STUDIA INFORMATICA 2001
Volume 22 Number 1 (43)

Andrzej BIAŁAS
SOTEL - Centrum Inżynierii Bezpieczeństwa Systemów Komputerowych
i Telekomunikacyjnych

WPROWADZENIE DO PROBLEMATYKI PROJEKTOWANIA I OCENY ZABEZPIECZEŃ TELEINFORMATYCZNYCH

Streszczenie. Artykuł poświęcono problematyce oceny zabezpieczeń teleinformatyki, opartej na Wspólnych Kryteriach (ISO 15408). Omówiono przyjęty model bezpieczeństwa oraz proces jego konkretyzacji do dwóch wzorcowych specyfikacji wymagań. Przedstawiono zasady konstruowania specyfikacji formalnych na podstawie komponentów z katalogów komponentów funkcjonalnych oraz uzasadniających zaufanie. Na przykładzie pokazano zasady wydawania werdyktów podczas prowadzenia ocen.

INTRODUCTION TO INFORMATION TECHNOLOGY SAFEGUARDS DESIGN AND EVALUATION

Summary. The paper deals with IT Security Evaluation according to CC – Common Criteria (ISO 15408). General model was presented and its compilation process to formal specifications: Security Target (ST) and Protection Profile (PP). Functional and assurance components catalogues were discussed. Evaluation process and verdicts assignments were illustrated by an example.

1. Wprowadzenie

Celem niniejszego artykułu jest przybliżenie problematyki projektowania, oceny i certyfikacji bezpieczeństwa środków teleinformatycznych według aktualnie rozwijanej i wdrażanej rodziny norm międzynarodowych pt. **Wspólne Kryteria do Oceny Zabezpieczeń** (*ang. CC – Common Criteria for Information Technology Security Evaluation*) [1-6], które w grudniu ubiegłego roku uzyskały status standardu ISO (**ISO/IEC 15408: Information Technology – Security Techniques – Evaluation criteria for IT**

security). Powstały wysiłkiem międzynarodowym z ujednolicenia standardów lokalnych [11],[12],[13].

Wstępnie przez pojęcie certyfikacji należy rozumieć ocenę środków teleinformatycznych prowadzoną przez niezależną, prestiżową instytucję wg uzgodnionych procedur i kryteriów, w zakresie spełnienia zakładanych wymagań dotyczących poufności, integralności i dostępności informacji, poświadczającą, że produkt zwany tu Przedmiotem Oceny:

- realizuje prawidłowo określone funkcje bezpieczeństwa (występują w nim zamierzone i pożądane zachowania),
- posiada mierzalny poziom wiarygodności – zaufania (brak w nim niepożądanych zachowań).

Stosowanie środków teleinformatycznych do wytwarzania, przetwarzania, przesyłania i przechowywania informacji jest zawsze związane z pewnym ryzykiem. Certyfikacja minimalizuje to ryzyko, gdyż produkty są wnikliwie oceniane pod kątem ich zdolności do zapewnienia poufności, integralności i dostępności informacji przed ich zastosowaniem. Przedmiotami Oceny (*ang. TOE – Target of Evaluation*) mogą być:

- środki sprzętowe, np. kryptoprocesory,
- środki programowe, np. szyfratory plików,
- ich kombinacje, np. system operacyjny współpracujący z kartami inteligentnymi,
- aplikacje, np. bazodanowe,
- narzędzia do rozwoju innych produktów.

W toku skomplikowanego procesu niezależne służby, zwykle państwowe lub będące pod kontrolą państwa, dokonują szeroko pojętej oceny produktu i poświadczają swym autorytetem zgodność produktu z obowiązującymi wymaganiami oraz możliwość jego zastosowania w określonych warunkach. Pomaga to użytkownikom przy wyborze i zakupie środków teleinformatycznych o adekwatnym dla danego zastosowania poziomie bezpieczeństwa.

Poddanie produktu procesowi ocen i certyfikacji przynosi wiele korzyści, głównie technicznych i marketingowych:

- certyfikacja wymusza staranne opracowanie dokumentacji,
- certyfikacja, zwłaszcza towarzysząca tworzeniu produktu, znacząco podnosi jego jakość i bezpieczeństwo,
- może być wykorzystana w celach reklamowych jako argument w rozmowach handlowych, na seminariach, przez co wpływa na zwiększenie sprzedaży,
- dzięki międzynarodowemu zasięgowi standardów produkty certyfikowane łatwiej wchodzą na obce rynki.

Certyfikacja środków teleinformatycznych stała się możliwa po opracowaniu kryteriów opisu i oceny produktów o szerokim zasięgu międzynarodowym tak, aby wyniki ocen były porównywalne i maksymalnie niezależne od gremiów oceniających.

Dokument normatywny składa się z trzech podstawowych części:

- **Common Criteria – Part 1: Introduction and general model** (Wprowadzenie i model ogólny) [1], [6]. Przedstawia przyjęty model bezpieczeństwa, który ma odzwierciedlenie w specyfikacjach wymagań bezpieczeństwa opisanych w jego załącznikach. Część pierwsza prezentuje także konstrukcje pomagające artykułować cele bezpieczeństwa i tworzyć specyfikacje produktów na wysokim poziomie abstrakcji.
- **Common Criteria – Part 2: Security functional requirements** [2] (Wymagania dotyczące funkcjonalności zabezpieczeń). Część drugą poświęcono tworzeniu funkcjonalnych modeli bezpieczeństwa (wymagań funkcjonalnych zabezpieczeń) dla przedmiotu oceny. Zawiera ona **katalog komponentów funkcjonalnych** (*ang. functional components*) podzielonych na rodziny i klasy, za pomocą których modeluje się bezpieczeństwo środków teleinformatycznych, czyli wspomniane ich pożądane zachowanie.
- **Common Criteria – Part 3: Security assurance requirements** [3] (Wymagania dotyczące uzasadnienia zaufania do zabezpieczeń). Część trzecia poświęcona jest ocenie zaufania (wiarygodności) tworzonych modeli. Zawiera ona katalog **komponentów uzasadniających zaufanie** (*ang. assurance components*), również podzielonych na rodziny i klasy, służące do określenia wymagań na uzasadnienie zaufania do TOE. W części tej przedstawiono kryteria oceny dokumentów formalnych określających wymagania dla zabezpieczeń, a także zdefiniowaną skalę poziomów uzasadnionego zaufania (miary wiarygodności) EAL1-EAL7 (*ang. EAL – Evaluation Assurance Level*).

Dokumentami uzupełniającymi są:

- **Common Criteria Evaluation Methodology (CEM) – Part 2: Evaluation Methodology** [4] (dostępna tylko część 2 w wersji wstępnej – draft). Podaje on ogólne zasady stosowania CEM, terminologię, przebieg prowadzenia procesu ocen, zasady wydawania werdyktów oraz wskazówki dotyczące raportowania.
- **Guide for the production of protection profiles and security targets** [5]. Jest to poradnik służący opracowywaniu dokumentów formalnych wymagań bezpieczeństwa.

Wspólne Kryteria mogą być pomocne dla:

- konsumentów – wyniki oceny pomagają określić, czy dany produkt spełni ich oczekiwania oraz porównać szereg produktów i wybrać ten najwłaściwszy,

- twórców produktów – kryteria pomagają im precyzyjnie określić wymagania bezpieczeństwa, jakie tworzony produkt musi spełniać,
- audytorów (oceniających) prowadzących ewaluację – kryteria pozwalają formułować osąd na temat zgodności przedmiotu oceny z opracowanymi dla niego wymaganiami bezpieczeństwa,
- administratorów systemów, audytorów bezpieczeństwa, konstruktorów, osób odpowiedzialnych za akredytację, managerów i wielu innych.

