STUDIA INFORMATICA 2001
Volume 22 Number 4 (46)

Kazimierz MOCHOL
Wojskowe Służby Informacyjne

POLITYKA BEZPIECZEŃSTWA KLUCZEM DO CERTYFIKACJI WOJSKOWYCH SYSTEMÓW TELEINFORMATYCZNYCH (TI)

Streszczenie. Celem polityki bezpieczeństwa informacyjnego jest stworzenie podstaw, procedur i wymagań niezbędnych dla zapewnienia właściwej ochrony przetwarzanym informacjom. Jednym z podstawowych wymogów, jakie wprowadziła ustawa o ochronie informacji niejawnych z 22 stycznia 1999 r., jest wymóg posiadania certyfikatu dla systemu zawierającego informację klasyfikowaną, wydany przez właściwą służbę ochrony państwa. Warunkiem ubiegania się o certyfikat wyrobów, systemów i sieci jest opracowanie dokumentów typu szczególne warunki bezpieczeństwa, czy też procedury bezpieczeństwa.

THE SECURITY POLICY AS A KEY TO CERTIFICATION ISSUES IN MILITARY COMMUNICATION AND INFORMATION SYSTEMS (CIS)

Summary. The purpose of IT security policy is creation of basis, procedures and requirements necessary to ensure proper protection of processed information. One of the basic requirements in systems, where classified information is processed, which brought the act about classified information protection, dated January 22nd 1999 into effect, is requirement to possess suitable certificate. Proper national security authority should issue this certificate. Conditions to apply for products, systems and network security certification are included in appropriate documents (SSRS, SecOps, etc.).

1. Polityka bezpieczeństwa

W dobie niezwykłego wręcz rozwoju informatyki oraz technik przesyłu informacji, informacja staje się towarem szczególnie narażonym na wszelkiego rodzaju niebezpieczeństwa – zagrożenia. Zagrożenia te mogą być bardzo różnorodne. Polska Norma PN-I-13335-1 – "*Wy-*

tyczne do zarządzania bezpieczeństwem systemów informatycznych" wyróżnia m.in. następujące zagrożenia:

a) środowiskowe – niezależne od człowieka (trzęsienie ziemi, wyładowania elektryczne, powódź, pożar),
b) zależne od człowieka (ludzkie):
   - rozmyślne (podsłuch, modyfikacja informacji, włamania do systemu, złośliwy kod, kradzież),
   - przypadkowe (pomyłki i pominięcia, skasowanie pliku, nieprawidłowe skierowanie, wypadki fizyczne).

Informacja przekazywana w sieciach komputerowych może być dodatkowo narażona na takie niebezpieczeństwa, jak np.:

a) zawieszenie się komputera,
b) ataki wirusów,
c) włamania sieciowe (przejęcie kontroli nad siecią i włamania do kolejnych komputerów pracujących w sieci), np.
   - sniffing (pasywne nasłuchiwanie danych przez sieć, poczty, haseł, kopiowanych plików),
   - spoofing (omijanie przez hackera zabezpieczeń wprowadzonych do sieci przez jej administratora, podszywanie i udawanie innego komputera),
   - hijacking (przechwycenie transmisji pomiędzy dwoma zdalnymi komputerami).

W ostatnim czasie odnotowuje się gwałtowny wzrost włamań i innych naruszeń bezpieczeństwa systemów komunikacyjnych. Wprowadzenie nowych typów usług przez operatorów sieci, jak np. audioteks, telekonferencje, obsługa kart kredytowych i telefonicznych do opłat otwiera duże możliwości nadużyć i nielegalnego wykorzystania zasobów telekomunikacyjnych. Oszustwa telekomunikacyjne stały się niezwykle dochodowym międzynarodowym procederem. Szacuje się np., że straty ponoszone przez operatorów telekomunikacyjnych wskutek oszustw i nadużyć wynoszą od 2 do 5%, a w niektórych przypadkach do 20% całości obrotu danego operatora.

