Przegląd wybranych standardów i norm z zakresu bezpieczeństwa informacyjnego

Krzysztof LIDERMAN
Instytut Teleinformatyki i Automatyki WAT,
ul. Gen. W. Urbanowicza 2, 00–908 Warszawa 46
krzysztof.liderman@wat.edu.pl

STRESZCZENIE: Artykuł zawiera przegląd wybranych norm i standardów z dziedziny bezpieczeństwa informacyjnego. Celem artykułu jest dostarczenie zwięzłej informacji na temat standardów i norm aktualnie uznawanych za wiodące na świecie. Publikacja dotyczy przede wszystkim idei zawartych w opisywanych normach, a nie szczegółowego ich opisu, wydania normy – standardu. Treść artykułu jest kontynuacją tematyki, do której odwołania zawarto w literaturze dołączonej do niniejszej publikacji.

SŁOWA KLUCZOWE: Common Criteria (ISO/IEC 15408), COBIT, CAG/CIS, NIST SP 800-xxx, ISO/IEC 27001/27002

1. Wstęp

Celem prezentowanego artykułu jest dostarczenie zainteresowanym podmiotom zwięzłej informacji na temat standardów i norm z zakresu bezpieczeństwa informacyjnego aktualnie uznawanych za wiodące na świecie. Informacja ta dotyczy przede wszystkim idei zawartych w opisywanych normach, a nie szczegółowego opisu zawartości konkretnego wydania normy/standardu. Jeżeli są zamieszczone konkretne zapisy z norm lub standardów, to głównie w celu ilustracji wspomnianych w poprzednim zdaniu idei. Od tego schematu odstąpiono jedynie w przypadku norm dotyczących zarządzania bezpieczeństwem informacji – ISO/IEC 27001 i 27002 które, z opisywanych w tym artykule, są od lat najbardziej rozpowszechnione i znane, a do których w wydaniu z roku 2013 wprowadzono istotne zmiany.

Artykuł jest artykułem przeglądowym, co oznacza, że nie są w nim zawarte analizy przydatności opisanych norm i standardów do rozwiązywania

konkretnych problemów (analizę przydatności powinien wykonać zainteresowany rozwiązaniem problemu użytkownik takiego dokumentu) ani ich porównania. Można jedynie zwrócić uwagę, że ewentualne porównania mają sens tylko w obrębie każdej z dwóch wskazanych dalej grup. Czytelnikom zainteresowanym zmianami jakie przeszły w ciągu lat opisywane normy i standardy, można zarekomendować zapoznanie się, w celach porównawczych, z wcześniejszymi artykułami o tej tematyce [3], [4], [5].

Standard to pewien wzorzec zatwierdzony przez instytucję normalizacyjną[1] lub przyjęty nieformalnie wskutek dużego upowszechnienia. Można wyróżnić dwie grupy standardów z zakresu bezpieczeństwa informacyjnego i teleinformatycznego:

1. Standardy ustanawiające tzw. **miary gwarantowanej odporności** i będące zwykle podstawą certyfikacji systemów i produktów teleinformatycznych, takie jak Common Criteria[2], TCSEC[3], ITSEC[4]. Ponieważ standardy te zawierają wytyczne dotyczące projektowania i wytwarzania bezpiecznych produktów oraz systemów, w rozdziale 2 niniejszego artykułu zostały połączone w jedną grupę ze standardami takimi jak CIS Critical Security Controls oraz niektóre standardy NIST (ang. *National Institute of Standards and Technology*) serii SP 800-xxx które zawierają takie wytyczne, ale nie ustanawiają formalnych miar gwarantowanej odporności.
2. Standardy ustanawiające tzw. **najlepsze praktyki**, informujące o tym, jakie cechy powinny mieć „bezpieczne" systemy informacyjne i jak „bezpiecznie" nimi zarządzać, np. standard Brytyjskiego Instytutu Standaryzacji BS 7799 (i wzorowane na nim normy serii ISO/IEC 270xx), niektóre standardy NIST serii SP 800-xxx.

Miary gwarantowanej odporności są podawane w postaci:

– *klas* (dla TCSEC);
– *poziomów uzasadnionego zaufania EAL1-EAL7* (dla ISO/IEC-15408 i Common Criteria);
– *stopni E1-E6* (dla ITSEC do oceny „poprawności" realizacji produktu).

W dziedzinie bezpieczeństwa informacyjnego standardy systematyzują proces oceny systemu zabezpieczeń oraz stanowią platformę odniesienia pozwalającą uzyskać powtarzalność procesu oceny i porównywać uzyskane

[1] Wtedy taki zatwierdzony standard nazywa się zwykle normą.

[2] Opublikowany także jako norma ISO/IEC-15408.

[3] Trusted Computer System Evaluation Criteria (tzw. *Orange Book)* – opracowany na zlecenie Departamentu Obrony USA i opublikowany w 1983 roku [20].

[4] Information Technology Security Evaluation Criteria – opublikowany w 1991 r. (wersja 1.2) pod patronatem Komisji Europejskiej, przygotowany przez Francję, Niemcy, Holandię i W. Brytanię [19].

wyniki[5]. Ułatwiają także formułowaniu kontraktu na przeprowadzenie audytu informatycznego lub bezpieczeństwa, a projektantom i wykonawcom systemów i produktów teleinformatycznych wskazują, jak organizować proces projektowania i wytwarzania, aby wytworzony tak produkt cechował się wysoką jakością pozwalającą na bezproblemowe uzyskanie odpowiedniego certyfikatu (bezpieczeństwa, jakości).

Przyznanie produktowi lub systemowi certyfikatu oznacza tyle i tylko tyle, że produkt/system został wykonany zgodnie z zaleceniami określonego standardu. Jeżeli np. system operacyjny został zakwalifikowany do klasy B3 według standardu TCSEC, oznacza to że: umożliwia dostęp do zasobów na podstawie etykietowania, jest dostępna pełna dokumentacja projektowa systemu, system został zaprojektowany z wykorzystaniem metodyk strukturalnych itd. Zakłada się, że jeżeli produkt zostanie wytworzony zgodnie z wymaganiami określonego standardu, to jego cechy związane z bezpieczeństwem teleinformatycznym będą na wyższym poziomie jakościowym, niż wtedy, gdy z zaleceń standardów się nie korzysta.

W dalszej części artykułu zostaną krótko przedstawione wybrane standardy i normy z ww. dwóch grup. Wybór jest arbitralny i na pewno można by wskazać jeszcze inne, niewątpliwie wartościowe, opracowania.

2. Standardy i normy wspierające projektowanie i wytwarzanie bezpiecznych produktów oraz systemów

W tym rozdziale są przedstawione:

- standard Common Criteria i odpowiadająca mu norma ISO/IEC 15408;
- standardy NIST serii SP 800-xxx;
- CIS Critical Security Controls – zbiór zaleceń przyjęty w Wielkiej Brytanii i USA za podstawę szeroko rozumianej ochrony sektora publicznego i prywatnego przed tzw. cyberatakami[6].

[5] Uważam, że normy są potrzebne, ale jako element porządkujący działania inżyniera a nie jako element kluczowy, zastępujący „inżynierskie" myślenie. Jeżeli zatem przełoży się zapisy normy na listę w arkuszu kalkulacyjnym z kratkami „do odhaczenia" to tylko po to, żeby sprawdzić czy w analizach nie pominięto czegoś istotnego, ogólnie uważanego za ważne, a nie po to, aby takie mechaniczne wypełnianie kratek zastąpiło myślenie i rzetelną analizę.

[6] Ze strony www.sans.org/critical-security-controls/history (dostęp marzec 2017):
(…) *Also in December 2011, the United Kingdom's Centre for the Protection of National Infrastructure (CPNI) announced to UK government agencies and critical industries that the UK government would adopt the CIS Critical Controls as the*

2.1. Common Criteria i norma ISO/IEC 15408

Próby ujęcia w standardowe ramy zagadnień związanych z ochroną i oceną bezpieczeństwa informacji w systemach informatycznych, były podejmowane w praktyce od połowy lat sześćdziesiątych XX wieku, gdy zaczęły wchodzić do powszechnego użytku systemy wielodostępne. Pierwszymi udanymi (tj. takimi, które wywarły istotny wpływ na sposób rozumienia problematyki bezpieczeństwa w systemach informatycznych i na wiele lat stały się podstawą do opracowywania lokalnych standardów w tym zakresie) były zalecenia wydane w USA w 1983 w postaci tzw. „Pomarańczowej książki" – *Trusted Computer System Evaluation Criteria* (TCSEC). W latach 80-tych i 90-tych XX wieku w kilku krajach podjęto próby opracowania własnych kryteriów:

- pod patronatem Komisji Europejskiej opublikowano przygotowany przez Francję, Niemcy, Holandię i W. Brytanię projekt o nazwie *Information Technology Security Evaluation Criteria v. 1.2* (ITSEC);
- w Kanadzie opublikowano *Canadian Trusted Computer Product Evaluation Criteria v. 3.0* (CTCPEC) łączący cechy ITSEC i TCSEC;
- w USA opublikowano *Federal Criteria for Information Technology Security v.1.0 - draft (FC)* jako konkurencyjną do kanadyjskiej próbę połączenia standardów USA i Europy;

W czerwcu 1993 roku organizacje które opracowały CTCPEC, FC oraz ITSEC, podjęły wspólną pracę (w porozumieniu z WG3 ISO) w ramach projektu o nazwie Common Criteria (Wspólne Kryteria – dalej w tekście oznaczane jako CC), nad połączeniem ww. standardów w jedną spójną całość, która byłaby do zaakceptowania przez społeczność międzynarodową. W efekcie, w kwietniu 1996 roku opublikowano wersję 1.0 CC (tzw. Committee Draft) zaaprobowaną przez ISO, a w październiku 1997 roku opublikowano wersję „beta" CC v.2.0 stanowiącą podstawę do opracowania normy ISO/IEC 15408 o nazwie *Evaluation Criteria for Information Technology Security*.

