dr inż. ANDRZEJ BIAŁAS
Centrum Elektryfikacji i Automatyzacji Górnictwa EMAG

Konstruowanie zabezpieczeń produktów i systemów informatycznych posiadających mierzalny poziom uzasadnionego zaufania

Artykuł, w świetle standardu ISO/IEC 15408 Common Criteria, przedstawia przegląd zagadnień związanych z konstruowaniem i oceną zabezpieczeń wbudowywanych w dowolne produkty lub systemy informatyczne. Ocena ta dotyczy uzasadnionego zaufania do zabezpieczeń, utożsamianego potocznie z ich wiarygodnością. Po krótkim wprowadzeniu w tematykę związaną ze standardem, skrótowo opisano kilkuetapowy i dość sformalizowany proces konstruowania zabezpieczeń. W jego wyniku powstaje dokument zwany zadaniem zabezpieczeń, który specyfikuje zbiór funkcji zabezpieczających wbudowywanych w produkt lub system informatyczny. Ponadto precyzowany jest poziom uzasadnionego zaufania, utożsamiany z rygoryzmem, z jakim implementowane są te funkcje. Ciężar opracowania materiału dowodowego potwierdzającego zadeklarowany poziom uzasadnionego zaufania spoczywa głównie na konstruktorach i osobach odpowiedzialnych za procesy wytwarzania i utrzymania. Materiał wraz z produktem lub systemem informatycznym poddawany jest niezależnej ocenie według metodyki związanej ze standardem. Pozytywny i dodatkowo zweryfikowany wynik tej oceny pozwala na uzyskanie certyfikatu na spełnienie wymagań deklarowanego poziomu uzasadnionego zaufania. Produkty certyfikowane, dzięki tej niezależnej i wnikliwej ocenie, są uznawane za bardziej wiarygodne, więc mogą być używane do odpowiedzialnych zastosowań.

1. WSTĘP

Projektując czy wdrażając złożone systemy informatyczne, poza zagadnieniem funkcjonalności systemów, ich twórcy muszą często rozstrzygać następujące kwestie: jaka będzie wiarygodność tych systemów; od czego ona zależy; czy będzie ona na tyle wystarczająca, by móc powierzyć systemom zdrowie i życie ludzkie, żywotne procesy biznesowe instytucji czy też zasoby informacyjne, od których może zależeć przetrwanie i przyszłość instytucji? Problem dotyczy głównie instytucji silnie zinformatyzowanych, czyli w obecnych czasach większości z nich. Rozwiązanie tych zagadnień tkwi w odpowiednim doborze systemów i ich komponentów oraz w prawidłowym zarządzaniu ich bezpieczeństwem w oparciu o analizę ryzyka. Nie są to również zagadnienia oderwane od potrzeb i realiów współczesnego, zinformatyzowanego i zautomatyzowanego górnictwa.

Celem niniejszego artykułu jest przybliżenie informatykom, elektronikom i menadżerom zagadnień związanych z konstruowaniem, wytwarzaniem oraz stosowaniem produktów i systemów informatycznych, cechujących się tak zwanym „uzasadnionym zaufaniem" (ang. *assurance*), utożsamianym potocznie z wiarygodnością. Zaufanie jest określane jako „uzasadnione", gdyż jego źródłem jest rygorystyczny proces konstruowania, wytwarzania i utrzymywania produktu lub systemu oraz późniejszy proces oceny prowadzonej w niezależnym, akredytowanym laboratorium, oceny opartej na ściśle zdefiniowanych zasadach i kryteriach zawartych w standardzie ISO/IEC 15408 Common Criteria (CC) [1], [2], [3] a także w dokumentach z nim związanych.

W praktyce uzasadnione zaufanie oznacza, że urządzenie, program lub system informatyczny spełnia zdefiniowane dla niego cele bezpieczeństwa, czyli w sytuacji wystąpienia zagrożenia jego funkcje zabezpieczające (ang. *Security functions*) powinny odpowiednio zadziałać. W świetle standardu, bezpieczeństwo jest rozumiane w znaczeniu *security*, czyli w sensie ochrony obiektu przed zagrożeniami z zewnątrz, w przeciwieństwie do pojęcia *safety*, dla którego rozważa się negatywny wpływ, jaki obiekt może wywierać na swoje otoczenie. Dla niektórych

zastosowań oba te zagadnienia są rozpatrywane łącznie i oba są określane jednym polskim określeniem „bezpieczeństwo".

Produkt lub system informatyczny, według stosowanej tu terminologii zwany jest przedmiotem oceny (ang. *TOE – Target of Evaluation*), co wynika z faktu, że wraz ze swoją dokumentacją, stanowiącą tak zwany materiał dowodowy, w toku certyfikacji jest właśnie poddawany niezależnej i wnikliwej ocenie. Ocena ta rozstrzyga, czy TOE spełnia wymagania bezpieczeństwa związane z zadeklarowanym dla niego poziomem uzasadnionego zaufania. Uzasadnione zaufanie jest bowiem mierzalne. Wyróżniono jego poziomy (ang. *EAL – Evaluation Assurance Level*) od EAL1 (min.) do EAL7 (max.).

Zakres stosowania standardu Common Criteria jest dość szeroki – dotyczy zabezpieczeń wbudowanych w sprzęt, oprogramowanie, w tym układowe, oraz w zbudowane z nich systemy. W obecnych czasach urządzenia informatyczne, oprogramowanie i systemy nie mogą funkcjonować bez zabezpieczeń, a ich wiarygodność jest kwestią niezwykle ważną.

Produkty lub systemy informatyczne cechujące się uzasadnionym zaufaniem mogą być wykorzystywane do odpowiedzialnych zastosowań, w środowiskach obarczonych zwiększonym poziomem ryzyka, do przetwarzania zasobów znacznej wartości lub do świadczenia usług o charakterze krytycznym – stanowią one podstawę do wcielania w życie idei społeczeństwa informacyjnego.

Artykuł przedstawia podstawowe informacje dotyczące samego standardu Common Criteria, prezentuje proces konstruowania zabezpieczeń, jak również produktów i systemów, do których są wbudowywane te zabezpieczenia, a także proces oceny prowadzącej do uzyskania certyfikatu i stosowania się do jego treści.

2. WPROWADZENIE DO ZAGADNIEŃ ZAWARTYCH W STANDARDZIE

Standard *Common Criteria for Information Security Evaluation* (Wspólne kryteria do oceny zabezpieczeń informatycznych) jest rozwijany przez międzynarodowe grono ekspertów. Podstawowa część dokumentów związanych ze standardem publikowana jest jako norma ISO/IEC. Obecnie obowiązuje wersja CC 3.1. Szczegółowe informacje i sam standard znajdują się na portalu Common Criteria [4].