Przytoczone wyżej zagrożenia upoważniają do stwierdzenia, iż informacja musi być chroniona. Ochrona informacji ściśle powiązana jest z polityką bezpieczeństwa poszczególnych instytucji. Cytowana już wyżej Polska Norma PN-I-13335-1 definiuje politykę bezpieczeństwa instytucji w zakresie systemów informatycznych (ang. *IT security policy*) jako: zasady, procedury zarządzania, które określają, jakie zasoby (włącznie z informacjami wrażliwymi) są zarządzane, chronione i dystrybuowane w danej instytucji i jej systemach informatycznych.

Celem polityki bezpieczeństwa informacyjnego jest stworzenie podstaw, procedur i wymagań niezbędnych dla zapewnienia właściwej ochrony przetwarzanym informacjom.

Obejmuje ona bezpieczeństwo środków łączności i informatyki, a także bezpieczeństwo osobowe, fizyczne, przemysłowe i emisyjne. Głównym założeniem polityki bezpieczeństwa jest określenie:

- jakie grupy informacji będą chronione,
- w jakich systemach informacje te mogą być przetwarzane,
- kto i na jakich zasadach ma mieć do nich dostęp,
- kto jest odpowiedzialny za zarządzanie informacją,
- kto jest odpowiedzialny za zarządzanie bezpieczeństwem informacji,
- jakie warunki należy spełnić, aby uzyskać poświadczenia, świadectwa i certyfikaty.

Rodzi się pytanie: co jest przedmiotem polityki? System informatyczny? Czy informacje, które się w nim znajdują?

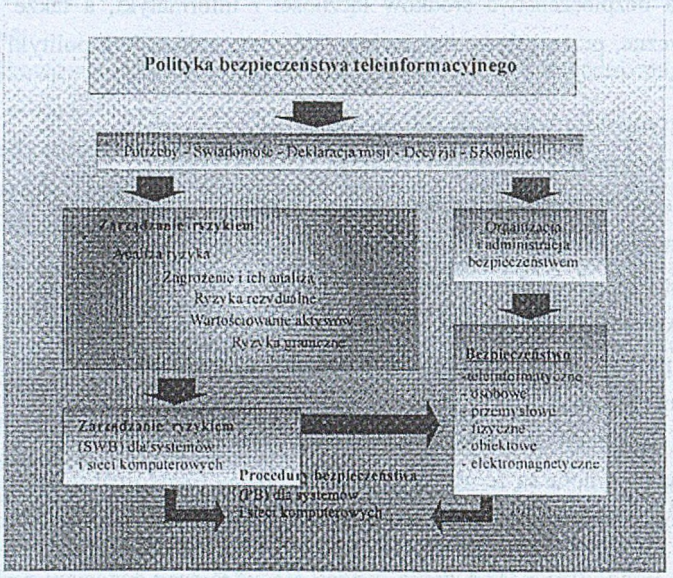
W każdej instytucji znajduje się wiele rodzajów informacji (danych) wymagających ochrony. Jedne chronione są ze względu na interes firmy (dane finansowe, inwestycyjne, patenty itp.), inne ze względu na wymagania wynikające z dokumentów normatywnych i przepisów prawa (zbiory danych osobowych, informacje niejawne), jeszcze inne są jawne, ale wymagają ochrony ze względu na konkurencyjne firmy (np. informacje marketingowe). Zatem to **rodzaj informacji (grupa)** jest punktem wyjścia do stworzenia polityki bezpieczeństwa!

Nie wszystkie zagrożenia są łatwe do przewidzenia, a skutki niepożądanego incydentu widoczne są dopiero wtedy, gdy nastąpiła już szkoda. Znane jest powiedzenie, iż łatwiej jest przeciwdziałać zagrożeniom, niż usuwać skutki ich wystąpienia, stąd też zaleca się stworzenie takiej polityki bezpieczeństwa, która powinna odzwierciedlać cele i strategie danej instytucji z uwzględnieniem środowiska, w jakim się znajduje.

