

# Przegląd najnowszych zaleceń best practice pod kątem bezpieczeństwa systemów informatycznych ze szczególnym uwzględnieniem zaleceń stosowanych w sektorze telekomunikacyjnym

Andrzej Adamczyk

*ITTI Sp. z o. o.*

*e-mail: andrzej.adamczyk@itti.com.pl*

Rafał Renk

*ITTI Sp. z o. o., Akademia Techniczno-Rolnicza w Bydgoszczy*

*e-mail: rafal.renk@itti.com.pl*

prof. Witold Holubowicz

*ITTI Sp. z o. o., Uniwersytet im. Adama Mickiewicza w Poznaniu*

*e-mail: witold.holubowicz@itti.com.pl*

## Abstrakt

W ostatnim czasie obserwuje się wzmożone działania w kierunku zwiększenia bezpieczeństwa funkcjonowania organizacji podejmowane w celu zmniejszenia ryzyka przerwania ciągłości funkcjonowania. W artykule dokonano analizy aktualnych zaleceń *best practice* dotyczących bezpieczeństwa m.in. zaleceń NRIC, GAISP. Dokonano selekcji zaleceń pod kątem stosowalności w dziedzinie systemów informatycznych rozumianych jako zasoby sprzętowe i programowe. Zalecenia *best practice* można stosować wprowadzając tzw. środki zaradcze (ang. *countermeasures*) obejmujące zarówno elementy materialne, jak i procedury postępowania. Wybrane w artykule zalecenia przedyskutowano podając przykłady środków zapobiegawczych stosowanych w praktyce w przedsiębiorstwach polskich i zagranicznych. Większość przykładów została opracowana na podstawie doświadczeń z wielu projektów dotyczących bezpieczeństwa prowadzonych przede wszystkim w firmach sektora telekomunikacyjnego. Omówione zalecenia obejmują m.in. następujące kategorie:

- projektowanie, wykonywanie, testowanie i dostarczanie oprogramowania (zapewnienie odpowiedniego poziomu odporności systemów na awarie, odporności na niewłaściwe działanie użytkownika),
- zabezpieczenia na etapie eksploatacji systemów informatycznych (auditing zabezpieczeń, zarządzanie danymi m.in. procedury synchronizacji, zarządzanie zmianami m.in. wersjonowanie, aktualizacja i zapewnienie kompatybilności systemów informatycznych, zabezpieczenie „dziur” w oprogramowaniu)
- zabezpieczenie przed wpływem informacji na etapie likwidacji przestarzałego sprzętu i oprogramowania.

Omówione zasady mogą wydatnie pomóc w opracowaniu i wdrożeniu własnych zaleceń mających na celu poprawę bezpieczeństwa tworzenia i eksploatacji systemów informatycznych.



## 1. Wprowadzenie

Wśród publikowanych zbiorów zaleceń typu najlepszych praktyk (ang. *best practice*) – które dalej w opracowaniu nazywane będą zaleceniami bądź najlepszymi praktykami – dotyczących bezpieczeństwa systemów informatycznych można znaleźć między innymi następujące dokumenty:

- zalecenia National Institute of Standards and Technology (NIST) ze Stanów Zjednoczonych – Computer Security Resource Center (CSRC),
- zalecenia „Generally Accepted Information Security Principles” [GAISP] opublikowane przez Information Systems Security Association (ISSA) wywodzące się z zaleceń „Generally Accepted System Security Principles” (GASSP) opracowanych przez Massachusetts Institute of Technology (MIT),
- zalecenia Network Reliability and Interoperability Council [NRIC] ze Stanów Zjednoczonych,
- „OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security” [OECD],
- IT Infrastructure Library [ITIL] opracowana przez Office of Government Commerce w Wielkiej Brytanii (rozpowszechniana na zasadzie komercyjnej).

Zalecenia tego typu powinny charakteryzować się cechami wymienionymi w tabeli 1 [GKBSP]:

Tabela 1. Cechy najlepszych praktyk

<i>Cechy najlepszych praktyk</i>	<i>Czym zalecenia nie są</i>
<b>Skierowane do człowieka;</b> jako powtarzalna lub indywidualna metoda używana przez ludzi w celu wykonania pewnego procesu.	Nie są one mechanizmem bezpieczeństwa IT, zaimplementowanym sprzętowo lub programowo.
<b>Dotyczące bezpieczeństwa;</b> czyli odgrywające rolę w zabezpieczeniu informacji, zasobów lub ciągłości działania w ramach organizacji.	Nie są one zaleceniami dotyczącymi prowadzenia firmy, mimo, że wspomagają działania biznesowe organizacji.
<b>Sprawdzone doświadczalnie;</b> czyli efektywne w procesie bezpieczeństwa; wynik doświadczenia operacyjnego.	Nie są one jakimikolwiek zaleceniami, które można wdrożyć. Nie są też wynikiem teoretycznych rozważań.
<b>Jedno z najbardziej efektywnych</b> (przynoszących skutek) istniejących zaleceń używanych w poszczególnych procesach systemu bezpieczeństwa	Nie są one jakimikolwiek zaleceniami wdrożonymi w praktyce.

Tego rodzaju zalecenia omówiono w kolejnych rozdziałach niniejszego artykułu. Do omówienia wybrano trzy grupy zaleceń: NIST, GAISP i NRIC. Dotyczą one ogólnych aspektów funkcjonowania instytucji (NIST, GAISP) oraz bardziej szczegółowo rozwoju systemów informatycznych (NRIC).

## 2. Zalecenia NIST

Organizacja NIST jest rządową agencją Stanów Zjednoczonych. Jedną z działalności NIST jest działalność jako organizacji standaryzującej rozwiązania dla systemów informatycznych. W ramach tej działalności działają działy. W dziale Bezpieczeństwa Komputerowego znajdują się m.in.: bieżące informacje na temat najnowszych zagrożeń, statystyki roczne, pokazujące liczbę słabych punktów w systemach z podziałem na kategorie (atak zdalnym, atak w sieci LAN, ataki DoS, słabe punkty systemów operacyjnych), biuletyny na temat bezpieczeństwa systemów (ang. *Security Bulletins*), specjalne publikacje (ang. *Special Publications*). Zaleceniami bezpieczeństwa zajmuje się w NIST Computer Security Resource Center (CSRC).

