Przegląd normy PN-I-07799-2:2005
Systemy zarządzania bezpieczeństwem informacji – Specyfikacja i wytyczne do stosowania

Krzysztof LIDERMAN

Zakład Systemów Komputerowych, Instytut Teleinformatyki i Automatyki WAT,
ul. S. Kaliskiego 2, 00–908 Warszawa

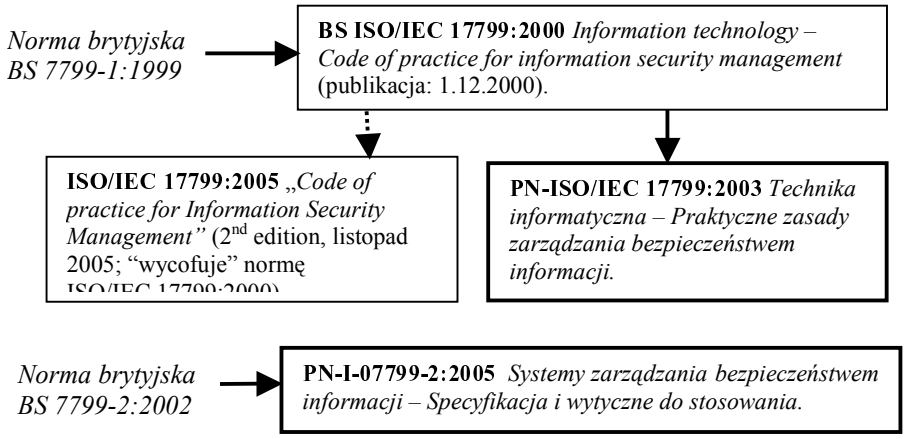
STRESZCZENIE: Artykuł zawiera przegląd zawartości polskiej edycji normy PN-I-07799-2:2005 z zakresu bezpieczeństwa teleinformatycznego. Jest on kontynuacją tematyki zawartej w [2] i [4].

1. Wstęp

W artykułach [2] i [4], opublikowanych w roku 2000 i 2002, zostały opisane podstawowe standardy z zakresu bezpieczeństwa teleinformatycznego, uznawane na forum międzynarodowym w tamtych latach. Od tego czasu, przynajmniej w realiach polskich, nastąpiła znacząca zmiana, związana z opublikowaniem przez Polski Komitet Normalizacyjny norm [10] i [11], będących odpowiednikami stosownych norm ISO i Brytyjskiego Instytutu Standaryzacji (por. rys. 1).

Wymienione normy stanowią z jednej strony zbiór „najlepszych praktyk", które powinny być stosowane w budowie „bezpiecznych" systemów teleinformatycznych [10], a z drugiej strony ustanawiają wymagania na zarządzanie bezpieczeństwem informacji przetwarzanej w systemach teleinformatycznych [11]. Wymagania te są podstawą do wydawania certyfikatów „bezpieczeństwa", tj. certyfikatów na zgodność z normą PN-I-07799-2:2005. Od połowy 2005 roku Polskie Centrum Akredytacji uruchomiło program akredytacji jednostek certyfikujących systemy zarządzania bezpieczeństwem informacji (ISMS) [13], co spowodowało, że niektóre organizacje polskie zajmujące się szeroko rozumianym audytem (np. Urząd Dozoru Technicznego) podjęły starania o uzyskanie takiej akredytacji.

Standardy Brytyjskiego Instytutu Standaryzacji (oznaczone symbolem BS) cieszą się dużym uznaniem na całym świecie, czego przejawem jest m.in. przyjęcie ich jako podstawę norm wydawanych przez ISO/IEC. Wiele firm, z szeroko rozumianych względów biznesowych, stara się uzyskać poświadczenia, w postaci certyfikatów, że przetwarzane, przechowywane i przesyłane przez nie informacje są chronione zgodnie z zapisami tych standardów. Dotychczas, ze względu na brak stosownej normy polskiej i polskiego programu akredytacji, certyfikaty takie firmy polskie, działające w Polsce, mogły uzyskać od firm zagranicznych, wystawiających certyfikaty, akredytowanych za granicą.



Rys. 1. Powiązania pomiędzy normami: brytyjskimi, ISO i polskimi

Krótką historię linii rozwojowej standardu BS 7799 Brytyjskiego Instytutu Standaryzacji można przedstawić następująco:

1. Początek

Opublikowanie w połowie lat 90. XX wieku dwuczęściowego standardu:

- BS 7799-1:1995 *Code of practice for Information Security Management*
- BS 7799-2:1998 *Specification for Information Security Management Systems*.

2. Stabilizacja

Pod koniec lat 90. opublikowanie drugiej wersji standardu. W części pierwszej BS 7799-1:1999 *Code of practice for Information Security Management* opisane są *najlepsze praktyki, które powinny być stosowane w budowie i zarządzaniu bezpiecznych systemów teleinformatycznych, zgrupowane w dziesięć tematów.*

W stosunku do wersji z roku 1995 nastąpiła zmiana numeracji rozdziałów, zmiany nazw niektórych rozdziałów oraz dodanie rozdziałów:

4.3. Outsourcing
7.3. General Controls
9.8. Mobile computing and teleworking
10.3. Cryptographic controls

W BS 7799-2:1999 *Specification for Information Security Management Systems* zdefiniowanych jest 127 punktów kontrolnych (wymagań na bezpieczeństwo teleinformatyczne) oraz zarys ISMS w postaci sześcioetapowego schematu jego budowy (rozdz. 3).