Główny dokument składa się z trzech części:

- *ISO/IEC 15408-1 (CC Part 1): Introduction and General Model* zawiera: wprowadzenie do standardu, przyjęty model ogólny służący do ograniczania ryzyka i kreowania uzasadnionego zaufania oraz opis struktur podstawowych dokumentów, opracowywanych na potrzeby certyfikacji produktu lub systemu (czyli wspomnianego TOE), tj.: Zadania zabezpieczeń (ang. *ST – Security Target*) i Profilu zabezpieczeń (ang. *PP – Protection Profile*);
- *ISO/IEC 15408-2 (CC Part 2): Security Functional Requirements (SFR)* zawiera katalog komponentów funkcjonalnych (ang. *functional components*) służących do modelowania funkcjonalnych wymagań bezpieczeństwa, czyli wymagań wobec funkcji zabezpieczających; komponenty funkcjonalne zostały podzielone tematycznie na 11 klas (tab. 1); każda klasa dzieli się na rodziny, zaś dana rodzina zawiera komponenty precyzujące dane zagadnienie bezpieczeństwa;

Tabela 1
Klasy komponentów funkcjonalnych

Klasa	Nazwa pełna
FAU	Audyt bezpieczeństwa (ang. *Security Audit*)
FCO	Transmisja (ang. *Communication*)
FCS	Ochrona kryptograficzna (ang. *Cryptographic Support*)
FDP	Ochrona danych użytkownika (ang. *User Data Protection*)
FIA	Identyfikacja i uwierzytelnianie (ang. *Identification and Authentication*)
FMT	Zarządzanie bezpieczeństwem (ang. *Security Management*)
FPR	Prywatność (ang. *Privacy*)
FPT	Ochrona funkcji zabezpieczających (ang. *Protection of the TSF*)
FRU	Wykorzystanie zasobów (ang. *Resource Utilization*)
FTA	Dostęp do TOE (ang. *TOE Access*)
FTP	Wiarygodne ścieżki i kanały (ang. *Trusted path/channels*)

- *ISO/IEC 15408-3 (CC Part 3): Security Assurance Requirements (SAR)* zawiera katalog komponentów uzasadniających zaufanie (ang. *assurance components*), służących do modelowania wymagań uzasadniających zaufanie do funkcji zabezpieczających; komponenty zostały podzielone tematycznie na 8 klas (tab. 2); podobnie jak poprzednio, każda klasa dzieli się na rodziny, zaś w danej rodzinie występują hierarchicznie uporządkowane komponenty, wyrażające elementarne zagadnienia dotyczące kreowania uzasadnionego zaufania.

Dodatkowo dla konstruktorów zabezpieczeń opracowano przewodnik dla opracowujących zadania i profile zabezpieczeń [5] (zgodny z wersją 2.x standardu). Dla specjalistów oceniających zabezpieczenia powstała dwuczęściowa metodyka oceny CEM [6], która nie ma jednak statusu dokumentu ISO/IEC.

Tabela 2

Klasy komponentów uzasadniających zaufanie

Klasa	Nazwa pełna
APE	Ocena dokumentu PP (ang. *Protection Profile Evaluation*)
ASE	Ocena dokumentu ST (ang. *Security Target Evaluation*)
ADV	Prace badawcze i rozwojowe (ang. *Development*)
AGD	Dokumentacja (ang. *Guidance Documents*)
ALC	Wsparcie cyklu życia produktu (ang. *Life-Cycle Support*)
ATE	Testowanie (ang. *Tests*)
AVA	Oszacowanie podatności (*ang. Vulnerability Assessment*)
ACO	Systemy złożone (ang. *Composition*)

Znaczenie poziomów, czyli miar uzasadnionego zaufania jest interpretowane w sposób następujący:

- EAL7 – oznacza, że „projekt TOE został formalnie zweryfikowany i przetestowany" (ang. *formally verified design and tested*),
- EAL6 – oznacza, że „projekt TOE został półformalnie zweryfikowany i przetestowany" (ang. *semiformally verified design and tested*),
- EAL5 – oznacza, że „TOE był półformalnie projektowany i testowany"(ang. *semiformally designed and tested*),
- EAL4 – oznacza, że „TOE był metodycznie projektowany, testowany i przeglądany" (ang. *methodically designed, tested and reviewed*),
- EAL3 – oznacza, że „projekt TOE był metodycznie sprawdzany i testowany" (ang. *methodically tested and checked*),
- EAL2 – oznacza, że „TOE był testowany strukturalnie" (ang. *structurally tested*),
- EAL1 – oznacza, że „TOE był testowany funkcjonalnie" (ang. *functionally tested*).

Deklarowanym przez konstruktorów poziomom uzasadnionego zaufania dla TOE, odpowiadają w rzeczywistości tak zwane pakiety [3], czyli zbiory komponentów uzasadniających zaufanie (przedstawione w dalszej części artykułu).

3. KREOWANIE UZASADNIONEGO ZAUFANIA DLA PRODUKTU LUB SYSTEMU INFORMATYCZNEGO PODCZAS JEGO KONSTRUOWANIA

Podstawy uzasadnionego zaufania do produktów i systemów informatycznych są tworzone podczas ich konstruowania. Wyróżnia się dwa etapy:

