BIULETYN INSTYTUTU AUTOMATYKI I ROBOTYKI
NR 17, 2002

Standardy w ocenie bezpieczeństwa teleinformatycznego[1]

Krzysztof LIDERMAN

Zakład Systemów Komputerowych, Instytut Automatyki i Robotyki WAT,
ul. Kaliskiego 2, 00-908 Warszawa

STRESZCZENIE: W artykule przedstawiono podstawowe zagadnienia związane ze standaryzacją procesu oceny bezpieczeństwa teleinformatycznego. Krótko scharakteryzowano standardy: amerykański (TCSEC), europejski (ITSEC), brytyjski (BS7799), organizacji ISACA (COBIT) oraz ponadnarodowy standard *Common Criteria*, wydany przez organizację ISO jako norma ISO/IEC 15408. W końcowej części referatu zamieszczono kilka uwag na temat procesu audytu bezpieczeństwa teleinformatycznego.

1. Ocena poziomu bezpieczeństwa teleinformatycznego

Zarówno użytkownicy systemów teleinformatycznych jak i kierownictwo instytucji eksploatujących te systemy (szczególnie po zainwestowaniu dużych sum w bezpieczeństwo teleinformatyczne, które przecież nie przynosi natychmiastowych, wymiernych zysków), są zainteresowani odpowiedzią na pytanie „*czy eksploatowany system teleinformatyczny jest bezpieczny"*? (w sensie: czy *informacja* w nim przetwarzana jest dobrze chroniona). Żeby móc rzetelnie odpowiedzieć na takie pytanie, należy najpierw przeprowadzić proces oceny bezpieczeństwa teleinformatycznego, a to z kolei wymaga zdefiniowania pojęcia „*bezpieczeństwa teleinformatyczneg*o".

Ochrona informacji jest zagadnieniem szerokim i generalnie jest związana z tzw. *bezpieczeństwem informacyjnym*, obejmującym wszystkie formy (także werbalne) wymiany informacji. Zawężeniem zakresu bezpieczeństwa

1 Niniejszy artykuł jest nieco zmienioną wersją materiału uzupełniającego (white paper) do wykładu, przygotowanego na konferencje WinSecurity 2002 w Szczyrku.

informacyjnego jest tzw. *bezpieczeństwo teleinformacyjne*, obejmujące wszystkie formy wymiany informacji za pomocą technicznych środków łączności (np. poprzez telefony stacjonarne i komórkowe, radiostacje, sieci komputerowe, itd.). Kolejnym zawężeniem zakresu bezpieczeństwa informacyjnego jest *bezpieczeństwo teleinformatyczne*[2]:

> *Termin* ***bezpieczeństwo teleinformatyczne*** *oznacza* ***ochronę informacji*** *przetwarzanej, przechowywanej i przesyłanej za pomocą systemów teleinformatycznych, przed niepożądanym (przypadkowym lub świadomym) ujawnieniem, modyfikacją, zniszczeniem lub uniemożliwieniem jej przetwarzania.*

Podstawowe **atrybuty informacji związane z jej bezpieczeństwem** to:

- **tajność** – termin ten oznacza stopień ochrony przed nieuprawnionym dostępem, jakiej ma ona podlegać. Stopień ten jest uzgadniany przez osoby lub organizacje dostarczające i otrzymujące taką informację;
- **integralność** – termin ten oznacza, że dane i informacje są poprawne, nienaruszone i nie zostały poddane manipulacji;
- **dostępność** – termin ten charakteryzuje system informatyczny i oznacza dostępność danych, procesów i aplikacji zgodnie z wymaganiami użytkownika.

W literaturze przedmiotu można spotkać jeszcze inne atrybuty wymieniane jako związane z bezpieczeństwem informacji, np. rozliczalność (ang. *accountability*), w sensie identyfikacji użytkowników i wykorzystywanych przez nich usług.

Z przedstawionych dotąd uwag o informacji i bezpieczeństwie wynika jeden podstawowy wniosek (który znajduje wsparcie w omawianych dalej standardach bezpieczeństwa): system bezpieczeństwa powinien być systemem **kompleksowym**, wykorzystującym w spójny sposób zabezpieczenia:

- organizacyjne i kadrowe,
- fizyczne i techniczne,
- sprzętowo-programowe,

pozwalającym na wykrycie przełamania zabezpieczeń (oraz prób takich działań) oraz skuteczną ochronę pomimo przełamania części zabezpieczeń.

[2] W najbliższym czasie będzie można obserwować coraz większe zacieranie różnic pomiędzy *bezpieczeństwem teleinformacyjnym* a *teleinformatycznym* – w chwili obecnej telefony komórkowe pełnią już funkcje terminali umożliwiających dostęp do sieci komputerowej oraz rozwijane są metody łączenia elementów sieci komputerowej za pomocą łączności radiowej (np. technologia Bluetooth).

Wiedząc co kryje się pod pojęciem bezpieczeństwa teleinformatycznego, można przyjrzeć się bliżej procesowi oceny poziomu bezpieczeństwa teleinformatycznego:

> ***Ocenianiem bezpieczeństwa informacji w systemach teleinformatycznych*** *nazywa się proces określenia wartości miary gwarantowanej odporności systemu teleinformatycznego na czynniki mogące spowodować utratę tajności, integralności i/lub dostępności przetwarzanej w nim informacji.*

Ocenianie bezpieczeństwa informacji w systemach teleinformatycznych powinno być realizowane na podstawie:

- konkretnej polityki bezpieczeństwa teleinformatycznego,
- spójnego opisu wymaganych funkcji zabezpieczenia,
- docelowego, pożądanego poziomu miary gwarantowanej odporności.