Można wyróżnić wiele elementów wchodzących w skład polityki bezpieczeństwa, jak np.:

- potrzeby, świadomość, deklaracja misji, decyzje, szkolenie,
- analiza i zarządzanie ryzykiem,
- organizacja i administracja bezpieczeństwem,
- INFOSEC (bezpieczeństwo teleinformatyczne, osobowe, przemysłowe, fizyczne, obiektowe, elektromagnetyczne,...),
- itd.

Opracowanie spójnej polityki bezpieczeństwa jest w obecnej sytuacji rozwoju rynku usług elektronicznych swoistą koniecznością. Praktycznie większość firm powołuje w swoich strukturach komórki odpowiedzialne wyłącznie za bezpieczeństwo i ochronę gromadzonej i przesyłanej informacji. Specjalizacja jest dobrą praktyką, ponieważ należy oddzielać funkcje i role administracji zasobami teleinformatycznymi firmy od czynności i procedur związanych z podwyższeniem ich bezpieczeństwa.



Rys. 1. Polityka bezpieczeństwa teleinformacyjnego
Fig. 1. CIS security policy

Przyjmuje się, że polityka bezpieczeństwa systemów teleinformatycznych musi być podporządkowana ogólnej polityce bezpieczeństwa firmy. Ogólna polityka określa bowiem zakres prac oraz obszary szczególnej ochrony. Opracowanie polityki bezpieczeństwa rozpoczyna się od określenia zasobów podlegających ochronie. Zasoby należy zidentyfikować, sklasyfikować oraz pogrupować. Wiedza nt. rodzaju ochranianych zasobów jest kluczowa co do dalszego zakresu czynności. Kolejnym krokiem jest oszacowanie wartości chronionych zasobów. Może to być bardzo trudne do jednoznacznego określenia, jednakże nawet zgrubna estymacja pozwoli później trafnie wybrać lub odrzucić techniki ochrony.

Zastosowany system ochrony powinien być na tyle skuteczny, aby koszt jego złamania zniechęcał potencjalnego włamywacza, czyli był wyższy aniżeli zabezpieczana przez niego informacja. Wybór właściwego systemu ochrony jest tym prostszy, im analiza zagrożeń oraz stopnia ryzyka pełniejsza. Administrator bezpieczeństwa podczas opracowywania zasad powinien uwzględniać m.in. takie elementy, jak:

- logiczny nadzór bezpieczeństwa,
- fizyczny nadzór bezpieczeństwa,
- integralność systemu oraz informacji,
- poufność informacji,
- opracowanie zasad oraz procedur dla personelu odpowiedzialnego za sieć,
- opracowanie zasad oraz procedur dla użytkowników wewnętrznych oraz zewnętrznych zasobów sieciowych,

– zorganizowanie szkolenia w zakresie polityki bezpieczeństwa.

Opracowana polityka bezpieczeństwa w miarę rozwoju systemu teleinformatycznego ulega zmianie, modyfikowana jest również, jeżeli wykryte zostają w jej funkcjonowaniu luki.

Problem ochrony zasobów informacyjnych dotyczy również systemów wojskowych. Wynika to przede wszystkim z samej specyfiki wojska, gdzie duży nacisk kładzie się na szeroko rozumianą ochronę informacji. Dotyczy to w szczególności takich dziedzin, jak (wg poglądów państw sojuszniczych NATO, w kolejności priorytetów):

– operacji związanych z procesem walki,
– obraz wspólnych działań operacyjnych,
– rozpoznanie wojskowe,
– logistyka / transport,
– informacje o obiektach wojskowych,
– systemy łączności oraz systemy informatyczne,
– zbieranie informacji, koordynacja działań, zarządzanie procesem obiegu informacji,
– logistyka / dostawy,
– logistyka / wsparcie medyczne,
– utrzymanie stanu osobowego,
– logistyka / utrzymanie sprzętu, konserwacja,
– plany operacyjne,
– prowadzona polityka,
– analiza operacyjna.