3. Doskonalenie

Opublikowanie w 2002 roku kolejnej wersji standardu, uwzględniającej modne „podejście procesowe":

- BS 7799-1:2002 *Code of practice for Information Security Management*;
- BS 7799-2:2002 *Specification for Information Security Management Systems*.

14 października 2005 roku została opublikowana przez organizację ISO, na podstawie brytyjskiej normy BS 7799-2:2005, norma ISO/IEC 27001:2005 *Information Security Management – Specification With Guidance for Use*.

Norma ISO/IEC 27001:2005:

- zawiera specyfikację systemów zarządzania bezpieczeństwem informacji;
- na zgodność z tą normą będą wydawane certyfikaty.

Nowy standard jest podwójnie oznaczony:

ISO/IEC 27001:2005 BS 7799-2:2005,

dlatego przez okres ok. 2 lat nie przewiduje się różnic w certyfikacji na jeden lub drugi standard. Przy certyfikacji według BS 7799-2:2002 muszą być brane pod uwagę (*update*) różnice w stosunku do BS 7799-2:2005.

W tym kontekście należy zwrócić uwagę na to, że od października 2005 roku nowo opublikowana norma polska PN-I-07799-2:2005 staje się normą

przestarzałą (sic!). Piszący te słowa zetknął się już w praktyce, w tak krótkim okresie od wydania obu norm, z zapytaniami ofertowymi o możliwość certyfikacji na zgodność z normą ISO/IEC 27001:2005, ponieważ jest ona postrzegana przez potencjalnych klientów jako bardziej „międzynarodowa" i perspektywiczna niż polska norma PN-I-07799-2:2005.

W dalszym okresie planowane są przez ISO publikacje kolejnych norm tej serii:

- ISO/IEC 27000 – słownictwo i terminologia,
- ISO/IEC 27002 (obecnie znane jako BS 7799-1 oraz ISO/IEC 17799) – praktyczne zasady zarządzania bezpieczeństwem informacji, przewidywany termin publikacji –2007 rok,
- ISO/IEC 27003 – porady i wskazówki dotyczące implementacji systemu zarządzania bezpieczeństwem informacji (ISMS),
- ISO/IEC 27004 – *System Zarządzania Bezpieczeństwem Informacji. Wskaźniki i pomiar*,
- ISO/IEC 27005 (obecnie BS 7799-3) – zarządzanie ryzykiem bezpieczeństwa informacji.

2. Zawartość normy PN-I-07799-2:2005: Systemy zarządzania bezpieczeństwem informacji – Specyfikacja i wytyczne do stosowania

Aktualne wydanie normy PN-I-07799-2:2005 to 53 strony o zawartości przedstawionej na rysunku 2. Z zawartych w rozdziale 1.2 zapisów wynika, że wykluczenie jakiegokolwiek wymagania określonego w rozdziałach **4, 5, 6** i **7** nie może być zaakceptowane. Niestety, nie został wyjaśniony sposób interpretacji zapisów normy. Przykład takiego zapisu:

> **4.3.3 Nadzór nad zapisami**
>
> W celu dostarczenia świadectwa potwierdzającego zgodność z wymaganiami oraz skutecznej eksploatacji ISMS powinny być ustanowione i utrzymywane odpowiednie zapisy. Zapisy te powinny być nadzorowane. ISMS powinien uwzględniać wszystkie odnośne wymagania przepisów prawa. Zapisy powinny być czytelne, łatwe do zidentyfikowania i odtwarzalne. Należy udokumentować zabezpieczenia służące identyfikowaniu, przechowywaniu, ochronie, odtwarzaniu, archiwizacji oraz niszczeniu zapisów. Proces zarządzania powinien określać potrzebę i zakres zapisów. Zapisy powinny dotyczyć realizacji procesów, zgodnie z opisem zawartym w 4.2 oraz wszystkich incydentów związanych z bezpieczeństwem w odniesieniu do ISMS.

Spis treści

Komitet odpowiedzialny za normę brytyjską

Przedmowa

0. Wprowadzenie

1. Zakres normy

2. Powołania normatywne

3. Pojęcia i definicje

4. System zarządzania bezpieczeństwem informacji (ISMS) (59)

5. Odpowiedzialność kierownictwa (17)

6. Przegląd ISMS realizowany przez kierownictwo (24)

7. Doskonalenie ISMS (19)

(119)

Załącznik A (**normatywny**): Cele stosowania zabezpieczeń oraz zabezpieczenia.

Załącznik B (informacyjny): Wytyczne do stosowania normy.

Załącznik C (informacyjny): Powiązanie między
BS EN ISO 9001:2000,
BS EN ISO 14001:1996 a BS 7799-2:2002.

Załącznik D (informacyjny): Zmiany wewnętrznej numeracji.

Bibliografia.