Wynikiem oceniania jest **raport** sporządzany przez osobę (osoby) oceniającą, opisujący procedury badawcze i testujące zastosowane podczas analizy właściwości zabezpieczenia systemu teleinformatycznego, **wraz z opisem i wynikami testów** zastosowanych w celu potwierdzenia lub zaprzeczenia istnienia określonych wad (podatności) systemu.

Miary gwarantowanej odporności są zwykle określane przez odpowiednie standardy, np: w *Common Criteria* będą to tzw. *Evaluation Assurance Level* (EAL), a w TCSEC klasy bezpieczeństwa D, C, B, A.

Zaprezentowany w zarysie proces oceny może być przeprowadzony własnymi siłami firmy, o ile posiada ona odpowiednio kompetentny w tym zakresie pion teleinformatyki i komórkę bezpieczeństwa (i wtedy mówi się o ocenie poziomu bezpieczeństwa teleinformatycznego według np. zaleceń standardu BS 7799) lub ocena może być zlecona zewnętrznemu, niezależnemu zespołowi (i wtedy jest to **audyt**).

2. Standardy oceny bezpieczeństwa teleinformatycznego

Można wyróżnić dwie grupy standardów z zakresu bezpieczeństwa teleinformatycznego:

1) standardy na podstawie których można przeprowadzać certyfikacje systemów i produktów teleinformatycznych, np. ISO–15408 (*Common Criteria*), ITSEC, TCSEC;

2) standardy stanowiące tzw. *best practices*, np. BS 7799, PN–I–13335–1 (niestety, dalsze arkusze tego raportu technicznego ISO nie zostały wydane jako norma polska), traktujące o tym jak powinno budować się bezpieczne (cokolwiek by to słowo miało znaczyć) systemy teleinformatyczne.

Cechą charakterystyczną standardów z grupy 1) jest podawanie miar w postaci:

- klas – w TCSEC (np. Windows NT 4.0 oceniany jako **produkt** – przy pewnych ograniczeniach – posiada klasę C2 wg TCSEC);
- poziomów E0–E6 – w ITSEC;
- poziomów uzasadnionego zaufania EAL (tak zostało to przetłumaczone w projekcie normy polskiej) w ISO/IEC–15408, czyli *Common Criteria*.

Np. taki produkt jak Oracle 9i może posiadać certyfikaty wydane na podstawie standardów z grupy 1. Dla systemów i produktów ocenianych według standardów z grupy 2 certyfikatów się nie wystawia, bo nie podają one miar, dla których taką certyfikację można przeprowadzić. Obie grupy standardów mogą natomiast stanowić podstawę audytu w zakresie bezpieczeństwa teleinformatycznego dla konkretnych systemów teleinformatycznych.

Podstawową zaletą standardów z **punktu widzenia audytora** jest to, że systematyzują proces oceny systemu zabezpieczeń oraz stanowią platformę odniesienia pozwalającą na powtarzalność procesu oceny i porównywanie uzyskanych wyników. Mogą stanowić również punkt wyjścia przy formułowaniu kontraktu na przeprowadzenie audytu, ponieważ zawarcie w kontrakcie klauzuli określającej, że proces oceny ma zostać przeprowadzony np. zgodnie z zaleceniami ISO/IEC 15408, znacznie upraszcza rozliczalność takiego przedsięwzięcia.

Próby standaryzacji zagadnień związanych z ochroną i oceną bezpieczeństwa informacji w systemach informatycznych były podejmowane w praktyce od połowy lat sześćdziesiątych, gdy zaczęły wchodzić do powszechnego użytku systemy wielodostępne oraz pojawiły się pierwsze sieci komputerowe. 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 opracowane na zlecenie Departamentu Obrony USA i wydane w 1983 w postaci tzw. „Pomarańczowej książki".

Zarys historii opracowywania międzynarodowych standardów bezpieczeństwa teleinformatycznego został przedstawiony w artykule

zamieszczonym w Biuletynie IAiR nr 11/2000. Przedstawioną tam historię należy obecnie uzupełnić o dwa zapisy:

- 5.10.1998:

  podpisanie umowy pomiędzy organizacjami (z 14 państw uczestniczących w projekcie CC) certyfikującymi produkty informatyczne o wzajemnym uznawaniu certyfikatów bezpieczeństwa wydawanych na podstawie CC. Porozumienie weszło w życie 23.05.2000r. i obejmuje uznawanie certyfikatów dla poziomów bezpieczeństwa EAL1-EAL4.

- rok 1999:

  podkomisja SC27 (jedna z podkomisji komitetu JTC1) ustanawia *Common Criteria* jako trzyczęściowy międzynarodowy standard ISO/IEC-15408, a wszystkie państwa-członkowie tej podkomisji (w tym Polska) – rozpoczynają prace nad ustanowieniem standardu u siebie. W Polsce zakończenie ustanawiania ww. standardu jako normy jest przewidziane na koniec 2002 roku.

2.1. Kryteria oceny bezpieczeństwa teleinformatycznego według TCSEC

Standard *Trusted Computer System Evaluation Criteria* (TCSEC) został opracowany na zlecenie Departamentu Obrony USA i opublikowany w 1983 roku (ze względu na okładki w jakich został wydany, popularnie nazywany „pomarańczową książką"). Podstawowe koncepcje zawarte w tym standardzie to:

a) klasyfikacja informacji (w sensie nadawania informacji etykiet „poufne", „tajne" itp.), pozwalająca na tej podstawie różnicować do niej dostęp podmiotom (użytkownikom lub procesom);

b) mechanizm dostępu wykorzystujący model Bell-LaPadula w postaci tzw. *monitora referencyjnego*;

c) „zaufane środowisko przetwarzania" (*Trusted Computing Base*), na które składa się sprzęt komputerowy i oprogramowanie realizujące funkcje ochronne w systemie

