych i wszelkich powiązanych połączeń systemów informatycznych; oraz (iv) na bieżąco monitorować środki bezpieczeństwa systemu informatycznego w celu zapewnienia ciągłej skuteczności zabezpieczeń.

Zarządzanie konfiguracją (*ang. Configuration Management - CM*): Organizacje powinny: (i) ustanowić i utrzymywać podstawowe konfiguracje i wykazy organizacyjnych systemów informatycznych (w tym sprzętu, oprogramowania, oprogramowania układowego i dokumentacji) w odpowiednich cyklach życia rozwoju systemu; oraz (ii) ustanowić

i egzekwować ustawienia konfiguracji zabezpieczeń dla produktów technologii informatycznych stosowanych w organizacyjnych systemach informatycznych.

Planowanie awaryjne / ciągłość działania (*ang. Contingency Planning - CP*): Organizacje powinny ustanawiać, utrzymywać i skutecznie wdrażać plany reagowania w sytuacjach awaryjnych, operacji tworzenia kopii zapasowych i odzyskiwania po awarii dla organizacyjnych systemów informatycznych, aby zapewnić dostępność krytycznych zasobów informatycznych i ciągłość operacji w sytuacjach awaryjnych.

Identyfikacja i uwierzytelnianie (*ang. Identification and Authentication - IA*): Organizacje powinny identyfikować użytkowników systemu informatycznego, procesy działające w imieniu użytkowników lub urządzenia oraz uwierzytelniać (lub weryfikować) tożsamości tych użytkowników, procesów lub urządzeń, jako wymóg zasadniczy umożliwiający dostęp do organizacyjnych systemów informatycznych.

Reagowanie na incydenty (*ang. Incident Response - IR*): Organizacje powinny: (i) ustanowić operacyjną zdolność obsługi incydentów dla organizacyjnych systemów informatycznych, która obejmuje odpowiednie przygotowanie, wykrywanie, analizę, powstrzymywanie, odzyskiwanie i działania związane z reagowaniem na potrzeby użytkownika; oraz (ii) śledzić, dokumentować i zgłaszać incydenty odpowiednim organom.

Utrzymanie i wsparcie (*ang. Maintenance - MA*): Organizacje powinny: (i) przeprowadzać okresową i terminową obsługę organizacyjnych systemów informatycznych; oraz (ii) zapewniać skuteczne zabezpieczenia narzędzi, technik, mechanizmów i personelu wykorzystywanego do przeprowadzania konserwacji systemu informatycznego.

Ochrona nośników danych (*ang. Media Protection - MP*): Organizacje powinny: (i) chronić nośniki systemowe, zarówno papierowe, jak i cyfrowe; (ii) zezwolić na dostęp do informacji o nośnikach systemu informatycznego tylko upoważnionym użytkownikom; oraz (iii) przeprowadzać sanityzację lub niszczyć nośniki systemu informatycznego przed utylizacją lub dopuszczeniem do ponownego użycia.

Ochrona fizyczna i środowiskowa (*ang. Physical and Environmental Potection* - PE): Organizacje powinny: (i) ograniczyć fizyczny dostęp do systemów informatycznych, sprzętu

i odpowiednich środowisk operacyjnych tylko do upoważnionych osób; (ii) chronić fizyczne instalacje i infrastrukturę wsparcia systemów informatycznych; (iii) zapewnić narzędzia wsparcia dla systemów informatycznych; (iv) chronić systemy informatyczne przed zagrożeniami środowiskowymi; oraz (v) zapewnić odpowiednie zabezpieczenia środowiskowe w obiektach zawierających systemy informatyczne.

Planowanie (*ang. Planning - PL*): Organizacje powinny opracowywać, dokumentować, okresowo aktualizować i wdrażać plany bezpieczeństwa dla organizacyjnych systemów informatycznych, które opisują mechanizmy zabezpieczeń obowiązujące lub planowane dla systemów informatycznych oraz reguły zachowania osób uzyskujących dostęp do systemów informatycznych.

Programy zarządzania (*ang. Program Management – PM*): Organizacje powinny: (i) opracowywać i rozpowszechniać plan programu bezpieczeństwa informacji (*ang. Information Security Program Plan*)[5]; (ii) przeglądać i aktualizować plan programu bezpieczeństwa informacji; (iii) chronić plan bezpieczeństwa informacji przed nieautoryzowanym ujawnieniem i modyfikacją.

Bezpieczeństwo osobowe (*ang. Personnel Security - PS*): Organizacje powinny: (i) zapewnić, aby osoby zajmujące odpowiedzialne stanowiska w organizacjach (w tym zewnętrzni dostawcy usług) były godne zaufania i spełniały ustalone kryteria bezpieczeństwa dla tych stanowisk; (ii) zapewnić ochronę informacji i systemów informatycznych organizacji w trakcie i po działaniach personalnych, takich jak rozwiązania umowy o pracę (współpracy) i zmiana zajmowanych stanowisk; oraz (iii) stosować formalne sankcje za brak przestrzegania przez personel zasad i procedur bezpieczeństwa organizacyjnego.