Poniżej zaprezentowane zostały najważniejsze zalecenia opracowane w oparciu o publikację NIST 800-14 p.t.: „Rekomendowane praktyki i reguły w zabezpieczaniu systemów informatycznych” (ang. „*Generally Accepted Principles and Practices for Securing Information Technology Systems*”) [NIST].

Zalecenia te można zakwalifikować do następujących grup:

### 1. Bezpieczeństwo proceduralne:

- a. rozpocznij od strategii i polityki bezpieczeństwa,
- b. określ jakiego rodzaju procedur potrzeba: polityki bezpieczeństwa informacji, podręczników administrowania systemami, zaleceń dotyczących utrzymania witryn internetowych, czy może zasad świadczenia usług e-commerce,
- c. ustal, kto powinien przestrzegać tych procedur: wszyscy pracownicy używający w swej pracy komputerów, administratorzy systemów, help desk, pracownicy zajmujący się utrzymaniem systemów, pracujący na zasadach outsourcing IT, zajmujący się zakupem i dostawą aplikacji,
- d. określ osoby posiadające klucze umożliwiające dostęp do dokumentów,
- e. zabezpiecz archiwa dokumentów i informacji kontaktowych,
- f. kontroluj politykę haseł dostępu w taki sposób, by utrudnić odgadnięcie hasła, złamanie hasła używając oprogramowania słownikowego i metody *brute force*, zapewnij, aby hasła składały się co najmniej z ośmiu znaków, nie zawierały nazwisk i dat urodzenia, zawierały co najmniej jedną dużą literę, małą literę, cyfrę i znak specjalny; usuń hasła, które nie spełniają tych wymagań; zmieniaj hasła co 45-60 dni; ogranicz możliwość zmiany haseł na wcześniej używane; staraj się stosować hasła będące wyrażeniami zawierającymi wiele słów,
- g. stosuj standardy i poradniki bezpieczeństwa, analizuj ryzyko i zagrożenia.

### 2. Bezpieczeństwo używania Internetu:

- a. nie pobieraj plików z nie znanych źródeł (np. witryn internetowych),
- b. nie uruchamiaj plików ze stron WWW,
- c. zabezpiecz hasła, numery kart kredytowych i prywatne informacje przy korzystaniu z przeglądarki internetowej,
- d. włącz w przeglądarce opcję wysokiego bezpieczeństwa.

### 3. Bezpieczeństwo korzystania z poczty elektronicznej:

- a. bądź ostrożny, gdy otwierasz załączniki,

- b. upewnij się, że oprogramowanie pocztowe, z którego korzystasz jest odpowiednio skonfigurowane,
  - c. nie odpowiadaj na wszystkie wiadomości, które nie wymagają odpowiedzi.
4. Bezpieczeństwo korzystania z komputera:
- a. używaj haseł dostępu (nie zapisuj haseł na papierze ani elektronicznie),
  - b. używaj własnych kont na komputerze (nie korzystaj ze wspólnych kont systemowych),
  - c. używaj blokady ekranu, kiedy odchodzisz od komputera,
  - d. wyloguj się lub zablokuj komputer przenośny, kiedy kończysz pracę.
5. Bezpieczeństwo osobowe:
- a. potwierdzaj tożsamość osób i instytucji,
  - b. towarzyszyć wszystkim sprzedawcom i ekipom naprawczym w trakcie ich pobytu w firmie,
  - c. przekazuj tylko niezbędne informacje,
  - d. dokładnie niszczyć informacje osobowe,
  - e. przeprowadzaj weryfikacje przeszłości osób zatrudnionych,
  - f. kontroluj wejścia i wyjścia z firmy,
  - g. kontroluj wyjazdy osób (np. dłuższe nieobecności),
  - h. zapewniaj odpowiednie zaangażowanie zarządu (wyznacz odpowiedzialności, zapewnij środki) i świadomość pracowników w zakresie bezpieczeństwa (stosuj szkolenia, informuj pracownika w pierwszym dniu pracy o procedurach bezpieczeństwa i rzeczach, które wolno i których nie należy robić).
6. Procedury zapewniające odtworzenie stanu normalnego danych i funkcjonowania systemów:
- a. wykonuj kopie zapasowe wszystkich plików, oprogramowania i danych konfiguracyjnych,
  - b. prowadź na bieżąco inwentaryzację sprzętu i oprogramowania.
7. Bezpieczeństwo fizyczne:
- a. stosuj i używaj zamki w drzwiach,
  - b. stosuj alarmy,
  - c. zapewnij ochronę fizyczną.
8. Bezpieczeństwo sprzętu i oprogramowania:
- a. przechowuj w bezpieczny sposób,
  - b. izoluj dane wrażliwe ze względów bezpieczeństwa,
  - c. monitoruj połączenia wykonywane z modemów telefonicznych,
  - d. oddziel fizycznie komputery od sieci, jeśli to konieczne,
  - e. zainstaluj wymienne dyski twarde lub podobne nośniki informacji,

- f. śledź podatności stosowanych systemów i zabezpieczaj je instalując odpowiednie aktualizacje.

9. Bezpieczeństwo antywirusowe:

- a. stosuj narzędzia antywirusowe w zakresie całej firmy,
- b. stosuj procesy antywirusowe w całej firmie,
- c. przydziel odpowiedzialności poszczególnym osobom,
- d. aktualizuj na bieżąco bazę wirusów używaną przez narzędzia.

Jak widać zalecenia te mają naturę dość ogólną i są skierowane do organizacji dowolnego typu i sektora działalności.