2. Modelowanie własności bezpieczeństwa

Stworzenie zapisu formalnego własności bezpieczeństwa nie było zadaniem prostym. Należało opracować jednolity aparat formalny, pozwalający na wyrażanie funkcjonalności zabezpieczeń, mierzalnej wiarygodności zabezpieczeń, a przy tym zapewnić jednorodność i powtarzalność ocen. Opracowanie wspomnianych standardów lokalnych i ich stosowanie przez prawie dziesięć lat było swoistym poligonem doświadczalnym w tym zakresie.

Zaczęto od opracowania pewnego modelu obiektu o określonych własnościach bezpieczeństwa, eksploatowanego w określony sposób i eksponowanego w środowisku zagrożeń. Model ten nie różni się zasadniczo od modeli powszechnie stosowanych w analizie ryzyka, ale jest bardziej dostosowany do procesu specyfikacji własności zabezpieczeń jak i ich oceny dokonywanej podczas ewaluacji. Pozwala na artykułowanie własności zabezpieczeń od ogólnego opisu słownego poprzez stopniową konkretyzację stwierdzeń, aż po wyrażanie ich za pomocą języka formalnego, wykorzystującego komponenty funkcjonalne oraz komponenty uzasadniające zaufanie, pobierane z katalogów CC.

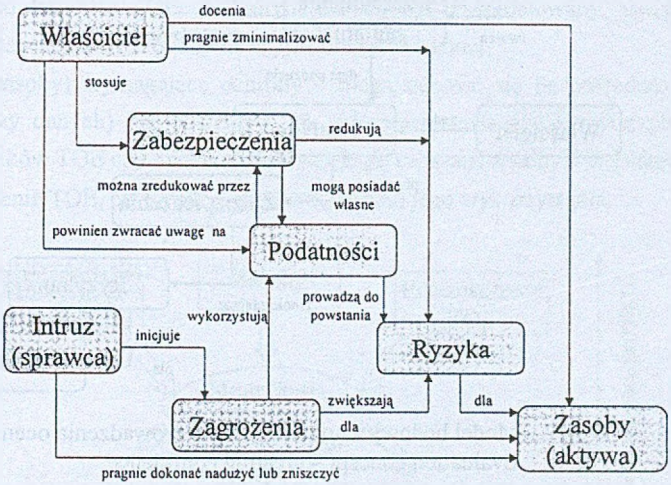
2.1. Model podstawowy

Bezpieczeństwo w CC jest rozumiane jako ochrona zasobów przed zagrożeniami, zaś zagrożenie jako potencjalna możliwość utraty chronionych zasobów. Rozpatrywane są wszelkie kategorie zagrożeń, przy czym szczególną uwagę poświęca się tym, które wynikają ze świadomej lub przypadkowej działalności człowieka. Ogólny model bezpieczeństwa, z którego wypływa filozofia CC, przedstawiono na rys. 1.

Zasoby (aktywa), dla ich właścicieli (użytkowników) mają określoną wartość, więc użytkownicy starają się je chronić. Również dla intruzów zasoby mają wartość, ale ich interes jest odmienny niż interes użytkowników. Pobudzając potencjalne zagrożenia, intruz dąży do zniszczenia lub osłabienia zasobów, stając się wtedy sprawcą szkód. Z punktu widzenia bezpieczeństwa, najczęstsze uszkodzenia zasobów to:

- utrata poufności, np. ujawnienie informacji nieautoryzowanym podmiotom,
- utrata integralności, np. modyfikacja pliku przez osobę niepowołaną,
- utrata dostępności, np. pozbawienie dostępu do zasobu.

Właściciel zasobów powinien przeanalizować wszelkie możliwe zagrożenia i określić, które z nich są istotne dla jego środowiska. Wynikiem tej analizy są wyznaczone ryzyka (w ujęciu matematycznym to prawdopodobieństwa niekorzystnych zdarzeń), zaś sama analiza pomaga w doborze zabezpieczeń, ograniczających ryzyko do akceptowalnego poziomu, czyli do ryzyka szczątkowego.



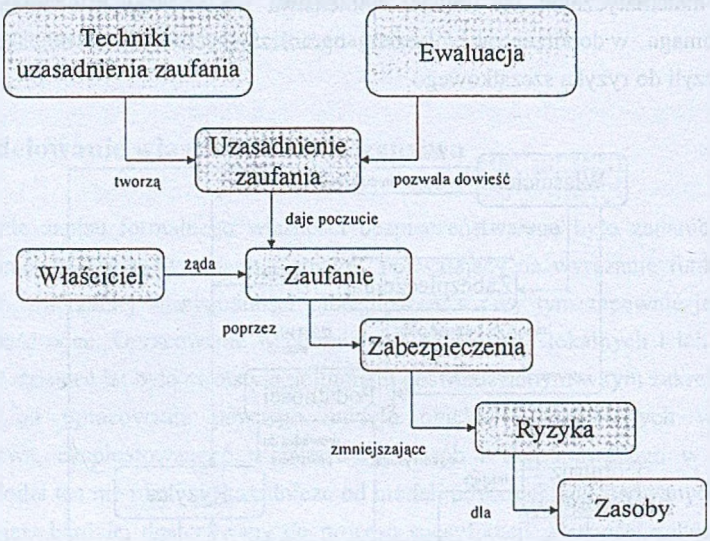
Rys. 1. Model bezpieczeństwa
Fig. 1. Security concept

Zabezpieczenia są stosowane także do ograniczenia podatności oraz do spełnienia wymagań narzuconych przez politykę bezpieczeństwa przez właściciela w stosunku do zasobów. Podatność szczątkowa istnieje po wprowadzeniu zabezpieczeń.

Właściciel zasobów musi zdobyć zaufanie do zabezpieczeń, dobranych stosownie do zagrożeń. Dopiero wówczas może wyeksponować zabezpieczone zasoby środowisku, w którym występują zagrożenia, pamiętając jednak o istnieniu ryzyka szczątkowego.

Właściciel zasobów nie jest jednak w stanie samodzielnie ocenić wszelkich aspektów bezpieczeństwa zastosowanych zabezpieczeń. Pomocą mogą służyć niezależni eksperci wydający werdykt podczas ewaluacji. W jej wyniku formułowany jest precyzyjny osąd na temat wiarygodności („zaufania do") zabezpieczeń, redukujących ryzyko dla chronionych zasobów.

Wiarygodność zabezpieczeń jest atrybutem zabezpieczeń, tworzącym podstawy zaufania do nich. Zaufanie to musi być uzasadnione i w pewien sposób mierzalne, czyli poddające się weryfikacji. Osąd dotyczący uzasadnionego zaufania może być wykorzystany przez właściciela zasobów do podjęcia decyzji, czy zaakceptować ryzyko ekspozycji swoich zasobów w sytuacji istnienia zagrożeń, czy też nie, co przedstawia rys. 2.



Rys. 2. Model budowy zaufania podczas prowadzenia ocen
Fig. 2. Evaluation concept – creating confidence

2.2. Konkretyzacja – tworzenie wymagań formalnych

Przyjęta w CC, a przedstawiona poniżej koncepcja bezpieczeństwa, znajduje odzwierciedlenie w treści tworzonych dokumentów – formalnych konstrukcji wymagań bezpieczeństwa:

- Zadania Zabezpieczeń (ang. ST – Security Target),
- Profilu Zabezpieczeń (ang. PP – Protection Profile).

Zadanie Zabezpieczeń (ST) tworzone jest dla konkretnego produktu lub systemu, czyli Przedmiotu Oceny (TOE) i jest zależne od sposobu implementacji, zaś Profil Zabezpieczeń (PP), niezależny od implementacji, dotyczy pewnej klasy podobnych TOE, różniących się sposobem implementacji.