Według oszacowań ekspertów NATO

– w ciągu najbliższych 3 do 5 lat można spodziewać się znacznego wzrostu wszelkiego rodzaju ataków na szeroko rozumiane systemy teleinformacyjne,
– właściwe zabezpieczenie informacji jest problemem globalnym i stanowi niezwykłe wyzwanie dla całego społeczeństwa,
– zabezpieczenie zasobów informacyjnych wymaga połączenia wysiłków wszystkich korporacji (w tym czynników rządowych) w zakresie integracji osiągnięć naukowych oraz władz odpowiedzialnych za bezpieczeństwo.

2. Certyfikacja w systemach niewojskowych

Definicja:

"Certyfikacja – jest to działanie trzeciej strony wskazujące, że: zapewniono odpowiedni stopień zaufania, iż należycie zidentyfikowany proces, lub usługa danego dostawcy

są zgodne z wymaganiami jednej lub ewentualnie wielu norm, przyjętych za podstawę certyfikacji."

Certyfikacja systemu/sieci na zgodność z wymaganiami określonymi w normach jest potwierdzeniem przez niezależną i uznaną stronę trzecią, że w danej instytucji / przedsiębiorstwie istnieje system / sieć, dla których zostały opisane zasady eksploatacji, zarządzania oraz że zasady te zostały wprowadzone w życie i przestrzegane są odpowiednie procedury postępowania.

W odniesieniu do instytucji, która pomyślnie przeszła proces certyfikacji, można mieć przekonanie, że wdrożyła przyjęty model zarządzania. Certyfikat stanowi tym samym rzeczywistą podstawę zaufania w układach handlowych, w stosunkach pomiędzy klientami i dostawcami, szczególnie wtedy gdy chodzi o nowych klientów. Korzyści z przeprowadzonej certyfikacji mogą być następujące:

- usprawnienie zarządzania i umożliwienie utrzymania stabilności procesu;
- dowód na wprowadzenie właściwego nadzoru w instytucji / przedsiębiorstwie;
- zapewnienie określonej jakości produktu;
- zwiększenie konkurencyjności jako dostawcy, a zatem i oferowanych przez niego wyrobów i usług;
- podniesienie wartości dostawcy w opinii klientów zagranicznych i krajowych;
- uznanie zagranicznych jednostek certyfikujących i postrzeganie firmy przez klientów jako stabilnej na rynku;
- bezpieczeństwo prawne firmy.

Posiadanie certyfikatu uznanej niezależnej jednostki oznacza:

- wzmocnienie konkurencyjności instytucji / przedsiębiorstwa;
- utrwalony, pozytywny stosunek do klientów;
- ograniczenie lub zaniechanie audytów przeprowadzanych przez klienta;
- istotny argument w reklamie i marketingu,
- stałe doskonalenie systemu.

Przed przystąpieniem do certyfikacji, firma ubiegająca się o certyfikat powinna zwrócić się do jednostek certyfikujących z prośbą o informacje dotyczące sposobu i kosztów jej przeprowadzenia. Bardzo istotnym tutaj czynnikiem są referencje firmy.

Krajową jednostką akredytującą, upoważnioną ustawą Sejmu Rzeczypospolitej Polskiej z dnia 28 kwietnia 2000 r. o systemie oceny zgodności, akredytacji oraz zmianie niektórych ustaw (DzU Nr 43, poz. 489) do akredytowania jednostek certyfikujących wyroby, systemów zarządzania, personelu, jednostek kontrolujących (inspekcyjnych), laboratoriów badawczych oraz laboratoriów pomiarowych (wzorcujących) jest POLSKIE CENTRUM AKREDYTACJI.

W procesach akredytacji, którym poddawane są wnioskujące o akredytację jednostki laboratoria, ocenia się kompetencje techniczne, organizację oraz system zarządzania.