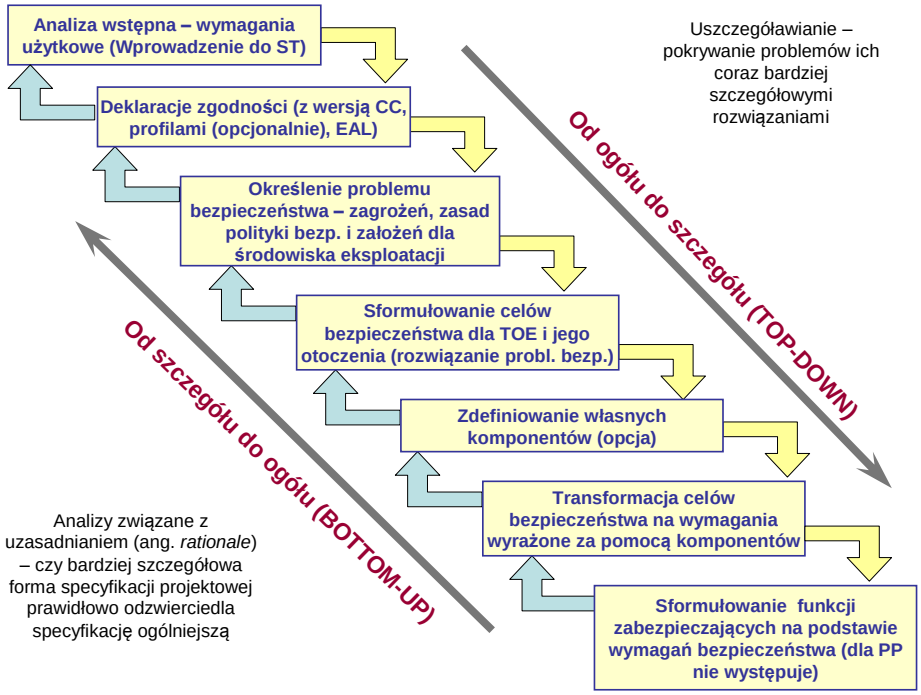
- proces konstruowania zabezpieczeń produktu lub systemu informatycznego, (ang. *TOE security development*); w jego wyniku zostaje wypracowany sformalizowany dokument zwany zadaniem zabezpieczeń (ST), którego istotną częścią jest specyfikacja funkcji zabezpieczających (ang. *TSS – TOE Summary Specification*),
- proces konstruowania przedmiotu oceny (ang. *TOE development*); obejmuje projekt implementacji tych funkcji zabezpieczających według przyjętej technologii i zgodnie z zadeklarowanym dla TOE poziomem uzasadnionego zaufania EAL.

3.1. Konstruowanie zabezpieczeń produktów lub systemów informatycznych

Należy podkreślić, że dany zbiór funkcji zabezpieczających, reprezentujący tak zwaną funkcjonalność zabezpieczeń przedmiotu oceny (ang. *TSF – TOE Security Functionality*) może być realizowany na dowolnym poziomie EAL, co wpływa na wiarygodność i koszt opracowania produktu lub systemu informatycznego. Z treści komponentów uzasadniających zaufanie, odpowiadających zadeklarowanemu poziomowi EAL wynika zakres i szczegółowość materiału dowodowego, który konstruktor powinien dostarczyć, a oceniający sprawdzić. W niektórych przypadkach istnieje konieczność dodania (ang. *addition*) do standardowego pakietu EALn pewnego dodatkowego komponentu lub zastąpienia któregoś z komponentów pakietu EALn komponentem bardziej rygorystycznym pochodzącym z wyższego EAL (ang. *augmentation*). Takie sytuacje oznaczane są jako EALn+.

Nieco uwagi należy poświęcić strukturze wspomnianego profilu zabezpieczeń (PP), która jest podobna do zadania zabezpieczeń, jednak nie zawiera ona funkcji zabezpieczających (TSS), zawsze ukierunkowanych na określoną technologię ich realizacji. Można przyjąć, że PP to oceniony zbiór wymagań bezpieczeństwa (SFR i SAR) bez wskazania na sposób ich implementacji w postaci funkcji zabezpieczających. Profile są tworzone w oparciu o wymagania klasy APE, zaś zadania zabezpieczeń w oparciu o wymagania klasy ASE (tab. 2). Profil zabezpieczeń jest więc pewnym abstrakcyjnym artefaktem, reprezentującym ocenione wymagania bezpieczeństwa dla całej rodziny produktów lub systemów. Można więc deklarować zgodność z ocenionymi (zarejestrowanymi) profilami przy tworzeniu zadań zabezpieczeń albo też innych profili.

Zadania zabezpieczeń mogą więc być tworzone bezpośrednio na podstawie profili, jednak typową, pełną ścieżką postępowania jest tworzenie ST od



Rys. 1. Przebieg procesu konstruowania zabezpieczeń przedmiotu oceny – wypracowanie treści zadania zabezpieczeń

podstaw, zaczynając od analizy wymagań i oczekiwań przyszłych klientów. Ten rodzaj procesu konstruowania zabezpieczeń produktu lub systemu informatycznego zawiera następujące fazy, którym odpowiadają poszczególne sekcje dokumentu ST (rys. 1):

1. Analiza wstępna produktu lub systemu informatycznego i opracowanie sekcji pt. „Wprowadzenie do zadania zabezpieczeń" (ang. *ST Introduction*), zawierającej różnego typu identyfikatory i opisy charakteryzujące TOE i jego zastosowanie. Na marginesie należy wspomnieć, że informacje tam zawarte służą nie tylko celom identyfikacji, lecz jako „informacje dla zarządu", są pomocne różnym decydentom w wyborze odpowiednich produktów do swoich potrzeb.
2. Opracowanie deklaracji zgodności (ang. *Conformance claims*) – ze stosowaną wersją standardu (obecnie jest to wersja CC 3.1), z profilami zabezpieczeń i z pakietem EALn, czasem z EALn+.
3. Zdefiniowanie problemu bezpieczeństwa dla TOE (ang. *Security problem definition*), w starszej wersji standardu określane mianem „otoczenia zabezpieczeń" – ang. *Security environment*). Obejmuje to identyfikację zagrożeń dla TOE i jego otoczenia, określenie zasad polityki bezpieczeństwa dla TOE oraz przyjęcie założeń warunkujących bezpieczeństwo TOE odnoszących się do jego środowiska eksploatacji).
4. Sformułowanie celów bezpieczeństwa (ang. *Security objectives*) dla TOE i otoczenia na podstawie analizy problemu bezpieczeństwa i ich uzasadnienie. Cele stanowią rozwiązanie zidentyfikowanego wcześniej problemu bezpieczeństwa.
5. Zdefiniowanie własnych, specyficznych komponentów funkcjonalnych lub uzasadniających zaufanie zgodnie z konwencją stosowaną przez twórców standardu (ang. *Extended components definition*), gdyby nie było odpowiednich komponentów w katalogu [2] lub w katalogu [3].
6. Wypracowanie i uzasadnienie specyfikacji wymagań bezpieczeństwa (ang. *SFR – Security functional requirements and SAR – Security assurance requirements*), czyli wyrażenie celów dla TOE za pomocą komponentów funkcjonalnych typu SFR i określenie wymagań uzasadniających zaufanie typu SAR, określających podstawy zaufania, że przedmiot oceny spełni wymagania SFR. Wymagania SAR wynikają głównie z deklarowanego poziomu EAL.
7. Wypracowanie i uzasadnienie specyfikacji końcowej (ang. *TSS – TOE summary specification*) zadania zabezpieczeń, zawierającej zbiór funkcji zabezpieczających, które pokazują w jaki sposób poszczególne wymagania są realizowane, np. komponent FCS_COP.1 dotyczący operacji kryptograficznych może być zaimplementowany w postaci funkcji zabezpieczających różniących się stosowanym algorytmem czy długością stosowanych kluczy, itp.).