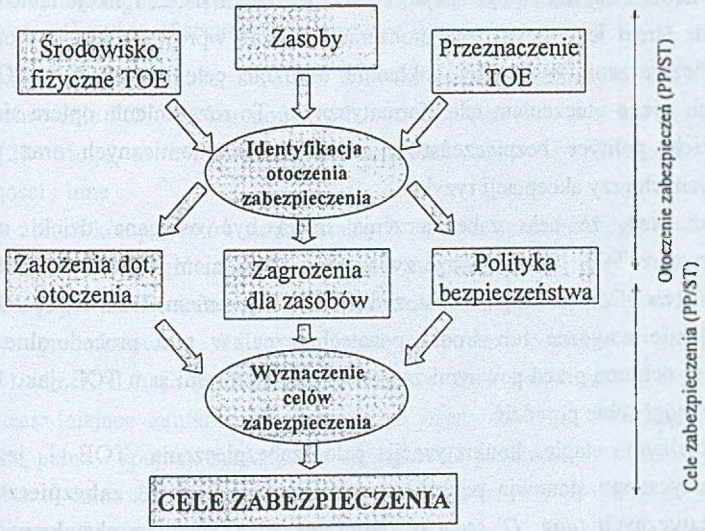
Opracowanie przez konstruktorów tych dokumentów przebiega w kilku etapach konkretyzacji, pokazanych na rys. 3 oraz rys. 4:

- określenie otoczenia zabezpieczenia,
- określenie celów zabezpieczenia,

- specyfikacja wymagań funkcjonalnych oraz wymagań uzasadniających zaufanie z wykorzystaniem skatalogowanych komponentów,
- opracowanie zwięzłej specyfikacji TOE związanej z implementacją (dotyczy wyłącznie ST).

Z punktu widzenia wymagań bezpieczeństwa istotny jest nie tylko sam produkt, ale również środowisko, w którym ma on pracować. Środowisko zabezpieczenia obejmuje regulacje prawne, zasady wynikające z polityki bezpieczeństwa instytucji, przyzwyczajenia, wiedzę ekspercką, w tym również występujące zagrożenia. Środowisko to podlega identyfikacji, zaś przy jego opisie uwzględnić należy:

- środowisko fizyczne TOE, w którym ma on być eksploatowany, uwzględniając wszelkie aspekty fizyczne, organizacyjne oraz personalne,
- aktywa (zasoby) wymagające ochrony – mogą odnosić się bezpośrednio do TOE (pliki, bazy danych) lub pośrednio, np. informacje związane z uwierzytelnianiem użytkowników TOE czy informacje wewnętrzne związane z samym działaniem TOE,
- przeznaczenie TOE, czyli rodzaj produktu, sposób jego wykorzystania.



Rys. 3. Wyznaczenie celów zabezpieczenia
Fig. 3. Determination of security objectives

Na podstawie dalszych szczegółowych dociekań, uwzględniających zasady polityki bezpieczeństwa, zagrożenia oraz ryzyka, formułowane są stwierdzenia charakteryzujące **otoczenie zabezpieczenia** TOE, czyli:

- założenia, które musi spełniać środowisko eksploatacyjne, aby można było przyjąć, że TOE jest w nim bezpieczny – w procesie ewaluacji założenia te będą traktowane jako aksjomaty,
- zagrożenia dla zasobów istotne dla TOE, które charakteryzowane są przez określenie:
  - intruza, który pobudza zagrożenie,
  - przewidywanej metody ataku,
  - podatności, będącej podstawą zagrożenia,
  - zasobu, będącego przedmiotem zagrożenia.

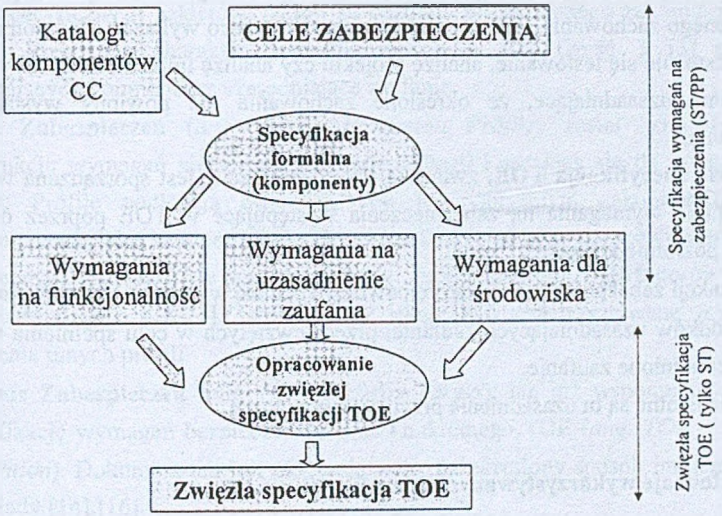
  Ocena ryzyka każdego zagrożenia uwzględnia prawdopodobieństwo wystąpienia zagrożenia dla danego ataku, prawdopodobieństwo, że atak się powiedzie oraz szkody, które mogą w jego wyniku powstać.
- zasady polityki bezpieczeństwa, które należy wdrożyć, aby bezpiecznie użytkować Przedmiot Oceny.

Kolejnym etapem konkretyzacji jest określenie **celów zabezpieczenia**. Uwzględniają one założenia dotyczące otoczenia, przewidywane zagrożenia oraz zasady polityki bezpieczeństwa. Cele muszą być spójne z przeznaczeniem TOE, funkcjonalnością użytkową i wiedzą na temat jego fizycznego otoczenia. Intencją wprowadzenia wymogu określenia celów zabezpieczenia było, aby dokładnie odróżnić cele związane z TOE od celów związanych z jego otoczeniem teleinformatycznym. To rozróżnienie opiera się na opiniach inżynierskich, polityce bezpieczeństwa, czynnikach ekonomicznych oraz na decyzjach podejmowanych przy akceptacji ryzyka.

Wynika stąd, że cele zabezpieczenia mogą być osiągane dzięki mechanizmom wbudowanym w TOE lub mogą być związane z otoczeniem TOE i uwzględniać politykę bezpieczeństwa. Cele zabezpieczenia związane z otoczeniem TOE są realizowane przez środki teleinformatyczne lub środki pozatechniczne, w tym proceduralne. Te ostatnie związane są ochroną przed pewnymi zagrożeniami, z którymi sam TOE, jako twór techniki, nie będzie mógł sobie poradzić.

W kolejnym etapie konkretyzacji cele zabezpieczenia TOE i jego otoczenia teleinformatycznego stanowią podstawę opracowania **wymagań zabezpieczenia** środków teleinformatycznych (*ang. IT security requirements)* za pomocą skatalogowanych w CC dwóch rodzajów komponentów:

- funkcjonalnych (*ang. functional components*),
- uzasadniających zaufanie (*ang. assurance components*).



Rys. 4. Szczegółowe specyfikacje wynikające z celów zabezpieczeń
Fig. 4. Creating of security specifications based on objectives

Wymagania na funkcjonalność, stawiane funkcjom zabezpieczającym TOE, określają oczekiwane zachowanie TOE, zaś komponenty to wyrażające zawarte są w katalogu w części drugiej CC [2]. Mogą to być wymagania dotyczące identyfikacji, uwierzytelniania, niezaprzeczalności i inne.

Dla danego zbioru komponentów funkcjonalnych poziom uzasadnionego zaufania może się różnić znacząco i zależy głównie od rygoryzmu zaaplikowanego przy tworzeniu TOE. Część trzecia CC [3] zawiera katalog komponentów uzasadniających zaufanie oraz wyrażoną za ich pomocą predefiniowaną skalę pomiarową w postaci poziomów uzasadnionego zaufania EAL1 do EAL7 *(ang. EAL – Evaluation Assurance Level)*. Przykładowo, komponenty uzasadniające zaufanie mogą dotyczyć oceny samego dokumentu ST (czy specyfikacja jest pełna i spójna), zarządzania konfiguracją produktu, warunków i sposobu tworzenia produktu, dokumentowania, czasu życia produktu (czy nowa wersja produktu jest tak samo bezpieczna jak poprzednia ?) itp.