Trzyczęściowa norma międzynarodowa ISO/IEC 15408: *Information technology – Security techniques – Evaluation criteria for IT security* została opracowana przez Wspólny Komitet Techniczny ISO/IEC JTC 1, Technika Informatyczna, we współpracy z organizacjami sponsorującymi projekt *Wspólnych Kryteriów*[7]. Tekst identyczny z ISO/IEC 15408 jest publikowany

framework for securing the critical infrastructure going forward. And in May of 2012, the Commander of the US Cyber Command and Director of NSA announced that he believed adoption of the CIS Critical Controls was a good foundation for effective cybersecurity, and that they are a excellent example of how public and private sector organizations can voluntarily come together to improve security.

[7] Canada: *Communications Security Establishment*

przez organizacje sponsorujące projekt *Wspólnych Kryteriów* jako *Common Criteria for Information Technology Security Evaluation*.

Polski Komitet Normalizacyjny po raz pierwszy wydał normę PN-ISO/IEC 15408 (tłumaczenie wersji angielskiej ww. normy, ale tylko część 1 i 3) w 2002 roku. Obecnie te normy zostały wycofane i zastąpione normami w wersji angielskiej:

1. PN-ISO/IEC 15408-1:2016-10 (wersja angielska): Technika informatyczna – Techniki bezpieczeństwa – Kryteria oceny zabezpieczeń informatycznych – *Część 1: Wprowadzenie i model ogólny*.
2. PN-ISO/IEC 15408-2:2016-10 (wersja angielska): Technika informatyczna – Techniki bezpieczeństwa – Kryteria oceny zabezpieczeń informatycznych – *Część 2: Komponenty funkcjonalne zabezpieczeń*.
3. PN-ISO/IEC 15408-3:2016-10 (wersja angielska): Technika informatyczna – Techniki bezpieczeństwa – Kryteria oceny zabezpieczeń informatycznych – *Część 3: Komponenty uzasadnienia zaufania do zabezpieczeń*.

Charakterystyczne cechy zaleceń sformułowanych w normie 15408 są następujące:

– są zaleceniami mającymi na celu wprowadzenie ujednoliconego sposobu konstrukcji i oceny systemów (produktów) informatycznych pod względem szeroko rozumianego bezpieczeństwa;
– są katalogiem (wyrażonym w kategoriach klas, rodzin, komponentów i elementów) schematów konstrukcji wymagań funkcjonalnych (część 2 normy) oraz związanych z ochroną informacji w systemach informatycznych (część 3 normy), pisanych z użyciem specyficznej terminologii;
– mogą być stosowane zarówno do produktów programowych jak i sprzętowych stosowanych w informatyce;
– nie zalecają ani nie wspierają żadnej ze znanych metodyk projektowania i wytwarzania systemów informatycznych oraz metodyki oceny systemów informatycznych (tzn. podają, jak np. skonstruować profil ochrony, ale nie podają jak go wykorzystać);

France:	*Service Central de la Sécurité des Systémes d'Information*
Germany:	*Bundesamt für Sicherheit in der Informationstechnik*
Netherlands:	*Netherlands National Communications Security Agency*
United Kingdom:	*Communications-Electronics Security Group*
United States:	*National Institute of Standards and Technology*
United States:	*National Security Agency*

– są przeznaczone zarówna dla użytkowników (*customers*) i projektantów (*developers*) systemów/produktów informatycznych[8], jak i osób oceniających te systemy i produkty (*evaluators*).

W standardzie CC wyróżnia się trzy podstawowe procesy:

1. Konstruowania zabezpieczeń (ang. *TOE security development*).
2. Konstruowania produktu (ang. *TOE development*).
3. Oceny zabezpieczeń (ang. *TOE security evaluation*).

Wynikiem oceny TOE (systemu, produktu informatycznego) według zaleceń normy[9] jest dokument stwierdzający:

– zgodność tego systemu (produktu) z określonym *profilem zabezpieczeń* (ang. *Protection Profile*, PP) lub,
– spełnienie wymagań bezpieczeństwa określonych w *zadaniach zabezpieczeń* (ang. *Security Target*, ST) lub,
– przypisanie produktowi konkretnego *poziomu uzasadnienia zaufania* (ang. *Evaluation Assurance Level* – EAL).

Tab. 1. Elementy konstrukcyjne według normy ISO/IEC 15408:2016

Klasa uzasadniająca zaufanie	Rodzina (komponent) uzasadniająca zaufanie	Nazwa skrócona
Klasa ADV: Konstruowanie	Specyfikacja funkcjonalna	ADV_FSP
	Architektura zabezpieczeń	ADV_ARC
	Reprezentacja implementacji	ADV_IMP
	Organizacja wewnętrzna TSF	ADV_INT
	Projekt TOE	ADV_TDS
	Modelowanie polityki bezpieczeństwa	ADV_SPM
Klasa AGD: Dokumentacja	Instrukcja operacyjna dla użytkownika	ADV_OPE
	Procedury instalacyjne	ADV_PRE
Klasa ALC: Wsparcie w czasie cyklu życia	Możliwości zarządzania konfiguracją	ALC_CMC
	Zakres zarządzania konfiguracją	ALC_CMS
	Dostawa	ALC_DEL
	Bezpieczeństwo konstruowania	ALC_DVS
	Naprawa usterek	ALC_FLR
	Definicja cyklu życia	ALC_LCD
	Narzędzia i techniki	ALC_TAT
Klasa ATE: Testowanie	Pokrycie	ATE_COV
	Głębokość	ATE_DPT
	Testowanie funkcjonalne	ATE_FUN
	Testowanie niezależne	ATE_IND

[8] W normie/standardzie nazywane TOE **(**ang. *Target Of Evaluation* **–** przedmiot oceny).

[9] Dalej w tekście terminy „standard CC" i „norma 15408" są używane zamiennie.

Klasa AVA: Szacowanie podatności	Analiza podatności	AVA_VAN
Klasa ACO: Systemy złożone	Uzasadnienie wytwarzania złożonego TOE	ACO_COR
	Dokumentacja projektowa	ACO_DEV
	Zaufanie do komponentów składowych	ACO_REL
	Testowanie złożonych TOE	ACO_CTT
	Analiza podatności złożonego TOE	ACO_VUL

W normie wprowadzono koncepcję profili zabezpieczeń i zadań zabezpieczeń[10], gdzie:

– *Profil Zabezpieczeń* – formalny dokument opisujący w terminologii CC niezależny od implementacji zbiór wymagań na zabezpieczenia dla pewnej kategorii spełniających potrzeby odbiorców Przedmiotów Oceny (TOE).

– *Zadania Zabezpieczeń* – formalny dokument opisujący w terminologii CC zestaw wymagań na zabezpieczenia które są zaimplementowane w konkretnym Przedmiocie Oceny (TOE).

Norma definiuje zbiór elementów konstrukcyjnych, które składają się na zestawy wymagań na zabezpieczenia o znanej przydatności, które mogą być wykorzystywane przy ustalaniu wymagań na zabezpieczenia dla planowanych produktów i systemów (por. tabela 1). Uporządkowanie przez normę wymagań na zabezpieczenia w hierarchię klas, rodzin i komponentów ma na celu ułatwienie odbiorcom zlokalizowania konkretnych wymagań na zabezpieczenia (por. tab. 2). Wymagania na funkcjonalność i wymagania na uzasadnienie zaufania są przedstawiane w tym samym ogólnym stylu oraz przy użyciu tej samej organizacji opisu i terminologii. Należy mieć na uwadze, że:

– ocena „bezpieczeństwa" produktu z oczywistych względów nie obejmuje jego środowiska eksploatacyjnego;

– ocena „bezpieczeństwa" systemu zakłada znane i dobrze zdefiniowane środowisko w którym ten system jest eksploatowany.

Zawartość normy ISO/IEC 15408:2016 można krótko opisać następująco:

Część 1: *Wprowadzenie i model ogólny* (93 strony)

Jest to przewodnik po strukturze Profilów Zabezpieczeń (PP) i Zadań Zabezpieczeń (ST). Zawiera zasady oceny systemów informatycznych oraz przedstawia ogólny model na podstawie którego taka ocena jest prowadzona. W tej części są wyjaśnione również terminy używane w tej i pozostałych częściach dokumentu oraz metoda konstruowania złożonych wymagań.

Część 2*: Komponenty funkcjonalne zabezpieczeń* (321 stron)

[10] Zdefiniowane w części I normy PN-ISO/IEC 15408 profile i zadania zabezpieczenia, to nic innego jak wzorcowe szablony dokumentacyjne.

Zawiera katalog komponentów funkcjonalnych (pogrupowanych w rodziny i klasy) z których można „składać" wymagania funkcjonalne (ang. *Security Functional Requirements* – SFR) na TOE, tj. produkt lub system informatyczny wraz z dokumentacją administratora i/lub użytkownika.