Rys. 2. Zawartość normy PN-I-07799-2:2005. Liczby w nawiasach oznaczają oszacowaną przez autora liczbę wymagań przy literalnej interpretacji zapisów normy

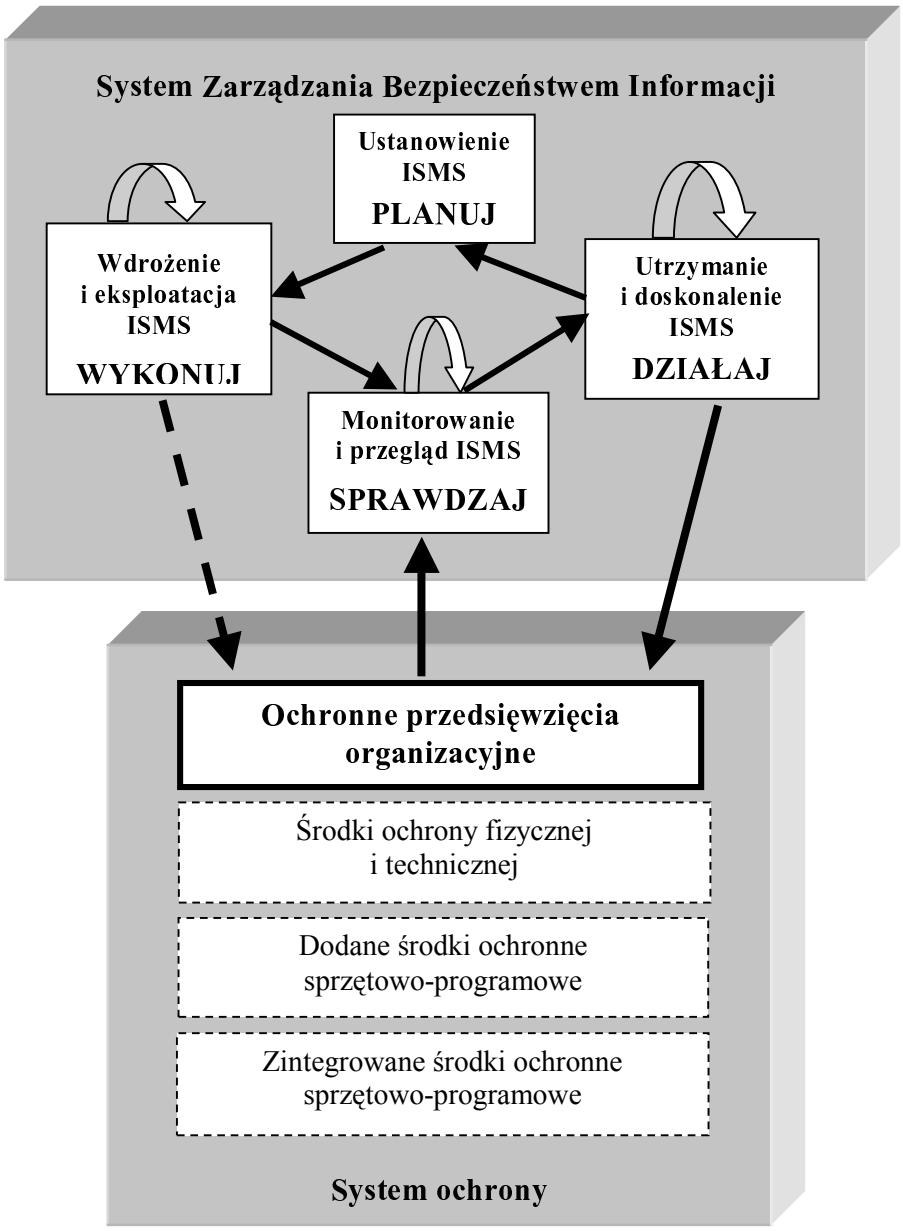
W związku z tym zapisem nasuwa się pytanie, czy jako wymaganie (jedno) liczy się punkt 4.3.3 normy jako całość, czy też jest to w sumie 17 wymagań, przekładających się na następujący podzbiór pytań kontrolnych:

1) Czy są ustanowione odpowiednie zapisy?
2) Czy są utrzymywane odpowiednie zapisy?
3) Czy zapisy są nadzorowane?
4) Czy ISMS uwzględnia wszystkie odnośne wymagania przepisów prawa?
5) Czy zapisy są czytelne?
6) Czy zapisy są łatwe do zidentyfikowania?
7) Czy zapisy są odtwarzalne?
8) Czy są udokumentowane zabezpieczenia służące identyfikowaniu zapisów?
9) Czy są udokumentowane zabezpieczenia służące przechowywaniu zapisów?
10) Czy są udokumentowane zabezpieczenia służące ochronie zapisów?
11) Czy są udokumentowane zabezpieczenia służące odtwarzaniu zapisów?
12) Czy są udokumentowane zabezpieczenia służące archiwizacji zapisów?
13) Czy są udokumentowane zabezpieczenia służące niszczeniu zapisów?
14) Czy proces zarządzania określa potrzebę zapisów?
15) Czy proces zarządzania określa zakres zapisów?
16) Czy zapisy dotyczą realizacji procesów, zgodnie z opisem zawartym w 4.2?
17) Czy zapisy dotyczą wszystkich incydentów związanych z bezpieczeństwem w odniesieniu do ISMS?

3. PN-I-07799-2:2005 – uwagi ogólne

Norma została przygotowana dla kierownictw przedsiębiorstw oraz ich personelu w celu przedstawienia modelu tworzenia oraz zarządzania skutecznym systemem zarządzania bezpieczeństwem informacji (ISMS – w języku polskim można używać także skrótu SZBI). Zaleca się, aby wprowadzenie ISMS było dla organizacji decyzją strategiczną.

Norma PN-I-07799-2:2005 może być stosowana przez komórki wewnętrzne i organizacje zewnętrzne, w tym jednostki certyfikujące, w celu oceny zdolności organizacji do spełniania zarówno postawionych przez siebie wymagań, jak i oczekiwań ze strony klientów lub organów nadzoru.