Komponenty uzasadniające zaufanie wyrażają elementarne rygory, które twórca uwzględnia przy opracowaniu TOE, zaś oceniający podczas jego ewaluacji. Produkty o tej samej funkcjonalności bezpieczeństwa (ten sam zbiór komponentów funkcjonalnych) mogą powstawać w mniej lub bardziej rygorystyczny sposób, więc uzasadnione zaufanie do nich, wyrażone w skali EAL1 do EAL7, może być różne.

Należy zwrócić uwagę, że wymagania na funkcjonalność wyrażają pożądane zachowanie TOE, zaś wymagania na uzasadnione zaufanie określają brak niepożądanego zachowania.

Pożądane zachowanie można łatwo zademonstrować lub wykazać za pomocą testów. Brak niepożądanego zachowania nie zawsze da się rozstrzygająco wykazać, stąd pomocniczo przy ewaluacji stosuje się testowanie, analizę projektu czy analizę implementacji. Wynikiem są tu stwierdzenia uzasadniające, że określone zachowania nie powinny wystąpić podczas użytkowania.

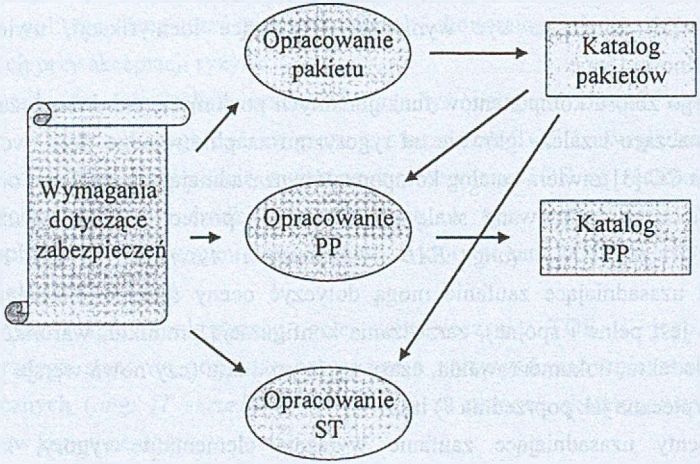
Zwięzła specyfikacja TOE, związana z implementacją, jest sporządzana wyłącznie dla ST. Definiuje wymagania na zabezpieczenia występujące w TOE poprzez określenie na wysokim poziomie abstrakcji:

- funkcji zabezpieczających, które powinny spełniać wymagania na funkcjonalność,
- środków uzasadniających zaufanie, przedsięwziętych w celu spełnienia wymagań na uzasadnione zaufanie.

Niezwykle istotne są tu uzasadnienia przyjętych rozwiązań.

2.3. Rodzaje wykorzystywanych specyfikacji

Wspólne Kryteria określają trzy typy elementów konstrukcyjnych wyrażających wymagania dotyczące bezpieczeństwa: ST, PP oraz pakiet. Związki między nimi pokazano na rys. 5, zaś określić je można w sposób następujący:



Rys. 5. Związki między konstrukcjami wymagań
Fig. 5. Relationships between security specifications

- **Pakiet** (*ang. package),* posiadający zwykle charakter tymczasowy i pomocniczy, grupuje wymagania dotyczące pewnego podzbioru celów zabezpieczeń i służy do wielokrotnego wykorzystania. Może zawierać w sobie inne pakiety, zaś często

występuje w pozostałych dwóch konstrukcjach. W tym miejscu należy zaakcentować zbiór specyficznych pakietów, jakimi są poziomy uzasadnionego zaufania EAL1 do EAL7. Mają one charakter predefiniowanych w CC Część 3 [3] pakietów, zawierających komponenty uzasadniające zaufanie.

- **Profil Zabezpieczeń** (*ang. PP – Protection Profile*) został pomyślany jako konstrukcja wymagań niezależna od implementacji i nadająca się do wielokrotnego użycia. Profile podlegają ewaluacji i po jej pomyślnym zakończeniu zostają skatalogowane jako wzorce, z których można korzystać przy opracowywaniu ST dla konkretnego produktu w ramach rodziny produktów, np. szyfratorów plików. Przykłady profili: [18-21]. Istniejące PP mogą być wykorzystywane również do tworzenia innych profili.
- **Zadanie Zabezpieczeń** (*ang. ST – Security Target*), jak już wspomniano, stanowi specyfikację wymagań bezpieczeństwa dla konkretnego TOE (*ang. TOE – Target of Evaluation*). Dokument ten jest ukierunkowany na określony sposób implementacji – przykłady [14],[16].

2.4. Rodzaje prowadzonych ocen

CC pozwalają realizować trzy rodzaje ewaluacji:

- **Ocena Profilu Zabezpieczeń PP**

  Stanowi sprawdzenie zgodności opracowanego PP z kryteriami. Celem jest tu ocena, czy dokument PP jest kompletny, spójny wewnętrznie i poprawny pod względem technicznym, przez co może stanowić bazę do tworzenia rodziny podobnych TOE (produktów, systemów) lub innych PP. Ocena przebiega zgodnie z kryteriami zawartymi w części 3 [3], głównie w rozdziałach 3 oraz 4.
- **Ocena Zadania Zabezpieczeń ST**

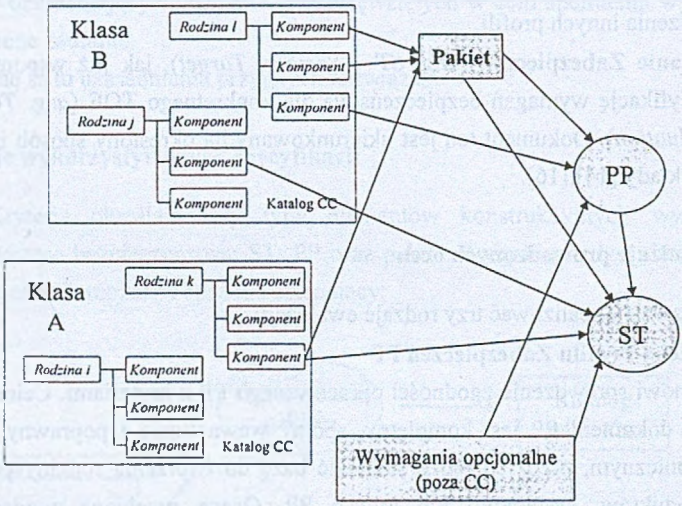
  Stanowi sprawdzenie zgodności opracowywanego ST z kryteriami. Również i w tym przypadku celem jest sprawdzenie, czy dokument ST jest kompletny, spójny wewnętrznie i poprawny pod względem technicznym oraz ponadto, jeśli opracowano go na podstawie PP, to dodatkowym celem jest wykazanie jego zgodności z tym profilem. Wymagania ST po pozytywnej ocenie stanowią podstawę do rozpoczęcia ewaluacji samego TOE. Ocena ST odbywa się zgodnie z kryteriami zawartymi w części 3 [3], głównie w rozdziałach 3 oraz 5.
- **Ocena TOE**

  Mając zweryfikowane Zadanie Zabezpieczeń ST jako dokument odniesienia można przystąpić do oceny opracowywanego na jego podstawie produktu lub sytemu (TOE).

Celem jest tu pokazanie, czy Przedmiot Oceny spełnia wymagania na zabezpieczenia zawarte w jego Zadaniu zabezpieczeń.

3. Formalna notacja własności bezpieczeństwa

Podstawowym modułem do tworzenia specyfikacji jest komponent. Niezależnie od rodzaju oba typy mają podobną budowę i wchodzą w skład pakietów oraz wymagań ST i PP, co pokazano na rys 6.