Cechy charakterystyczne TCSEC to:

1) zdefiniowanie **czterech poziomów** kryteriów ochrony oznaczonych odpowiednio **D, C, B,** oraz **A**
2) do każdego z poziomów (za wyjątkiem D) przydzielenie pewnej liczby **klas oceny,** przy zachowaniu hierarchicznego porządku narastania możliwości ochrony danych (najmniejsze możliwości odpowiadają poziomowi D, największe poziomowi A)
3) dla każdej z klas sformułowanie wymagań bezpieczeństwa, pogrupowanych na wymagania związane z zapewnianiem:
   a) realizacji polityki bezpieczeństwa (*security policy*)
   b) rozliczalności działań w systemie (*accountability*)
   c) zaufania do mechanizmów ochronnych (*assurance*)
   d) wytworzenia dokumentacji chronionego systemu (*documentation*);
4) każdy wzrost możliwości ochrony oznacza jednocześnie zmniejszenie ryzyka penetracji systemu
5) kolejne poziomy reprezentują **istotne jakościowo różnice** w zdolności systemu do spełniania wymagań ochrony danych. Klasy wewnątrz poziomów oznaczają sukcesywne, lecz umiarkowane, wzmocnienie skuteczności środków ochrony danego poziomu (por. tabela 1)
6) przejście do kolejnej klasy (a tym bardziej następnego poziomu) oznacza wydatne **zwiększenie możliwości ochronnych**.

Tabela 1. TCSEC - klasy oceny

NAZWA OPISOWA	KLASA
Minimalna ochrona	D
Ochrona nakazowa	C1
Kontrolowany dostęp	C2
Etykietowanie zasobów	B1
Strukturyzacja produktu	B2
Domeny ochronne	B3
Weryfikowane projektowanie	A1

2.2. Kryteria oceny bezpieczeństwa teleinformatycznego według ITSEC

Standard *Information Technology Security Evaluation Criteria* (ITSEC) [4] opracowany pod patronatem Komisji Europejskiej przez Francję, Niemcy, Holandię i W. Brytanię zawiera kryteria oceny bezpieczeństwa stawiające określone wymagania dla:

- produktu
- jego procesu projektowania i wytwarzania
- jego środowiska projektowania i wytwarzania
- jego dokumentacji
- zalecanego środowiska eksploatacyjnego.

Kryteria ITSEC umożliwiają zatem ocenę nie tylko systemów teleinformatycznych, ale również np. sprzętu kryptograficznego. Według tych kryteriów, problemy związane z bezpieczeństwem teleinformatycznym powinny być uwzględniane już na etapie projektowania systemu w postaci:

- analizy kosztów wprowadzonych zabezpieczeń;
- analizy ryzyka (powinna zapewnić stopień bezpieczeństwa proporcjonalny do wagi chronionej informacji i do ilości użytych środków).

Na podstawie ITSEC może zostać dokonana ocena mechanizmów bezpieczeństwa pod względem ich poprawności realizacji, siły zabezpieczeń i stopnia spełnienia wymagań funkcjonalnych, gdzie:

- *siła zabezpieczeń* określa stopień skuteczności zabezpieczeń do przeciwstawienia się zagrożeniom i jest określana trójstopniowo: niska, średnia, wysoka.
- *poprawność realizacji* określa, za pomocą siedmiu poziomów pewności E0–E6, dokładność i jakość procesu kontroli mechanizmów bezpieczeństwa produktu poddawanego ocenie.
- *stopień spełnienia wymagań funkcjonalnych* określa 10 klas funkcjonalności: F-C1, F-C2, F-B1, F-B2, F-B3, F-IN, F-AV, F-DI, F-DC, F-DX[3] (plus klasy, które mogą by definiowane przez konstruktora, co pozwala np. na ocenianie programów antywirusowych). Ocena funkcjonalności polega na oszacowaniu stopnia spełnienia wymagań w zakresie bezpieczeństwa teleinformatycznego (np. stopień

[3] Klasa F-DX definiuje wymagania na urządzenia szyfrujące.

„przystawania" ocenianego obiektu do pewnego wzorcowego profilu zabezpieczeń) przez poddawany ocenie obiekt.

W tabeli 2 pokazano, jak kryteria ITSEC „przekładają" się na kryteria TCSEC.

Tabela 2. Kompatybilność ocen według kryteriów ITSEC i kryteriów TCSEC

Kryteria ITSEC	Kryteria TCSEC
E0	D
F-C1, E1	C1
F-C2, E2	C2
F-B1, E3	B1
F-B2, E4	B2
F-B3, E5	B3
F-B3, E6	A1

2.3. Kryteria oceny bezpieczeństwa teleinformatycznego według COBIT™

Jednym z tzw. „otwartych" standardów związanych z oceną bezpieczeństwa teleinformatycznego, jest standard COBIT™ opracowany i rozwijany w ramach ISACA (*Information Systems Audit and Control Association*)[4].

Działania ISACA koncentrują się na zagadnieniach audytu i bezpieczeństwa systemów teleinformatycznych. W ramach tej problematyki ISACA opracowuje standardy, prowadzi szkolenia i certyfikacje. Wraz z ISACF[5] tworzy i publikuje opracowania pomagające dotrzymywać kroku ciągle zmieniającemu się środowisku systemów informatycznych.

Najbardziej znanymi działaniami ISACA są: program certyfikacji CISA (*Certified Information System Auditor*), którym w ciągu kilkunastu lat zostało już objętych ok. 20000 osób (także nie będących członkami ISACA) oraz

[4] Polski Oddział ISACA powstał w 1998 roku. 12.03.1999 odbyło się pierwsze walne zgromadzenie członków.