Rys. 3. Architektura systemu bezpieczeństwa teleinformatycznego: perspektywa zarządzania bezpieczeństwem

W normie stosuje się i wskazuje na możliwość stosowania do wszystkich procesów ISMS modelu „Planuj – Wykonuj – Sprawdzaj – Działaj" (PDCA – por. rys. 3):

1. Planuj (ustanowienie ISMS)

   Ustanowienie polityki bezpieczeństwa, celów, zakresu stosowania, procesów i procedur odpowiednich dla zarządzania ryzykiem oraz doskonalenia bezpieczeństwa, tak aby uzyskać wyniki zgodne z ogólnymi politykami i celami organizacji.

2. Wykonuj (wdrożenie i eksploatacja ISMS)

   Wdrożenie i eksploatacja polityki bezpieczeństwa, zabezpieczeń, procesów i procedur.

3. Sprawdzaj (monitorowanie i przegląd ISMS)

   Szacowanie oraz, pomiar (tam, gdzie ma zastosowanie) wykonania procesów w odniesieniu do polityki bezpieczeństwa, celów i praktycznych doświadczeń oraz przekazywanie kierownictwu wyników do przeglądu.

4. Działaj (utrzymanie i doskonalenie ISMS)

   Podejmowanie działań korygujących i zapobiegawczych w oparciu o wyniki przeglądu realizowanego przez kierownictwo, tak aby osiągnąć ciągłe doskonalenie ISMS.

4. Przegląd treści wstępnej części normy PN-I-07799-2:2005 (rozdziały 1-3)

W normie określono wymagania dotyczące ustanawiania, wdrażania, eksploatacji, monitorowania, przeglądu, utrzymywania i doskonalenia udokumentowanego ISMS w całościowym kontekście ryzyk biznesowych. Określono wymagania dla wdrażania zabezpieczeń dostosowanych do potrzeb pojedynczych organizacji lub ich części (zob. załącznik B, zawierający wytyczne do stosowania normy).

ISMS został zaprojektowany tak, aby zapewnić adekwatne i proporcjonalne zabezpieczenia, które odpowiednio chronią aktywa informacyjne oraz uzyskać zaufanie klientów oraz innych zainteresowanych stron. Można to przełożyć na utrzymywanie i zwiększanie konkurencyjności, przepływów finansowych, zyskowności, zgodności z przepisami prawa i wizerunek handlowy.

4.1. Zastosowanie

Wymagania opisane w normie PN-I-07799-2:2005 są ogólne i przeznaczone do stosowania we wszystkich organizacjach, niezależnie od typu, rozmiaru i natury biznesu.

Jeżeli jakiegokolwiek wymagania tej normy nie da się zastosować, z uwagi na naturę organizacji lub prowadzonej działalności, to można rozważyć jego wykluczenie.

W przypadku dokonania wykluczenia, twierdzenia o zgodności z niniejszą normą nie są akceptowane, **chyba że takie wykluczenia nie mają wpływu na możliwości organizacji lub jej odpowiedzialność co do zapewnienia stanu bezpieczeństwa informacji** i spełniają wymagania bezpieczeństwa wyznaczone przez oszacowanie ryzyka i zastosowane wymagania nadzoru.

Każde wyłączenie zabezpieczeń, o którego potrzebie zdecydowano na podstawie kryteriów akceptowania ryzyka, należy uzasadnić. Temu uzasadnieniu ma towarzyszyć odpowiednie potwierdzenie, że związane ryzyka zostały we właściwy sposób zaakceptowane przez osoby odpowiedzialne. **Wykluczenie jakiegokolwiek wymagania określonego w rozdziałach 4, 5, 6 i 7 nie może zostać zaakceptowane.**

4.2. Pojęcia i definicje

Pojęcia i definicje zamieszczone w normie są przytaczane głównie za [12]. Do podstawowych należą:

- **system zarządzania bezpieczeństwem informacji ISMS** (ang. ***I**nformation **S**ecurity **M**anagement **S**ystem*):
  ta część całościowego systemu zarządzania, oparta jest na podejściu wynikającym z ryzyka biznesowego; odnosi się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji. ISMS obejmuje strukturę organizacyjną, polityki, działania planistyczne, zakresy odpowiedzialności, praktyki, procedury, procesy i zasoby.
- **deklaracja stosowania** (ang. *statement of applicability*):
  dokument, w którym opisano cele stosowania zabezpieczeń oraz zabezpieczenia, które mają zastosowanie w ISMS danej organizacji, oparte o rezultaty i wnioski wynikające z procesów szacowania i postępowania z ryzykiem.

Oprócz definicji zawartych w rozdziale 4.3 normy, pojawiają się określenia precyzowane bezpośrednio w tekście. Przykłady:

- tam, gdzie w normie pojawia się termin „udokumentowana procedura", oznacza to, że procedura jest zdefiniowana, udokumentowana, wdrożona i utrzymywana,
- termin „procedura" jest umownie stosowany w bezpieczeństwie informacji w celu określenia „procesu", który jest realizowany przez ludzi, w przeciwieństwie do procesów wykonywanych przez komputery lub inne środki elektroniczne.