3. Certyfikacja w systemach wojskowych – aspekty prawne

Wejście w życie Ustawy o ochronie informacji niejawnych z dnia 22 stycznia 1999 r. (DzU Nr 11, poz. 95), jak również niektórych rozporządzeń typu Rozporządzenie Prezesa Rady Ministrów z dnia 25 lutego 1999 r. w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych (DzU Nr 18, poz. 162), wymusiło zmiany w podejściu do zagadnień związanych z ochroną informacji niejawnych w systemach i sieciach teleinformatycznych. Rozdział 10 ustawy "Bezpieczeństwo systemów i sieci teleinformatycznych" został w całości poświęcony poruszanym problemom. Określa on podstawowe zasady i środki wykorzystywane do zapewnienia bezpieczeństwa teleinformatycznego.

Znajduje to również odzwierciedlenie w kolejnych nowelizacjach ww. ustawy (ostatnia nowelizacja – 03.02.2001). Przepisy ustawy znacznie rozszerzają krąg zainteresowania. Szczególną uwagę zwraca się w niej na ochronę informacji niejawnych w odniesieniu do przedsiębiorstw, jednostek naukowych, badawczo-naukowych. Istotnym elementem, na który położono nacisk, jest posiadanie poświadczenia bezpieczeństwa przez osoby mające bezpośredni dostęp do informacji niejawnych, wydanego przez właściwe służby ochrony państwa. Zostały również uściślone procedury sprawdzające postępowanie odwoławcze i skargowe. Dużym zmianom uległy np. rozdziały 10 (bezpieczeństwo systemów i sieci teleinformatycznych) oraz 11 (bezpieczeństwo przemysłowe), gdzie baczną uwagę zwrócono na techniki kryptograficzne i certyfikację urządzeń.

Podstawowe wymagania dotyczące bezpieczeństwa teleinformatycznego, jakim powinny odpowiadać systemy i sieci teleinformatyczne służące do przetwarzania informacji niejawnych, zostały określone również w drodze rozporządzenia Prezesa Rady Ministrów – *Rozporządzenie Prezesa Rady Ministrów z 25 lutego 1999 r. w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych.*

Systemy i sieci teleinformatyczne, służące do wytwarzania, przechowywania, przetwarzania lub przekazywania informacji niejawnych stanowiących tajemnicę państwową, podlegają szczególnej ochronie przed nieuprawnionym ujawnieniem tych informacji, a także przed możliwością przypadkowego lub świadomego narażenia ich bezpieczeństwa. Powyższe przepisy dostosowały wymagania dotyczące bezpieczeństwa teleinformatycznego do poziomu wymagań, jakie obowiązują w krajach członkowskich Organizacji Traktatu Północnoatlantyckiego (NATO) oraz innych wysoko rozwiniętych państwach (np. w Australii).

Jednym z podstawowych wymogów, które wprowadziła ustawa, jest wymóg posiadania certyfikatu przez system, w którym ma być przetwarzana informacja niejawna stanowiąca tajemnicę państwową. Certyfikat taki wydaje **właściwa służba ochrony państwa** po uprzednim:

- uzyskaniu przez cały personel, mający dostęp do systemu, poświadczeń bezpieczeństwa osobowego;
- zatwierdzeniu przez właściwą służbę ochrony państwa dokumentów szczególnych wymagań bezpieczeństwa (SWB) oraz procedur bezpieczeństwa (PB);
- przeprowadzeniu przez właściwą służbę ochrony państwa badania i oceny zdolności systemu do ochrony informacji niejawnych (sprawdzenia zgodności zapisów w SWB oraz PB ze stanem faktycznym).

W stosunku do resortu obrony narodowej oraz do podmiotów gospodarczych założonych przez MON funkcję służby ochrony państwa realizują Wojskowe Służby Informacyjne (WSI) (Decyzją nr 100/MON Ministra Obrony Narodowej z dnia 06 czerwca 2000 r. została utworzona w WSI Jednostka Certyfikująca Wyroby).

W sferze cywilnej funkcje służby ochrony państwa wykonuje Urząd Ochrony Państwa, w zakresie bezpieczeństwa teleinformatycznego w imieniu Szefa UOP – Biuro Bezpieczeństwa Łączności i Informatyki UOP.