[5] ISACF (*Information Systems Audit and Control Foundation*) – fundacja prowadząca prace standaryzacyjne oraz badania w dziedzinie kontroli przetwarzania informacji w systemach teleinformatycznych.

opracowanie i opublikowanie w 1996 roku standardu COBIT™ *(Control Objectives for Information and Related Technology)* [6].

Celem tego ostatniego przedsięwzięcia jest („jest" a nie „było", ponieważ jest to ciągle rozwijany, otwarty standard dostępny częściowo również w Internecie) „… *badanie, rozwijanie, publikowanie i promowanie autorytatywnego, aktualnego, zbioru celów kontroli systemów teleinformatycznych dla codziennego użytku przez kierownictwo i audytorów, akceptowanych przez społeczność międzynarodową*". Podstawowe elementy standardu to:

- Executive Summary
- Framework
- Implementation Tool Set
- Control Objectives
- Audit Guidelines

Zasadniczą częścią tego zestawu są *Control Objectives*, które zawierają 302 szczegółowe wymagania przypisane do 34 procesów przebiegających w systemach informatycznych. Te 34 procesy (podane jest skrótowe oznaczenie zgodne z anglojęzyczną wersją standardu i rozwinięcie w tłumaczeniu zgodnym z zamieszczonym w Internecie przez polski Oddział ISACA) to:

1. PO1 Definiowanie planu strategicznego
2. PO2 Definiowanie architektury informacyjnej
3. PO3 Określanie kierunków rozwoju technologicznego
4. PO4 Określanie organizacji i relacji IT
5. PO5 Zarządzanie inwestycjami IT
6. PO6 Przedstawianie kierownictwu kierunków
7. PO7 Zarządzanie zasobami ludzkimi
8. PO8 Zapewnianie zgodności z regulacjami zewnętrznymi
9. PO9 Szacowanie ryzyka
10. PO10 Zarządzanie projektami
11. PO11 Zarządzanie jakością
12. AI1 Identyfikowanie rozwiązań
13. AI2 Pozyskiwanie i utrzymywanie aplikacji
14. AI3 Pozyskiwanie i utrzymywanie architektury technologicznej
15. AI4 Opracowywanie i utrzymywanie procedur IT
16. AI5 Instalowanie i akredytowanie systemów
17. AI6 Zarządzanie zmianami
18. DS1 Ustalanie poziomów serwisowych
19. DS2 Zarządzanie obcymi serwisami

20. DS3 Zarządzanie wydajnością i pojemnością
21. DS4 Zapewnianie ciągłości działania serwisów
22. DS5 Zapewnianie bezpieczeństwa systemów
23. DS6 Identyfikowanie i rozliczanie kosztów
24. DS7 Edukowanie i szkolenie użytkowników
25. DS8 Wspomaganie i doradzanie odbiorcom usług IT
26. DS9 Zarządzanie konfiguracją
27. DS10 Zarządzanie problemami i incydentami
28. DS11 Zarządzanie danymi
29. DS12 Zarządzanie urządzeniami
30. DS12 Zarządzanie operacjami
31. M1 Monitorowanie procesów
32. M2 Ocenianie odpowiedniości kontroli wewnętrznej
33. M3 Uzyskiwanie niezależnej opinii
34. M4 Zapewnianie niezależnego audytu.

2.4. Kryteria oceny bezpieczeństwa teleinformatycznego według BS 7799

Standard BS 7799 został opracowany w połowie lat 90-tych przez British Standards Institute i podlega cały czas aktualizacji. W części pierwszej *„Code of practice for Information Security Management”* [7] dokumentu standaryzacyjnego opisane są „najlepsze praktyki”, które powinny być stosowane w budowie bezpiecznych systemów komputerowych. Na tej podstawie, w części drugiej BS 7799 pt. *„Specification for Information Security Management Systems”* [8], zdefiniowanych jest 127 punktów kontrolnych (wymagań na bezpieczeństwo teleinformatyczne), zgrupowanych w dziesięć tematów. Te tematy to:

1. Polityka bezpieczeństwa
2. Organizacja bezpieczeństwa
3. Kontrola i klasyfikacja zasobów
4. Bezpieczeństwo a personel
5. Bezpieczeństwo fizyczne
6. **Zarządzanie komputerami i siecią komputerową**
7. **Kontrola dostępu do systemu**
8. **Projektowanie i utrzymywanie systemu**

9. Planowanie ciągłości procesów biznesowych
10. Zgodność z obowiązującymi regulacjami prawnymi.

Warto zauważyć, że to co w powszechnym rozumieniu kojarzy się z pojęciem bezpieczeństwa teleinformatycznego i audytu w tym zakresie, to punkty 6-8 powyższej listy. Jest to niestety prowadzący do nieporozumień powszechny pogląd kadry kierowniczej (a więc osób zlecających i płacących za audyt!) i również (przynajmniej części) informatyków. Zdarza się bowiem, że realizując zlecenie na audyt, gdy padają pytania o:

- inwentaryzację zasobów teleinformatycznych w firmie,
- schemat obiegu informacji w firmie,
- podległość wykorzystywanej w firmie informacji pod obowiązujące ustawy, itp.

spotyka się niezrozumienie i pytanie „*a po co wam to, przecież macie sprawdzić czy nie ma luk w sieci*".

Przedstawiona lista tematów pokazuje również, że system bezpieczeństwa musi być systemem kompleksowym w sensie, jaki przedstawiono na początku poprzedniego rozdziału.

Od 1.12.2000 zalecenia brytyjskie opublikowane w „*Code of practice for Information Security Management"* zostały przyjęte jako norma ISO/IEC 17799:2000. Obecnie (jesień 2002) w Polsce trwają prace Polskiego Komitetu Normalizacyjnego nad wydaniem tej normy jako normy polskiej.