5. System zarządzania bezpieczeństwem informacji (ISMS)

4.1. Wymagania ogólne.

4.2. Ustanowienie i zarządzanie ISMS.

4.2.1. Ustanowienie ISMS.

4.2.2. Wdrożenie i eksploatacja ISMS.

4.2.3. Monitorowanie i przegląd ISMS.

4.2.4. Utrzymanie i doskonalenie ISMS.

4.3. Wymagania dotyczące dokumentacji.

4.3.1. Wstęp.

4.3.2. Nadzór nad dokumentami.

4.3.3. Nadzór nad zapisami.

Dalej są opisane poszczególne punkty rozdziału 4 normy z zachowaniem oryginalnej numeracji. Liczby podane w nawiasach to ilość wymagań dla każdego z punktów przy literalnej interpretacji wymagań.

4.1. Wymagania ogólne.

Organizacja powinna opracować, wdrożyć, utrzymać i stale doskonalić udokumentowany ISMS w kontekście całościowych działań biznesowych i ryzyka, które występują w organizacji. Zastosowany w normie proces opiera się na modelu PDCA.

4.2. Ustanowienie i zarządzanie ISMS. (26)

4.2.1. Ustanowienie ISMS. (9)

Organizacja powinna podjąć następujące działania:

a) *Określić zakres ISMS.*

b) *Określić politykę ISMS.*

c) *Określić systematyczne podejście do szacowania ryzyka.*

Należy:

- wskazać metodę szacowania ryzyka odpowiednią dla ISMS,
- określić bezpieczeństwo informacji w kontekście biznesowym oraz wymagania prawne i wymagania nadzoru,
- ustanowić politykę i cele ISMS w celu zmniejszenia ryzyk do akceptowalnych poziomów,
- wyznaczyć kryteria akceptowania ryzyka,
- zidentyfikować akceptowalne poziomy ryzyka.

d) *Określić ryzyka.*

e) *Oszacować ryzyka.*

f) *Zidentyfikować i ocenić warianty postępowania z ryzykami.*

g) *Wybrać cele stosowania zabezpieczeń oraz zabezpieczenia jako środki postępowania z ryzykami.*

Odpowiednie cele stosowania zabezpieczeń oraz zabezpieczenia **powinny zostać wybrane z listy zawartej w Załączniku A** normy, a wybór powinien być uzasadniony wnioskami wynikającymi z procesu szacowania ryzyka i postępowania z ryzykiem. Cele stosowania zabezpieczeń oraz zabezpieczenia wymienione w Załączniku A nie są listą wyczerpującą, zatem można wybrać dodatkowe cele stosowania zabezpieczeń oraz zabezpieczenia.

h) *Przygotować deklarację stosowania.*

Odpowiednie cele stosowania **zabezpieczeń oraz zabezpieczenia wybrane w 4.2.1g) oraz uzasadnienia ich wyboru powinny być udokumentowane w deklaracji stosowania.** Wykluczenie któregokolwiek z celów stosowania zabezpieczeń oraz zabezpieczenia z listy przedstawionej w Załączniku A także powinno być odnotowane.

i) *Uzyskać akceptację kierownictwa dla zaproponowanych ryzyk szczątkowych oraz autoryzację do wdrażania i eksploatacji ISMS.*

4.2.2. Wdrożenie i eksploatacja ISMS. (7)

Organizacja powinna podjąć następujące działania:

a) *Sformułować plan postępowania z ryzykiem*.

b) *Wdrożyć plan postępowania z ryzykiem*.

c) *Wdrożyć zabezpieczenia wybrane w 4.2.1g.*

d) *Wdrożyć programy uświadamiania i szkolenia*.

e) *Zarządzać eksploatacją*.

f) *Zarządzać zasobami*.

g) *Wdrożyć procedury i inne zabezpieczenia wykrycia i reakcji na incydenty związane z naruszeniem bezpieczeństwa*.

4.2.3. Monitorowanie i przegląd ISMS. (6)

Organizacja powinna podjąć następujące działania:

a) *Wykonywać procedury i stosować inne zabezpieczenia*.

b) *Wykonywać regularne przeglądy skuteczności ISMS (w tym zgodność z polityką i celami oraz przegląd zabezpieczeń)*.

c) *Dokonywać przeglądów poziomu ryzyka szczątkowego oraz ryzyka akceptowalnego*.

d) *W zaplanowanych odstępach czasu przeprowadzać audyty wewnętrzne ISMS.*

e) *W regularnych odstępach czasu podejmować przeglądy ISMS realizowane przez kierownictwo* (co najmniej raz do roku).

f) *Rejestrować działania i zdarzenia, które mogą mieć wpływ na skuteczność lub jakość realizacji ISMS.*

4.2.4. Utrzymanie i doskonalenie ISMS. (4)

Organizacja powinna regularnie podejmować następujące działania:

a) *Wdrażać w ISMS zidentyfikowane udoskonalenia*.

b) *Podejmować odpowiednie działania korygujące lub zapobiegawcze.*

c) *Informować o wynikach działań i uzgadniać je ze wszystkimi zainteresowanymi stronami*.

d) *Zapewniać, że udoskonalenia osiągają zamierzone cele*.

4.3. Wymagania dotyczące dokumentacji. (33)

4.3.1. Wstęp. (7)

Dokumentacja ISMS powinna obejmować:

a) Udokumentowane deklaracje polityki bezpieczeństwa oraz celów stosowania zabezpieczeń.
b) Zakres ISMS oraz procedury i zabezpieczenia służące realizacji ISMS.
c) Raport z procesu szacowania ryzyka.
d) Plan postępowania z ryzykiem.
e) Udokumentowane procedury bezpieczeństwa informacji.
f) Zapisy wymagane przez niniejszą normę.
g) Deklarację stosowania.