Znowelizowana ustawa wprowadziła m.in. zapis, iż "urządzenia i narzędzia kryptograficzne wchodzące w skład systemów i sieci teleinformatycznych, służące do wytwarzania, przechowywania, przetwarzania lub przekazywania informacji niejawnych stanowiących tajemnicę służbową oznaczonych klauzulą "poufne" podlegają także certyfikacji".

Wytwarzanie, przechowywanie, przetwarzanie lub przekazywanie informacji niejawnych stanowiących tajemnicę państwową odpowiednio do ich klauzuli tajności wymaga certyfikatu dla systemu wydanego przez właściwą służbę ochrony państwa.

Certyfikat taki wydaje się na podstawie:

1) badania i oceny zdolności systemu lub sieci teleinformatycznych do ochrony informacji niejawnych przed nieuprawnionym ujawnieniem oraz przed możliwością narażenia ich bezpieczeństwa,
2) przeprowadzonych zgodnie z ustawą postępowań sprawdzających,
3) zatwierdzonych przez służby ochrony państwa szczególnych wymagań bezpieczeństwa systemu lub sieci teleinformatycznych.

Za przeprowadzenie badań urządzeń oraz wydanie certyfikatu pobiera się opłaty (z wyjątkiem jednostek organizacyjnych będących jednostkami budżetowymi). Wysokość opłat za przeprowadzenie czynności oraz wydanie certyfikatu określa w drodze rozporządzenia Prezes Rady Ministrów.

4. Certyfikacja w systemach wojskowych – rodzaje certyfikatów, aspekty organizacyjne

Jednostka certyfikująca wyroby może wydawać następujące rodzaje certyfikatów:

- certyfikat typu (bezpieczeństwa dla urządzeń i aplikacji w rozumieniu ustawy),
- certyfikat zgodności,
- certyfikat systemów i sieci teleinformacyjnych (w rozumieniu ustawy).

Certyfikat typu wydaje się na moduł kryptograficzny, urządzenie lub oprogramowanie wchodzące w skład systemu. Zawiera on szczegółowe zastrzeżenia dotyczące wydanego certyfikatu oraz termin jego ważności. Uzyskanie tego certyfikatu dla przedmiotu oceny jest warunkiem umieszczenia wyrobu na liście wyrobów preferowanych.

Certyfikat zgodności jest urzędowym dokumentem, formalnym poświadczeniem stwierdzającym zgodność (powtarzalność) przedmiotu oceny z dokumentacją i wzorami wyrobów, stanowiącymi podstawę wydania certyfikatu typu.

W zależności od rodzaju przedmiotu oceny wyróżnia się trzy podstawowe modele dokonywania oceny zgodności (5 ISO, 7 ISO, 8 ISO).

Badania przeprowadza się na wybranej przez jednostkę certyfikującą próbce wyrobu. Pozytywne zakończenie procesu certyfikacji kończy się wydaniem certyfikatu, który (w myśl ustawy) upoważnia do wdrożenia przedmiotu oceny i zastosowania go w resorcie ON.

Certyfikat zgodności zawiera szczegółowe zastrzeżenia dotyczące wydanego certyfikatu oraz termin jego ważności.

Certyfikat systemów i sieci teleinformacyjnych (w rozumieniu ustawy) jest urzędowym dokumentem (formalnym poświadczeniem) gwarantującym, że oceniane przez laboratorium badawcze zabezpieczenia systemu lub sieci teleinformatycznej odpowiadają określonym wymaganiom związanym z ich bezpieczeństwem. Wynika to z faktu, iż w sieciach tych są wytwarzane, przechowywane, przetwarzane lub przekazywane informacje niejawne, stanowiące tajemnicę państwową.