Część 3: *Komponenty uzasadnienia zaufania do zabezpieczeń* (233 strony)
Zawiera katalog „komponentów bezpieczeństwa" (pogrupowanych w rodziny i klasy) z których można „składać" specyfikację wymagań na bezpieczeństwo TOE (dokładniej: wymagań uzasadniających zaufanie do zabezpieczeń – ang. *Security Assurance Requirements* – SAR), tj. produkt lub system informatyczny wraz z dokumentacją administratora i/lub użytkownika. Podstawowym elementem jest tutaj tzw. *element uzasadnienia zaufania* stanowiący pojedyncze, niepodzielne wymaganie dotyczące bezpieczeństwa. Każdy z takich elementów należy do jednego z trzech zbiorów:

– elementów działania konstruktora, np.:

  ADV_FSP.1.1D Konstruktor powinien dostarczyć specyfikację funkcjonalną.

  ADV_FSP.1.2D Konstruktor powinien dostarczyć opis przejścia od specyfikacji funkcjonalnej do SFR.

– elementów określających zawartość i postać elementów dowodu, np.:

  ADV_FSP.1.1C Specyfikacja funkcjonalna powinna opisywać przeznaczenie i metody użycia dla każdego zbioru SFR realizującego (SFR-enforcing) i każdego zbioru SFR wspierającego (SFR-supporting) funkcje bezpieczeństwa interfejsów TOE (TSFI −TOE Security Functionality Interface).

  ADV_FSP.1.2C Specyfikacja funkcjonalna powinna określać wszystkie parametry związane z każdym SFR-enforcing i SFR-supporting TSFI.

– elementów działania osoby oceniającej, np.:

  ADV_FSP.1.1E Oceniający powinien potwierdzić, że dostarczona informacja spełnia wszystkie wymagania, co do zawartości i prezentacji dowodu.

  *ADV_FSP.1.2**E** Oceniający powinien określić czy specyfikacja funkcjonalna jest dokładną i kompletną konkretyzacja wymagań na funkcjonalność zabezpieczeń TOE.*

W części trzeciej zdefiniowano także dwie klasy wymagań związanych z oceną *profili zabezpieczeń* i *zadań zabezpieczeń*:

– klasa APE: ocena Profilu Zabezpieczeń

– klasa ASE: ocena dokumentu Zadania Zabezpieczeń

oraz poziomy uzasadnienia zaufania[11]:

[11] W użyciu są także poziomy rozszerzone, oznaczone jako EAL+. Rozszerzenie oznacza, że oprócz wymaganego dla danego poziomu EAL zbioru wymagań dodano

– EAL1 – testowane funkcjonalnie
– EAL2 – testowane strukturalnie
– EAL3 – metodycznie testowane i sprawdzane
– EAL4 – metodycznie projektowane, testowane i weryfikowane
– EAL5 – półformalnie zaprojektowane i testowane
– EAL6 – projekt półformalnie weryfikowany i testowany
– EAL7 – projekt formalnie weryfikowany i testowany.

Zbiór funkcji zabezpieczających zebrany w TSF może być w konkretnym produkcie (TOE) zaimplementowany z różnym rygoryzmem wyrażonym przez poziom EAL. Dla danego TOE w jego zadaniu zabezpieczeń musi być zadeklarowany jeden, konkretny poziom EAL. Elementy uzasadniające zaufanie wchodzące w skład pakietu EAL wskazują zakres i szczegółowość materiału dowodowego, który konstruktor powinien dostarczyć na uzasadnienie zadeklarowanego poziomu EAL, a oceniający jest zobowiązany to sprawdzić.

Jednym z powodów opracowania CC było dążenie do uniknięcia wielokrotnej certyfikacji produktów w zależności od kraju i uznawanego przez niego schematu certyfikacyjnego, co dla producentów było ze względu na wysokie koszty takiego procesu niekorzystne. Dlatego po opracowaniu CC zawarto porozumienie o wzajemnym respektowaniu rezultatów oceny i certyfikacji bezpiecznych produktów informatycznych CCRA (ang. *Common Criteria Recognition Arrangement*), do którego należy obecnie 27 państw i w którym rozróżnia się dwie grupy państw w zależności od zakresu stosowania standardu.

Pierwsza grupa to *Certificate Authorizing Members* zrzeszająca państwa, które opracowały i prawnie przyjęły do stosowania własne schematy oceny i które mają prawo do wykonywania ocen i wydawania certyfikatów. Należy do tej grupy 17 następujących państw (rok 2016): Australia, Kanada, Francja, Niemcy, Włochy, Japonia, Malezja, Holandia, Nowa Zelandia, Norwegia, Korea Południowa, Hiszpania, Szwecja, Turcja, Wielka Brytania, Stany Zjednoczone, Indie.

Druga grupa to *Certificate Consuming Members* zrzeszająca państwa, które respektują certyfikaty wydane przez innych członków CCRA, ale jeszcze nie przyjęły własnych schematów oceny i nie mogą na razie wykonywać ocen i certyfikacji produktów. Do tej grupy należy 10 następujących państw (rok

pewne wymagania dodatkowe (zwykle z rodziny ALC_FLR – Flaw Remediation – postępowanie z usterkami) albo standardowy komponent z określonego poziomu EAL zastąpiono komponentem z poziomu wyższego.

2016): Austria, Czechy, Dania, Finlandia, Grecja, Węgry, Izrael, Pakistan, Singapur, Katar.

Jak widać, Polska do tej pory (początek roku 2017) nie przystąpiła do grona sygnatariuszy porozumienia CCRA, ale na początku 2017 roku dołączyła do grupy państw sygnatariuszy porozumienia SOG-IS (*Senior Official Group Information Security Systems*)[12]. Porozumienie SOG-IS (zawarte w roku 1997) ustanowiono w odpowiedzi na decyzję Rady Unii Europejskiej z 31.03.1992 r. w dziedzinie bezpieczeństwa systemów informatycznych oraz w następstwie zalecenia Rady z 7.04.1995 r. w sprawie wspólnych kryteriów oceny bezpieczeństwa technologii informacyjnej.

Porozumienie reguluje współpracę krajów Unii Europejskiej oraz EFTA, pracujących nad koordynowaniem polityk certyfikacji wyrobów sektora technologii informatyczno-komunikacyjnych. W przyszłości Polska będzie mogła samodzielnie wystawiać certyfikaty, zgodne z przyjętą do polskiego systemu prawnego międzynarodową normą ISO/IEC 15408.

W ramach działań upowszechniających wyniki projektu CCMODE[13] zrealizowanego w katowickim Instytucie Technik Innowacyjnych EMAG zapoczątkowano budowanie społeczności użytkowników standardu Common Criteria w Polsce. Obecnie społeczność ta obejmuje kilkadziesiąt podmiotów, ale pomimo szeroko prowadzonych działań edukacyjnych i stosunkowo licznej grupy zainteresowanych użytkowników, stosowanie standardu w Polsce nadal pozostaje wybiórcze i nieformalne [2].

Dokumentację uzupełniającą do standardu Common Criteria można znaleźć m.in. na stronie projektu[14]. Podstawowym dokumentem uzupełniającym jest licząca 433 strony metodyka oceny [14]. Polskojęzycznym, wartym polecenia źródłem informacji o CC są publikacje [1], [2]. Na stronie projektu CC jest zamieszczona także lista certyfikowanych produktów wraz z odpowiednią dokumentacją oraz różne szczegółowe statystyki.

Istotne dla rozwoju CC było także przyjęcie ich jako standardu NATO, zastępującego prawie dwudziestoletni standard NTCSEC (rozpoczęcie

[12] Obecnie (rok 2017) uczestnikami umowy są: Austria, Francja, Niemcy, Finlandia, Holandia, Norwegia, Hiszpania, Szwecja oraz Zjednoczone Królestwo Wielkiej Brytanii i Irlandii Północnej.

[13] „Środowisko rozwojowe produktów i systemów informatycznych o podwyższonych wymaganiach bezpieczeństwa (ang. *Common Criteria Modular Open Development Environment* – CCMODE)". Projekt zrealizowany w ramach Programu Operacyjnego Innowacyjna Gospodarka, 2007-2013, Priorytet 1 „Badania i rozwój nowoczesnych technologii" (POIG 1.3.1). Patrz też *http://www.commoncriteria.pl*.

[14] *http://www.commoncriteria.pl/index.php/pl/standard-common-criteria/dokumentacja-standardu/ dokumentacja-uzupelniajaca* (dostęp marzec 2017).

wykorzystywania CC w NATO to trzeci kwartał 2001, pełne stosowanie CC – od 2 kwartału 2003 roku) i związane z tym utworzenie repozytorium profili zabezpieczeń i pakietów wymagań, oraz utworzenie rejestru produktów NATO spełniających kryteria CC.