Podstawowe, a zarazem najtrudniejsze do wykonania fazy konstruowania zabezpieczeń to fazy: 3, 4, 6

i 7. Każda z faz 4, 6 i 7 wymaga tak zwanego uzasadnienia (ang. *rationale*), wykazującego, że elementy specyfikacji w danej fazie są konieczne i wystarczające do pokrycia elementów specyfikacji fazy poprzedniej.

W zasadzie proces konstruowania zabezpieczeń ma charakter zstępujący (ang. *Top-down*), choć wymagane analizy i uzasadnienia powodują konieczność przejścia do wcześniejszej fazy i wprowadzenia stosownych poprawek.

Tworzenie dokumentów ST i PP (od podstaw) przebiega podobnie, przy czym faza 7 dla PP nie występuje, natomiast działania opisane w tej fazie stanowią podstawowe działania przy tworzeniu ST na podstawie ocenionego PP. Począwszy od wersji 3.0 wprowadzono uproszczone wersje PP i ST (ang. *low assurance PP/ST*), które mogą być stosowane wyłącznie dla EAL1. Tworzenie uproszczonego ST obejmuje fazy 1, 2, 5, 6 i 7, zaś uproszczonego PP fazy 1, 2, 5 i 6.

W pracach [7-12] wprowadzono modele półformalne procesu konstruowania zabezpieczeń oraz język do wyrażania specyfikacji bezpieczeństwa, obejmujący komponenty zdefiniowane przez standard oraz wprowadzone przez autora tak zwane udoskonalone generyki (ang. *enhanced generics*), dorównujące możliwościami komponentom, a służące do specyfikowania tych faz konstruowania, dla których standard nie podaje środków specyfikacji (zasobów, podmiotów, zagrożeń, założeń, reguł polityki, celów bezpieczeństwa i funkcji zabezpieczających).

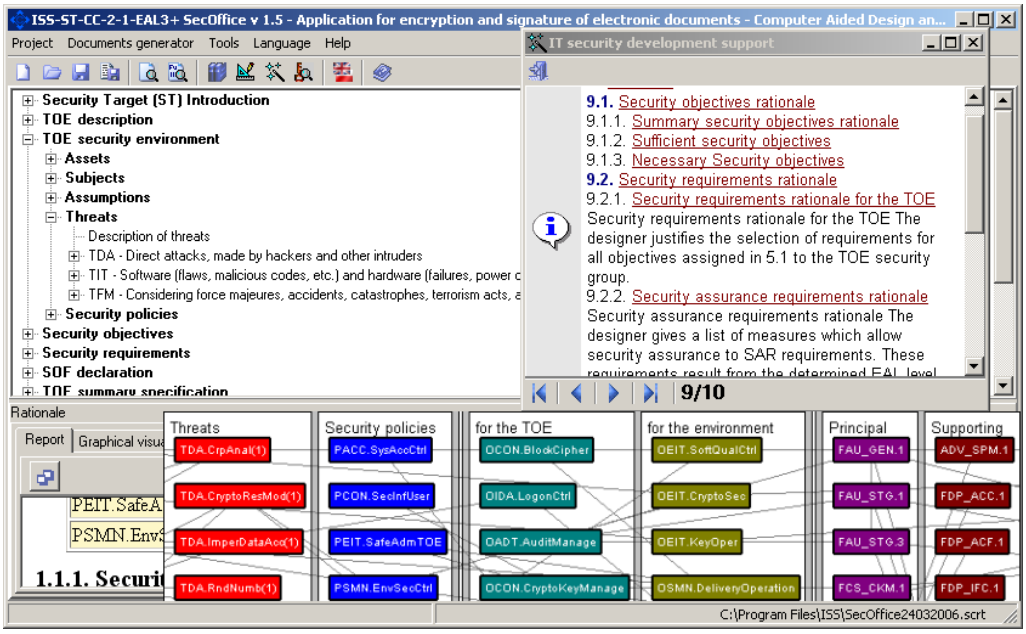
Wyniki tych prac wykorzystano w Instytucie Systemów Sterowania do zbudowania narzędzia automatyzującego procesy konstruowania i oceny zabezpieczeń SecCert (rys. 2), zgodnego z wersją CC 2.1.

W pracy [13] zaprezentowano podejście ontologiczne do realizacji procesu konstruowania zabezpieczeń.

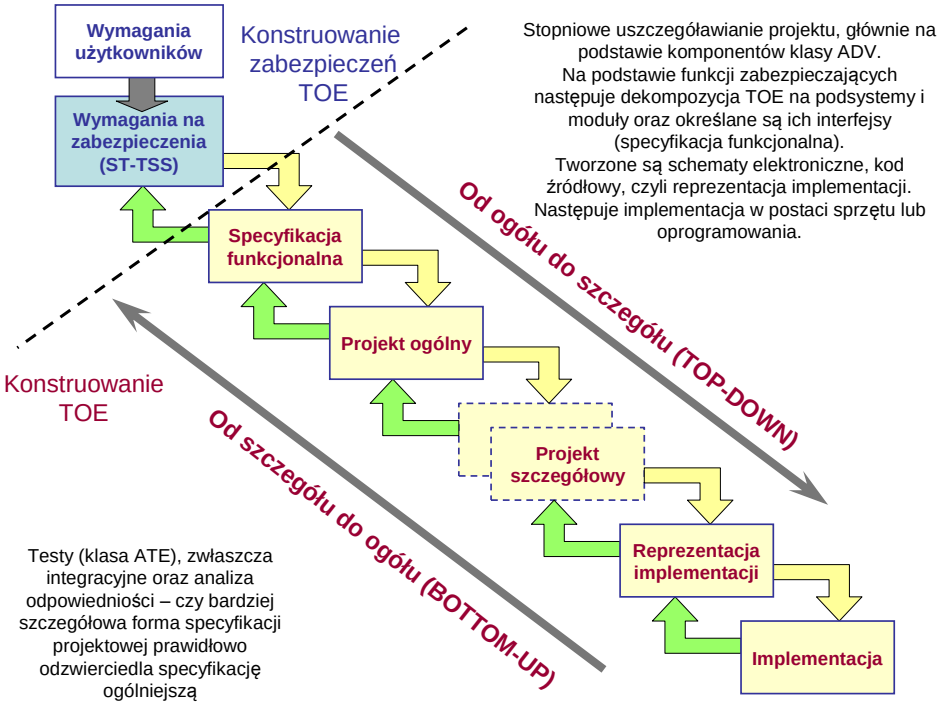
3.2. Konstruowanie produktów lub systemów informatycznych według standardu Common Criteria

Przebieg procesu konstruowania produktu lub systemu informatycznego w świetle ISO/IEC 15408 przedstawiono na rys. 3.