### 3. Zasady GAISP

Projekt, którego wynikiem są „Ogólnie przyjęte zasady bezpieczeństwa informacji” (ang. *Generally Accepted Information Security Project – GAISP*) jest projektem zmierzającym do formułowania uniwersalnych zasad bezpieczeństwa informacji. Projekt GAISP jest kontynuacją opracowywania GASSP (ang. *Generally Accepted System Security Principles*) prowadzonego przez Internet Information Security Foundation (IISF). Projekt GASSP przerodził się w GAISP za sprawą Information Systems Security Association (ISSA).

Zasady GAISP opierają się na następujących standardach i dokumentacji:

- Detailed Principles – STROWMAN,
- „Common Body of Knowledge” używane przez International Information System Security Certification Consortium (ISC)<sup>2</sup> do certyfikowania na stopień Certified Information Systems Security Professional (CISSP),
- „Standards of Good Practice for Information Security” rozpowszechniane przez Information Security Foundation (ISF),
- ISO 17799,
- „Control Objectives for Information Technology” (CobIT) opracowane przez Information Security & Audit Control Association (ISACA),
- „Generally Accepted Principles and Practices for Securing Information Technology Systems” (SP 800-14) wydane przez National Institute of Standards and Technology (NIST).

Treść GAISP uszeregowana jest według dwóch kryteriów:

- zasad szerzenia (ang. *pervasive principles* - PP),
- zasad funkcjonalnych (ang. *broad functional principles* - BFP).

Każdej z zasad towarzyszy uzasadnienie jej sensu oraz przykład zastosowania.

Dokument zawiera następujące zasady szerzenia GAISP:

- Zasada rejestrowania dostępu do danych (PP1) – Dane o dostępie do informacji oraz odpowiedzialność za nią muszą być jasno zdefiniowane i potwierdzone.

- Zasada świadomości (PP2) – Właściciele danych oraz pracownicy zajmujący się bezpieczeństwem informacyjnym którzy potrzebują dostępu do danych powinni mieć dostęp do zastosowanych standardów, zasad, konwencji i mechanizmów służących zapewnieniu bezpieczeństwa informacji i systemów informatycznych i powinni być poinformowani o możliwych zagrożeniach bezpieczeństwa informacji.
- Zasada etyki (PP3) – Informacje powinny być używane – a administracja bezpieczeństwem informacji wykonywana – w sposób etyczny.
- Zasada wielodyscyplinarna (PP4) – Zasady, standardy, konwencje i mechanizmy służące zapewnieniu bezpieczeństwa informacji i systemów informatycznych powinny brać pod uwagę punkt widzenia wszystkich zainteresowanych stron.
- Zasada proporcjonalności (PP5) – Regulacje w zakresie bezpieczeństwa powinny być proporcjonalne do ryzyka modyfikacji, uniemożliwienia użycia i ujawnienia informacji.
- Zasada integracji (PP6) – Zasady, standardy, konwencje i mechanizmy służące zapewnieniu bezpieczeństwa informacji powinny być skoordynowane i zintegrowane ze sobą oraz z polityką organizacji, procedurami tworzenia i utrzymania bezpieczeństwa w kontekście wszystkich systemów informatycznych.
- Zasada aktualności (PP7) – Wszystkie strony powinny działać bez opieszałości w kierunku zabezpieczenia lub odpowiedzi na naruszenie prawa i zagrożenia bezpieczeństwa informacji i systemów informatycznych.
- Zasada oceny (PP8) – Ryzyko zagrożenia informacji i systemów informatycznych powinno być oceniane okresowo.
- Zasada sprawiedliwości (PP9) – kadra zarządzająca będzie respektowała prawa i godność jednostek w trakcie ustalania polityki bezpieczeństwa oraz w trakcie wyboru, wdrażania i prowadzenia działań bezpieczeństwa.

Dokument określa następujące zasady funkcjonalne:

- Polityka bezpieczeństwa informacji (BFP-1) – Kierownictwo zadba o to, aby przy tworzeniu i utrzymywaniu polityki bezpieczeństwa, wspomagających standardów, procedur i porad brać pod uwagę wszystkie aspekty bezpieczeństwa informacji. Takie kierowanie powinno uwzględniać odpowiedzialności, akceptowalny poziom dowolności i jak duże ryzyko jest akceptowalne w kontekście osób i organizacji.
- Edukacja i uświadamianie (BFP-2) – Kierownictwo przekaze treść polityki bezpieczeństwa informacji całemu personelowi i zapewni, aby personel posiadał odpowiedni poziom świadomości. Szkolenie obejmie standardy, procedury, porady odpowiedzialności, sposoby wdrożenia i potencjalne konsekwencje niestosowania.
- Monitorowanie aktywności (BFP-3) – Kierownictwo zapewni monitoring dostępu i użycia informacji np. dodawania, modyfikacji, kopiowania i usuwania, oraz zasobów wspomagających. Wszystkie ważne zdarzenia powinny być rejestrowane wraz z datą i czasem użycia oraz odpowiedzialnością dla każdej osoby oddzielnie.
- Zarządzanie zasobami informacyjnymi (BFP-4) – Kierownictwo będzie w sposób proceduralny katalogować i wyceniać zasoby informacyjne oraz przypisywać im poziom poufności i krytyczności. Informacja jako zasób musi posiadać unikatowy identyfikator i określoną odpowiedzialność.