Tab. 2. Poziomy uzasadnienia zaufania (tabela za [9])

Klasa uzasadnienia zaufania	**Rodzina** uzasadnienia zaufania	**Komponenty** uzasadnienia zaufania wchodzące w skład poziomów uzasadnienia zaufania						
		EAL1	**EAL2**	**EAL3**	**EAL4**	**EAL5**	**EAL6**	**EAL7**
Konstruowanie	ADV_ARC		**1**	1	1	1	1	1
	ADV_FSP	**1**	**2**	**3**	**4**	**5**	5	**6**
	ADV_IMP				**1**	1	**2**	2
	ADV_INT					**2**	**3**	3
	ADV_SPM						**1**	1
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**
Dokumentacja	AGD_OPE	**1**	1	1	1	1	1	1
	AGD_PRE	**1**	1	1	1	1	1	1
Wsparcie w czasie cyklu życia	ALC_CMC	**1**	**2**	**3**	**4**	4	**5**	5
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	**5**
	ALC_DEL		**1**	1	1	1	1	1
	ALC_DVS			**1**	1	1	**2**	2
	ALC_FLR	Opcjonalnie dla dowolnego EAL						
	ALC_LCD			**1**	1	1	1	**2**
	ALC_TAT				**1**	**2**	**3**	3
Ocena bezpieczeństwa TOE	ASE_CCL	**1**	1	1	1	1	1	1
	ASE_ECD	**1**	1	1	1	1	1	1
	ASE_INT	**1**	1	1	1	1	1	1
	ASE_OBJ	**1**	**2**	2	2	2	2	2
	ASE_REQ	**1**	**2**	2	2	2	2	2
	ASE_SPD		**1**	1	1	1	1	1
	ASE_TSS	**1**	1	1	1	1	1	1
Testy	ATE_COV		**1**	**2**	2	2	**3**	3
	ATE_DPT			**1**	1	**3**	3	**4**
	ATE_FUN		**1**	1	1	1	**2**	2
	ATE_IND	**1**	**2**	2	2	2	2	**3**
Szacowanie podatności	AVA_VAN	**1**	**2**	2	**3**	**4**	**5**	5

Uwaga: pogrubiona cyfra oznacza pierwsze wystąpienie w tabeli tego elementu uzasadnienia zaufania.

2.2. Publikacje specjalne NIST serii 800

NIST jest organizacją opracowującą standardy i zalecenia techniczne dla administracji rządowej USA. Szczególnie cenne dla osób zajmujących się ochroną informacji są publikacje specjalne (SP – *Special Publication*)[15]. Krótka, przykładowa lista tych publikacji jest następująca:

1. SP 800-12 (DRAFT) Rev. 1: *An Introduction to Information Security*. Jan. 2017.
2. SP-800-39: *Managing Risk from Information Systems. An Organizational Perspective*.
3. SP-800-50: *Building an Information Technology Security Awareness and Training Program*.
4. SP-800-53 Rev.4: *Recommended Security Controls for Federal Information System*. April 2013.
5. SP-800-53A: *Guide for Assessing the Security Controls in Federal Information Systems. Building Effective Security Assessment Plans*.
6. SP-800-60: *Guide for Mapping Types of Information and Information Systems to Security Categories*. Vol. I and II.
7. SP-800-61*: Computer Security Incident Handling Guide*.
8. SP-800-64: *Security Considerations in the Information System Development Life Cycle*.
9. SP-800-82: *Guide to Industrial Control Systems (ICS) Security*.
10. SP-800-86: Guide to Computer and Network Data Analysis: *Applying Forensic Techniques to Incident Response*.
11. SP-800-92: *Guide to Computer Security Log Management*.
12. SP-800-95: *Guide to Secure Web Services*.
13. SP-800-115: *Technical Guide to Information Security Testing*.

Osoby budujące systemy zabezpieczeń powinny przede wszystkim zapoznać się z zaleceniami zawartymi w **SP 800-53**. Natomiast osobom, które chcą sobie wyrobić pogląd na zakres przedsięwzięć związanych z zapewnianiem szeroko rozumianego bezpieczeństwa teleinformatycznego (i jednocześnie zakresem dostępnych publikacji NIST), a nie mają czasu na studiowanie wszystkich dokumentów serii SP-800, poleca się publikację **SP 800-12**. Na jej 87 stronach zawarty jest przegląd takich przedsięwzięć wraz z odsyłaczami do innych publikacji tej serii, w których poszczególne zagadnienia są szczegółowo opisane.

[15] Dostępne w formacie .pdf pod adresem *http://csrc.nist.gov/publications/PubsSPs.html* (dostęp marzec 2017).

W odróżnieniu od ogólnych norm ISO, standardy NIST są bardziej „techniczne" i szczegółowe. Pomimo ich przeznaczenia dla administracji federalnej USA, ich zalecenia można z powodzeniem stosować także w innych krajach. Szczególną uwagę należy zachować tylko przy odwołaniach w zaleceniach do konkretnych przepisów prawa USA lub systemu klasyfikacji informacji.

Przykład 1.

Zbiór zaleceń zawartych w publikacjach NIST zawiera m.in. schemat konstrukcji „bezpiecznych" systemów i sieci teleinformatycznych. Na zbiór ten składają się standardy FIPS (*Federal Information Processing Standards*) Pub. 199 [15] i FIPS Pub. 200 [16] oraz SP 800-53. Ten zestaw standardów implikuje:

a) Podejście „zasobowe" do wyznaczania zestawu zabezpieczeń. Zasobem w rozumieniu ww. standardów jest zasób informacyjny.

b) Ocenę wymaganej siły ochrony (zabezpieczeń) dla każdego z kryteriów jakości (tajność, integralność, dostępność) z osobna, dla każdego z zasobów wchodzących w skład systemu (tele)informatycznego, tj. przetwarzanych w systemie.

c) Stosowanie ocen opisowych **z**e zbioru trójelementowego {LOW, MODERATE, HIGH} i formuły składania ocen $\max\{x_{1,\ldots,}\, x_i\}$.

d) Ocenę wymaganej siły ochrony, na podstawie predefiniowanych tabel konstruowanych na podstawie spodziewanych skutków (ang. *impact*) realizacji zagrożeń, poprzez wskazanie jednej z ocen ze zbioru {LOW, MODERATE, HIGH}.

e) Posługiwanie się predefiniowanymi (zawartymi w SP 800-53) bazowymi zabezpieczeniami odpowiadającymi sile ochrony LOW, MODERATE, HIGH.

f) Prostą regułę konstrukcyjną systemu ochrony: dobór zabezpieczeń w zależności od wyznaczonej wymaganej siły ochrony systemu (tele)informatycznego, tj. LOW, MODERATE, HIGH z odpowiedniego, predefiniowanego zbioru bazowego zabezpieczeń, tj. LOW, MODERATE, HIGH.

g) Dopasowanie zbioru zabezpieczeń do realiów eksploatacyjnych na podstawie obserwacji (monitorowania) działania i/lub analizy ryzyka[16].

* * * *

[16] W ww. publikacjach analiza ryzyka jest w zasadzie „niekoniecznym" dodatkiem. Poza tym istnieją pewne niekonsekwencje w użyciu tego terminu: raz analiza ryzyka jest rozumiana potocznie, innym razem formalnie, w rozumieniu działań wynikających z zapisów normy SP 800-30.

2.3. CIS Critical Security Controls

W 2008 roku, administracja rządu USA (w tym m.in. National Security Agency oraz SANS Institute) w porozumieniu z członkami organizacji biznesowych opracowała zbiór zaleceń o nazwie *Consensus Audit Gudelines* (CAG). Zalecenia te zostały udostępnione publicznie przez instytut SANS w 2009 roku pod adresem *www.sans.org*.

Przedstawiony w dokumencie CAG zbiór 20 zalecanych przedsięwzięć z zakresu ochrony przed działaniami intruzów (ang. Critical Controls, dalej w skrócie CCO) został uznany przez autorów opracowania jako **minimalny, ale łatwy do szybkiego wdrożenia, standard zabezpieczenia systemów i sieci komputerowych przed cyberatakami**. Dalej jest przedstawiona lista (wraz z tłumaczeniami) wszystkich punktów Critical Control dokumentu CAG v.6.1[17] Liczby w nawiasach oznaczają liczbę zalecanych przedsięwzięć w ramach każdego z punktów[18].

1. *Inventory of Authorized and Unauthorized Devices* (6) – inwentaryzacja autoryzowanego i nieautoryzowanego sprzętu.
2. *Inventory of Authorized and Unauthorized Software* (4) – inwentaryzacja autoryzowanego i nieautoryzowanego oprogramowania.
3. *Secure Configurations for Hardware and Software* (7) – utwardzająca konfiguracja sprzętu i oprogramowania na laptopach, stacjach roboczych i serwerach.
4. *Continuous Vulnerability Assessment and Remediation* (8) – ciągłe monitorowanie podatności i ich minimalizowanie.
5. *Controlled Use of Administrative Privileges* (9) – nadzór nad kontami administratorów i używaniem przywilejów administracyjnych.
6. *Maintenance, Monitoring, and Analysis of Audit Logs* (6) – utrzymanie, monitorowanie i analiza dzienników bezpieczeństwa.
7. *Email and Web Browser Protections* (8) – ochrona poczty elektronicznej i przeglądarek.
8. *Malware Defenses* (6) – ochrona przed programami i kodami złośliwymi.
9. *Limitation and Control of Network Ports* (6) – ograniczenie i kontrola portów, protokołów i usług sieciowych.
10. *Data Recovery Capability* (4) – zapewnianie zdolności do odzyskiwania danych.

[17] Punkty 1-10 dotyczą systemu, punkty 11-13 sieci a punkty 14-20 aplikacji.

[18] W sumie daje to 149 punktów sprawdzeń do audytu zgodności.