Ogólnie ma on charakter zstępujący z możliwością powrotu do etapu bardziej ogólnego celem wprowadzenia poprawek wynikających z testów, czy też tak zwanych analiz odpowiedniości. Proces konstruowania TOE oparty jest na treści zadania zabezpieczeń (ST), które w swej końcowej sekcji (TSS) zawiera zbiór funkcji zabezpieczających, który jest implementowany zgodnie z rygorem wynikającym z zadeklarowanego poziomu EAL, zaś od tego poziomu zależy zakres i szczegółowość materiału dowodowego.



Rys. 2. Okienko aplikacji SecCert, służącej do wspomagania procesu konstruowania zabezpieczeń. Lewa górna część okienka przedstawia strukturę zadania zabezpieczeń dla aplikacji kryptograficznej SecOffice i trzy przykładowe dotyczące jej zagrożenia, wyrażone za pomocą tak zwanych udoskonalonych generyków. Prawa górna część rysunku przedstawia kreator projektów, zaś dolna część wizualizuje relacje pokrycia między elementami specyfikacji (generykami i komponentami)



Rys. 3. Przebieg procesu konstruowania przedmiotu oceny na podstawie specyfikacji funkcji zabezpieczających zawartych w dokumencie zadania zabezpieczeń

Materiał ten, przedkładany do oceny wraz z opracowanym produktem lub systemem informatycznym (TOE), wynika z treści komponentów uzasadniających zaufanie i może przybierać różną postać.

Materiał dowodowy może być dokumentem, np. planem zarządzania konfiguracją, podręcznikiem użytkownika lub administratora, procedurą instalacji lub kalibracji urządzenia, czy też dokumentacją opisującą cykl życia produktu lub systemu. Udokumentowane wyniki niezależnych badań lub obserwacji, np. raport dotyczący analizy podatności TOE i jego środowiska rozwojowego, raport z niezależnego testowania TOE, raport z inspekcji środowiska rozwojowego TOE przeprowadzonej przez przedstawicieli niezależnego laboratorium oceniającego, czy też lista rankingowa przypadków ryzyka zidentyfikowanych w środowisku rozwojowym są również materiałem dowodowym.

Innym przykładem materiału dowodowego może być stwierdzone zachowanie lub postępowanie osób pełniących określone role w cyklu życia TOE, np. stosowanie określonej procedury (akceptacji produktu lub systemu przed wysłaniem do klienta). Tego typu dowodem może być też protokół, notatka czy tak zwane zapisy (ang. *records*), czyli różnego typu ślady operacji odnotowywane przez system zarządzania.

Materiał dowodowy tworzony jest na podstawie zagadnień zawartych w komponentach uzasadniających zaufanie, uporządkowanych w postaci klas i ich rodzin (tab. 2). Każdy komponent uzasadniający zaufanie zawiera tak zwane elementy, które określają:

- jaki artefakt (dowód na spełnienie wymagania wyrażonego przez komponent) konstruktor powinien dostarczyć (element D), na przykład opracować określony dokument lub jego część,
- jaką postać powinien mieć i co ma zawierać ten artefakt (element C),
- w jaki sposób dostarczony element o określonej postaci będzie sprawdzany przez oceniającego (element E).

Zauważmy, że dla klasy ASE materiałem dowodowym jest zadanie zabezpieczeń, zaś dla APE – profil zabezpieczeń. Nietypową klasą jest klasa ACO dotycząca dekompozycji. W pewnym uproszczeniu można stwierdzić, że ma ona zastosowanie w przypadkach, gdy konstruowany TOE zawiera w sobie inne, wcześniej już ocenione TOE. Pozostałe klasy związane są z przedmiotem oceny, czyli z TOE, a także z jego środowiskiem rozwojowym, ściślej ze środowiskiem obejmującym cały cykl życia TOE. Uwzględnienie tego środowiska jest istotne, gdyż środowisko w którym TOE jest konstruowany, wytwarzany, serwisowany, itp., wpływa na zaufanie, jakim przyszli klienci mogą go obdarzać.

Tabela 3, opracowana na podstawie podobnej tabeli, zawartej w trzeciej części standardu [3], przedstawia komponenty uzasadniające zaufanie odnoszące się bezpośrednio do TOE (pominięto klasy APE, ASE, ACO).

Kolumny zawierają komponenty wchodzące w skład danego pakietu EAL, zaś wiersze przedstawiają komponenty danych rodzin. Zamiast pełnej nazwy komponentu podany jest tylko jego numer w ramach danej rodziny. Na przykład, rodzina ADV_ARC zawiera tylko jeden komponent ADV_ARC.1, z kolei rodzina ADV_FSP posiada sześć komponentów: ADV_FSP.1, ADV_FSP.2, ADV_FSP.3, ADV_FSP.4, ADV_FSP.5 oraz ADV_FSP.6. Komponenty w ramach rodziny są zawsze ułożone hierarchicznie. Ponadto, komponent o numerze wyższym – bardziej rygorystyczny – zawiera wszystkie wymagania niższego (kumulacja wymagań).

W poszczególnych kolumnach pokazano komponenty wchodzące w skład pakietów (poziomów) EAL. Na przykład EAL1 zawiera tylko siedem komponentów: ADV_FSP.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.1, ALC_CMS.1, ATE_IND.1 i AVA_VAN.1, zaś EAL2 zawiera już ich dwanaście: ADV_ARC.1, ADV_FSP.2, ADV_TDS.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.2, ALC_CMS.2, ALC_DEL.1, ATE_COV.1, ATE_FUN.1, ATE_IND.2 i AVA_VAN.2, przy czym niektóre ze wskazanych dla EAL1 wymieniono na komponenty bardziej rygorystyczne (o wyższym numerze).