Przejrzystość przetwarzanie danych osobowych *(ang. Personally Identifiable Information Processing and Transparency - PT*): Organizacje powinny: (i) opracowywać polityki i procedury w zakresie przejrzystości przetwarzania danych osobowych; (ii) opracowywać programy bezpieczeństwa i ochrony prywatności uwzględniające polityki i procedury przejrzystości przetwarzania danych osobowych; (iii) aktualizować polityki i procedury

[5] Patrz: NSC 800-53, NSC 7298.

dotyczące przejrzystości przetwarzania danych osobowych w oparciu o zaistniałe zdarzenia obejmujące wyniki oceny lub audytu, incydenty lub naruszenia bezpieczeństwa, lub zmiany w przepisach prawa, zarządzeniach, dyrektywach, rozporządzeniach, zasadach, standardach i wytycznych.

Ocena ryzyka (*ang. Risk Assessment - RA*): Organizacje powinny okresowo oceniać ryzyko odnoszące się do operacji organizacyjnych (w tym misji, funkcji, wizerunku lub reputacji), zasobów organizacyjnych i osób fizycznych, wynikających z działania organizacyjnych systemów informatycznych i związanego z nimi przetwarzania, przechowywania lub przekazywania informacji organizacyjnych.

Nabywanie systemu i usług (*ang. System and Services Acquisition - SA*): Organizacje powinny: (i) alokować wystarczające zasoby, zapewniające odpowiednią ochronę organizacyjnych systemów informatycznych; (ii) stosować procesy cyklu życia rozwoju systemu, które uwzględniają względy bezpieczeństwa informacji; (iii) stosować ograniczenia dotyczące używania oprogramowania i instalacji; oraz (iv) zapewnić, aby dostawcy zewnętrzni stosowali adekwatne środki bezpieczeństwa w celu ochrony informacji, aplikacji i/lub usług zleconych przez organizację.

Ochrona systemów i sieci telekomunikacyjnych (*ang. System and Communications Protection - SC*): Organizacje powinny: (i) monitorować, kontrolować i chronić komunikację organizacyjną (tj. informacje przekazywane lub odbierane przez organizacyjne systemy informatyczne) na zewnętrznych granicach i kluczowych granicach wewnętrznych systemów informatycznych; oraz (ii) stosować projekty architektoniczne, techniki tworzenia oprogramowania i zasady inżynierii systemów, które promują skuteczne bezpieczeństwo informacji przetwarzanych w organizacyjnych systemach informatycznych.

Integralność systemu i informacji (*ang. System and Information Integrity - SI*): Organizacje powinny: (i) w odpowiednim czasie identyfikować, zgłaszać i korygować błędy informacji i systemów informatycznych; (ii) zapewnić ochronę przed złośliwym kodem w stosownych lokalizacjach w ramach organizacyjnych systemów informatycznych; oraz (iii) monitorować ostrzeżenia i porady systemu informatycznego oraz w odpowiedzi na to podejmować odpowiednie działania.

Zarządzanie ryzykiem w łańcuchu dostaw (*ang. Supply Chain Risk Management - SR*): Strategia zarządzania ryzykiem uwzględnia koszty, harmonogram, wyniki i kwestie dotyczące łańcucha dostaw powiązane z projektowaniem, rozwojem, pozyskiwaniem, wdrażaniem, eksploatacją, utrzymaniem i utylizacją systemów organizacyjnych. Proces zarządzania ryzykiem jest następnie stosowany w celu bieżącego zarządzania ryzykiem.

Organizacje powinny: (i) opracowywać polityki i procedury w zakresie zarządzania ryzykiem w łańcuchu dostaw; (ii) opracowywać programy bezpieczeństwa i ochrony prywatności uwzględniające polityki i procedury zarządzania ryzykiem w łańcuchu dostaw; (iii) aktualizować polityki i procedury zarządzania ryzykiem w łańcuchu dostaw w oparciu o zaistniałe zdarzenia obejmujące wyniki oceny lub audytu, incydenty lub naruszenia bezpieczeństwa, lub zmiany w przepisach prawa, zarządzeniach, dyrektywach, rozporządzeniach, zasadach, standardach i wytycznych.

5. WYBÓR ZABEZPIECZEŃ

Organizacje powinny spełniać minimalne wymagania bezpieczeństwa określone w niniejszym standardzie, stosując odpowiednie środki bezpieczeństwa opisane w standardzie NSC 800-53. Proces wyboru odpowiednich zabezpieczeń i wymagań mających na celu osiągnięcie przez systemy informatyczne organizacji adekwatnego poziomu bezpieczeństwa jest wieloaspektową, opartą na szacowaniu ryzyka działalnością obejmującą personel zarządzający i operacyjny w organizacji.