2.5. Kryteria oceny bezpieczeństwa teleinformatycznego według ISO/IEC 15408

Ponieważ norma ISO/IEC 15408 była przedmiotem odrębnego artykułu zamieszczonego w Biuletynie IAiR nr 11/2000, dalej dla kompletności informacji zawartych w niniejszym opracowaniu, zostanie przedstawiona tylko jej skrócona charakterystyka.

Charakterystyczne cechy zaleceń sformułowanych w „*Evaluation Criteria for Information Technology Security*" (tj. normie ISO/IEC-15408, opracowanej na podstawie wyników projektu o nazwie *Common Criteria* – dalej w tekście na oznaczenie tych zaleceń będzie stosowany skrót CC, por. przypis 2) są następujące:

- CC są zaleceniami mającymi na celu wprowadzenie ujednoliconego sposobu oceny systemów (produktów) informatycznych pod względem szeroko rozumianego bezpieczeństwa; mówią tylko o tym, ***co*** należy

zrobić, aby osiągnąć zadane cele, nie mówią natomiast nic o tym, ***jak*** to zrealizować.

- CC są **katalogiem** (wyrażonym w kategoriach klas, rodzin, komponentów i elementów) schematów konstrukcji wymagań związanych z ochroną informacji w systemach informatycznych, pisanych z użyciem specyficznej **terminologii**[6].

- CC mogą być stosowane zarówno do produktów programowych, jak i sprzętowych stosowanych w informatyce.

- CC nie zalecają ani nie wspierają żadnej ze znanych metodyk projektowania i wytwarzania systemów informatycznych oraz nie mówią nic na temat metodyki oceny systemów informatycznych (tzn. podają, jak np. skonstruować profil ochrony, ale nie podają jak go wykorzystać).

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

- Wynikiem oceny systemu (produktu) informatycznego według zaleceń CC jest dokument stwierdzający:

  - ☞ zgodność tego systemu (produktu) z określonym *profilem zabezpieczenia* lub,

  - ☞ spełnienie wymagań bezpieczeństwa określonych w *zadaniach zabezpieczenia* (*security target*) lub,

  - ☞ przypisanie do konkretnego *poziomu uzasadnionego zaufania* (EAL – *Evaluation Assurance Level*)[7]

2.5.1. Struktura Common Criteria

Dokument *Common Criteria* w wydaniu ISO/IEC-15408: *Evaluation Criteria for Information Technology Security* [1], [2], [3] składa się z następujących części:

[6] Z tego względu w niniejszym opracowaniu nie próbowano w zasadzie tłumaczyć terminów angielskich (w tym języku opublikowano CC) – to będzie musiał zrobić zespół tłumaczący ISO/IEC 15408 w celu stworzenia z nich norm polskich. Z dostępnych podczas opracowania niniejszego tekstu projektów tych norm wynika, że tłumaczenie jest niezbyt udane.

[7] Jak zatem widać, wynikiem oceny **nie są** stwierdzenia typu: *system bezpieczny*, *system zaufany* itp.!

Part 1: Introduction and General Model (52 strony)

Zawiera zasady oceny systemów teleinformatycznych oraz przedstawia ogólny model na podstawie którego taka ocena jest prowadzona. W tej części są wyjaśnione również terminy używane w całym dokumencie. W *Dodatku B* w [1] podana jest specyfikacja tzw. profilu zabezpieczenia, a w *Dodatku C* – zadań zabezpieczenia.

Profil zabezpieczenia (PP – *Protection Profile*) opisuje koncepcję bezpieczeństwa dla określonego typu przedmiotu oceny (w sposób niezależny od implementacji, może być zatem stosowany do wielu systemów/produktów)[8].

Zadania zabezpieczenia (ST – *Security Target*) opisują koncepcję bezpieczeństwa dla konkretnego przedmiotu oceny i stanowią podstawę takiej oceny.

Zarówno „profil zabezpieczenia" jak i „zadania zabezpieczenia" to określony standard dokumentacyjny – szablon ustalający kolejność i nazwy (a przez to i zawartość) rozdziałów dokumentu. Odpowiednie szablony w tłumaczeniu zgodnym z PrPN-ISO/IEC-15408 zamieszczone są w DODATKU do niniejszej publikacji.

Part 2: Security Functional Requirements (168 stron)

Zawiera katalog komponentów funkcjonalnych pogrupowanych w rodziny i klasy, z których można „składać" wymagania funkcjonalne na TOE (*Target of Evaluation* – tj. Przedmiot Oceny – produkt lub system teleinformatyczny wraz z dokumentacją administratora i/lub użytkownika). Mówiąc inaczej, w tej części są podane **szablony wymagań na funkcje produktu/systemu w zakresie bezpieczeństwa** związanej (przetwarzanej, pamiętanej) z nim informacji.

Part 3: Security Assurance Requirements (214 stron)

Zawiera katalog „komponentów bezpieczeństwa" (pogrupowanych w rodziny i klasy, analogicznie jak dla wymagań funkcjonalnych[9]), z których można „składać" **wymagania na procesy związane z projektowaniem, wytwarzaniem, testowaniem, przygotowywaniem dokumentacji, konfiguracją, dostarczaniem i zarządzaniem TOE**. Klasy i rodziny wymagań bezpieczeństwa są wyszczególnione w tabeli 3 (liczba w tabeli oznacza numer komponentu, numer pogrubiony oznacza pierwsze wystąpienie danego komponentu w EAL)

[8] Definicja wg Pr PN-ISO/IEC 15408-1: „...niezależny od implementacji zbiór wymagań na zabezpieczenia dla pewnej kategorii Przedmiotów Oceny spełniający potrzeby odbiorców".
[9] W nazwie skróconej *assurance class* są identyfikowane literą A, tzn: AXX_YYY.