11. *Secure Configurations for Network Devices* (7) – bezpieczna konfiguracja urządzeń sieciowych.
12. *Boundary Defense* (10) – stosowanie ochrony brzegowej.
13. *Data Protection* (9) – ochrona danych.
14. *Controlled Access Based on the Need to Know* (7) – kontrola dostępu na podstawie wiedzy koniecznej.
15. *Wireless Access Control* (9) – nadzór nad dostępem bezprzewodowym.
16. *Account Monitoring and Control* (14) – monitorowanie i kontrola kont użytkowników.
17. *Security Skills Assessment and Appropriate Training to Fill Gaps* (5) – ocena umiejętności personelu w zakresie bezpieczeństwa i odpowiednie szkolenia w celu eliminacji braków.
18. *Application Software Security* (9) – zapewnianie bezpieczeństwa aplikacji.
19. *Incident Response and Management* (7) – reagowanie na incydenty i zarządzanie incydentami.
20. *Penetration Tests and Red Team Exercises* (8) – wykonywanie testów penetracyjnych i ćwiczeń zespołów typu Red Team.

CCO 1-5 składają się na tzw. „Pierwszą piątkę" (ang. *„First Five"*), która powinna zostać zaimplementowana w pierwszej kolejności, ponieważ w sumie stanowi podstawową ochronę przed działaniami intruzów. Należą do niej:

1. Przygotowanie listy dopuszczonego do użytku w organizacji oprogramowania, jej opublikowanie i nadzór nad przestrzeganiem zasad stosowania.
2. Utwardzająca konfiguracja sprzętu i oprogramowania na laptopach, stacjach roboczych i serwerach.
3. Instalacja (maksymalnie w ciągu 48 godzin) łat bezpieczeństwa oprogramowania.
4. Instalacja (maksymalnie w ciągu 48 godzin) łat bezpieczeństwa systemu.
5. Zapewnienie, że przywileje poziomu administratora systemu nie są aktywne podczas surfowania w Internecie lub korzystania z poczty elektronicznej.

Zaleca się dodatkowo ciągłe monitorowanie podatności i ich minimalizowanie (CCO4) oraz kontrole efektywności ww. przedsięwzięć.

Każde zalecenie, traktowane także z innej perspektywy jak tzw. *punkt kontrolny*, zawiera wszystkie lub część wymienionych dalej elementów. Każdy opisuje pewne zagadnienia zabezpieczenia systemu w zakresie danego punktu kontrolnego lub wdrażania w organizacji zaleceń wskazanych w tym punkcie:

1. *How do Attackers Exploit the Absence of this Control?* – możliwy sposób wykorzystania przez intruza niezabezpieczonej podatności opisanej w danym punkcie CAG.
2. *How to Implement, Automate, and Measure the Effectiveness of this Control?* – zalecenia odnośnie minimalizowania danej podatności.
3. *Associated NIST Special Publication 800-53 Revision 3, Priority 1 Controls* – powiązania z dokumentami NIST.
4. *Associated NSA Manageable Network Plan Milestones and Network Security Tasks* – powiązania z dokumentami NSA (*National Security Agency* – Narodowa Agencja Bezpieczeństwa USA).
5. *Procedures and Tools to Implement and Automate this Control* – opis możliwości wspomagania procesu zabezpieczania za pomocą narzędzi i przedsięwzięć organizacyjnych.
6. *Control xx Metric* – wymagania, jakie musi spełniać system, aby wypełniał założenia zawarte w danym punkcie.
7. *Control xx Test* – propozycje sprawdzeń jakie muszą być przeprowadzone, aby ocenić implementację danego punktu CAG w praktyce biznesowej organizacji.
8. *Control xx Sensors, Measurements and Scoring* – propozycje sposobu realizacji i oceny sprawdzeń opisanych w punkcie Control xx Test.

Najnowsza wersja CAG[19] to wersja 6.1 wydana w 2016 roku. Od wersji 6.0 zmieniła się nazwa dokumentu/projektu na *The CIS Critical Security Controls for Effective Cyber Defense*. Ma to związek m.in. z połączeniem *Center for Internet Security* z *The Council on Cybersecurity* czyli przekształceniami w grupie konsorcjantów ówczesnego projektu CAG. Udostępnianie kolejnych wersji artefaktów projektu (patrz dalej) odbywa się poprzez stronę *www.cisecurity.org*.

Na *The CIS Critical Security Controls for Effective Cyber Defense* składa się trzynaście następujących komponentów (kwiecień 2017):

1. CIS Controls Version 6.1 (PDF)
2. CIS Community Attack Model
3. Privacy Implications Guide (PDF)
4. Executive Summary (PDF)
5. Practical Guidance for Implementing the Critical Security Controls (PDF)
6. CIS Controls Change Log (Excel Spreadsheet)
7. CIS Controls Version 6.0 (PDF)

[19] W czasie przygotowywania niniejszego opracowania, tj. początek 2017 roku.

8. CIS Controls Version 6.1 (Excel Spreadsheet)
9. CIS Controls Version 6.0 (Excel Spreadsheet)
10. CIS Controls Measurement Companion Guide (PDF)
11. CIS Controls internet of Things Companion Guide (pdf)
12. CIS Controls Mobile Security Companion (pdf)
13. CIS Controls Privacy Companion (pdf)

Koncepcja CAG/CIS jest zbliżona do metodyki proponowanej przez NIST (patrz przykład 1).

3. Standardy i normy i wspierające zarządzanie bezpieczeństwem informacji

W tym rozdziale są przedstawione:

- Standard COBIT opracowany przez organizację ISACA.
- Zestaw norm ISO/IEC 270xy dotyczących Systemu Zarządzania Bezpieczeństwem Informacji[20].

3.1. COBIT™ – dobre praktyki w zakresie ładu informatycznego

Jednym z uznanych na całym świecie opracowań związanych m.in. z oceną i zapewnianiem bezpieczeństwa informatycznego jest zbiór dobrych praktyk (ang. *framework*) COBIT™, opracowany i rozwijany w ramach ISACA[21]. Działania ISACA koncentrują się na zagadnieniach audytu

[20] Przegląd norm serii ISO/IEC 270xy jest na stronie: *http://www.iso27001security.com/html/27799.html* (dostęp 07.04.2017).

[21] Stowarzyszenie znane wcześniej jako *Information Systems Audit and Control Association* (Stowarzyszenie ds. audytu i kontroli systemów informatycznych), obecnie używa jedynie akronimu ISACA, by zaznaczyć, że służy szerokiemu gronu osób zawodowo zajmujących się ogólnie pojętym nadzorem IT:
(…) *Obecnie stowarzyszenie ISACA liczy ponad 115 000 członków i sympatyków, których cechuje duża różnorodność. Mieszkają i pracują w ponad 180 krajach i zajmują wiele różnych stanowisk związanych z IT – są między innymi audytorami SI, konsultantami, wykładowcami, specjalistami ds. bezpieczeństwa SI, osobami nadzorującymi tworzenie i przestrzeganie przepisów prawa, szefami działów informatyki i audytorami wewnętrznymi.* (…). *Członkowie Stowarzyszenia pracują w praktycznie wszystkich gałęziach gospodarki, wliczając w to finanse i bankowość, księgowość, agencje rządowe i sektor państwowy, przedsiębiorstwa użyteczności publicznej oraz firmy produkcyjne*.

i bezpieczeństwa systemów informacyjnych oraz tzw. ładu informatycznego – w ramach tej problematyki ISACA opracowuje metodyki, prowadzi szkolenia i certyfikacje. Najbardziej znanymi przedsięwzięciami ISACA są:

1) program certyfikacji osób:
   - Certified in the Governance of Enterprise IT® (CGEIT®);
   - Certified Information Systems Auditor® (CISA®);
   - Certified Information Security Manager® (CISM®);
   - Certified in Risk and Information Systems Control™ (CRISC™).
2) opracowanie i opublikowanie w 1996 roku pierwszej wersji metodyki COBIT™ *(Control Objectives for Information and Related Technology)*[22].

Wraz z rozwojem informatycznego wsparcia zarządzania organizacją, produkcją, świadczeniem usług itd. stwierdzono, że „informatyki" nie można postrzegać jako elementu odrębnego (chociaż współdziałającego) od „biznesu" – obie domeny działalności organizacji powinny być ściśle zintegrowane. Takiemu podejściu sprzyjają też tworzone aktualnie przepisy prawa i wdrażane regulacje. W szczególności, wymóg zintegrowanego podejścia dotyczy nadzoru i zarządzania technologiami informatycznymi w celu uzyskania optymalnej wartości z IT poprzez zachowanie równowagi pomiędzy osiąganiem korzyści a optymalizacją ryzyka oraz wykorzystaniem zasobów. Metodycznym wsparciem takich zintegrowanych działań w tym zakresie jest właśnie COBIT. Zawarte w COBIT opisy dobrych praktyk stanowią dla audytora kryteria oceny stanu informatyki (tzw. *wzorzec audytowy*) w ramach wyznaczonego celu i zakresu audytu IT[23].

Obecnie, w roku 2017, dostępna jest wersja 5.0 COBIT której podstawą jest *„Metodyka biznesowa w zakresie nadzoru nad technologiami informatycznymi w przedsiębiorstwie i zarządzania nimi"* [17]. Rodzina produktów COBIT 5 obejmuje następujące elementy:

1. COBIT 5 (metodyka).
2. Przewodniki do czynników umożliwiających (ang. *enablers*) COBIT 5,

Ze strony: *http://www.isaca.org/About-ISACA/History/Polski/Pages/Default.aspx* (dostęp 29.04.2017).

[22] Pierwsza wersja ograniczała się do audytu informatycznego. Obecna, piąta wersja przez członków ISACA nazywana jest *schematem ładu informatycznego*, który umożliwia kierownictwu organizacji opracowanie dobrych praktyk nadzoru i kontroli IT (obejmuje: audit, control, management, IT Governance, Governance of Enterprise IT).