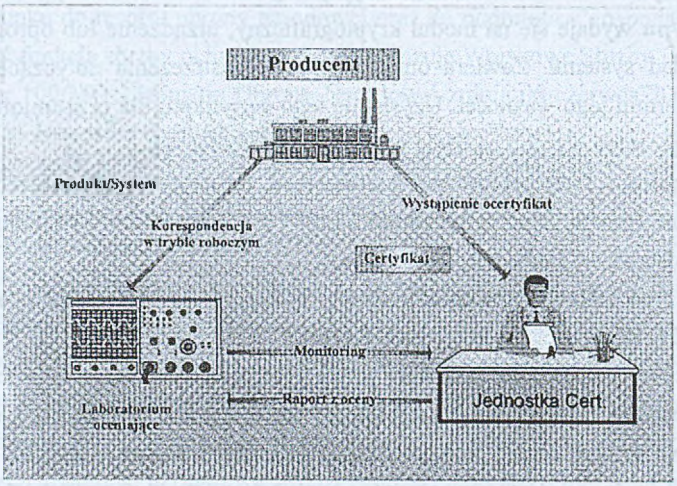
Zgodnie z ustawą certyfikat wydaje się na podstawie:

- wyników badań i oceny zdolności systemu lub sieci teleinformatycznych przeznaczonych do ochrony informacji niejawnych przed nieuprawnionym ujawnieniem oraz przed możliwością narażenia ich bezpieczeństwa;
- przeprowadzonego zgodnie z ustawą postępowania sprawdzającego,
- zatwierdzonych przez Wojskowe Służby Informacyjne Szczególnych Wymagań Bezpieczeństwa Systemów lub Sieci Teleinformatycznych.

Proces prowadzenia badań i certyfikacji można podzielić na następujące etapy:

- złożenie wniosku strony zainteresowanej do jednostki certyfikującej (JCW) WSI,
- wstępne oszacowanie złożoności badań i kosztów przez laboratorium badawcze,

- podpisanie umowy o badania i certyfikację,
- dostarczenie przedmiotu oceny wraz z wymaganą dokumentacją do JCW WSI,
- zlecenie przez JCW WSI dokonania badania przez laboratorium badawcze,
- rejestracja wniosku i umieszczenie przedmiotu oceny na liście wyrobów będących w certyfikacji JCW WSI,
- rozpoczęcie badań laboratoryjnych.



Rys. 2. Proces certyfikacji
Fig. 2. Certification process

Proces certyfikacji nakłada na wnioskodawcę dodatkowe zobowiązania, m.in.:

- nieodpłatnego dostarczenia do laboratorium badawczego wymaganych przezeń dokumentów, narzędzi oraz oprogramowania, niezbędnych do przeprowadzenia oceny;
- udziału kompetentnych przedstawicieli firmy w procesie badawczym.

Przed dokonaniem rejestracji wniosku dokonywana jest wstępna analiza kompletności dostarczonej dokumentacji. Fakt rejestracji wniosku oznacza rozpoczęcie właściwej procedury certyfikacji. Po zarejestrowaniu wniosku przedmiot oceny umieszcza się na liście wyrobów będących w certyfikacji w JCW WSI.

Certyfikat wydaje się jedynie w przypadku, gdy przedmiot oceny odpowiada uznanym i zatwierdzonym kryteriom bezpieczeństwa. Badania zabezpieczeń urządzeń, systemów i sieci teleinformatycznych, jakie wykonywane są przez laboratorium, prowadzi się w chwili obecnej na podstawie europejskich kryteriów określonych w normie – Information Technology Security Evaluation Criteria z 1991 r. (ITSEC), a w przyszłości – wg międzynarodowych kryteriów Common Criteria (CC), na bazie których opracowywana jest aktualnie Polska Norma (PN-ISO/IEC 15408).

W zakresie dokumentacji wnioskodawca zobowiązany jest dostarczyć m.in.