- Zarządzanie środowiskowe (BFP-5) – Kierownictwo rozważy i postara się skompensować nieodłączne ryzyko związane z wewnętrznym i zewnętrznym środowiskiem, w którym zasoby informacyjne i inne z nimi związane, są przechowywane, transmitowane, obrabiane lub używane.
- Kwalifikacje personalne (BFP-6) – Kierownictwo będzie weryfikowało kwalifikacje związane z integralnością, potrzebą informowania, kompetencjami technicznymi wszystkich mających dostęp do zasobów informacyjnych lub innych z nimi związanych.
- Zarządzanie incydentami (BFP-7) – Kierownictwo umożliwi odpowiedź i rozwiązywanie incydentów związanych z naruszeniem bezpieczeństwa informacji błyskawicznie i efektywnie, aby zapewnić jak najmniejszy jego wpływ na działalność biznesową i zminimalizować prawdopodobieństwo wystąpienia podobnych incydentów w przyszłości.
- Cykl życia systemów informatycznych (BFP-8) – Kierownictwo zapewni bezpieczeństwo na wszystkich etapach cyklu życia systemu.
- Kontrola dostępu (BFP-9) – Kierownictwo ustanowi odpowiednie mechanizmy regulacji w celu równoważenia przydzielanego dostępu do zasobów informacyjnych i innych z nimi związanych w stosunku do ponoszonego ryzyka.
- Planowanie ciągłości operacyjnej i działania w sytuacji wyjątkowej (BFP-10) – Kierownictwo będzie planować i wykorzystywać technologie informacyjne w taki sposób, aby chronić ciągłość działania firmy.
- Zarządzanie ryzykiem zagrożeń informacji (BFP-11) – Kierownictwo zapewni takie działania na rzecz bezpieczeństwa informacji, aby były odpowiednie w stosunku do wartości zasobów i zagrożeń, na które te zasoby są podatne.
- Bezpieczeństwo sieciowe i internetowe (BFP-12) – Kierownictwo rozważy potencjalny wpływ na całą infrastrukturę np. Internet, publiczną sieć telekomunikacyjną i inne połączone systemy w procesie stosowania działań na rzecz bezpieczeństwa.
- Prawne, regulacyjne i umowne aspekty bezpieczeństwa informacji (BFP-13) – Kierownictwo podejmie kroki aby uświadomić sobie i weźmie pod uwagę prawo, regulacje i wymagania charakterystyczne dla zasobów informacyjnych.
- Praktyki etyczne (BFP-14) – Kierownictwo będzie respektować prawa i godność osób przy wdrożeniu polityki bezpieczeństwa oraz wyborze i podjęciu działań na rzecz bezpieczeństwa.

#### 4. Zalecenia NRIC

Statut organizacji NRIC (Departament ds. niezawodności i kompatybilności sieci, ang. *Network Reliability and Interoperability Council*) został opracowany w roku 1992, chociaż od tego czasu był wielokrotnie zmieniany<sup>1</sup>. Według najnowszych danych zamieszczonych w statucie (wersja VI), komitet ma na celu przygotowanie rekomendacji w zakresie bezpieczeństwa sieci, dla Federalnej Komisji Komunikacji (*Federal Communications Commission - FCC*) oraz całego sektora telekomunikacyjnego.

NRIC wspólnie z organizacjami, które uczestniczyły ochotniczo w pracach nad bezpieczeństwem (Cisco, Alcatel, Ericsson, AT&T, Lucent Technologies, Lockheed Martin, Motorola, Nokia

---

<sup>1</sup> ostatnia modyfikacja statutu pochodzi z roku 2001.

i inni), zaproponował zbiór najlepszych praktyk z zakresu bezpieczeństwa krajowej sieci telekomunikacyjnej. Obecnie istnieje niespełna 1000 takich praktyk. Chociaż nie mają one charakteru standardu to głównym celem przyświecającym podczas ich opracowywania była i jest ochrona krytycznej infrastruktury sieciowej w Stanach Zjednoczonych oraz poprawa niezawodności sieci telekomunikacyjnej. Głównymi adresatami najlepszych praktyk są usługodawcy, operatorzy sieci oraz dostawcy sprzętu. Przedstawiane rekomendacje, dotyczące niezawodności sieci zostały do tej pory zaimplementowane przez znaczną liczbę organizacji. Komitet do spraw niezawodności sieci NRSC (*Network Reliability Steering Committee*) w swoich raportach niejednokrotnie podkreślał, że wiele dotychczasowych awarii nie miałyby miejsca gdyby wcześniej zaimplementowano najlepsze praktyki. W drugiej połowie 2002 roku przeprowadzono w Stanach Zjednoczonych dokładne badania odnośnie stosowalności najlepszych praktyk. W ich wyniku dokonano następujących spostrzeżeń:

- brak implementacji najlepszych praktyk prowadzi do wzrostu ryzyka do poziomu od średniego do wysokiego,
- koszt wdrożenia najlepszych praktyk nie jest przeważnie wysoki,
- potwierdzono efektywność zastosowania najlepszych praktyk,
- poziom implementacji najlepszych praktyk jest wysoki.

Po wydarzeniach z 11 września 2001, zalecenia NRIC podzielono na zbiory praktyk: pierwszy dotyczy bezpieczeństwa fizycznego, natomiast drugi - tzw. *cyberspace security*. Najlepsze praktyki obejmujące bezpieczeństwo fizyczne poruszają trzy aspekty: niezawodność usług, bezpieczeństwo sieci oraz bezpieczeństwo przedsiębiorstw.

Podmiotem, do jakiego skierowane są zalecenia NRIC wybrane do omówienia w niniejszym artykule, jest dostawca sprzętu lub/i oprogramowania. Przedmiotem zaś dostarczany system sprzętowo-informatyczny.

Wybrane zalecenia NRIC w przeciwieństwie do pozostałych omówionych w niniejszym artykule zaleceń nie mają charakteru ogólnego i koncentrują się na zapewnieniu bezpieczeństwa działania dostawców sprzętu i oprogramowania ze szczególnym uwzględnieniem produktów dla sektora telekomunikacyjnego.