[23] Należy mieć na uwadze, że dobre praktyki zawarte w COBIT nie są metodyką audytu IT – audyt IT został opisany w standardach, wytycznych oraz narzędziach i technikach audytu IT – dokumentach opracowanych przez ISACA.

w których szczegółowo opisano czynniki związane z nadzorem i zarządzaniem. Należą do nich:

- COBIT 5: procesy umożliwiające
- COBIT 5: informacje umożliwiające
- pozostałe przewodniki dotyczące czynników umożliwiających.

3. Specjalistyczne przewodniki COBIT 5, w tym:
   - COBIT 5: Wdrożenie
   - COBIT 5: Bezpieczeństwo informacji
   - COBIT 5: Audyt
   - COBIT 5: Ryzyko
   - inne specjalistyczne przewodniki.
4. Środowisko współpracy sieciowej, które będzie wspierać korzystanie z metodyki COBIT 5.

Metodyka COBIT 5 jest oparta na pięciu zasadach dotyczących nadzoru nad technologiami informatycznymi w organizacji i zarządzania nimi:

1. Spełnienie potrzeb interesariuszy.
2. Uwzględnienie wszystkich aspektów działania przedsiębiorstwa.
3. Stosowanie jednej zintegrowanej metodyki.
4. Wdrożenie podejścia całościowego.
5. Oddzielenie nadzoru od zarządzania.

W metodyce COBIT 5 wskazano także siedem tzw. *czynników umożliwiających*, które wspierają wdrożenie kompleksowego systemu nadzoru i zarządzania dla technologii informatycznych w organizacji[24]:

1. Zasady, polityki i metodyki.
2. Procesy.
3. Struktury organizacyjne.
4. Kultura, etyka i zachowanie.
5. Informacja.
6. Usługi, infrastruktura i aplikacje.
7. Ludzie, umiejętności i kompetencje.

Każdy z czynników umożliwiających dotyczy: interesariuszy, celów,

[24] „Czynnik umożliwiający" to pojęcie bardzo szerokie – obejmuje wszystko, co może ułatwić osiągnięcie celów organizacji. Czynniki umożliwiające (razem bądź pojedynczo), mają wpływ na to, czy coś zadziała – w tym przypadku nadzór nad technologiami informatycznymi (IT) w organizacji oraz zarządzanie nimi.

cyklu życia i dobrych praktyk. Te cztery wspólne (dla czynników umożliwiających) elementy w COBIT 5 są nazywane „wymiarami".

Już we wcześniejszych wersjach metodyki COBIT wprowadzono szereg organizacyjno-technicznych wzorców, klasyfikacji, wskaźników i kryteriów, które mogą być pomocne w przejrzystym i wymiernym ujęciu skomplikowanych związków pomiędzy zarządzaniem biznesem a wsparciem informatycznym, i tym samym przyczynić się do rzetelnej oceny stanu „ładu informatycznego". W najbardziej dojrzalej formie elementy te zostały zaprezentowane w wersji 4.1 COBIT [18]. W wersji tej są opisane:

- 4 domeny informatyczne[25]:
  - PO – Planowanie i Organizacja
  - AI – Nabywanie i Wdrażanie
  - DS – Dostarczanie i Obsługa
  - M – Monitorowanie i Ocena.
- 34 procesy IT[26].
- 31 ogólne cele kontrolne (w wersji 5.0 są to praktyki zarządcze).
- 214 szczegółowe cele kontrolne przypisane poszczególnym procesom.
- 7 kryteriów jakości przetwarzania informacji: *efektywność, wydajność, poufność, integralność, dostępność, zgodność, rzetelność*.
- 4 rodzaje zasobów: *aplikacje, informacje, infrastruktura, ludzie*.
- Mechanizmy kontrolne w aplikacji (AC), zdefiniowane jako zautomatyzowane mechanizmy kontrolne zakodowane w aplikacji biznesowej.
- Macierze odpowiedzialności (RCAI), zawierające wytyczne odnośnie ról i odpowiedzialności na poszczególnych stanowiskach, czyli kto będzie *odpowiedzialny* (R), *konsultowany* (C), *rozliczany* (A), *informowany* (I).
- Wskaźniki wyznaczone dla procesów IT, pokazujące jak te procesy spełniają cele biznesowe IT. Obejmują:
  - kluczowe wskaźniki *wydajności*
  - kluczowe wskaźniki *celu procesu*
  - kluczowe wskaźniki *celu IT*.

[25] W COBIT 5 wprowadzono nową domenę EDM: *Ocena, kierowanie i monitorowanie*. Zmieniono także nieco symbole domen: PO na APO (*dopasowanie, planowanie i organizacja*), AI na BAI (*budowanie, nabywanie i wdrażanie*), DS na DSS (*dostarczanie, obsługa i wsparcie*), M na MEA (*monitorowanie, ocena i oszacowanie*).

[26] W COBIT 5 wskazano 37 procesów w ww. pięciu domenach.

– Poziomy dojrzałości procesów (CMM): *brak* (0), *początkowy* (1), *powtarzalny* (2), *zdefiniowany* (3), *zarządzany* (4), *zoptymalizowany* (5).

Poszczególne wersje COBIT różnią się m.in. liczbą celów kontrolnych, zdefiniowanych dla każdego procesu, dla których osoba przeprowadzająca ocenę musi znaleźć uzasadnione potwierdzenie ich spełnienia (lub niespełnienia) w ramach ocenianej organizacji.

Przykład 2.[27]

Dla procesu DS12 „Zarządzanie urządzeniami" punkty kontrolne dotyczą:

– DS12.1: wybór miejsca i rozmieszczenia.
– DS12.2: fizyczne środki bezpieczeństwa.
– DS12.3: fizyczny dostęp.
– DS12.4: ochrona przed czynnikami środowiskowymi.
– DS12.5: zarządzanie infrastrukturą fizyczną.

* * * *

3.2. Zarządzanie bezpieczeństwem informacji – standard BS 7799 i normy serii ISO/IEC 2700x

Początek historii rozwoju tej grupy standardów to opublikowanie w połowie lat 90-tych XX wieku przez Brytyjski Instytut Standaryzacji (BSI – *British Standard Institute*) dwuczęściowego standardu:

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

Standardy BSI z zakresu zarządzania bezpieczeństwem informacji cieszą się dużym uznaniem na całym świecie, czego przejawem jest m.in. przyjęcie ich za podstawę szeregu norm z zakresu bezpieczeństwa teleinformatycznego i ochrony informacji wydawanych przez *International Organization for Standardization* (ISO) w serii oznaczonej jako ISO/IEC 270xx. Obecnie (początek roku 2017) dostępne są wydane przez Polski Komitet Normalizacyjny polskie wersje tych norm ISO z roku 2013 [6], [7].

Poszczególne wydania normy różnią się nie tylko zawartością merytoryczną wynikającą z dodania zabezpieczeń których nie było we wcześniejszych wydaniach normy, ale także układem, numeracją i nazwami obszarów. To powoduje, że narzędzia opracowane do wspomagania badania

[27] W pracy [5] podano specyfikację dla tego samego procesu, ale w wersji 4.1 COBIT.

zgodności stanu ochrony informacji w organizacji z wymaganiami np. ISO/IEC 27001:2005 wymagają zmian, jeżeli mają służyć do wspomagania badania zgodności z wymaganiami ISO/IEC 27001:2013.

Wspomniane zmiany w normach, w stosunku do wydań wcześniejszych, są spowodowane wprowadzeniem w 2012 roku przez ISO nowego standardu zarządzania (MSS – ang. *Management System Standard*), do którego muszą być doprowadzone wszystkie normy dotyczące zarządzania[28]. W jednym z załączników do dokumentu wymienionego w przypisie 31, oznaczonym „Annex SL: *Proposals for management system standards*", opisane są ramy ogólnego systemu zarządzania, które w praktyce powinny być rozwijane poprzez dodawanie wymagań specyficznych dla danej dyscypliny. Zgodnie z Aneksem SL, wszystkie normy ISO z zakresu zarządzania (jakością, ciągłością działania, bezpieczeństwem informacji itd.) muszą mieć następującą strukturę[29] (patrz też rys.4):

1. Scope
2. Normative references
3. Terms and definitions
4. Context of the organization
5. Leadership
6. Planning
7. Support
8. Operation
9. Performance evaluation
10. Improvement

Dla celów certyfikacyjnych najważniejsze obszary (*clauses*) to obszary 4-10. Dla obszarów 4,5,7,9,10 we wszystkich normach tekst jest w zasadzie identyczny. Różnice występują w obszarach 6 i 8, np.:

- obszary 6 i 8 normy ISO 9001 dotyczą: *Product/Service planning and realization*;
- obszary 6 i 8 normy ISO 14001 dotyczą: *Environmental management*;
- obszary 6 i 8 normy ISO 27001 dotyczą: *Risk management*.

[28] Zasady opracowywania takich dokumentów normatywnych przez ISO przedstawione są w dokumencie *ISO/IEC. Directives. Part 1. Consolidated ISO Supplement – Procedures specific to ISO. Fifth edition. 2014*.