1. Dokumentację wymaganą „Przepisami o Dokumentacji Urządzeń Techniki Wojskowej DUTW-73" oraz „Wojskowymi Polskimi Normami WPN-84", zawierającą:
   a) zatwierdzone: „Założenia Taktyczno-Techniczne (ZTT)" oraz „Metodykę Badań" lub „Warunki Techniczne".
   b) „Protokół badań (Końcowy protokół badań kwalifikacyjnych)".
   c) „Dokumentację konstrukcyjną".
   d) „Dokumentację eksploatacyjną".
2. Dokumentację do celów oceny i certyfikacji", zawierającą:
   a) „Dokument Wymagań Bezpieczeństwa", opisujący funkcjonalność według ITSEC.
   b) „Dokument analizy skuteczności zabezpieczeń" opisujący pewność-skuteczność według ITSEC.
   c) „Dokument autentyczności dostarczania" opisujący pewność-poprawność według ITSEC.
   d) „Dokument poprawności i jakości wykonania" opisujący pewność-poprawność według ITSEC.
   e) Dokumentację algorytmu kryptograficznego.

W procesie badawczym prowadzonym przez laboratorium dokonuje się oceny:

- funkcjonalności przedmiotu oceny,
- poprawności w zakresie:
  - kompletności dokumentacji oraz jej poprawności i spójności wykonania;
  - zgodności opisów ze stanem faktycznym;
- skuteczności rozwiązań w zakresie:
  - ochrony kryptograficznej;
  - ochrony elektromagnetycznej;
  - odporności na nieuprawnioną penetrację.

Współpraca laboratorium z wnioskodawcą i producentem pod nadzorem jednostki certyfikującej WSI dotyczy:

- uzupełnienia i poprawienia dokumentacji wymaganej przez ustalone kryteria,
- poprawienia wykrytych usterek i błędów w przedmiocie oceny,
- zmiany w konstrukcji ocenianego produktu, w celu dostosowania wymagań związanych z klauzulą tajności.

Efektem końcowym jest opracowanie raportu końcowego, w którym przedstawione są wyniki badań oraz opracowanie załączników do ww. raportu, zawierającego:

- zastrzeżenia dla producenta,
- zastrzeżenia dla użytkownika.

Raport opracowany w laboratorium oraz zastrzeżenia podlegają zatwierdzeniu przez jednostkę certyfikującą, która wydaje stosowny certyfikat.

LITERATURA

1. Polska Norma PN-I-13335-1 – "Wytyczne do zarządzania bezpieczeństwem systemów informatycznych. Pojęcia i modele bezpieczeństwa systemów informatycznych", cz. 1.
2. Wiśniewski A.: Analiza ryzyka. Wytyczne dla administratorów systemów. AZW.
3. Weierbach R.: Vulnerability assessments. INFS 762, 2000.
4. Gallagher B. P.: Software acquisition. Risk management. Key Process Area (KPA) – A guidebook. 1999.
5. Materiały konferencyjne – II Sympozjum "Bezpieczeństwo systemów informacyjnych".

Recenzent: Prof. dr hab. inż. Andrzej Grzywak

Wpłynęło do Redakcji 6 listopada 2001 r.

Abstract

The purpose of IT security policy is creation of basis, procedures and requirements necessary to ensure proper protection of processed information. It includes security of communication and IT means, as well as personal, physical, industrial and emission security. The main security policy assumption is qualification of:

- what information groups will be protected,
- in which systems these information may be processed,
- who and on which principles should have an access to them,
- who is responsible for information management,
- who is responsible for security of information management,
- what conditions should be met to gain authentication, testimonies and certificates.

The constant element of security policy is conducting of current analyses, connected with vulnerability IT systems to threats, so called threaten analysis. This includes inseparably another one – risk management. Risk management encompasses methods and activities towards decreasing influence of risk level on system functionality, which allows to take an optimal decision. Detailed recognition of character and range of potential risk let to choose

preventive activities or to minimise its impact and result at the right time. This presentation show suitable methods of risk management in IT systems and networks.

There are many of networks and IT systems threats, like: environmental – independent of human as well as human depended. Information transferred in computer networks can be subject to number of threats, like: computer suspension, virus attacks, unauthorised access to networks. So, the substantial problem is a proper protection.

One of the basic requirements in systems, where classified information is processed, which brought the act about classified information protection, dated January 22nd 1999 into effect, is certification possessing requirement. This certification should be issued by proper national security services. Fulfilment of presented conditions, working up suitable documents (SSRS, SecOps) are essential to apply for products, systems and network security certification.