Do rozważenia wybrano następujące zalecenia NRIC:

- Nr 6-5-0535. Firma powinna współpracować z operatorami oraz innymi dostawcami sprzętu i oprogramowania w celu "zamykania dziur" bezpieczeństwa w używanych systemach.
- Nr 6-5-0536. Firma powinna zamieszczać aktualizacje oprogramowania zapewniające bezpieczeństwo i niezawodność funkcjonowania w głównych wydaniach swoich systemów informatycznych.
- Nr 6-5-0538. Oprogramowanie elementów sieciowych (włączając w to systemy typu OSS – ang. *Operational Support System*) powinno być kompatybilne wstecz.
- Nr 6-5-0541. Oprogramowanie używane w krytycznych elementach sieci powinno posiadać własności umożliwiające przechowywanie go w kilku wersjach instalacyjnych, które pozwolą na powtórna instalację wcześniejszej wersji oprogramowania w przypadku wystąpienia takiej potrzeby.
- Nr 6-5-0550. Powinny istnieć procedury synchronizacji i zapewnienia bezpieczeństwa bazom danych. W ramach tych procedur powinna być przewidziana ręczna zmiana konfiguracji i synchronizacji, jeśli okazałaby się potrzebna w sytuacji wyjątkowej. Obsługa techniczna powinna posiadać uprawnienia do wykonywania tylko tych funkcji,

które są niezbędne dla ich pracy. Udostępnianie wszystkich funkcji wszystkim pracownikom grozi poważnymi konsekwencjami.

- Nr 6-5-0552. Integralnym elementem procesu rozwoju oprogramowania powinno być testowanie z iniekcją błędów (ang. *fault injection testing*) włączając w to testy symulujące masowo-występujące błędy funkcjonowania sieci.
- Nr 6-5-0553. Błędy w funkcjonowaniu sprzętu i oprogramowania powinny być testowane i/lub symulowane. W testowaniu tym należy położyć nacisk na obserwację działania oprogramowania odtwarzającego funkcjonowanie systemu przed wystąpieniem błędu (ang. *fault recovery software*).
- Nr 6-5-0554. Projektowanie funkcjonalności oprogramowania odtwarzającego funkcjonowanie systemu przed wystąpieniem błędu powinno rozpocząć się jak najwcześniej, jako element cyklu rozwoju systemu.
- Nr 6-5-0555. Firma powinna w sposób ciągły ulepszać metodykę rozwoju oprogramowania stosując nowoczesne procesy wewnętrznej oceny produktu. Jako część cyklu produkcyjnego firma winna przeprowadzać formalne inspekcje kodu źródłowego i projektu systemu. Środowisko testowe powinno być skonstruowane w taki sposób, aby zapewnić warunki najbardziej zbliżone do rzeczywistych. Firma powinna dzielić się z operatorami informacjami na temat poziomu tolerancji błędów i prawdopodobieństwa występowania poszczególnych klas błędów występujących w ich oprogramowaniu.
- Nr 6-5-0557. Powinno się zadbać o to, aby minimalizować prawdopodobieństwo występowania „cichych usterek” (ang. *silent failure*), czyli takich, których wykrycie jest trudne. „Ciche usterki” są niemożliwe do wykrycia przez system a mogą powodować długotrwałą przerwę w funkcjonowaniu lub powodować wystąpienie kolejnych usterek bezpośrednio powodujących wystąpienie przerw w funkcjonowaniu. Firma powinna także dokonywać stałych przeglądów jakości inspekcji i nadzoru nad krytycznymi składnikami systemu w celu zabezpieczenia się przed występowaniem „cichych usterek” w całym cyklu życia systemu.
- Nr 6-5-0559. Wszystkie zmiany konfiguracji sieci i oprogramowania powinny być kompleksowo testowane w laboratorium zanim zostaną wprowadzone w życie w ramach funkcjonującego systemu.
- Nr 6-5-0590. Metody postępowania (ang. *methods of procedure*) i listy kontrolne służące akceptacji lub weryfikacji, zmian lub rozbudowy sprzętu i oprogramowania powinny być przygotowane dla wszystkich działań tego typu. W możliwym zakresie metody postępowania powinny być przygotowywane przez ludzi będących ekspertami w tej dziedzinie. Metoda postępowania powinna być zatwierdzona przez kierowników odpowiedzialnych za technikę, obsługę połączeń, instalację i inne funkcje właściwe dla danej metody; a odstępstwa od udokumentowanych procesów powinny również podlegać akceptacji tego zespołu osób. Jeśli istnieje konieczność odwołania się w metodzie postępowania do innych dokumentów, takie odwołanie powinno być szczegółowe i zawierać przedmiot odwołania i datę. Metoda postępowania powinna określać każdy krok wymagany w trakcie pracy. Po wykonaniu każdej z funkcji fakt ten powinien być odnotowywany w metodzie postępowania. Należy używać również list kontrolnych, aby zapewnić, że wykonywane działania zostały przeprowadzone w poprawny sposób.
- Nr 6-5-0749. Firma powinna ulepszać standardy i wprowadzać nowe, zapewniające odporność krytycznych systemów na działania wpływające na funkcjonowanie usług bez stanowczego potwierdzenia użytkownika.