Przegląd i ogólne zasady tworzenia materiału dowodowego przedstawiono w pracy [14]. Najczęściej materiał dowodowy jest organizowany tematycznie według zagadnień bezpieczeństwa zamkniętych w poszczególnych rodzinach komponentów. Przy jego tworzeniu korzysta się z różnego typu wzorców opracowanych w danej firmie oraz jej *know-how*. Ciężar opracowania większości materiału dowodowego spoczywa na konstruktorach, z wyjątkiem materiału dla ATE_IND, czyli raportu z przeprowadzenia w laboratorium niezależnych testów i dla AVA_VAN, czyli raportu z wykonanej tam analizy podatności.

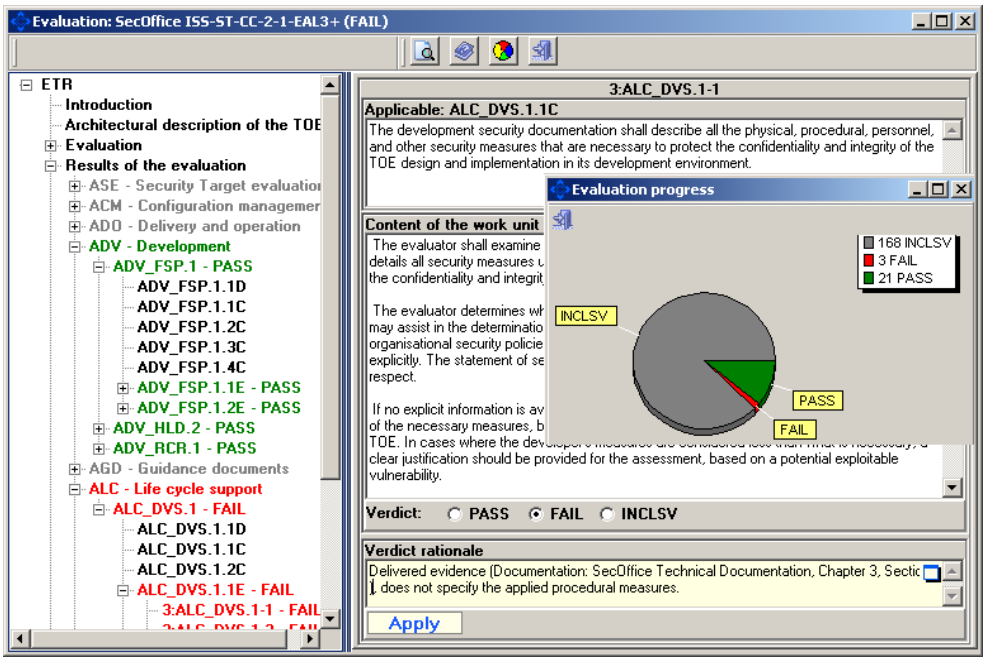
4. OCENA I CERTYFIKACJA PRODUKTÓW I SYSTEMÓW INFORMATYCZNYCH

Ocena produktu lub systemu informatycznego oraz dostarczonego materiału dowodowego jest prowadzona przez niezależnych ekspertów w akredytowanym i wyspecjalizowanym w danej dziedzinie laboratorium. Odbywa się ona w oparciu o przyjęty dla danego kraju tak zwany schemat certyfikacji i z wykorzystaniem metodyki oceny [6]. Wspomniano już wcześniej o trzech elementach D, C i E zawartych w komponentach uzasadniających zaufanie (SAR). W pewnym uproszczeniu, metodyka oceny dostarcza

Tabela 3

Komponenty uzasadniające zaufanie odnoszące się do przedmiotu oceny

Klasa	Rodzina	Poziom uzasadnionego zaufania						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
ADV	ADV_ARC (Architektura systemu)		1	1	1	1	1	1
	ADV_FSP (Specyfikacja funkcjonalna)	1	2	3	4	5	5	6
	ADV_IMP (Reprezentacja implementacji)				1	1	2	2
	ADV_INT (Wewn. struktura funkcji zabezp.)					2	3	3
	ADV_SPM (Model polityki bezpieczeństwa)						1	1
	ADV_TDS (Projekt TOE)		1	2	3	4	5	6
AGD	AGD_OPE (Dokumentacja użytkowa)	1	1	1	1	1	1	1
	AGD_PRE (Procedury przygotowawcze)	1	1	1	1	1	1	1
ALC	ALC_CMC (Możliwości systemu zarządz. konfiguracją	1	2	3	4	4	5	5
	ALC_CMS (Zakres zarządz. konfiguracją	1	2	3	4	5	5	5
	ALC_DEL (Procedury dostawy)		1	1	1	1	1	1
	ALC_DVS (Bezp. środow. rozwojowego)			1	1	1	2	2
	ALC_FLR (Usuwanie usterek)	opcjonalne dla dowolnego EAL						
	ALC_LCD (Definicja cyklu życia)			1	1	1	1	2
	ALC_TAT (Narzędzia konstruktora)				1	2	3	3
ATE	ATE_COV (Pokrycie TOE testami)		1	2	2	2	3	3
	ATE_DPT (Głębokość testowania)			1	2	3	3	4
	ATE_FUN (Testy funkcjonalne)		1	1	1	1	2	2
	ATE_IND (Testowanie niezależne)	1	2	2	2	2	2	3
AVA	AVA_VAN (Analiza podatności)	1	2	2	3	4	5	5



Rys. 4. Okienko aplikacji SecCert, służącej do wspomagania procesu oceny zabezpieczeń. Lewa część okienka przedstawia wybrane, oceniane komponenty klas ADV i ALC zadania zabezpieczeń dla aplikacji kryptograficznej SecOffice, zaś prawa pokazuje szczegóły aktualnie rozpatrywanej jednostki oceny ALC_DVS.1-1. Oceniający wydał werdykt negatywny wraz uzasadnieniem. W prawej części występuje dodatkowe, nałożone okienko pokazujące postępy procesu oceny

uszczegółowienia elementów E i określa tak zwane jednostki oceny (ang. *work unit*). Sprowadza się to do dostarczenia zbioru zagadnień (zapytań) dotyczących treści i postaci materiału dowodowego. Te elementarne zagadnienia są ocenialne – można im przypisać tak zwane werdykty z zastosowaniem logiki trójwartościowej: *Pass* (werdykt pozytywny), *Fail* (werdykt negatywny) i *Inconclusive* (kwestia nierozstrzygalna). Każdy z werdyktów wymaga zwięzłego uzasadnienia (ang. *verdict rationale*). Na rys. 4 pokazano przykład dotyczący oceny wspomaganej komputerowo z wykorzystaniem wspomnianego wcześniej narzędzia SecCert. Należy zwrócić uwagę na konieczność uzyskania ocen pozytywnych dla wszystkich jednostek oceny występujących w ramach danego projektu. Nie jest to zadanie łatwe i wymaga współpracy oceniających i konstruktorów w bieżącym usuwaniu braków w projekcie.