Rys. 6. Struktura katalogów komponentów
Fig. 6. Components catalogues – class structure

Przyjęto trójpoziomową, hierarchiczną strukturę katalogów: klasa – rodzina – komponent. Klasa obejmuje grupę wymagań z pewnego wspólnego obszaru, np. grupy celów zabezpieczeń. Zawiera ona rodziny ukierunkowane na realizację wybranych celów, różniące się jednak rygoryzmem. Rodzina składa się z jednego lub kilku komponentów. Dodatkowo, komponent składa się z elementów, które stanowią najniższy poziom języka wyrażającego aspekty bezpieczeństwa i które mogą być weryfikowane. Między komponentami mogą występować zależności – zastosowanie danego komponentu pociąga za sobą konieczność użycia innych. Występują trzy typy zależności, precyzyjnie określone w kryteriach:

- zależność między komponentami funkcjonalnymi,
- zależność między komponentami uzasadniającymi zaufanie,

- zależność między komponentem funkcjonalnym a komponentem uzasadniającym zaufanie.

Przykład 1

Przykład skupia uwagę na budowie klasy FPR, stąd zawartość merytoryczną tej klasy omówiono w znacznym uproszczeniu.

Class FPR, zwana PRIVACY, dotyczy prywatności i grupuje następujące rodziny:

FPR_ANO: Anonymity

FPR_PSE: Pseudoanonymity

FPR_UNL: Unlinkability

FPR_UNO: Unobservability

Rodzina FPR_ANO zapewnia użytkownikowi możliwość korzystania z zasobu lub usługi bez ujawniania jego tożsamości i zawiera dwa komponenty:

FPR_ANO.1 Anonymity

z jednym elementem:

FPR_ANO.1.1 oraz

FPR_ANO.2 Anonymity without soliciting information

z dwoma elementami:

FPR_ANO.2.1

FPR_ANO.2.2

Przykładowo, element FPR_ANO.1.1 ma postać:

TSF (czyli funkcja zabezpieczająca w TOE) shall ensure that [assignement: set of users and/or subjects] are unable to determine the real user name bound to [assignement: list of subjects and/or operation and/or objects]

Ponadto, wspomniane komponenty nie wykazują współzależności z innymi, zaś FPR_ANO.2 jest usytuowany w hierarchii wyżej w stosunku do FPR_ANO.1, gdyż wprowadza dodatkowy rygor.

3.1. Zbiór komponentów określających funkcjonalność zabezpieczeń

Część druga CC [2] stanowi katalog komponentów funkcjonalnych. Jak wiadomo, komponenty są uporządkowane pod względem przeznaczenia (tabela 1). Klasy obejmują od kilku do kilkunastu rodzin, zaś dana rodzina zawiera jeden lub więcej komponentów. Klasa odnosi się do pewnej grupy zagadnień, np.: komunikacja, rewizje, prywatność. Pojęcie rodziny wiąże się z realizacją pojedynczego celu zabezpieczenia, np. rodzina FDP_UIT opisuje, jak za pomocą trójki swych komponentów zapewnić integralność wymiany danych wewnątrz samego TOE. Komponenty mogą być zależne lub niezależne od innych komponentów, mogą też być ułożone sekwencyjnie lub hierarchicznie, co w tym przypadku

oznacza, że dany komponent wprowadza dodatkowy rygor dla komponentu bardziej ogólnego, położonego niżej w hierarchii.

Tabela 1

Klasy komponentów funkcjonalnych

Klasa	Nazwa pełna	Charakterystyka
FAU	Audyt bezpieczeństwa (ang. security audit)	Rozpoznawanie, rejestrowanie, zapamiętywanie oraz analiza informacji dotyczących działań związanych z bezpieczeństwem – jakie zdarzenie miało miejsce i kto jest za nie odpowiedzialny.
FCO	Transmisja (ang. Communication)	Niezaprzeczalność pochodzenia (źródła) informacji oraz niezaprzeczalność otrzymania informacji
FCS	Ochrona kryptograficzna (ang. Cryptographic support)	Zarządzanie kluczami szyfrującymi oraz operacje kryptograficzne
FDP	Ochrona danych użytkownika (ang. User Data Protection)	Cztery rodziny komponentów obejmują politykę ochrony danych użytkownika, sposoby ochrony, przechowywanie danych na zewnątrz TOE oraz ich import/eksport, transfer danych wewnątrz TOE
FIA	Identyfikacja i uwierzytelnianie (ang. Identification and authentication)	Identyfikacja i uwierzytelnianie użytkowników – nadanie im właściwych atrybutów bezpieczeństwa
FMT	Zarządzanie bezpieczeństwem (ang. Security management)	Zarządzanie bezpieczeństwem w TOE – atrybutami, danymi i funkcjami
FPR	Prywatność (ang. Privacy)	Ochrona użytkownika przed ujawnieniem i nadużyciami ze strony innych użytkowników
FPT	Ochrona funkcji zabezpieczających (ang. Protection of the TSF)	Zapewnienie integralności i bezpieczeństwa samego TOE – wewnętrzne mechanizmy bezpieczeństwa, niezależne od zasad narzuconych przez politykę bezpieczeństwa ochrona informacji związanych z działaniem samego TOE
FRU	Wykorzystanie zasobów (ang. Resource Utilisation)	Zapewnienie wymaganych zasobów (czas procesora, pamięć), tolerowanie błędów, priorytetowanie zadań
FTA	Dostęp do TOE (ang. TOE Access)	Dostęp użytkownika – operatora do TOE
FTP	Wiarygodne ścieżki i kanały (ang. Trusted path/channels)	Zaufana wymiana informacji między użytkownikiem a TOE oraz między TOE a innymi zaufanymi urządzeniami

Komponenty funkcjonalne stanowią pewne wzorcowe moduły, za pomocą których można zamodelować funkcje zabezpieczeń przewidziane przez konstruktora w tworzonym urządzeniu lub programie (TOE). Przykładowo, jeśli konstruktor chce wprowadzić szyfrowanie informacji, to musi świadomie uwzględnić komponenty z tym związane.

Dopuszczalne jest stosowanie własnych, nie zdefiniowanych w CC komponentów bezpieczeństwa, np. związanych z zastosowaniem generatora liczb losowych. Muszą one być jednak określone zgodnie z konwencją obowiązującą w CC.

3.2. Zbiór komponentów uzasadniających zaufanie do zabezpieczeń

Część trzecia CC [3] stanowi katalog komponentów uzasadniających zaufanie, służących do oceny wiarygodności zabezpieczeń oraz zawiera definicje poziomów uzasadnionego zaufanie EAL1 do EAL 7.

3.2.1. Katalog komponentów uzasadniających zaufanie

Struktura katalogu komponentów uzasadniających zaufanie jest podobna do przedstawionej na rys 6. Również w tym przypadku komponenty dzielą się na klasy (tabela 2), klasy obejmują od kilku do kilkunastu rodzin, zaś dana rodzina zawiera jeden lub więcej komponentów. Klasa odnosi się tu do pewnej grupy zagadnień, np. sposobu opracowania produktu, oceny podatności, sposobu testowania. Pojęcie rodziny wiąże się z pojedynczym zagadnieniem, np. ASE_ENV skupia się na ocenie prawidłowości określenia otoczenia TOE w dokumencie ST. Komponenty mogą być zależne lub niezależne od innych komponentów, mogą też być ułożone sekwencyjnie lub hierarchicznie, co oznacza, że dany komponent wprowadza dodatkowy rygor dla komponentu bardziej ogólnego, położonego niżej w hierarchii.

Dwie klasy APE oraz ASE są specyficzne w tym sensie, że służą do oceny dokumentów, jakimi są Zadanie Zabezpieczeń ST oraz Profil Zabezpieczeń PP. Pozostałe klasy odnoszą się już do Przedmiotów Oceny TOE. Zawsze bowiem ocena TOE poprzedzana jest oceną opracowanych dla niego dokumentów – PP albo ST.