Podstawowym elementem w zstępującej dekompozycji struktury wymagań jest tzw. *assurance element* stanowiący pojedyncze, niepodzielne wymaganie dotyczące bezpieczeństwa. Każdy z takich elementów należy do jednego z trzech zbiorów[10]:

- elementów określających zadania dla projektanta, np:
  ADV_FSP.1.1D The developer shall provide a functional specification.
- elementów określających zawartość informacyjną i cechy prezentacji, np:
  ADV_FSP.1.2C The functional specification shall be internally consistent.
- elementów określających czynności wykonywane przez oceniającego, np: ***ADV_FSP.1.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.***

Dodatkowo, w tej części zdefiniowano dwie klasy wymagań związanych z oceną *profili zabezpieczenia* i *zadań zabezpieczenia*:

- Class APE: Protection Profile evaluation
- Class ASE: Security Target evaluation

oraz zdefiniowano poziomy uzasadnionego zaufania (*Evaluation Assurance Levels*):

- Evaluation assurance level 1 (EAL1) - functionally tested
- Evaluation assurance level 2 (EAL2) - structurally tested
- Evaluation assurance level 3 (EAL3) - methodically tested and checked
- Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed
- Evaluation assurance level 5 (EAL5) - semiformally designed and tested
- Evaluation assurance level 6 (EAL6) - semiformally verified design and tested
- Evaluation assurance level 7 (EAL7) - formally verified design and tested

[10] Typ zbioru jest identyfikowany przez literę dołączaną do nazwy skróconej elementu:
D - Developer (projektant), **C** - Content (zawartość), **E** - Evaluator (oceniający).

Tabela 3. Poziomy uzasadnionego zaufania - EAL

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration management	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
Delivery and operation	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
Development	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
Guidance documents	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
Life cycle support	ALC_DVS			1	1	1	2	2
	AFC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4

Podsumowując, od początku 1999 roku *Common Criteria* są wdrażane do użytku w państwach uczestniczących w projekcie. Opracowywane są procedury uznawania certyfikatów bezpieczeństwa wydawanych dotychczas na podstawie zaleceń ITSEC. W trakcie opracowania znajduje się także uzupełnienie CC w postaci *Common Methodology for Information Technology Security Evaluation* (CEM), które ma stanowić ogólnie uznawany zbiór metodyk prowadzenia procesu oceny. Jak bowiem już zostało wspomniane wcześniej, CC

mówią tylko co należy oceniać, natomiast CEM mają powiedzieć jak to zrealizować.

Przy ISO/IEC powstała instytucja zajmująca się katalogowaniem i udostępnianiem profili zabezpieczenia, opracowanych przez konstruktorów z państw biorących udział w projekcie. Docelowo powinno to ułatwić projektowanie zabezpieczeń konkretnych systemów teleinformatycznych, ponieważ na podstawie ogólnych wymagań bezpieczeństwa określonych dla systemu teleinformatycznego w jego polityce i planie bezpieczeństwa teleinformatycznego, będzie można dobrać odpowiedni profil zabezpieczenia, a na jego podstawie – konkretny produkty teleinformatyczne.

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

3. Proces audytu

W celu uniknięcia nieporozumień warto przyjąć, że audytem (bez dodatkowych przymiotników) będzie nazywane postępowanie (sprawdzanie, ocenianie) prowadzone przez stronę niezależną (osobę lub zespół). Ta niezależność jest w stosunku do:

1) organizacji/zespołu budującego system zabezpieczeń;
2) dostawców sprzętu i oprogramowania;
3) organizacji podlegającej przeglądowi w takim sensie, że w skład zespołu audytowego nie mogą wchodzić pracownicy organizacji zlecającej audyt.

Jeżeli nie jest dotrzymany któryś z ww. punktów, to można mówić co najwyżej o „*przeglądzie zabezpieczeń według listy audytowej ...",* a nie o audycie.

W praktyce audyt dla celów bezpieczeństwa teleinformatycznego przeprowadza się, aby:

1) wykazać, że informacja i system teleinformatyczny został zabezpieczony zgodnie z ustaleniami pomiędzy zleceniodawcą a zespołem budującym system bezpieczeństwa lub

2) wykazać, że system bezpieczeństwa spełnia wymagania norm i standardów w tym zakresie, np. ISO/IEC-15408 lub

3) wystawić ocenianemu systemowi tzw. *certyfikat bezpieczeństwa*, co w związku z wejściem Polski do NATO (i obowiązującej ustawie „*o ochronie informacji niejawnych"*) oraz dążeniem do wejścia do Unii Europejskiej[11] jest coraz częstsze lub

4) ocenić jakość systemu bezpieczeństwa i przedstawić ocenę zleceniodawcy do decyzji (modernizujemy/zostawiamy jak jest).

Z przytoczonych uwag wynika, że:

1) audyt **nie jest** sprawdzaniem zapisów w dziennikach systemowych i zabezpieczeń systemu teleinformatycznego (inspekcja logów) w celu wykrycia ewentualnych włamań, chociaż takie sprawdzanie może być **elementem** procesu audytu;

2) audyt **nie jest** sprawdzaniem konfiguracji stacji roboczych, serwerów i urządzeń sieciowych, chociaż takie sprawdzanie może być **elementem** procesu audytu;

3) w szczególności audytem (ani elementami audytu) **nie są** czynności wymienione w punktach 1 i 2, jeżeli są przeprowadzane przez administratorów konkretnych systemów w ramach ich bieżących bądź zleconych zadań.

Z jakich elementów składa się zatem proces audytu?

