ACTA UNIVERSITATIS LODZIENSIS
FOLIA OECONOMICA 157, 2002

*Katarzyna Lange-Sadzińska**

BEZPIECZEŃSTWO SYSTEMÓW KOMPUTEROWYCH I PRODUKTÓW IT – OBOWIĄZUJĄCE STANDARDY OCENY

Artykuł ukazuje w jaki sposób standard Common Criteri, ujednolica istniejące standardy bezpieczeństwa systemów komputerowych i produktów technologii informacyjnej.

The paper presents how standard Common Criteria unifiedes present computer systems and information technology products security standards.

Wstęp

Wszelkie rozważania dotyczące bezpieczeństwa muszą obejmować cały cykl życia systemu - od projektowania, poprzez konstruowanie, wdrożenie, eksploatację i zakończenie użytkowania.

Odpowiedzialni za bezpieczeństwo systemu informatycznego czy jakiegokolwiek produktu IT (Information Technology) muszą brać pod uwagę aspekty techniczne, kwestie organizacyjne i prawne, również w wymiarze międzynarodowym. Środowisko pracy systemu zmienia się bardzo dynamicznie. Szybki postęp technologiczny zmienia sposoby zabezpieczeń i jednocześnie generuje pole do powstania nowych zagrożeń. W związku z tym należy rozumieć zapewnienie bezpieczeństwa dużego systemu jako proces, „na którego przebieg wpływają stale nowe wyniki światowych badań teoretycznych, pojawienie się nowych technologii i produktów na rynku a także zmiany w regulacjach prawnych i ustalenia standaryzacyjne."[1]

Istotne jest zatem wyraźne określenie polityki bezpieczeństwa.

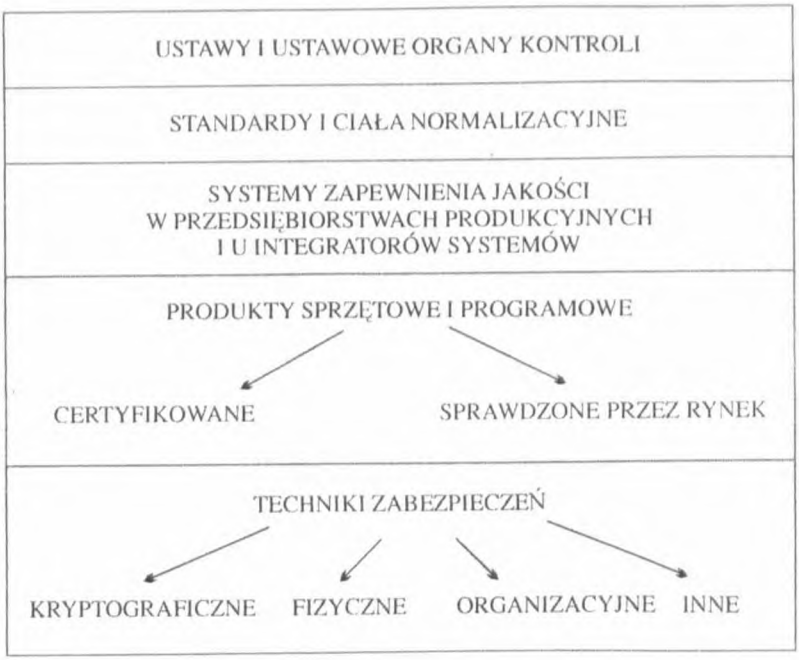
---

* Zakład Analizy i Projektowania Systemów, Uniwersytet Łódzki

[1] Carlson P. „Rola standardów w ochronie informacji", referat IT forum „Bezpieczeństwo systemów informatycznych"

Istnieje wiele aspektów bezpieczeństwa, które powinny być rozważane przy definiowaniu polityki bezpieczeństwa. Należy do nich integralność danych (zabezpieczenie przed zmianami danych), dostępność danych (zabezpieczenie przed zakłóceniami danej usługi), poufność danych (zabezpieczenie przed wglądem przez niepowołane osoby).

Tabela 1. Czynniki środowiska w którym działa produkt IT wpływające na jego bezpieczeństwo.
Na podstawie: Carlson P. "Rola standardów w ochronie informacji", referat IT forum „Bezpieczeństwo systemów informatycznych" www.it.forum.pl/3/referaty/referat3_1.htm



Standardy TCSEC i ITSEC

TCSEC czyli Trusted Computer Security Evaluation - (Kryteria oceny wiarygodności oceny systemów komputerowych) zwane też „Orange Book" zostały opublikowane po raz pierwszy w 1983 przez Ministerstwo Obrony Stanów Zjednoczonych.