Tabela 2

Klasy komponentów uzasadniających zaufanie

Klasa	Nazwa pełna	Charakterystyka
APE	Ocena dokumentu PP (ang. Protection Profile evaluation)	Kryteria do oceny PP – sprawdzają kompletność, zwięzłość i poprawność techniczną specyfikacji PP, będącej podstawą do późniejszego tworzenia specyfikacji ST
ASE	Ocena dokumentu ST (ang. Security Target evaluation)	Kryteria do oceny ST – sprawdzają kompletność, zwięzłość i poprawność techniczną specyfikacji ST, będącej podstawą ewaluacji TOE
ACM	Zarządzanie konfiguracją (ang. Configuration Management)	Dotyczą kontroli zmian w konfiguracji TOE podczas eksploatacji – śledzenie zmian, kontrola autoryzacji zmian, itp.
ADO	Dostarczanie i eksploatacja (ang. Delivery and operation)	Poprawność dostarczenia, instalacji, generacji i ustawień początkowych TOE

cd. tab.2

ADV	Prace badawcze i rozwojowe (ang. Development)	Poprawność specyfikacji produktu i jego funkcji zabezpieczeń na różnych etapach jego tworzenia
AGD	Dokumentacja (ang. Guidance documents)	Dokumentacja administratora i użytkownika
ALC	Wsparcie cyklu życia produktu (ang. Life cycle support)	Kontrola dyscypliny zmian w produkcie podczas jego opracowywania i eksploatacji
ATE	Testowanie (ang. Tests)	Testy sprawdzające TOE – rodziny komponentów dotyczą stopnia pokrycia i głębokości testów, testów niezależnych, wykonywanych przez oceniających, testów funkcjonalnych
AVA	Oszacowanie podatności (ang. Vulnerability assessment)	Oszacowanie podatności, w tym „bocznych wejść", możliwość wykorzystania błędów w konfiguracji, możliwość ataku na mechanizmy permutacyjne i probabilistyczne (klucze, hasła, skróty), podatności wprowadzone podczas tworzenia i eksploatacji produktu
AMA	Utrzymywanie osiągniętego poziomu uzasadnionego zaufania (ang. Maintenance of assurance)	Zarządzanie zabezpieczeniami – realizacja celów zabezpieczeń TOE podczas zmian zachodzących w nim lub w jego środowisku (wykrywanie nowych zagrożeń i podatności, zmiany wymagań użytkowych, poprawianie błędów w TOE już po jego ocenie)

3.2.2. Formalne i nieformalne określenia poziomów uzasadnionego zaufania

Skala poziomów uzasadnionego zaufania EAL1 do EAL 7 służy do formalnej jego oceny w Przedmiotach Oceny. Wraz ze wzrostem EAL rośnie uzasadnione zaufanie do TOE, gdyż oznacza to, że TOE był opracowywany i badany w sposób bardziej formalny i rygorystyczny. Poszczególne EAL w stosowanej tu terminologii CC są pakietami. Każdy z nich zawiera podzbiór komponentów uzasadniających zaufanie. Należy zauważyć, że nie wszystkie rodziny i komponenty są w tych pakietach reprezentowane.

Tablica 3 przedstawia sformalizowaną definicję poziomów EAL. Kolumny – to poziomy uszeregowane wg stopnia uzasadnionego zaufania, zaś wiersze przedstawiają rodziny komponentów. Na przecięciu występuje numer zastosowanego komponentu, pole szare oznacza brak komponentu dla rozważanego EAL. Dany EAL zawiera co najwyżej jeden komponent z danej rodziny, przy czym należy pamiętać o zależności (*ang. dependencies*) między komponentami (wstawienie danego komponentu może pociągnąć za sobą konieczność użycia innego). Zwiększenie stopnia uzasadnionego zaufania (poruszając się z lewa na prawo) osiągane jest na dwa sposoby:

- przez zastąpienie (*ang. substitution*) komponentu o niższym numerze (mniej rygorystycznego) komponentem o wyższym numerze (bardziej rygorystycznym), co oznaczono pogrubioną czcionką,

- przez dołączenie (*ang. addition*) komponentu, czyli przypadki, dla których szare pole zastąpiono konkretnym komponentem.

Przykład 2

Rodzina ACM_CAP dotyczy zarządzania konfiguracją. W odniesieniu do oprogramowania, komponenty te mogą służyć do kontroli jego integralności:

- *zapewniają aby program był wysyłany do klienta kompletny,*
- *zapewniają aby żaden jego składnik nie był pominięty podczas oceniania,*
- *chronią przed nieautoryzowaną modyfikacją, dodaniem elementów lub ich skasowaniem.*

Taką kontrolę można prowadzić na różnym poziomie szczegółowości i rygoru. Dla EAL1 wystarczy ACM_CAP.1, czyli np. sprawdzanie numeru wersji programu, zaś dla wyższych EAL wprowadza się bardziej rygorystyczne mechanizmy kontroli:

- *EAL2: ACM_CAP.2 dodatkowo wprowadza listę składników oprogramowania,*
- *EAL3: ACM_CAP.3 dodatkowo wprowadza autoryzację zmian,*
- *EAL4: ACM_CAP.4 dodatkowo wprowadza procedury zmian,*
- *EAL5 i EAL6: ACM_CAP.5 dodatkowo wprowadza mechanizm kopii odniesienia.*

ACM_CAP4 pojawia się w EAL4, stąd na przecięciu kolumny EAL4 i wiersza ACM_CAP występuje ***4 (pogrubiona czcionka).*** *W EAL5 nadal występuje ten sam ACM_CAP.4, co oznaczono zwykłą czcionką. Należy zwrócić uwagę, że np. komponent ACM_CAP.4 zawiera w sobie wszystkie rygory swych poprzedników.*

Tworząc wymagania ST/PP, należy zadeklarować EAL, a potem wykazać, że TOE go spełnienia. Nie jest dopuszczalne wyłączenie jakiegoś komponentu z EAL, np. nie jest możliwe, aby projektowane urządzenie czy program spełniało EAL3 bez ACM_SCP.1, bo trudno to zrealizować. Można natomiast:

- **wzbogacać** dany EAL dodatkowymi komponentami zdefiniowanymi w trzeciej części CC *(ang. augmentation)*, np. EAL3 wzbogacony o AMA_AMP (w EAL klasy AMA się nie używa),
- **rozszerzać** dany EAL o dodatkowe komponenty zewnętrzne, nie zdefiniowane w CC *(ang. extension)*, np. EAL3 rozszerzony o własny komponent MOJ_EXT,
- **zastąpić** (*ang. substitution*) standardowo występujący w pakiecie EAL komponent na bardziej rygorystyczny, np. EAL3 z komponentem ALC_DVS.2.

Tabela 3

Definicja poziomów uzasadnionego zaufania EAL

Klasa	Rodzina	Komponenty poziomów uzasadnionego zaufania						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Class ACM Configuration Management	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3

cd. tab.3

Class ADO Delivery and operation	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
Class ADV Development	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	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
Class AGD Guidance documents	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
Class ALC Life cycle support	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
Class ATE 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
Class AVA 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

Przykład 3

*Pakiet EAL 3 zawiera następujące komponenty uzasadniające zaufanie (**pogrubiona czcionka** oznacza nowe elementy w stosunku do EAL2 – zastąpienie lub wzbogacenie):*

- *z rodzin klasy ACM (zarządzanie konfiguracją):*
  ACM_CAP.3 Authorisation controls
  ACM_SCP.1 TOE CM coverage
- *z rodzin klasy ADO (dostarczanie i eksploatacja):*
  ADO_DEL.1 Delivery procedures
  ADO_IGS.1 Installation, generation, and start-up procedures
- *z rodzin klasy ADV (prace badawcze i rozwojowe):*
  ADV_FSP.1 Informal functional specification
  ADV_HLD.2 Security enforcing high-level design
  ADV_RCR.1 Informal correspondence demonstration
- *z rodzin klasy AGD (dokumentacja):*
  AGD_ADM.1 Administrator guidance
  AGD_USR.1 User guidance
- *z rodzin klasy ALC (wsparcie cyklu życia produktu):*
  ALC_DVS.1 Identification od security measures

- *z rodzin klasy ATE (testowanie):*
  ATE_COV.2 Analysis of coverage
  ATE_DPT.1 Testing: high-level design
  ATE_FUN.1 Functional testing
  ATE_IND.2 Independent testing – sample
- *z rodzin klasy AVA (oszacowanie podatności na zagrożenia):*
  AVA_MSU.1 Examination of guidance
  AVA_SOF.1 Strength of TOE security function evaluation
  AVA_VLA.1 Developer vulnerability analysis

Każdy z hierarchicznych poziomów EAL został precyzyjnie określony w tabeli 3, tym niemniej poszczególne poziomy można dodatkowo scharakteryzować w sposób opisowy:

EAL1 – *"functionally tested"*

Ma zastosowanie, gdy wymagane jest uzasadnione zaufanie co do poprawności działania, lecz zagrożeń nie rozważa się zbyt głęboko. Ewaluacja odbywa się bez udziału twórców i obejmuje wykonanie niezależnych testów TOE w postaci, w jakiej jest on dostarczany dla użytkowników. Sprawdzana jest zgodność TOE ze specyfikacją ST oraz dokumentacją użytkową. Ewaluacja pozwala na osąd, czy TOE jest zgodny z dokumentacją oraz czy zapewnia wystarczającą ochronę przed znanymi zagrożeniami.