Pozytywny wynik oceny TOE i jego materiału dowodowego, zweryfikowany dodatkowo przez jednostkę akredytującą dane laboratorium, pozwala na wydanie stosownego certyfikatu. Certyfikaty są publikowane w portalu Common Criteria [4]. Są tam umieszczane dokumenty zadań zabezpieczeń i profili zabezpieczeń oraz raporty z procesu oceny z dołączonymi certyfikatami. Z informacji tych korzystają klienci, poszukujący produktów o odpowiedniej funkcjonalności i wiarygodności, użytkownicy, poszukujący wskazówek dotyczących eksploatacji, menadżerowie, sponsorzy, konstruktorzy i oceniający inne produkty.

Obecnie (stan na dzień 16.11.2008) certyfikaty uzyskało 929 produktów lub systemów informatycznych oraz zarejestrowano 128 profili zabezpieczeń. Są one podzielone na następujące kategorie (w nawiasach, pierwsza liczba określa liczbę produktów lub systemów, druga liczbę profili zabezpieczeń):

1) Access Control Devices and Systems (35/2),
2) Boundary Protection Devices and Systems (90/16),
3) Data Protection (37/0),
4) Databases (37/6),
5) Detection Devices and Systems (21/12),
6) Products for Digital Signatures (44/5),
7) ICs, Smart Cards and Smart Card related Devices and Systems (243/32),
8) Key Management Systems (24/2),
9) Network and Network related Devices and Systems (79/12),
10) Operating systems (84/9),
11) Other Devices and Systems (250/33).

W tabeli 4 podano liczbę wydanych certyfikatów dla określonych poziomów EAL w poszczególnych latach. Co roku wydawanych jest około 200 takich certyfikatów, a poza tym rejestrowanych jest kilkanaście profili (tabela ich nie obejmuje). Najczęściej wydawane są certyfikaty z zakresu środka skali EAL. Dla najwyższych poziomów EAL liczba ta jest znikoma, co świadczy o olbrzymich trudnościach w stosowaniu metod formalnych, które wówczas są wymagane.

Tabela 4

Liczba certyfikowanych produktów i systemów informatycznych w ostatnich latach, według poziomów EAL [4] – stan na dzień 16.11.2008

EAL	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	Total
EAL1	0	0	4	1	0	3	5	2	1	5	7	3	31
EAL1+	0	0	4	3	9	2	0	0	0	0	1	1	20
EAL2	0	1	1	1	2	7	7	17	45	38	31	18	168
EAL2+	0	0	0	1	0	5	4	5	7	13	25	19	79
EAL3	0	0	2	2	3	3	3	13	14	18	39	12	109
EAL3+	1	0	0	0	1	0	2	17	13	24	16	5	79
EAL4	0	1	1	5	4	12	14	8	10	13	14	3	85
EAL4+	0	0	0	9	7	15	17	25	43	47	73	43	279
EAL5	0	0	0	0	0	0	2	1	1	0	3	0	7
EAL5+	0	0	0	0	1	6	3	4	12	10	15	19	70
EAL7	0	0	0	0	0	0	0	0	1	0	0	0	1
EAL7+	0	0	0	0	0	0	0	0	0	1	0	0	1
Total	1	2	12	22	27	53	57	92	147	169	224	123	929

Stosowanie standardu i związaną z tym współpracę międzynarodową reguluje porozumienie CCRA (*Common Criteria Recognition Arrangement*), podpisane przez ponad 20 krajów. Liczbę laboratoriów komercyjnych w poszczególnych krajach podano poniżej w nawiasach (2008). Są to kraje wiodące w tej dziedzinie, które w pełni wdrożyły standard i mają status „*Certificate Authorizing*":
Australia i Nowa Zelandia (3),
Kanada (3),
Francja (5),
Niemcy (12),
Japonia (4),
Republika Korei (3),
Holandia (1),
Norwegia (2),
Hiszpania (3),
Szwecja (2),
Wielka Brytania (4),
USA (9).

Pozostałych 12 sygnatariuszy Umowy CCRA, czyli takie kraje, jak: Austria, Czechy, Dania, Finlandia, Grecja, Węgry, Indie, Izrael, Włochy, Malezja, Singapur oraz Turcja nie wdrożyły jeszcze w pełni standardu i posiadają status „*Certificate Consuming*". Nasz kraj wykazuje ogromne opóźnienie w tej dziedzinie i nie należy ani do pierwszego, ani do drugiego grona państw.

Liczba akredytowanych laboratoriów oceny, działających na zasadach komercyjnych, świadczy o zaawansowaniu danego kraju w rozwijaniu inżynierii zabezpieczeń, jak również o wielkości samego rynku w danym kraju. Ze względu na globalizację i ścisłą specjalizację technologiczną laboratoriów zdarza się, że produkty powstałe w danym kraju są kierowane do oceny w innym kraju.

PODSUMOWANIE

W artykule przedstawiono zarys zagadnień dotyczących budowy podstaw zaufania do produktów lub systemów informatycznych. W świetle ISO/IEC 15408 źródłem tego zaufania jest rygorystyczny proces konstruowania i niezależna ocena w akredytowanym laboratorium. Metodykę tę należy uznać za metodykę dojrzałą, ale i ciągle doskonaloną na podstawie gromadzonych doświadczeń. Mimo że metodyka jest uznawana za specjalistyczną i dość trudną do opanowania, to obecnie nie ma ona alternatywy i przynosi wiele korzyści, spośród których można wymienić:

- wymuszenie starannego projektowania i dokumentowania produktu lub systemu, stosowania przez informatyków i elektroników dobrych praktyk i zasad inżynierskich,
- zwiększenie zaufania do produktów lub systemów informatycznych, zwłaszcza po ocenie prowadzonej w trakcie tworzenia produktu lub systemu,
- zmniejszenie ryzyka stosowania środków informatycznych do zadań biznesowych – częstsze wykorzystywanie ocenionych produktów do budowy złożonych systemów przeznaczonych do najbardziej odpowiedzialnych zastosowań,
- ułatwienie użytkownikom wyboru i zakupu produktów lub systemów o właściwie dobranym poziomie uzasadnionego zaufania,
- wejście na obce rynki – certyfikaty mają zasięg międzynarodowy, więc kosztownego procesu oceny nie trzeba powtarzać w różnych krajach.