Raport TCSEC określa kryteria, które stanowią podstawę oceny wiarygodności danego systemu. W zależności od spełnianych wymagań system otrzymuje

klasę bezpieczeństwa. Kryteria oceny wiarygodności określone w standardzie TCSEC są podzielone na cztery grupy:

- polityka bezpieczeństwa (sposób dostępu do informacji),
- możliwość kontroli (mechanizmy identyfikacji, uwierzytelniania, śledzenia, wiarygodnej ścieżki-czyli ew. przechwycenia logu i podszycia się pod system),
- gwarancja działania mechanizmów zabezpieczających (kategorie bezpieczeństwa A, B, C i odpowiednio dla każdej z nich klasy A1, B1, B2, B3, C1, C2),
- wymagana dokumentacja (forma i szczegółowość dokumentacji ocenianego produktu).

Kolejnym ważnym standardem jest ITSEC (Information Technology Security Evaluation Criteria).

Za moment powstania standardu ITSEC można uznać ustanowienie oceny dotyczącej bezpieczeństwa rządowych systemów komputerowych w 1985 r. w Wielkiej Brytanii. W maju 1991 wszedł w życie nowy projekt - nazwany UK IT Security Evaluation and Certification scheme (w skrócie "UK ITSEC scheme").

W tym czasie w innych krajach europejskich trwały prace nad standardami. W Niemczech Agencja ds. Bezpieczeństwa Informacji opracowała pierwszą własną wersję kryteriów bezpieczeństwa.

Francja opracowała kryteria zwane Blue-White-Red Book.

Prace tych krajów posłużyły do opracowania zestawu kryteriów znanych pod nazwą Information Technology Security Evaluation Criteria (ITSEC)- Kryteria oceny bezpieczeństwa technologii informacyjnej.

ITSEC uznają - Wielka Brytania, Francja, Niemcy, Holandia i Komisja Unii Europejskiej. Ponadto obustronne umowy obowiązujące między Wielką Brytanią, Francją i Niemcami są formalnie uznawane również przez Finlandię, Grecję, Holandię, Szwecję i Szwajcarię.

Skala ocen przyznawanych ocenianemu obiektowi jest siedmiopoziomowa od najmniej bezpiecznego E0 do najbardziej bezpiecznego E6.

Porównanie standardów ITSEC i TCSEC pozwala zauważyć odpowiedniość poszczególnych poziomów i klas. Przedstawia to poniższa tabela. Zachowana odpowiedniość daje szansę na ujednolicenie tych standardów i ich migrację ku wspólnemu o szerszym zasięgu.

Tabela 2. Odpowiedniość poziomów wg kryteriów ITSEC i TCSEC.
Na podstawie: Ahuja V.: "Bezpieczeństwo w sieciach"

	ITSEC	TCSEC
poziomy zabezpieczeń	E0	D
	E1	C1
	E2	C2
	E3	B1
	E4	B2
	E5	B3
	E6	A1

Standard Common Criteria (CC)

Odpowiedniość wymienionych wcześniej standardów wyraźnie sugeruje dążenie do jednego standardu o znacznie szerszym zasięgu. Rezultatem tego dążenia jest projekt COMMON CRITERIA.

Dokumentacja COMMON CRITERIA obejmuje trzy części.

Część pierwsza – „Introduction and general model" jest wstępem do CC. Definiuje podstawowe koncepcje bezpieczeństwa i prezentuje model oceny.

Część druga – „Security functional requirements" wprowadza zbiór funkcjonalnych komponentów bezpieczeństwa.

Część trzecia – „Security assurance requirements" wprowadza zbiór wymagań funkcjonalnych dla produktu IT.

Common Criteria ma siedem poziomów zabezpieczeń od EAL1 do EAL7. Zawarto je w poniższej tabeli.

Tabela 3. Poziomy zabezpieczeń w standardzie Common Criteria.
Na podstawie Common Assurance Levels
http://www.commoncriteria.org/cc/art3/ Part304.html

COMON CRITERIA	OPIS
EAL1	Testowanie funkcjonalne. Analiza funkcji bezpieczeństwa wykonywana poprzez niezależne testowanie tych funkcji.
EAL2	Testowanie strukturalne. Jw., dodatkowo analiza na wysokim poziomie projektu podsystemów testowanego obiektu.
EAL3	Metodologiczne testowanie i sprawdzanie. Jw., dodatkowo wymagana jest kontrola środowiska pracy obiektu.
EAL4	Metodyczne testowanie, sprawdzanie i przeglądanie. Jw., dodatkowo analiza na niskim poziomie projektu modułów testowanego obiektu.
EAL5	Półformalne sprawdzanie i testowanie. Analiza obejmuje całą implementację.
EAL6	Półformalne weryfikowanie projektu i testowanie. Analiza wykonywana przy modularnym i warstwowym podejściu do projektu.
EAL7	Formalne weryfikowanie projektu i testowanie. Model formalny jest uzupełniany formalną prezentacją specyfikacji funkcjonalnej.