- Nr 6-5-0750. Firma powinna dostarczać mechanizmy rekonfiguracji (dodawania i włączania opcji) bez potrzeby reinicjalizacji całego systemu. Firma powinna dostarczać funkcjonalności pozwalających na zarządzanie pamięcią (rekonfiguracji i zwiększania pamięci) w sposób on-line nie zakłócających obsługi połączeń oraz innych krytycznych procesów (np. taryfikacji).
- Nr 6-6-0802. Firma powinna, jeśli to jest potrzebne, stosować technologie zarządzania ruchem w swoich urządzeniach, wyposażając je w narzędzia potrzebne do utrzymania wydajności i zarządzania ruchem abonentów na poziomie umów abonenckich i umów dotyczących poziomu usług (ang. *service level agreement*) oraz zabezpieczających przed obniżeniem jakości usługi postrzeganej przez abonenta.
- Nr 6-6-5061. Firma powinna projektować interfejs użytkownika (np. oznakowanie sprzętu, oprogramowanie i dokumentacja) zgodnie ze standardami przemysłowymi koncentrującymi się na użytkowniku. Takie podejście minimalizuje ryzyka błędu spowodowanego przez człowieka.
- Nr 6-6-5084. Firma powinna zagwarantować, że wykorzystywany sprzęt oraz oprogramowanie firm zewnętrznych jest poprzedzone odpowiednimi testami bezpieczeństwa i jakości (np. GR929 (RQMS), GR815, TL9000) zanim zostanie ostatecznie zaakceptowane.
- Nr 6-6-5121. Firma powinna rozwijać i ciągle wdrażać procedury regulujące sposób dostarczania oprogramowania, gwarantujące jego spójność w trakcie instalacji.
- Nr 6-6-5142. Firma powinna współpracować z operatorami, dostawcami usług oraz innymi dostawcami sprzętu i oprogramowania w celu stosowania zabezpieczeń oprogramowania (tj. wydawania aktualizacji) ładowanych do urządzeń sieciowych z wykorzystaniem znanych i bezpiecznych protokołów komunikacyjnych, zapobiegając w ten sposób możliwości sabotażu.
- Nr 6-6-5165. Firma powinna zapewnić “zdalnym pracownikom” (np. programistom pracującym poza firmą) sprzęt i pomoc w zakresie zabezpieczenia ich platform komputerowych i systemów w sposób analogiczny, jak są one zabezpieczone na terenie firmy. Powinno się przy tym wziąć pod uwagę zastosowanie narzędzia zapewniających bezpieczeństwo, zapory ogniowe i zabezpieczanie plików hasłem.
- Nr 6-6-5167. Firma powinna stosować fizyczne i elektroniczne metody zabezpieczeń w procesie wewnętrznej dystrybucji materiałów związanych z rozwojem i produkcją oprogramowania.
- Nr 6-6-5172. Firma nie powinna zezwalać na stosowanie niezabezpieczonych połączeń bezprzewodowych w celu przesyłania danych i oprogramowania.
- Nr 6-6-5200. Firma powinna wypracować i wdrożyć procedury zapewniające odpowiednie pozbycie się lub/i zniszczenie sprzętu (np. dysków twardych), który zawiera informacje wrażliwe ze względów bezpieczeństwa lub stanowiące własność intelektualną firmy.
- Nr 6-6-5218. Firma, której działanie opiera się na zagranicznych filiach lub współpracy z zagranicznymi partnerami biznesowymi w procesie rozwoju oprogramowania powinna wypracować i wdrożyć kompleksowy program bezpieczeństwa, aby chronić produkty w trakcie rozwoju i dostawy przed złośliwą modyfikacją kodu.
- Nr 6-6-5219. Firma, której działanie opiera się na zagranicznych filiach lub współpracy z zagranicznymi partnerami biznesowymi w procesie rozwoju oprogramowania powin-

na wypracować i wdrożyć kompleksowy program bezpieczeństwa, aby chronić produkty w trakcie rozwoju i dostawy przed fałszerstwem.

- Nr 6-6-5278. Firma powinna zapewnić istnienie odpowiedniego programu ochrony zabezpieczającego produkty przed kradzieżą i szpiegostwem, biorąc pod uwagę, że środowiska rozwoju oprogramowania stosowane na świecie charakteryzują się różnym poziomem ryzyka. Wyższy poziom ryzyka powinien być wzięty pod uwagę podczas wprowadzania programu ochrony.
- Nr 6-6-5279. Firma powinna być świadoma, że środowiska rozwoju oprogramowania stosowane na świecie charakteryzują się różnym poziomem i typem ryzyka. Specyficzne dla regionu zagrożenia informacji powinien być wzięty pod uwagę podczas wprowadzania programu ochrony.

Zalecenia NIST i GAISP były głównie zaleceniami dotyczącymi działań proceduralnych. Natomiast wybrane zalecenia NRIC dotyczą konkretnie cyklu życia sprzętu i systemów informatycznych oraz zarówno działań proceduralnych jak i zabezpieczeń materialnych i logicznych. Dlatego w ramach analizy i klasyfikacji tych zaleceń można dokonać podziału na następujące grupy według dwóch niezależnych kryteriów:

- według cyklu życia systemu:
  - zalecenia do zastosowania na etapie produkcyjnym systemu informatycznego,
  - zalecenia do zastosowania na etapie wdrożenia i eksploatacji systemu informatycznego,
- według rodzaju zalecanego zabezpieczenia:
  - zalecenia zawierające opis zabezpieczeń materialnych (związane z wdrożeniem zasobów fizycznych, sprzętowych lub programowych),
  - działania proceduralne (związane z podjęciem określonych działań lub wdrożeniem określonych procedur i metod pracy).

W tabeli 2 wymieniono dokonano kategoryzacji zaleceń według tych kryteriów.