UWAGI:

– Wszystkie dokumenty powinny być dostępne zgodnie z wymaganiami określonymi w polityce ISMS.
– Zakres dokumentacji ISMS może być odmienny dla różnych organizacji.
– Dokumenty i zapisy mogą przybrać dowolną formę lub być przechowywane na dowolnym typie nośnika.

4.3.2. Nadzór nad dokumentami (9)

Powinna być ustanowiona udokumentowana procedura – w celu określenia działań kierownictwa potrzebnych do zatwierdzenia, przeglądu, aktualizacji i identyfikacji zmian oraz zapewnienia, że:

a) najnowsze wersje odpowiednich dokumentów są dostępne w miejscach ich używania;
b) dokumenty pozostają czytelne i łatwe do zidentyfikowania;
c) dokumenty zewnętrzne są identyfikowane;
d) rozpowszechnianie dokumentów jest kontrolowane;
e) zapobiega się niezamierzonemu stosowaniu nieaktualnych dokumentów;
f) stosuje się odpowiednią ich identyfikację, jeżeli są zachowane z jakichkolwiek powodów.

4.3.3. Nadzór nad zapisami (17)

W celu dostarczenia świadectwa potwierdzającego zgodność z wymaganiami oraz skutecznej eksploatacji ISMS powinny być ustanowione, utrzymywane i nadzorowane odpowiednie zapisy. Zapisy powinny dotyczyć realizacji procesów, zgodnie z opisem zawartym w 4.2 oraz wszystkich incydentów związanych z bezpieczeństwem w odniesieniu do ISMS.

6. Odpowiedzialność kierownictwa

5.1. Zaangażowanie kierownictwa.

5.2. Zarządzanie zasobami.

5.2.1. Zapewnienie zasobów.

5.2.2. Szkolenie, uświadamianie i kompetencje.

Dalej są opisane poszczególne punkty rozdziału 5 normy z zachowaniem oryginalnej numeracji. Liczby podane w nawiasach to ilość wymagań dla każdego z punktów, przy literalnej interpretacji wymagań.

5.1. Zaangażowanie kierownictwa. (7)

Kierownictwo powinno zapewnić świadectwo swojego zaangażowania w ustanowienie, eksploatację, monitorowanie, przegląd, utrzymanie i doskonalenie ISMS.

5.2. Zarządzanie zasobami. (10)

5.2.1. Zapewnienie zasobów. (6)

Organizacja powinna określić i zapewnić zasoby potrzebne do:

a) ustanowienia, wdrożenia, eksploatacji i utrzymania ISMS;

b) zapewnienia, że procedury bezpieczeństwa informacji wspierają wymagania biznesowe;

c) zidentyfikowania i odniesienia się do wymagań przepisów prawa i wymagań nadzoru oraz zobowiązań umownych związanych z bezpieczeństwem;

d) utrzymania odpowiedniego bezpieczeństwa przez poprawne zastosowanie wszystkich wdrażanych zabezpieczeń;

e) przeprowadzenia przeglądów, kiedy zachodzi taka potrzeba, oraz odpowiedniego reagowania na wyniki tych przeglądów;

f) poprawy skuteczności ISMS tam, gdzie jest to wymagane.

5.2.2. Szkolenie, uświadamianie i kompetencje. (4)

Organizacja powinna zapewnić, że cały personel, któremu przypisano zakresy obowiązków określone w ISMS, ma kompetencje do realizacji wymaganych zadań (**4 wymagania**).

Organizacja powinna zapewnić także, że cały odnośny personel jest świadomy związku i znaczenia swoich działań dotyczących bezpieczeństwa informacji oraz wkładu dla osiągnięcia celów ISMS.

7. Przegląd ISMS realizowany przez kierownictwo

6.1. Wstęp.
6.2. Dane wejściowe przeglądu.
6.3. Dane wyjściowe przeglądu.
6.4. Wewnętrzne audyty ISMS.

Dalej są opisane poszczególne punkty rozdziału 6 normy z zachowaniem oryginalnej numeracji. Liczby podane w nawiasach to ilość wymagań dla każdego z punktów, przy literalnej interpretacji wymagań.

6.1. Wstęp. (4)

Kierownictwo powinno przeprowadzać przeglądy ISMS organizacji w zaplanowanych odstępach czasu w celu zapewnienia jego ciągłej poprawności, odpowiedniości i skuteczności. Przegląd powinien zawierać ocenę możliwości doskonalenia i potrzeby zmian w ISMS, w tym polityki bezpieczeństwa i celów bezpieczeństwa. Wyniki przeglądów powinny być jasno udokumentowane, a odpowiednie zapisy powinny być utrzymywane.

6.2. Dane wejściowe przeglądu. (8)

Dane wejściowe przeglądu realizowanego przez kierownictwo powinny zawierać informacje dotyczące:

a) wyników audytów i przeglądów ISMS;

b) informacji zwrotnych od zainteresowanych stron;

c) technik, produktów i procedur, które mogłyby być zastosowane w organizacji w celu ulepszenia realizacji i skuteczności ISMS;

d) statusu działań korygujących i zapobiegawczych;

e) podatności lub zagrożeń, do których nie było odpowiedniego odniesienia w poprzednim oszacowaniu ryzyka;

f) działań podjętych na skutek poprzednich przeglądów realizowanych przez kierownictwo;

g) jakichkolwiek zmian, które mogłyby dotyczyć ISMS;

h) zaleceń dotyczących doskonalenia.