EAL2 – *"structurally tested"*

Zakłada się ograniczoną współpracę z twórcami TOE w zakresie dostarczenia oceniającym informacji dotyczących architektury TOE oraz wyników testów. EAL2 ma zastosowanie w okolicznościach, w których twórcy lub użytkownicy wymagają pewnego niskiego lub umiarkowanego poziomu bezpieczeństwa, potwierdzonego przez niezależne gremia, np. w sytuacji braku pełnej dokumentacji projektowej czy utrudnionego dostępu do twórców.

EAL3 – *"methodically tested and checked"*

Przez dokładną analizę projektu, ale bez jego głębszych modyfikacji, formułowana jest precyzyjna ocena zabezpieczeń. Nie zakłada się tu istotnej adaptacji procedur i zasad projektowania dla potrzeb bezpieczeństwa. Ma zastosowanie, kiedy twórcy lub użytkownicy wymagają pewnego umiarkowanego poziomu uzasadnionego zaufania, potwierdzonego przez niezależne gremium, osiągniętego przez analizę TOE i jego projektu bez wprowadzania gruntownych modyfikacji.

EAL4 – *"methodically designed, tested and reviewed"*

Pozwala twórcom osiągnąć zakładany poziom uzasadnionego zaufania poprzez wykorzystanie typowych metod inżynierii projektowej, używanych przy tworzeniu produktów komercyjnych, jednak już z zastosowaniem pewnych rygorów. Nie są tu

wymagane: specjalistyczna wiedza, doświadczenie, zasoby czy narzędzia z dziedziny bezpieczeństwa.

EAL5 – *"semiformally designed and tested"*

Bezpieczeństwo jest tu osiągane poprzez rygorystyczne stosowanie metod inżynierii projektowej, przeznaczonych do tworzenia produktów komercyjnych, jednak wspartych w sposób umiarkowany metodami inżynierii zabezpieczeń. Rozważana jest konieczność poniesienia umiarkowanych nakładów na środki bezpieczeństwa. EAL5 ma zastosowanie w sytuacji, kiedy twórcy lub użytkownicy wymagają potwierdzenia przez niezależnych ekspertów wysokiego poziomu bezpieczeństwa opracowywanego produktu lub wymagają uzasadnienia ponoszonych kosztów związanych ze specjalnym sposobem tworzenia produktu.

EAL6 – *"semiformally verified design and tested"*

Twórcy osiągają wysoki poziom bezpieczeństwa przez zastosowanie technik inżynierii bezpieczeństwa do rygorystycznego środowiska projektowania i rozwoju produktu. Ma to zastosowanie przy opracowywaniu zaawansowanych produktów chroniących zasoby o znacznej wartości w środowisku obarczonym znacznym ryzykiem. Ewaluacja ma uzasadnić wysokość poniesionych kosztów zabezpieczeń.

EAL7 – *"formally verified design and tested"*

Ten poziom uzasadnionego zaufania ma zastosowanie przy opracowywaniu produktów przeznaczonych dla środowisk obarczonych ekstremalnie dużym ryzykiem lub do ochrony zasobów o bardzo dużej wartości. Ich wartość ma uzasadniać koszty opracowania takich produktów. W praktyce stosowanie EAL7 ogranicza się obecnie do produktów o ściśle ukierunkowanych funkcjach bezpieczeństwa, podlegających złożonej weryfikacji formalnej.

4. Metodyka prowadzenia ocen

4.1. Budowa komponentu uzasadniającego zaufanie

Kluczem do prawidłowego przedstawienia procesu ewaluacji jest omówienie budowy komponentów uzasadniających zaufanie [3]. Składają się one z elementów trzech typów D, C oraz E:

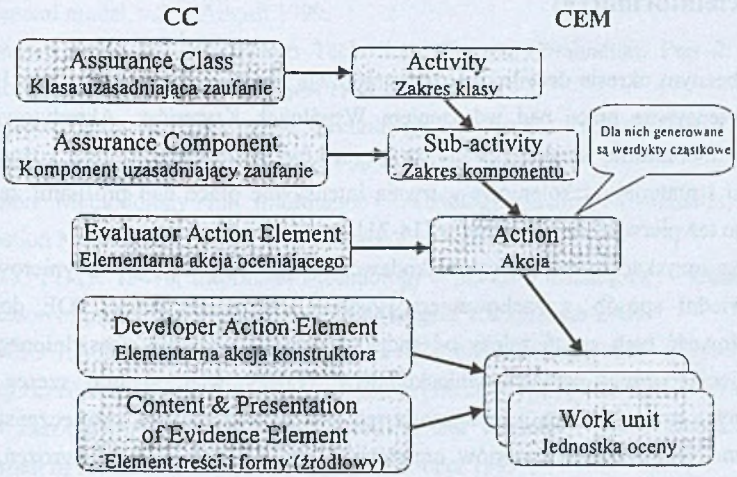
- **Elementarna akcja konstruktora** (*ang. Developer Action Element*) – określa czynności, za które odpowiada konstruktor; oznaczane są literka **D** na końcu nazwy elementu; zwykle określają, że powinien on coś opracować, coś dostarczyć, nie precyzując przy tym jaka to ma mieć postać – określa to dopiero kolejny typ elementu
- **Element treści i formy** (*ang. Content & Presentation of Evidence Element*) – określa wymagania co do wykazu informacji źródłowych, ich zawartości oraz postaci,

dostarczanych przez konstruktora, a potrzebnych dla oceniającego do prowadzenia ewaluacji (np. mogą to być: zawartość wybranego rozdziału dokumentacji użytkowej, opis procedury instalacji, urządzenie, test, itp.); oznaczany jest literką C

- **Elementarna akcja oceniającego** (*ang. Evaluator Action Element*) – określa czynności, które wykonuje oceniający – sprawdza, czy konstruktor dostarczył to coś i czy posiada to odpowiednią zawartość i postać; takie elementy oznaczane są literką E na końcu swej nazwy.

4.2. Przebieg procesu prowadzenia ocen

Przyjęto następujące związki między pojęciami podstawowymi CC oraz CEM, przedstawione na rys 7:



Rys. 7. Związki między pojęciami specyfikacji i oceny
Fig. 7. Relationships between specification and evaluation terminology

- Klasie uzasadniającej zaufanie (*ang. Assurance Class*) w CC odpowiada zakres klasy (*ang. Activity*) w CEM, co określa zastosowanie zbioru komponentów uzasadniających zaufanie określonych przez tę klasę do procesu ewaluacji
- Komponentowi uzasadniającemu zaufanie (*ang. Assurance Component*) w CC odpowiada zakres komponentu (*ang. Sub-activity*) w CEM, określający czynności, jakie musi wykonać oceniający dla każdego elementu treści i formy, określone przez ten komponent (*przyp. oznaczane literką „E" na końcu*)

- Realizacja elementarnej akcji oceniającego (*przyp. oznaczane literką „E" na końcu*) na „argumencie", którym jest element treści i formy lub jego część (*przyp. oznaczane literką „C" na końcu*) odpowiada jednostce oceny (*ang. Work unit*). Elementarna akcja oceniającego generuje co najmniej jedną jednostkę oceny, która jest elementarną czynnością wyodrębnioną dla procesu ewaluacji. Nie w każdym przypadku danemu elementowi oznaczonemu literką „C" na końcu odpowiada jedna jednostka oceny.