[29] *https://advisera.com/27001academy/blog/2015/10/05/how-to-implement-integrated-management-systems/ ?utm_source=iso-27001-vs-iso-22301-matrix&utm_medium=downloaded-content&utm_content=lang-en&utm_campaign=free-blog-27001* (dostęp 18.05.2017)

3.2.1. Przegląd zawartości normy ISO/IEC 27002:2013

Ta 90-cio stronicowa norma zawiera specyfikację 14 obszarów bezpieczeństwa (w normie nazwanych *clauses*, odpowiadających tytułom rozdziałów głównych 5-18 – patrz rys.2) zawierających łącznie 35 głównych kategorii bezpieczeństwa (odpowiadających tytułom podrozdziałów rozdziałów 5-18) i 114 zabezpieczeń. Podanej w normie kolejności obszarów (wyrażonej ich numeracją) nie należy traktować jak listy priorytetowej – znaczenie poszczególnych obszarów będzie się zwykle różniło w zależności od stosującej normę organizacji.

Każda główna kategoria bezpieczeństwa (ang. *main security control category*) zawiera:

- cele zabezpieczeń, wskazujące co należy osiągnąć,
- wskazanie jednego lub więcej zabezpieczeń, które powinny zostać zastosowane dla osiągnięcia celów.

Każde z zawartych w normie 114 zabezpieczeń jest opisanych w następującej formie:

- nazwa zabezpieczenia i krótki opis,
- wskazówki do implementacji zabezpieczenia (ang. *implementation guidance*),
- informacje dodatkowe (ang. *other information*).

Contents
Page
Foreword
0 Introduction
1 Scope
2 Normative references
3 Terms and definitions
4 Structure of this standard
    4.1 Clauses
    4.2 Control categories
5 Information security policies
    5.1 Management direction for information security
6 Organization of information security
    6.1 Internal organization
    6.2 Mobile devices and teleworking
7 Human resource security
    7.1 Prior to employment
    7.2 During employment
    7.3 Termination and change of employment
8 Asset management
    8.1 Responsibility for assets
    8.2 Information classification
    8.3 Media handling
9 Access control
    9.1 Business requirements of access control
    9.2 User access management
    9.3 User responsibilities
    9.4 System and application access control
10 Cryptography
    10.1 Cryptographic controls
11 Physical and environmental security
    11.1 Secure areas
    11.2 Equipment
12 Operations security
    12.1 Operational procedures and responsibilities
    12.2 Protection from malware
    12.3 Backup
    12.4 Logging and monitoring
    12.5 Control of operational software
    12.6 Technical vulnerability management
    12.7 Information systems audit considerations
13 Communications security
    13.1 Network security management
    13.2 Information transfer
14 System acquisition, development and maintenance
    14.1 Security requirements of information systems
    14.2 Security in development and support processes
    14.3 Test data

15 Supplier relationships
15.1 Information security in supplier relationships
15.2 Supplier service delivery management
16 Information security incident management
16.1 Management of information security incidents and improvements
17 Information security aspects of business continuity management
17.1 Information security continuity
17.2 Redundancies
18 Compliance
18.1 Compliance with legal and contractual requirements
18.2 Information security reviews
Bibliography

Rys. 2. Struktura normy ISO/IEC 27002:2013

3.2.2. Przegląd zawartości normy ISO/IEC 27001:2013

Tytułowa norma znajduje zastosowanie we wszystkich rodzajach organizacji niezależnie od typu, rozmiaru i natury prowadzonej działalności biznesowej. Określono w niej wymagania dotyczące ustanowienia, wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymywania i doskonalenia udokumentowanego SZBI. Obligatoryjną podstawą tych działań jest zidentyfikowane ryzyko biznesowe. Zaleca się, aby wprowadzenie SZBI było dla organizacji decyzją strategiczną. Norma ISO/IEC 27001 może być wykorzystywana do szacowania zgodności przez zainteresowane strony wewnętrzne i zewnętrzne.

Przedstawiony w normie model SZBI został zaprojektowany tak, aby zapewnić adekwatne i proporcjonalne zabezpieczenia, które odpowiednio chronią aktywa informacyjne co w efekcie ma pozwolić uzyskać zaufanie zainteresowanych stron co do deklarowanej skuteczności ochrony zasobów informacyjnych. Do wydania z roku 2005 (polskiego – 2007) w normie stosowano do wszystkich procesów SZBI model „Planuj – Wykonuj – Sprawdzaj – Działaj" (PDCA, nazywany też „cyklem Deminga" – por. rys.3)[30]:

1. **Planuj** (ustanowienie SZBI)

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

[30] W najnowszych wydaniach normy podejście to nie jest już tak mocno akcentowane.

2. **Wykonuj** (wdrożenie i eksploatacja SZBI)

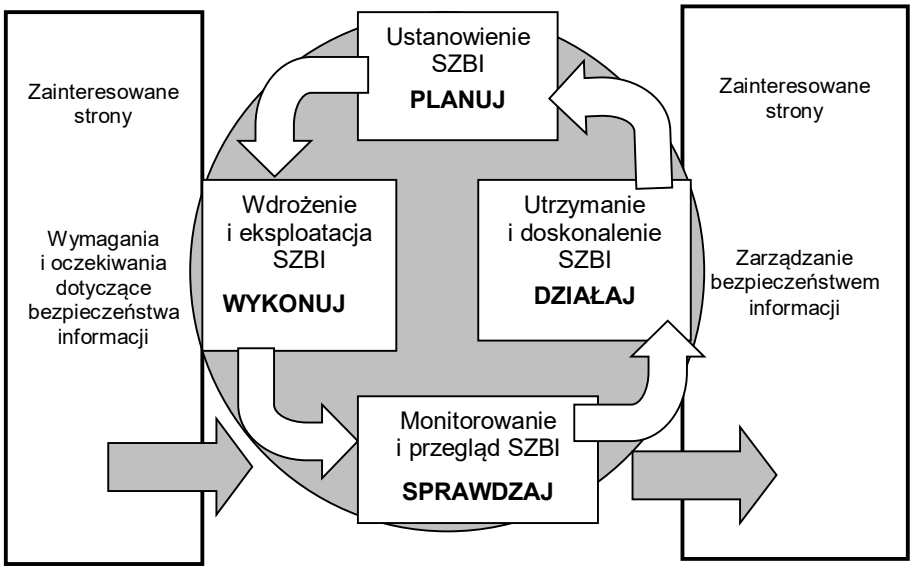
   Wdrożenie i eksploatacja SZBI – stosowanie polityki, zabezpieczeń, procesów i procedur.

3. **Sprawdzaj** (monitorowanie i przegląd SZBI)

   Szacowanie i tam, gdzie ma zastosowanie, pomiar wydajności procesów w odniesieniu do polityki bezpieczeństwa, celów i doświadczenia praktycznego oraz dostarczanie kierownictwu raportów do przeglądu.

4. **Działaj** (utrzymanie i doskonalenie SZBI)

   Podejmowanie działań korygujących i zapobiegawczych w celu zapewnienia ciągłego doskonalenia SZBI na podstawie wyników wewnętrznego audytu SZBI i przeglądu realizowanego przez kierownictwo (lub innych istotnych informacji).



Rys. 3. Model PDCA działań w ramach SZBI

Aktualne wydanie normy, tj. ISO/IEC 27001:2013, to 30 stron o zawartości przedstawionej na rysunku 4. Norma „jako taka" zajmuje 9 stron. Pozostałe strony to normatywny załącznik A, stanowiący podstawę konstrukcji deklaracji stosowania, który zawiera przedstawione w zwartej formie zalecenia z obszarów 5-18 normy ISO/IEC 27002:2013. Tytuły rozdziałów 4-10 normy to w zasadzie nazwy czynności (dokładniej – zbiorów czynności) które należy wykonać w celu zbudowania SZBI. Czynności te to:

1. **Ustal kontekst** działania organizacji, na co składa się zrozumienie uwarunkowań działania organizacji (w tym zrozumienie potrzeb i oczekiwań

zainteresowanych stron) oraz ustalenie zakresu SZBI i wyrażenie woli jego wdrożenia.

2. **Kieruj** (zorganizuj przywództwo, ang. *leadership*), na co składa się demonstrowanie przez naczelne kierownictwo organizacji zaangażowania we wdrożenie i utrzymywanie SZBI, w tym w doprowadzenie do ustanowienia i wdrożenia polityki bezpieczeństwa oraz określenia na jej podstawie ról i odpowiedzialności w zakresie bezpieczeństwa.
3. **Zaplanuj** działania (na podstawie wyników analizy ryzyka) mające doprowadzić do osiągnięcia założonych celów bezpieczeństwa[31].
4. **Wspieraj** wykonywane działania zapewniając odpowiednie zasoby, określając wymagane kompetencje personelu, budując świadomość (ang. *awareness*) celów i działań, organizując właściwą komunikację z personelem i zainteresowanymi stronami oraz wykonując i utrzymując wymaganą dokumentację SZBI.
5. **Zorganizuj pracę operacyjną** w zakresie SZBI (głównie w zakresie nadzoru nad kluczowymi wskaźnikami ryzyka i właściwym komunikowaniem stanu bezpieczeństwa organizacji).
6. **Oceniaj** jakość wykonywanych działań ustalając i nadzorując odpowiednie wskaźniki, monitorując wybrane procesy i zabezpieczenia, organizując audyty wewnętrzne oraz przeglądy zarządcze.
7. **Udoskonalaj** ciągle działanie SZBI.

Do podstawowych pojęć, używanych w tej normie[32], należą:

– **system zarządzania bezpieczeństwem informacji SZBI**:

ta część całościowego systemu zarządzania, oparta na podejściu wynikającym z ryzyka biznesowego, odnosząca się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji. SZBI obejmuje strukturę organizacyjną, polityki, planowane działania, zakresy odpowiedzialności, zasady, procedury, procesy i zasoby.