Standard ISO/IEC 15408 dostarcza jednolitego, półformalnego języka do opisu własności zabezpieczeń produktów i systemów informatycznych oraz

kryteriów będących podstawą oceny tych własności. Umożliwia to porównywanie wyników ocen produktów. Wiedzę inżynierską i wzorcowe praktyki zawarte w standardzie i dokumentach związanych można wykorzystywać do konstruowania szerokiego spektrum produktów i systemów informatycznych, niekoniecznie z myślą o ich późniejszej certyfikacji.

Grono korzystających ze standardu jest dość szerokie. Nabywcy rozwiązań teleinformatycznych zainteresowani są dokumentami zadań zabezpieczeń oraz raportami z przebiegu ocen. Pomaga im to dobrać, pod względem funkcjonalności i wiarygodności, właściwy produkt do zaspokojenia własnych, zidentyfikowanych potrzeb. Zdarza się, że standard pozwala sprecyzować wymagania bezpieczeństwa w aktach prawnych. Na przykład europejski dokument [15] podaje wzór zadania zabezpieczeń dla tachografu cyfrowego. Powołania na określony poziom EAL można spotkać w rodzimych przepisach (rozporządzeniach), na przykład dotyczących podpisu elektronicznego. Zdarza się, że w ogłaszanych przetargach spotyka się w ten sposób określone wymagania bezpieczeństwa – również w Polsce, która do tej pory standardu nie wdrożyła.

Twórcy produktów lub systemów (programiści, architekci, konstruktorzy), korzystając ze standardu, mogą precyzyjnie określać wymagania bezpieczeństwa oraz wyrażać i oceniać funkcjonalność zabezpieczeń. Podobnie oceniający są w stanie jednoznacznie formułować osądy na temat zgodności produktu z wymaganiami na zabezpieczenia. Z kolei administratorzy systemów uzyskują wytyczne dotyczące eksploatacji, tak by podczas eksploatacji TOE sprostać wymaganiom wynikającym z poziomu EAL. Do grona użytkowników standardu należą także: audytorzy, architekci zabezpieczeń, osoby akredytujące systemy, nadzorujące ocenę oraz sponsorzy, finansujący proces konstruowania i oceny.

Standard ISO/IEC 15408 ma coraz szersze zastosowanie – związane ogólnie z opracowywaniem, wytwarzaniem i utrzymywaniem produktów lub systemów informatycznych, którym powierza się zasoby znacznej wartości, a które przy tym są narażone na różnego typu zagrożenia zewnętrzne. Nie muszą to być wcale klasyczne produkty lub systemy informatyczne kojarzone z bezpieczeństwem, takie jak system zaporowy, szyfrator, czy karta procesorowa. Ogólnie są to wytwory myśli inżynierskiej informatyków i elektroników, wspomaganych przez specjalistów z innych dziedzin.. W ostatnim czasie rysują się nowe, dotąd nietypowe możliwości zastosowań, dotyczące systemów wbudowanych, czujników inteligentnych. Możliwości te rysują się także w zaawansowanych obszarach elektroniki i automatyki górniczej.

Literatura

1. ISO/IEC 15408-1, Information technology – Security techniques – Evaluation criteria for IT security – Introduction and general model (Common Criteria Part 1).
2. ISO/IEC 15408-2, Information technology – Security techniques – Evaluation criteria for IT security – Security functional requirements (Common Criteria Part 2).
3. ISO/IEC 15408-3, Information technology – Security techniques – Evaluation criteria for IT security – Security assurance requirements (Common Criteria Part 3).
4. Common Criteria portal: http://www.commoncriteriaportal.org/
5. ISO/IEC TR 15446 Guide for the production of protection profiles and security targets.
6. Common Evaluation Methodology for Information Technology Security (Part 1-2).
7. *Białas A*.: Semiformal Common Criteria Compliant IT Security Development Framework. Studia Informatica vol. 29, Number 2B(77), Silesian University of Technology Press, Gliwice 2008.
8. *Białas A*.: IT security development – computer-aided tool supporting design and evaluation. W: Kowalik J., Górski J., Sachenko A. (eds.): Cyberspace Security and Defense. vol. 196, Springer Verlag, Heidelberg 2005, s. 3-23.
9. *Białas A*.: A semiformal approach to the security problem of the target of evaluation (TOE) modeling. W: Arabnia H., Aissi S. (Eds), Vert G., Williams P. (Assoc. Co Eds): Proc. of the 2006 Int. Conf. on Security and Management. CSREA Press, Las Vegas 2006, s. 19-25.
10. *Białas A*.: Semiformal Approach to the IT Security Development. W: Zamojski W., Mazurkiewicz J., Sugier J., Walkowiak T.: Proceedings of the International Conference on Dependability of Computer Systems DepCoS-RELCOMEX 2007. IEEE Computer Society, Los Alamitos, Washington, Tokyo, s. 3-11.
11. *Białas A*.: Modeling the Security Objectives According to the Common Criteria Methodology. W: Aissi S., Arabnia H. (Editors), Daimi K., Gligoroski D., Markowsky G., Solo A.,M.,G. (Assoc. Co Eds), Proc. of the 2007 Int. Conf. on Security and Management. CSREA Press, Las Vegas 2007, s. 223-229.
12. *Białas A*.: Semiformal framework for ICT security development. The 8th International Common Criteria Conference (ICCC). Rome, 25-27 September 2007.
13. *Białas A*.: Ontology-based Approach to the Common Criteria Compliant IT Security Development. W: Proceedings of the 2008 International Conference on Security and Management – SAM'08 (The World Congress In Applied Computing). June, Las Vegas 2008.
14. *Białas A*.: Podstawy zaufania do produktu lub systemu informatycznego, Rozdział w: Grzywak A., Kapczyński A. (Praca zbiorowa pod red. naukową): Zastosowanie Internetu w społeczeństwie informacyjnym, Wydawnictwo Wyższej Szkoła Biznesu w Dąbrowie Górniczej, 2008, pp. 187-201.
15. Annex 1B of Commission Regulation (EC) No.1360/2002 on recording equipment in road transport: Requirements for Construction, Testing, Installation and Inspection (in: Official Journal of the European Communities, L 207 / 1 ff.), Commission of the European Communities, 05.08.2002, appendix 10, chapter 3.2.

Recenzent: dr Włodzimierz Boroń