Można więc stwierdzić, że elementy treści i formy dostarczane przez konstruktora w odpowiedniej postaci i posiadające odpowiednią zawartość stanowią „wejście" dla jednostek oceny wykonywanych przez oceniającego.

5. Znaczenie Wspólnych Kryteriów dla poprawy bezpieczeństwa teleinformatyki

W obecnym okresie decydujące znaczenie mają nadal certyfikaty lokalne [11-13], choć trwają intensywne prace nad wdrożeniem Wspólnych Kryteriów. Akredytowane zostały pierwsze laboratoria, opracowywane są procedury postępowania oraz różnego rodzaju poradniki i materiały szkoleniowe – trwają intensywne prace nad profilami zabezpieczeń, udzielono też pierwszych certyfikatów [14-21].

Chcąc uzyskać certyfikat wnioskodawca (jego projektanci, inżynierowie) muszą w odpowiedni sposób, z zachowaniem rygorów CC, przygotować TOE do ewaluacji. Szczegółowość tych zadań zależy od zadeklarowanego poziomu uzasadnionego zaufania, o osiągnięcie którego zabiega wnioskodawca. Należy więc spełnić szereg wymogów narzuconych przez kryteria, a to wymaga sporej wiedzy z zakresu bezpieczeństwa, wiedzy praktycznej w stosowaniu kryteriów, umiejętności prowadzenia analizy zagrożeń, niezwykłej staranności tworzenia i dokumentowania produktu itp. Wnioskodawca opracowuje zwięzły i sformalizowany dokument określający wymagania bezpieczeństwa. Wyrażając się precyzyjniej, dla produktu jest to Zadanie Zabezpieczeń (*ST – ang. Security Target*), zaś dla profilu jest to Profil Zabezpieczeń (*PP -ang. Protection Profile*).

Ponadto należy sobie uzmysłowić fakt, że obecnie prawie każdy program, adapter sprzętowy, czy też system – niekoniecznie posiadający charakter „typowego zabezpieczenia" – zawiera w sobie pewne funkcje kojarzone z bezpieczeństwem, np. hasło dostępu. Skoro taka funkcja występuje, to powinna być zaimplementowana prawidłowo, zgodnie z normami (CC) oraz zasadami sztuki.

W środowisku inżynierskim brak jest dostatecznej wiedzy na temat stosowania CC:

- jak prawidłowo specyfikować funkcjonalność bezpieczeństwa w produktach,

- jakimi miarami (ocenami) należy posługiwać się przy ewaluacji produktu, w jaki sposób mierzyć zaufanie do niego, czy też określać brak w nim zachowań niepożądanych,
- w jaki sposób audytorzy będą oceniać nasz produkt,
- jak projektować bezpieczne produkty i przygotowywać je do ewaluacji.

Propagowanie wiedzy praktycznej na temat stosowania CC wśród programistów i konstruktorów może być jednym z czynników rozwoju polskich produktów bezpieczeństwa.

LITERATURA

1. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, v.2.1, August 1999.
2. Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, v.2.1, August 1999.
3. Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, v.2.1, August 1999.
4. Common Methodology for Information Technology Security Evaluation, Part 2: Evaluation Methodology, v.1.0, August 1999.
5. ISO/IEC PDTR 15446, Information technology – Security techniques – Guide for the production of protection profiles and security targets, v.0.9, Januar 2000
6. PrPN-ISO 15408-1: Technika informatyczna – Techniki Zabezpieczeń – Kryteria Oceny Zabezpieczeń Teleinformatyki – Wprowadzenie i model ogólny, PKN, grudzień 1999.
7. BSI – Zertifizierung, Hinweise fuer Hersteller und Vertreiber, BSI – Bundesamt fuer Sicherheit in der Informationstechnik, Bonn, Oktober 1999.
8. Van Essen U., Ruhrmann I., IT – Sicherheitszertifizierung auf der Grundlage der Common Criteria (Internationaler Standard ISO/IEC 15408), Der Weg zur sicheren Informationstechnik – Aktuelle Beispiele, CeBIT Ausgabe, BSI – Bundesamt fuer Sicherheit in der Informationstechnik, Bonn, 2000.
9. IT – Sicherheitskriterien und Evaluierung nach ITSEC, BSI Kurzinformationen zu aktuellen Themen in der IT-Sicherheit, BSI – Bundesamt fuer Sicherheit in der Informationstechnik, Bonn, 2000.
10. Common Criteria ISO/IEC 15408, BSI Kurzinformationen zu aktuellen Themen der IT-Sicherheit, BSI – Bundesamt fuer Sicherheit in der Informationstechnik, Bonn, 2000.
11. Information Technology Security Evaluation Criteria (ITSEC), EGKS-EWG-EAG, Bruessel, Juni 1991.

12. Trusted Computer System Evaluation Criteria „Orange Book"/Federal Criteria for IT Security (TCSEC/FC).
13. Canadian Trusted Computer Product Evaluation Criteria (CTCPEC).
14. Security Target BSI-DSZ-CC-0153: First Evaluation of Philips P8WE5032 Secure 8-bit Smart Card Controller, Philips Semiconductors Hamburg, September 1999.
15. Certification Report BSI-DSZ-CC-0153-1999 for Philips Smart Card Controller P8WE5032V0B from Philips Semiconductors Hamburg, BSI, November 1999.
16. Security Target B1/EST-X version 1.1, BSI-DSZ-CC-0143, Bull and IBM, 1999.
17. Certification Report BSI-DSZ-CC-0143-1999 for B1/EST-X version 2.0.1 with AIX, version 4.3.1 from Bull S.A. and IBM Instrumentationssysteme Deutschland GmbH, 11.03.1999.
18. CSPP-OS Operating System Protection Profiles Draft v03, NIST.
19. Role-Based Access Control (RBAC) Protection Profile (Final 1.0), Logica and Syntegra.
20. Federal Government Firewall Protection Profile, NIST.
21. Smart Card Security Users Group Protection Profile v2.0, SCSUG.
22. Białas A.: Wprowadzenie do problematyki certyfikacji środków sprzętowych i programowych zapewniających bezpieczeństwo informacji, IT Security Magazine, 2000, Nr 10 (14).
23. Białas A.: Wspólne Kryteria – koncepcja i model bezpieczeństwa, IT Security Magazine, 2000,Nr 11 (15).
24. Białas A.: Wspólne Kryteria – formalna specyfikacja wymagań bezpieczeństwa, IT Security Magazine, 2000, Nr 12 (16).
25. Białas A.: Wspólne Kryteria – metodyka ewaluacji, IT Security Magazine, 2001, Nr 1 (17).

Recenzent: Prof. dr inż. Andrzej Grzywak

Wpłynęło do Redakcji 15 marca 2001 r.

Abstract

The paper deals with IT Security Evaluation according to CC – Common Criteria (ISO 15408). Security concept (Fig. 1) and evaluation concept (Fig. 2) allows to specify security objectives (Fig. 3) and key formal documents: Security Target (ST) or Protection Profile (PP) (Fig. 4). Relationships between formal documents and types of evaluations were discussed (Fig. 5). Structure (Fig. 6) and contents of functional (tab.1) and assurance (tab. 2)

components catalogues were presented. It was mentioned, that each EAL (Evaluation Assurance Level) (tab. 3) are special kind of package. Relationships between CC key terminology and CC Methodology (CEM) were shown (Fig. 7). As conclusions, some implementations problems and challenges for programmers, designers and evaluators were discussed.