1) Pierwszym z nich jest sporządzenie listy audytowej (*checklist*) według wybranego standardu. Dla standardu BS 7799 będzie to lista 127 punktów „do odhaczenia", dla COBIT™ 302 punkty (pogrupowane w 34 tematy), dla TCSEC 134 punktów itd. Zalecenia poszczególnych punktów audytowych (w miarę potrzeb opatrzone komentarzami) są kwalifikowane do jednej z poniższych klas:
   - *„spełnione",*
   - *„nie spełnione",*
   - *„spełnione częściowo",*
   - *„nie dotyczy".*

2) Następnym jest wypełnienie listy audytowej z punktu 1 na podstawie wywiadów, wizji lokalnych, kontroli dokumentów i wykonanych testów.

[11] Polecam uwadze Czytelników „Council Resolution of 28 January 2002 on a common approach and specificactions in the area of network and information security (2002/C 43/02)".

3) Kolejnym elementem audytu (a nie audytem, jak to się zwykło uważać!) są tzw. **testy penetracyjne**. Testy penetracyjne (tzw. kontrolowane włamania) są prowadzone w celu określenia podatności badanego systemu teleinformatycznego na ataki wewnętrzne i zewnętrzne i obejmują w obecnie przeprowadzanych przedsięwzięciach audytowych – pominę tu specyfikę i generalną klasyfikację tzw. „empirycznych prób ujawnień i słabości" – kontrolowane:
   - identyfikacje systemu (rodzaju i wersji systemu operacyjnego, użytkowanego oprogramowania, użytkowników itd.)
   - skanowania:
     - ☞ przestrzeni adresowej
     - ☞ sieci telefonicznej firmy
     - ☞ portów serwerów i urządzeń sieciowych firmy
   - włamania
   - podsłuch sieciowy (ang. *sniffing*)
   - badanie odporności systemu na ataki typu „*odmowa usługi*".
4) Ostatnim elementem jest sporządzenie dokumentacji z audytu (raportu), obejmującej udokumentowane przedsięwzięcia, wyniki i wnioski dla punktów 2 i 3. Dokumentacja końcowa musi być podpisana przez audytorów, imiennie gwarantujących rzetelność przeprowadzonej oceny.

4. Zamiast podsumowania...

Zamiast podsumowania dalej są zamieszczone wybrane fragmenty niedawnej dyskusji e–mailowej (dokładniej: pytania na które autor niniejszego artykułu starał się odpowiedzieć), która dotyczyła audytu i standardów.

[I] *Jak nazywać postępowanie będące:*
- *testem penetracyjnym;*
- *inspekcją logów lub dzienników zabezpieczeń;*
- *przeglądem zabezpieczeń;*
- *oceną konfiguracji?*

DOKŁADNIE TAK! Uważam, że te sformułowania są wystarczająco precyzyjne i nie wymagają strojenia ich w czapkę audytu. Z powodzeniem przecież zespół (osoba) może zawrzeć umowę np. na przeprowadzenie testów penetracyjnych. Takie okresowe obowiązki można też wyspecyfikować w zadaniach dla osoby odpowiedzialnej w firmie za bezpieczeństwo

teleinformatyczne. Oczywiście termin „audyt" lepiej się sprzedaje, jest bardziej tajemniczy i wzbudzający respekt, jednak jako inżynier jestem za precyzją sformułowań, bo one rzutują potem na precyzję działań.

[II] *Co oznacza posiadanie certyfikatu przez produkt?*

Oznacza 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 etc. 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. Podobnie posiadanie przez firmę certyfikatów z rodziny ISO-9000 nie chroni automatycznie przed produkcji bubli, chociaż powinno radykalnie taką możliwość zmniejszyć.

[III] *Po co nam zatem certyfikaty?*

Jeżeli nasze, polskie firmy nie będą ich posiadały dla eksploatowanych systemów teleinformatycznych i używanych produktów, to stracą możliwość równej walki konkurencyjnej z firmami zagranicznymi w Zjednoczonej Europie, do której to Europy tak konsekwentnie dążymy. Do uzasadnienia tej tezy może posłużyć chociażby zawartość dokumentu „*Council Resolutionof 28 January 2002 on a common approach and specificactions in the area of network and information security (2002/C 43/02)"*[12] i stosowane na Zachodzie praktyki. Na przykład w USA firma, która nie posiada certyfikatu SEI CMM określającego odpowiedni stopień „dojrzałości organizacyjnej", z definicji nie jest dopuszczana do kontraktów realizowanych na zamówienie Departamentu Obrony. Inny przykład: od III kwartału 2003 wszystkie kraje członkowskie NATO muszą (przynajmniej w zakresie związanym z działalnością NATO, a jest ona bardzo obszerna), wdrożyć stosowanie normy ISO-15408. Stąd m.in. starania UOP o wdrożenie tego standardu jako normy polskiej, bo do tego zobowiązują nas umowy międzynarodowe.
Podsumowując ten akapit: certyfikaty są potrzebne, bo wymagają ich formalne zasady postępowania w szeroko rozumianej działalności biznesowej, szczególnie jeżeli jest ona prowadzona na arenie międzynarodowej.

[12] Na marginesie: dokument ten zaleca stosowanie standardów ISO-15408 i ISO-17799.

[IV] *Normy, ustawy i rozporządzenia są pisane „trudnym" językiem, mało zrozumiałym dla przeciętnego admina.*

Zgadzam się, że język dokumentów typu ustawy czy normy jest trudny. Do tego dokładają się błędy powstające przy tłumaczeniu norm na język polski. Nie jestem prawnikiem tylko informatykiem, ale uważam, że również informatycy powinni być na bieżąco z dokumentami (w tym z regulacjami prawnymi obowiązującymi w naszym kraju) i normami, które dotyczą szeroko rozumianej informatyki. Szczególnie że większość tych unormowań dotyczy bezpieczeństwa informacji. Nie można podjąć się np. budowy systemu bezpieczeństwa dla systemów komputerowych w których ma być przetwarzana informacja niejawna (w rozumieniu ustawy), jeżeli nie zna się tej ustawy i wydanych na jej podstawie rozporządzeń!