Reprezentacje agencji bezpieczeństwa z USA, Kanady, Francji, Niemiec i Wielkiej Brytanii podpisały umowę o wzajemnym formalnym uznawaniu certyfikatów od EAL1 do EAL4 dla produktów bazujących na wersji 2.0 Common Criteria. Następnie umowa ta została rozszerzona o Australię i Nową Zelandię .

Common Criteria Version 2.1 ratyfikowano przez ISO jako standard ISO 15408.

Ze względów historycznych i dla kontynuacji prac używa się terminu **Common Criteria**, przy oficjalnej nazwie ISO "Evaluation Criteria for Information Technology Security".

Ocena produktu IT pod względem bezpieczeństwa

Oprócz definicji poziomów bezpieczeństwa standard CC zawiera wiele innych definicji. Kilka z nich zostanie przytoczonych poniżej.

COMMON CRITERIA definiują tzw. Protection Profile (PP) pozwalające na podstawie oczekiwań klientów stworzyć standaryzowany zbiór wymagań zaspokajających ich potrzeby.

Target of Evaluation (TOE) to część produktu lub systemu, która jest przedmiotem ewaluacji (oceny), do tej pory nazywana produktem IT.

Security Target (ST) jest używany przez oceniających jako baza dla oceny (ewaluacji). Jest bazą do porozumienia między klientami, oceniającymi i autorytetami ewaluacji na temat oceny zakresu bezpieczeństwa konkretnego TOE.

Podstawy oceny opierają się na trzech elementach :

1. Security Target (ST),
2. zbiorze dostarczonych informacji o produkcie, czyli TOE,
3. samym TOE.

Oczekiwany rezultat procesu ewaluacji to potwierdzenie, że TOE spełnia wymagania ST z zawartymi w raportach informacjami z przebiegu ewaluacji.

Przy ocenie produktu należy uczynić szereg założeń, dotyczących środowiska w jakim będzie pracował oceniany produkt IT. Może ono bowiem znacząco różnić się od ustalonych przy badaniu. Ponadto ważne jest z jakich elementów składa się oceniany TOE.

Rezultaty dokładności i kompletności oceny bezpieczeństwa zależą od dokładności i kompletności informacji i dokumentacji dostarczonej z TOE.

Rezultaty oceny bezpieczeństwa dają się stosować tylko do konkretnej wersji produktu w ocenianej konfiguracji.

Siedem rządowych organizacji (oficjalnie "Common Criteria Project Sponsoring Organizations"), zwanych w uproszczeniu w dokumentach sponsorami, posiada prawa do używania, kopiowania, rozpowszechniania, tłumaczenia lub modyfikowania Common Criteria for Information Technology Security Evaluations, version 2.1.

Tabela 4. Lista członków „Common Criteria Project Sponsoring Organizations"

Państwo	Organizacja
Francja	Service Central de la Sécurité des Systémes d'Information (SCSSI), http://www.scssi.gouv.fr
Holandia	Netherlands National Communications Security Agency (NLNCSA), http://www.tno.nl/instit/fel/refs/cc.html
Kanada	Communications Security Establishment (CSI) http://www.cse-cst.gc.ca/cse/english/cc.html
Niemcy	Bundesamt für Sicherheit in der Informationstechnik (BSI) Http://www.bsi.bund.de/cc
Stany Zjednoczone	National Institute of Standards and Technology (NIST) http://csrc.nist.gov/cc
Stany Zjednoczone	National Security Agency (NSA) http://www.radium.ncsc.mil/tpep
Wielka Brytania	Communications-Electronics Security Group (CESG) http://www.cesg.gov.uk/cc.html

Podsumowanie

W referacie przedstawiono w skrócie najważniejsze standardy oceny bezpieczeństwa, opracowane i obowiązujące w krajach Ameryki Północnej i Europy, ze szczególnym uwzględnieniem standardów międzynarodowych, czyli COMMON CRITERIA.

Porównując informacje o nich należy zauważyć, że siedem poziomów zabezpieczeń Common Criteria (CC) od EAL1 do EAL7 koresponduje z poziomami ITSEC i TCSEC.

Poniższa tabelka przedstawia tę odpowiedniość.