Tabela 2. Klasyfikacja wybranych zaleceń NRIC

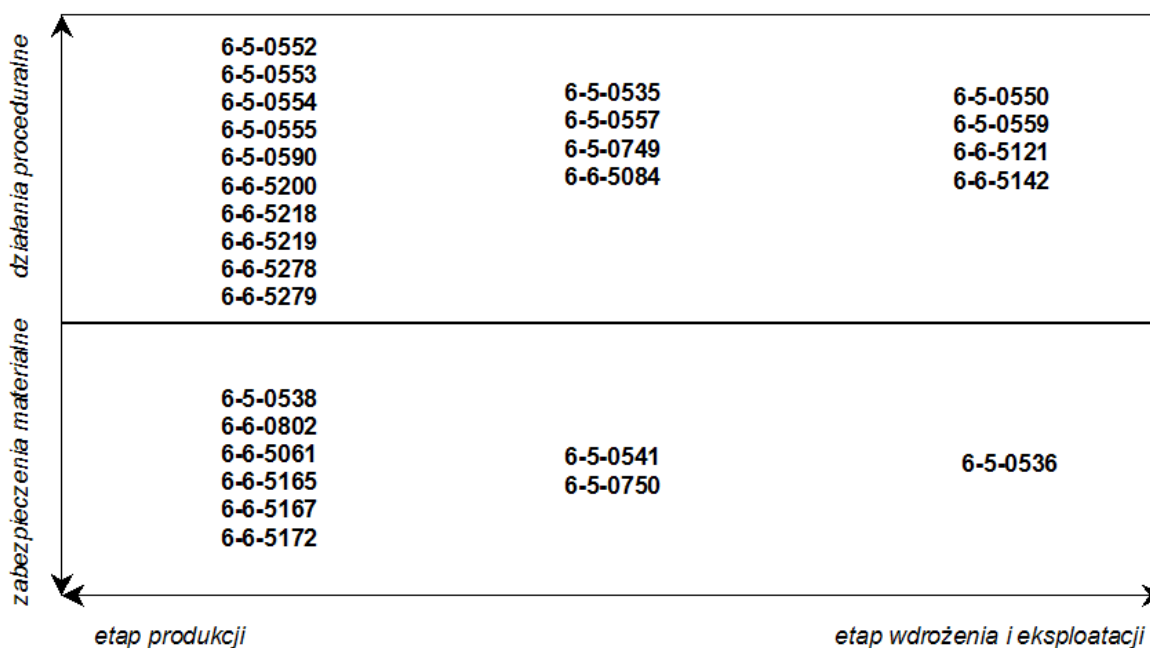
L.p.	Nr zalecenia	Etap produkcji	Etap wdrożenia i eksploatacji	Działania proceduralne	Zabezpieczenia materialne
1.	6-5-0535	+	+	+	
2.	6-5-0536		+		+
3.	6-5-0538	+			+
4.	6-5-0541	+	+		+
5.	6-5-0550		+	+	
6.	6-5-0552	+		+	
7.	6-5-0553	+		+	
8.	6-5-0554	+		+	
9.	6-5-0555	+		+	
10.	6-5-0557	+	+	+	

L.p.	Nr zalecenia	Etap produkcji	Etap wdrożenia i eksploatacji	Działania proceduralne	Zabezpieczenia materialne
11.	6-5-0559		+	+	
12.	6-5-0590	+		+	
13.	6-5-0749	+	+	+	
14.	6-5-0750	+	+		+
15.	6-6-0802	+			+
16.	6-6-5061	+			+
17.	6-6-5084	+	+	+	
18.	6-6-5121		+	+	
19.	6-6-5142		+	+	
20.	6-6-5165	+			+
21.	6-6-5167	+			+
22.	6-6-5172	+			+
23.	6-6-5200	+		+	
24.	6-6-5218	+		+	
25.	6-6-5219	+		+	
26.	6-6-5278	+		+	
27.	6-6-5279	+		+	

Powstały w ten sposób następujące grupy zaleceń:

- Zalecenia dotyczące działań proceduralnych na etapie produkcji: 6-5-0535, 6-5-0552, 6-5-0553, 6-5-0554, 6-5-0555, 6-5-0557, 6-5-0590, 6-5-0749, 6-6-5084, 6-6-5200, 6-6-5218, 6-6-5219, 6-6-5278 i 6-6-5279.
- Zalecenia dotyczące działań proceduralnych na etapie wdrożenia i eksploatacji: 6-5-0535, 6-5-0550, 6-5-0557, 6-5-0559, 6-5-0749, 6-6-5084, 6-6-5121 i 6-6-5142.
- Zalecenia dotyczące zabezpieczeń materialnych na etapie produkcji: 6-5-0538, 6-5-0541, 6-5-0750, 6-6-0802, 6-6-5061, 6-6-5165, 6-6-5167 i 6-6-5172.
- Zalecenia dotyczące zabezpieczeń materialnych na etapie wdrożenia i eksploatacji: 6-5-0536, 6-5-0541 i 6-5-0750.

Niektóre z zaleceń dotyczą całego cyklu życia systemu informatycznego, dlatego zostały zakwalifikowane zarówno do etapu produkcji, jak i do etapu wdrożenia i eksploatacji. Poniższy rysunek pokazuje poszczególne grupy zaleceń na płaszczyźnie wyznaczonej przez wymienione wcześniej cechy.



Rys. 1. Klasyfikacja zaleceń NRIC

## 5. Metoda wdrażania najlepszych praktyk

Proces formułowania i wdrażania najlepszych praktyk jest wieloetapowy. Praktyki występują w na każdym z etapów w następujących wersjach [OGIden]:

1. **ZŁOTA MYŚL** – nie potwierdzona: jeszcze nie poparta danymi ale intuicyjnie wydaje się dobra; może mieć pozytywny wpływ na działania biznesowe; wymaga dalszej analizy.
2. **DOBRA PRAKTYKA** – była już wdrożona i udowodniono jej dobry wpływ na organizację; poparta danymi zebranymi w ramach jednego przypadku zastosowania.
3. **LOKALNA NAJLEPSZA PRAKTYKA** – określono ją jako najlepsze podejście dla pewnych działów organizacji, w oparciu o dane pochodzące z analizy wydajności procesów. Analiza zawiera wstępną krytykę podobnych procesów stosowanych na zewnątrz firmy.
4. **PRZEMYSŁOWA NAJLEPSZA PRAKTYKA** – określono ją jako najlepsze podejście dla całej organizacji w oparciu o dane pochodzące z testów porównawczych (ang. *benchmarking*) wewnątrz i na zewnątrz organizacji włączając w to analizę danych wydajnościowych.

Można więc śmiało mówić o cyklu życia najlepszych praktyk. Poniższa tabela przedstawia fazy takiego cyklu wraz z uzasadnieniem ich istotności.