Kategoryzacja zabezpieczeń organizacyjnych informacji i systemów, zgodnie z wymogami standardu NSC 199, jest pierwszym krokiem w procesie zarządzania ryzykiem.[6] Po procesie kategoryzacji zabezpieczeń organizacje powinny wybrać odpowiedni zestaw środków bezpieczeństwa dla swoich systemów informatycznych, które spełniają minimalne wymagania bezpieczeństwa określone w niniejszym standardzie. Wybrany zestaw zabezpieczeń powinien zawierać jeden z trzech odpowiednio dostosowanych bazowych minimalnych środków bezpieczeństwa opisanych w publikacji NSC 800-53, które są skojarzone z oszacowanymi poziomami wpływu na organizacyjny system informatyczny, określonymi podczas procesu kategoryzacji zabezpieczeń.

- W przypadku systemów informatycznych o niskim wpływie, organizacje powinny co najmniej stosować odpowiednio dostosowane zabezpieczenia bazowe[7] (*ang. security control baselines*) zdefiniowane w standardzie NSC 800-53B, jako *Niski poziom wpływu na atrybuty bezpieczeństwa informacji*. Organizacje powinny mieć pewność, że minimalne wymagania zapewnione przez zastosowanie zabezpieczeń *Poziomu Niskiego*, są wystarczające.
- W przypadku systemów informatycznych o umiarkowanym wpływie, organizacje powinny co najmniej stosować odpowiednio dostosowane zabezpieczenia bazowe

[6] Kategoryzacja bezpieczeństwa musi być dokonana w aspekcie działalności całego przedsiębiorstwa z udziałem kluczowych urzędników / pracowników organizacyjnych, w tym między innymi pełniących role: CIO, SAISO, AO, właścicieli systemów informatycznych i właścicieli informacji (definicje ról – patrz publikacje NSC 800-37, NSC 7298).

[7] W potocznym języku technicznym – „bejslajny".

zdefiniowane w standardzie NSC 800-53B jako *Umiarkowany poziom wpływu na atrybuty bezpieczeństwa informacji*. Organizacje powinny mieć pewność, że minimalne wymagania zapewnione przez zastosowanie zabezpieczeń *Poziomu Umiarkowanego*, są wystarczające.

- W przypadku systemów informatycznych o wysokim wpływie, organizacje powinny co najmniej stosować odpowiednio dostosowane zabezpieczenia bazowe) zdefiniowane w standardzie NSC 800-53B jako *Wysoki poziom wpływu na atrybuty bezpieczeństwa informacji*. Organizacje powinny mieć pewność, że minimalne wymagania zapewnione przez zastosowanie zabezpieczeń *Poziomu Wysokiego*, są wystarczające.

Organizacje powinny stosować wszystkie mechanizmy zabezpieczeń w odpowiednich planach podstawowych zabezpieczeń, chyba, że określone wyjątki są zastosowane na podstawie wyników szacowania ryzyka dotyczących dostosowywania lub pominięcia zabezpieczeń opisanych w publikacji NSC 800-53. Aby zapewnić opłacalne, oparte na ryzyku podejście do osiągnięcia odpowiedniego bezpieczeństwa w całej organizacji, podstawowe działania w zakresie dostosowywania środków bezpieczeństwa powinny być koordynowane i zatwierdzane przez odpowiedni personel organizacyjny (np. dyrektorów ds. informacji, wyższy personel zajmujący się bezpieczeństwem informacji, personel zatwierdzający lub przez upoważnionych wyznaczonych przedstawicieli). Wynikowy zestaw zabezpieczeń musi być udokumentowany w planie bezpieczeństwa systemu informatycznego.

ZAŁĄCZNIK SŁOWNIK I AKRONIMY

PATRZ: NSC 7298, SŁOWNIK KLUCZOWYCH POJĘĆ Z ZAKRESU CYBERBEZPIECZEŃSTWA

ZAŁĄCZNIK REFERENCJE

NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA	
NSC 199	Standardy kategoryzacji bezpieczeństwa – na podstawie FIPS 199
NSC 800-18	Przewodnik do opracowywania planów bezpieczeństwa systemów informatycznych w podmiotach publicznych – na podstawie NIST SP 800- 18
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 800-53B	Zabezpieczenia bazowe systemów informatycznych 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 | CSRC (nist.gov)
NSC 800-60	Wytyczne w zakresie określania kategorii bezpieczeństwa informacji I kategorii bezpieczeństwa systemu informatycznego – na podstawie NIST SP 800-60

STANDARDS, AND GUIDELINES	
FIPS 199	*Standards for Security Categorization of Federal Information and Information Systems*, February 2004
NIST SP 800-18	*Guide for Developing Security Plans for Federal Information Systems*, February 2006
NIST SP 800-53	Security and Privacy Controls for Information Systems and Organizations, September 2020
NIST SP 800-60	*Guide for Mapping Types of Information and Information Systems to Security Categories*, June 2004