6.3. Dane wyjściowe przeglądu. (3)

Dane wyjściowe przeglądu realizowanego przez kierownictwo powinny zawierać wszystkie decyzje i działania związane z:

a) doskonaleniem skuteczności ISMS;

b) modyfikacją procedur dotyczących bezpieczeństwa informacji, jeśli jest to konieczne, w celu reakcji na wewnętrzne lub zewnętrzne zdarzenia, które mogą mieć konsekwencje dla ISMS;

c) potrzebnymi zasobami.

6.4. Wewnętrzne audyty ISMS. (9)

Organizacja powinna przeprowadzać wewnętrzne audyty ISMS, w zaplanowanych odstępach czasu, w celu określenia, czy cele stosowania zabezpieczeń, zabezpieczenia, procesy i procedury jej ISMS są:

a) zgodne z wymaganiami niniejszej normy i odpowiednimi przepisami prawa oraz z wymaganiami o charakterze regulacyjnym;

b) zgodne z określonymi wymaganiami bezpieczeństwa informacji;

c) efektywnie wdrożone i utrzymywane;

d) realizowane w oczekiwany sposób.

Program audytu powinien być zaplanowany, przy uwzględnieniu statusu i znaczenia procesów oraz obszarów, które mają być audytowane, jak również wyników poprzednich audytów. Należy określić kryteria, zakres, częstotliwość, a także metody audytów.

Wybór audytorów i przeprowadzenie audytów powinny zapewniać obiektywność oraz bezstronność procesu audytu. Audytorzy nie powinni kontrolować swojej własnej pracy.

Zakresy obowiązków, wymagania planowania i przeprowadzania audytów oraz informowania o wynikach, a także utrzymywania zapisów powinny być określone w udokumentowanej procedurze.

8. Doskonalenie ISMS

7.1. Ciągłe doskonalenie.

7.2. Działania korygujące.

7.3. Działania zapobiegawcze.

Dalej są opisane poszczególne punkty rozdziału 7 normy z zachowaniem oryginalnej numeracji. Liczby podane w nawiasach to ilość wymagań dla każdego z punktów, przy literalnej interpretacji wymagań.

7.1. Ciągłe doskonalenie. (7)

Organizacja powinna w sposób ciągły poprawiać skuteczność ISMS przez stosowanie polityki bezpieczeństwa informacji, celów bezpieczeństwa, wyników audytu, analiz monitorowanych zdarzeń, działań korygujących i zapobiegawczych oraz przeglądów realizowanych przez kierownictwo.

7.2. Działania korygujące. (6)

Organizacja powinna podjąć działanie w celu wyeliminowania przyczyny niezgodności związanych z wdrożeniem i eksploatacją ISMS, tak aby przeciwdziałać powtórnym ich wystąpieniom. Udokumentowane procedury dla działania korygującego powinny określać wymagania dla:

a) zidentyfikowania niezgodności wdrożenia i/lub eksploatacji ISMS;

b) stwierdzenia przyczyn niezgodności;

c) oceny potrzeby działań w celu zapewnienia, że niezgodności się nie powtórzą;

d) wskazania i wdrożenia potrzebnych działań korygujących;

e) wprowadzenia do dokumentacji zapisów rezultatów podjętych działań;

f) przeglądu podjętych działań korygujących.

7.3. Działania zapobiegawcze. (6)

- Organizacja powinna wskazywać działanie podejmowane w celu ochrony przed przyszłymi niezgodnościami, tak aby przeciwdziałać ich wystąpieniu.
- Podejmowane działania zapobiegawcze powinny być stosowne do wagi potencjalnych problemów.
- Należy wskazać priorytety działań zapobiegawczych, w oparciu o wyniki szacowania ryzyka.

9. Załącznik A (normatywny)

A.1. Wprowadzenie.	
A.2. Poradnik praktycznych zasad.	
A.3. Polityka bezpieczeństwa	(2)
A.4. Organizacja bezpieczeństwa	(10)
A.5. Klasyfikacja i kontrola aktywów	(3)
A.6. Bezpieczeństwo osobowe	(10)
A.7. Bezpieczeństwo fizyczne i środowiskowe	(13)
A.8. Zarządzanie systemami i sieciami	(24)
A.9. Kontrola dostępu do systemu	(31)
A.10. Rozwój i utrzymanie systemu	(18)
A.11. Zarządzanie ciągłością działania	(5)
A.12. Zgodność	(11)
	(127)

*) W nawiasach podana jest ilość „najlepszych praktyk” (zabezpieczeń) wyspecyfikowanych przy każdym temacie.

A.1. Wprowadzenie.

Cele stosowania zabezpieczeń oraz zabezpieczenia zebrane w punktach od A.3 do A.12 wynikają bezpośrednio i są zgodne z

BS ISO/IEC 17799:2000, rozdziały **3 do 12.**

Listy w tabelach nie są wyczerpujące i organizacja może rozważyć, czy nie są konieczne dodatkowe cele stosowania zabezpieczeń oraz zabezpieczenia. Cele stosowania zabezpieczeń i zabezpieczenia powinny być wybrane jako część procesu ISMS opisanego w 4.2.1.