– **deklaracja stosowania** (ang. *statement of applicability*):

dokument, w którym opisano i uzasadniono stosowanie w SZBI organizacji zabezpieczeń wymienionych w załączniku A normy (wskazanych na podstawie wyników analizy ryzyka) oraz uzasadniono niezastosowanie któregoś z tych zabezpieczeń.

[31] W ramach tego przedsięwzięcia powinna zostać wytworzona *deklaracja stosowania*.

[32] W zakresie terminologii, w tej normie są odwołania do normy terminologicznej ISO/IEC 27000 [8].

Foreword
0 Introduction
1 Scope
2 Normative references
3 Terms and definitions,
4 Context of the organization
  4.1 Understanding the organization and its context
  4.2 Understanding the needs and expectations of interested parties
  4.3 Determining the scope of the information security management system
  4.4 Information security management system
5 Leadership
  5.1 Leadership and commitment
  5.2 Policy
  5.3 Organizational roles, responsibilities and authorities
6 Planning
  6.1 Actions to address risks and opportunities
  6.2 Information security objectives and planning to achieve them
7 Support
  7.1 Resources
  7.2 Competence
  7.3 Awareness
  7.4 Communication
  7.5 Documented information
8 Operation
  8.1 Operational planning and control
  8.2 Information security risk assessment
  8.3 Information security risk treatment
9 Performance evaluation
  9.1 Monitoring, measurement, analysis and evaluation
  9.2 Internal audit
  9.3 Management review
10 Improvement
  10.1 Nonconformity and corrective action
  10.2 Continual improvement
Annex A (normative) Reference control objectives and controls
Bibliography

Rys. 4. Struktura normy ISO/IEC 27001:2013

Ze względu na znaczne upowszechnienie normy z roku 2005 (polskie wydanie 2007) warto wskazać za [21] istotne różnice pomiędzy zapisami z wydań 2005 i 2013:

- wprowadzenie pojęcia kontekstu organizacji,
- wprowadzenie *zainteresowanych stron* w miejsce *interesariuszy*,
- doprecyzowanie wymagań które musi spełnić kierownictwo organizacji,

- rozszerzenie wymagań w zakresie celów zapewniania bezpieczeństwa informacji[33],
- położenie większego nacisku na skuteczność planów postępowania z czynnikami ryzyka,
- rozszerzenie postępowania z czynnikami ryzyka o szanse,
- rozszerzenie zakresu oceny systemu o czynniki zewnętrzne,
- rozszerzenie zawartości załącznika A z 11 do 14 obszarów bezpieczeństwa,
- wprowadzenie wymagań dotyczących komunikowania (stanu ochrony zasobów informacyjnych),
- uelastycznienie podejścia do dokumentacji (zrezygnowano z wyspecyfikowania w normie wymaganej dokumentacji oraz z pojęcia „zapisów"),
- uproszczenie podejścia do szacowania ryzyka.

Są też zmiany, których wpływ na funkcjonowanie SZBI jest ograniczony:

- możliwość zastąpienia cyklu PDCA inną koncepcją doskonalenia,
- ściślejsze powiązanie zabezpieczeń z postępowaniem z czynnikami ryzyka,
- wprowadzenie pojęcia *właściciela czynnika ryzyka* zastępującego *właściciela aktywów*.

Podsumowanie

Opisywane w tym artykule standardy i normy podlegają dość dynamicznym zmianom, co można sprawdzić sięgając chociażby do wcześniejszych artykułów o tej tematyce zamieszczonych w artykułach [3], [4], [5]. Dotyczy to przede wszystkim opracowań Brytyjskiego Instytutu Standaryzacji i odpowiadających im norm ISO (głównie linii ISO/IEC 270xx). Są one zwykle co 2-3 lata aktualizowane; odpowiadające im normy ISO są publikowane z ok. półrocznym opóźnieniem. Standardy NIST także podlegają dość częstym zmianom – rekomenduje się okresowe sprawdzanie ich aktualności na stronie *http://csrc.nist.gov/publications/PubsSPs.html*. Common Criteria i COBIT, w porównaniu z ww., są bardziej stabilne.

Warto także zwrócić uwagę na sposób udostępniania standardów. Common Criteria[34], COBIT (częściowo), CAG/CIS i standardy NIST są

[33] Zwiększono nacisk na realne funkcjonowanie, a nie tylko dokumentowanie SZBI. Dlatego m.in. wprowadzono wymagania opracowania celów bezpieczeństwa informacji i planowania ich osiągania.

[34] Dostępne pod http://www.commoncriteriaportal.org.

dostępne w Internecie, za darmo. To pozytywnie odróżnia je od norm wydawanych przez takie organizacje jak ISO czy Polski Komitet Normalizacyjny – ich normy trzeba kupić.

Literatura

1. BIAŁAS A. (red.), *Komputerowe wspomaganie procesu rozwoju produktów informatycznych o podwyższonych wymaganiach bezpieczeństwa*. Wydawnictwo Instytutu Technik Innowacyjnych EMAG, Katowice, 2012.
2. BIAŁAS A. (red.), *Zastosowanie wzorców projektowych w konstruowaniu zabezpieczeń informatycznych zgodnych ze standardem Common Criteria*. Wydawnictwo Instytutu Technik Innowacyjnych EMAG, Katowice, 2011.
3. LIDERMAN K., *Standardy w ocenie bezpieczeństwa teleinformatycznego*. Biuletyn IAiR. nr 17, 2002, s. 97-119.
4. LIDERMAN K., *Przegląd normy PN-I-07799-2:2005. Systemy zarządzania bezpieczeństwem informacji – Specyfikacja i wytyczne do stosowania*. Biuletyn IAiR. nr 22, 2005, s. 71-92.
5. LIDERMAN K., *Normy i standardy z zakresu bezpieczeństwa informacyjnego i teleinformatycznego*. Biuletyn IAiR. nr 26, 2009, s. 29-43.
6. *PN-ISO/IEC 27001:2014-12: Technika informatyczna –Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania*. PKN, Warszawa, 2014.
7. *PN-ISO/IEC 27002:2014-12: Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zabezpieczania informacji*. PKN, Warszawa, 2014.
8. *PN-ISO/IEC 27000:2014-11: Technika informatyczna –Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Przegląd i terminologia*. PKN, Warszawa, 2014.
9. *PN-ISO/IEC 15408-1:2002: Technika informatyczna - Techniki zabezpieczeń - Kryteria oceny zabezpieczeń informatycznych - Część 1: Wprowadzenie i model ogólny*. PKN, Warszawa, 2002.
10. *PN-ISO/IEC 15408-3:2002: Technika informatyczna - Techniki zabezpieczeń - Kryteria oceny zabezpieczeń informatycznych - Część 3: Wymagania uzasadnienia zaufania do zabezpieczeń*. PKN, Warszawa, 2002.
11. *PN-ISO/IEC 15408-1:2016-10: Information technology – Security techniques – Evaluation criteria for IT security – Introduction and general model (Common Criteria Part 1)*. PKN, Warszawa, 2016.

12. *PN-ISO/IEC 15408-2:2016-10: Information technology – Security techniques – Evaluation criteria for IT security – Security functional components (Common Criteria Part 2)*. PKN, Warszawa, 2016.
13. *PN-ISO/IEC 15408-3:2016-10: Information technology – Security techniques – Evaluation criteria for IT security – Security assurance components (Common Criteria Part 3)*. PKN, Warszawa, 2016.
14. *Common Methodology for Information Technology Security Evaluation. Evaluation methodology*. September 2012. Version 3.1. Revision 4, CCMB-2012-09-004. (https://www.commoncriteriaportal.org/files/ccfiles/CEMV3.1R4.pdf).
15. *Standards for Security Categorization of Federal Information and Information Systems*. (FIPS Pub. 199). National Institute of Standards and Technology, Gaithersburg, 2004.
16. *Minimum Security Requirements for Federal Information and Information Systems*. (FIPS Pub. 200). National Institute of Standards and Technology, Gaithersburg, 2006.
17. *COBIT®5: Metodyka biznesowa w zakresie nadzoru nad technologiami informatycznymi w przedsiębiorstwie i zarządzania nimi* (wersja polska). ISACA. 2012.
18. *COBIT 4.1: Metodyka. Cele kontrolne. Wytyczne zarządzania. Modele dojrzałości* (wersja polska). IT Governance Institute, Rolling Meadows, 2007.
19. *Information Technology Security Evaluation Criteria (ITSEC)*. Version 1.2. Department of Trade and Industry, London, 1991.
20. *Trusted Computer System Evaluation Criteria*. (CSC-STD-001-83). Department of Defense Standard. 1985.
21. https://wawak.pl/pl/content/zmiany-wprowadzone-w-normie-iso-270012013

A survey on selected information security norms and standards

Abstract: The paper provides an overview of selected security information and standards. The aim of the presentation is to provide a brief overview about standards currently recognized as leading in the field. The ideas contained in the described standards are rather considered than detailed descriptions of contents of a specific edition of standards. The content of the paper is a continuation of the works previously done which are listed in the literature.

KEYWORDS: Common Criteria (ISO/IEC 15408), COBIT, CAG/CIS, NIST SP 800-xxx, ISO/IEC 27001/27002

Praca wpłynęła do redakcji: 5.06.2017 r.

Niniejsza strona służy jedynie zachowaniu odstępu.