[V] *Czy warto stosować pewne z góry założone procedury i metodyki przy testowaniu bezpieczeństwa? Czy intruzi trzymają się standardów czy sztywnych metodyk działania?*

Tak, trzeba trzymać się standardów, bo porządkują one proces audytu i umożliwiają porównywanie wyników. Brak metodyki przy każdym postępowaniu w dziedzinie technicznej (nie dotyczy to oczywiście różnych dziedzin sztuki ☺) jest amatorstwem a nie profesjonalizmem. Wbrew pozorom, również intruzi działają (zwykle) metodycznie. Gdyby było inaczej, nie można byłoby np. opracować sygnatur dla narzędzi IDS. Proszę jednak zauważyć, że zgodnie z proponowanym przeze mnie rozumieniem audytu, jest on **działaniem kompleksowym** – obejmuje czynności sprawdzające zgodność ze standardami (lista audytowa) jak i testy penetracyjne, które w pewnym sensie można potraktować jako element „sztuki".

5. Literatura:

[1] Common Criteria for Information Technology Security Evaluation. Part 1: *Introduction and general model*. May 1998. Version 2.0. CCIB-98-026.

[2] Common Criteria for Information Technology Security Evaluation. Part 2*: Security functional requirements*. May 1998. Version 2.0. CCIB-98-027

[3] Common Criteria for Information Technology Security Evaluation. Part 3: *Security assurance requirements*. May 1998. Version 2.0. CCIB-98-028.

[4] ITSEC. Version 1.2. June 1991.

[5] Trusted Computer System Evaluation Criteria. DoD. 15 August 1983. CSC-STD-001-83.

[6] COBIT™ Control Objectives. April 1998. 2nd Edition. COBIT Steering Committe and the Information Systems Audit and Control Foundation.

[7] BS 7799-1:1999: *Part 1: "Code of practice for Information Security Management"*. BSI.

[8] BS 7799-2:1999: *Part 2 "Specification for Information Security Management Systems"*. British Standards Institute.

[9] PN-I-02000: Technika informatyczna. *Zabezpieczenia w systemach informatycznych. Terminologia*.

[10] PN-I-13335-1: 1999. Technika informatyczna. *Wytyczne do zarządzania bezpieczeństwem systemów informatycznych. Pojęcia i modele bezpieczeństwa systemów informatycznych*.

DODATEK

Szablony dokumentacyjne według PrPN-ISO/IEC 15408

Używane skróty: PP – *Protect Profile (profil zabezpieczenia)*,
ST – *Security Target (zadania zabezpieczenia)*
TOE – *Target of Evaluation (przedmiot oceny)*,
IT – *Information Technology*.

Profil zabezpieczenia

1. Wprowadzenie
   - 1.1. Identyfikacja PP
   - 1.2. Ogólny opis PP
2. Opis TOE
3. Otoczenie zabezpieczenia TOE
   - 3.1. Założenia
   - 3.2. Zagrożenia
   - 3.3. Polityka bezpieczeństwa

4. Cele zabezpieczenia
   4.1. Cele zabezpieczenia TOE
   4.2. Cele zabezpieczenia otoczenia
5. Wymagania
   5.1. Wymagania na zabezpieczenia IT
      5.1.1. Wymagania na zabezpieczenie otoczenia IT
   5.2 Wymagania na zabezpieczenie TOE
      5.2.1. Wymagania na funkcjonalne zabezpieczenie TOE
      5.2.2. Wymagania na uzasadnienie zaufania do zabezpieczenia TOE
6. Uwagi dotyczące zastosowania PP
7. Uzasadnienie
   7.1. Uzasadnienie celów zabezpieczenia
   7.2. Uzasadnienie wymagań na zabezpieczenie

Zadania zabezpieczenia

1. Wprowadzenie do ST
   1.1. Identyfikacja PP
   1.2. Ogólny opis PP
   1.3. Postulat zgodności z CC
2. Opis TOE
3. Otoczenie zabezpieczenia TOE
   3.1. Założenia
   3.2. Zagrożenia
   3.3. Polityka bezpieczeństwa
4. Cele zabezpieczenia
   4.1. Cele zabezpieczenia TOE
   4.2. Cele zabezpieczenia otoczenia

5. Wymagania
   - 5.1. Wymagania na zabezpieczenia IT
     - 5.1.1. Wymagania na zabezpieczenie otoczenia IT
   - 5.2. Wymagania na zabezpieczenie TOE
     - 5.2.1. Wymagania na funkcjonalne zabezpieczenie TOE
     - 5.2.2. Wymagania na uzasadnienie zaufania do zabezpieczenia TOE

6. Ogólna specyfikacja TOE
   - 6.1. Funkcje zabezpieczające TOE
   - 6.2. Środki uzasadniające zaufanie

7. Postulat zgodności z PP
   - 7.1. Odniesienie dp PP
   - 7.2. Dostosowanie do PP
   - 7.3. Uzupełnienie PP

8. Uzasadnienie
   - 8.1. Uzasadnienie celów zabezpieczenia
   - 8.2. Uzasadnienie wymagań na zabezpieczenie
   - 8.3. Uzasadnienie ogólnej specyfikacji TOE
   - 8.4. Uzasadnienie postulatu zgodności z PP

Recenzent: dr hab. inż. Andrzej Chojnacki
Praca wpłynęła do redakcji 5.10.2002