A.2. Poradnik praktycznych zasad

Rozdziały od 3 do 12 normy BS ISO/IEC 17799:2000 są poradnikiem zawierającym najlepsze praktyki dotyczące zabezpieczeń określonych w rozdziałach od A.3 do A.12.

10. Załącznik A – przykład zawartości

A.3 Polityka bezpieczeństwa.

			Numeracja BS ISO/IEC 17799:2000
A.3.1 ***Polityka bezpieczeństwa informacji*** *Cel stosowania zabezpieczeń:* Zapewnienie kierunków działania i wsparcia kierownictwa dla bezpieczeństwa informacji.			**3.1**
Zabezpieczenia			
A.3.1.1	*Dokument polityki bezpieczeństwa informacji*	Dokument polityki powinien zostać zatwierdzony przez kierownictwo, opublikowany i udostępniony w odpowiedni sposób wszystkim pracownikom.	**3.1.1**
A.3.1.2	*Przegląd i ocena*	Polityka bezpieczeństwa powinna być poddawana regularnemu przeglądowi, a w przypadku istotnych zmian powinna zapewniać, że pozostaje adekwatna.	**3.1.2**

11. Podsumowanie

Wysiłek poniesiony na realizację operacyjnej części audytu, na zgodność (literalną) z normą PN-I-07799-2:2005, można oszacować liczbą:

- **119 wymagań** z części podstawowej normy (dotyczącej ISMS), na temat spełnienia których powinien w raporcie wypowiedzieć się audytor;
- **127 zabezpieczeń,** których zastosowanie należy rozważyć zgodnie z wymaganiem zawartym w punkcie 4.2.1g.

Ustalenie liczby spełnionych z 117 wymagań daje odpowiedź na pytanie:

Jaka jest jakość ISMS?;

przy czym wykluczenie z listy kontrolnej jakiegokolwiek wymagania nie może zostać zaakceptowane.

Ustalenie liczby potrzebnych (wynikających z analizy ryzyka) zabezpieczeń i porównanie z liczbą zastosowanych zabezpieczeń (wybranych z 127 z załącznika A), daje odpowiedź na pytanie:

Jaki jest poziom bezpieczeństwa teleinformatycznego?

Wykluczenie zabezpieczenia, którego potrzeba zastosowania została określona na podstawie analizy ryzyka, może zostać zaakceptowane pod warunkiem, że związane ryzyka zostały we właściwy sposób zaakceptowane przez osoby odpowiedzialne.

Norma PN-I-07799-2:2005 została zaprojektowana, tak aby umożliwić organizacji dopasowanie (zintegrowanie) swojego ISMS do wymagań powiązanych systemów zarządzania. Jest zgodna (dostosowana) z innymi systemami zarządzania:

- BS EN ISO 9001:2000 oraz
- BS EN ISO 14001:1996,

tak aby wspierać jej spójne oraz zintegrowane wdrażanie i eksploatację wraz ze związanymi normami dotyczącymi zarządzania (mapowanie – por. tabela C.1 w normie).

Literatura

[1] Liderman K.: *Podręcznik administratora bezpieczeństwa teleinformatycznego*, MIKOM, Warszawa, 2003.

[2] Liderman K.: *Międzynarodowe kryteria oceny bezpieczeństwa informacji w systemach informatycznych*, Biuletyn IAiR, nr 11, WAT, Warszawa, 2000.

[3] Liderman K.: *Analiza ryzyka dla potrzeb bezpieczeństwa teleinformatycznego*, Biuletyn IAiR, nr 16, WAT, Warszawa, 2001.

[4] Liderman K.: *Standardy w ocenie bezpieczeństwa teleinformatycznego*, Biuletyn IAiR, nr 17, WAT, Warszawa, 2002.

[5] Liderman K.: *Oszacowania jakościowe ryzyka dla potrzeb bezpieczeństwa teleinformatycznego*, Biuletyn IAiR, nr 19, WAT, Warszawa, 2003.

[6] Liderman K., Patkowski A.: *Metodyka przeprowadzania audytu z zakresu bezpieczeństwa teleinformatycznego*, Biuletyn IAiR, nr 19, WAT, Warszawa, 2003.

[7] Liderman K.: *Czy „audyt bezpieczeństwa teleinformatycznego" jest tym samym co „audyt informatyczny"?*, Biuletyn IAiR, nr 21, WAT, Warszawa, 2004.

[8] ISO/IEC TR 13335-3:1997 *Guidelines for the Management of IT Security – Part 3: Techniques for the Management of IT Security*.

[9] BS ISO/IEC 17799:2000 *Information technology – Code of practice for information security management*.

[10] PN-ISO/IEC 17799:2003 Technika informatyczna – Praktyczne zasady zarządzania bezpieczeństwem informacji.

[11] PN-I-07799-2:2005 *Systemy zarządzania bezpieczeństwem informacji – Specyfikacja i wytyczne do stosowania*.

[12] ISO Guide 73:2002, *Risk mamagement – Vocabulary – Guidelines for use in standards*.

[13] Polskie Centrum Akredytacji. *Program akredytacji jednostek certyfikujących systemy zarządzania bezpieczeństwem informacji* (ISMS), DAC-07, wydanie 1, Warszawa, 20.06.2005.

[14] Białas A.: *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, WMT, Warszawa, 2006.

Recenzent: prof. dr hab. inż. Stanisław Paszkowski

Praca wpłynęła do redakcji: 15.12.2005