Tabela 3. Cykl życia zaleceń typu najlepszych praktyk z uzasadnieniem jego faz

Etapy cyklu życia praktyki	Uzasadnienie etapu
<b>Identyfikacja kandydata na najlepszą praktykę:</b> znalezienie praktyki dotyczącej bezpieczeństwa, która wydaje się przynosić pozytywny skutek na podstawie badań i odpytywania różnych osób.	Praktyki są wypracowywane przez różne osoby i dlatego od nich należy uzyskiwać informacje na temat kandydatów na najlepszą praktykę.
<b>Udokumentowanie praktyki:</b> opisanie praktyki w postaci dokumentu o standardowym formacie.	Standardowy format zapewnia, że praktyki będą opisane w taki sposób, by każdy mógł je zastosować w swoistych okolicznościach.
<b>Ocena praktyki:</b> klasyfikacja praktyki według pewnego zbioru kryteriów, w celu określenia czy i do jakiego stopnia jest one dobra.	Ponieważ nieświadomi lub złośliwi ludzie mogą twierdzić, że przeciętne lub nawet szkodliwe praktyki są dobre, a ponieważ niektóre dobre praktyki są znacznie lepsze niż inne dobre praktyki, najlepsze praktyki muszą być ocenione pod względem faktycznej i względnej dobroci.
<b>Akceptacja praktyki:</b> przyjęcie praktyki i określenie zakresu jej obowiązywania w oparciu o poradę odpowiednich osób.	Jeżeli ocena praktyk została przeprowadzona przez kogoś innego, kierownicy zajmujący się najlepszymi praktykami potrzebują zachować pewną kontrolę nad wynikami tej oceny. Akceptacja jest oddzielnym etapem od oceny służącym zapewnieniu im takiej możliwości.
<b>Dostarczenie praktyki:</b> udostępnienie informacji o praktyce innym za pomocą WWW, CD, dokumentów papierowych, help desk-u i umożliwienie kontaktów z ekspertami.	Aby zapewnić, aby każdy użytkownik praktyki bez względu na okoliczności miał dostęp do informacji o praktykach i mógł ich użyć, należy zastosować wiele dróg przekazywania informacji o tych praktykach. Ponieważ nie wystarczają techniczne środki przekazu istnieje potrzeba przekazywania informacji w ramach kontaktów między osobami.
<b>Doskonalenie praktyki:</b> utrzymanie praktyki tak, aby była aktualna i uwzględniała pomysły racjonalizatorskie zgłoszone przez użytkowników tej praktyki.	Prawa, technologia potrzeby biznesowe zmieniają istniejące podatności praktyki powinny też się zmieniać, aby za tymi zmianami nadażyć. Także jak wszystkie produkty człowieka praktyki będą niedoskonałe i będą wymagały ciągłych udoskonaleń. Praktyka może być używana w wielu wersjach, a każda z nich może być lepsza od poprzedniej.

## 6. Podsumowanie

Omówione zalecenia stanowią najlepsze i aktualne praktyki w dziedzinie bezpieczeństwa informacji i systemów informatycznych. Zalecenia są opracowywane oraz zbierane przez organizacje głównie ze Stanów Zjednoczonych. Mimo tego ich zastosowanie jest dość ogólne i mogą być z powodzeniem wdrażane przez instytucje funkcjonujące w Europie.

Wybrane zalecenia dotyczą zabezpieczeń materialnych i proceduralnych. Rekomendacje NIST i GAISP obejmują ogólne aspekty funkcjonowania organizacji i ochrony informacji. Natomiast wybrane zalecenia NRIC dotyczą dostawców sprzętu i oprogramowania, a ich przedmiotem są

dostarczane systemy sprzętowo-programowe. Ochrona tych systemów odbywa się zarówno na etapie ich produkcji, jak i na etapie wdrożenia i eksploatacji. Pozytywnym aspektem jest również fakt, że NRIC nie zaniedbuje pracy nad swymi zaleceniami i ciągle je uaktualnia dopasowując do bieżących potrzeb i sytuacji. Niedługo ukaże się siódma edycja zaleceń. Warto wziąć je pod uwagę przy formułowaniu najlepszych praktyk dla firmy. Wiele z opisywanych norm jest dostępnych nieodpłatnie w sieci Internet.

Wdrożenie przedstawionych w artykule zaleceń, zasad i najlepszych praktyk może wydatnie podnieść bezpieczeństwo organizacji. Natomiast optymalne zarządzanie bezpieczeństwem jest na tyle ważne, aby nie powierzać przyszłości istnienia własnej organizacji przypadkowi. Dlatego należy stosować najlepsze praktyki, aby zapewnić bezpieczeństwo i ciągłość funkcjonowania. Przy formułowaniu najlepszych praktyk trzeba brać pod uwagę doświadczenia innych instytucji zgodnie z zasadą, że lepiej uczyć się na błędach innych, a nie własnych.

## **Bibliografia**

- [GKBSP] King G.: Best Security Practices, Computer Sciences Corporation, Defense Group, Information Security and Operations Center, <http://www.csrc.nist.gov/nissc/2000/proceedings/papers/022.pdf>
- [OGIden] O'Dell C., Jackson Grayson C.: Identifying and Transferring Internal Best Practices, APQC, <http://www.apqc.org/download.htm>
- [NIST] zalecenia National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC), 1996, <http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf>
- [GAISP] zalecenia Generally Accepted Information Security Principles (GAISP), Information Systems Security Association (ISSA), 1999, [http://www.issa.org/gaisp/\\_pdfs/v30.pdf](http://www.issa.org/gaisp/_pdfs/v30.pdf)
- [NRIC] NIST 800-14 „Generally Accepted Principles and Practices for Securing Information Technology Systems”, Network Reliability and Interoperability Council (NRIC), 1998, <http://www.bell-labs.com/cgi-user/krauscher/bestp.pl>
- [OECD] OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, [http://www.dti.gov.uk/industry\\_files/word/M00034478%202.doc](http://www.dti.gov.uk/industry_files/word/M00034478%202.doc)