Zachodniopomorski Uniwersytet Technologiczny w Szczecinie
Wydział Informatyki

Streszczenie pracy doktorskiej pt.:

Ocena bezpieczeństwa systemów teleinformatycznych przetwarzających informacje niejawne

Autor: mgr. inż. Damian Kacprowicz
Promotor: Prof. zw. dr hab. dr h.c. mult. Brunon Hołyst
Promotor pomocniczy: dr inż. Witold Maćków

Postęp w dziedzinie technologii teleinformatycznych spowodował, że większość działalności organizacyjnych opiera się na przetwarzaniu informacji w systemach teleinformatycznych. Z jednej strony ułatwia to gromadzenie i przesyłanie informacji, ale z drugiej strony stwarza dodatkowe zagrożenia związane z możliwością przestępczego kopiowania i modyfikacji danych.

Charakterystyka systemów teleinformatycznych wymaga zastosowania odpowiednich zabezpieczeń, aby chronić zasoby systemu przed różnymi zagrożeniami, którym są one narażone w swoim środowisku produkcyjnym. Zasoby systemów teleinformatycznych, w szczególności zasoby informacyjne, są niezwykle ważnymi aktywami organizacji i wymagają odpowiedniej ochrony, niezależnie od ich formy. Bezpieczeństwo elektronicznie przetwarzanych informacji ma fundamentalne znaczenie, zwłaszcza w przypadku poufnych informacji objętych ustawową ochroną.

Wiele norm oraz zaleceń określa potrzebę oceny poziomu bezpieczeństwa dla perspektywy ochrony. Istniejące metody charakteryzują się dużą złożonością a co za tym idzie podatną na błędy. Stosowanie zbyt złożonych metod tworzy ryzyko wykonania oceny bezpieczeństwa jedynie na etapie akredytacji systemów a nie zgodnie z zasadami aplikacji cyklicznie co pewien czas. Brak systematyczności zaniża poziom bezpieczeństwa chronionych systemów.

Koncepcja badawcza obejmuje przegląd istniejących standardów, metod oceny bezpieczeństwa w celu zaproponowania efektywnej procedury oceny poziomu bezpieczeństwa systemu teleinformatycznego.

Proponowana ocena mechanizmów bezpieczeństwa uwzględniać będzie najważniejsze atrybuty bezpieczeństwa tj. poufność, integralność oraz dostępność zawartości informacyjnej systemów teleinformatycznych.

Praca składa się z czterech rozdziałów.

Pierwszy rozdział wprowadza do tematu bezpieczeństwa informacji, przedstawiając podstawowe kategorie informacji wymagających ochrony, argumenty dla ich zabezpieczenia, klasyfikację informacji,

proces klasyfikacji i zawartość metadanych plików cyfrowych, cykl funkcjonowania systemu teleinformatycznego oraz kluczowe aspekty ochrony informacji. Obejmuje on również zwrócenie uwagi na różnorodne czynniki i zagrożenia, które mogą mieć wpływ na ich bezpieczeństwo, a także konieczność skoncentrowania się na zarządzaniu ryzykiem i minimalizacji potencjalnych zagrożeń.

Drugi rozdział koncentruje się na ocenie poziomu bezpieczeństwa informacji w systemie. Składa się z kilku etapów, które mają na celu ustalenie stopnia ochrony informacji oraz identyfikację zagrożeń i ryzyka z nimi związanego. Pierwszym etapem jest identyfikacja chronionych zasobów informacyjnych i określenie ich wartości. Następnie dokonuje się identyfikacji zagrożeń i ocenia ich poziom, co umożliwia identyfikację i oszacowanie ryzyka. Proces ten opiera się na analizie wartości informacji, zagrożeń i podatności, a wynikowa ocena ryzyka służy do ustalenia priorytetów w działaniach mających na celu zapewnienie odpowiedniego poziomu bezpieczeństwa informacji.

Trzeci rozdział przedstawia kompleksową metodę oceny bezpieczeństwa informacji. Składa się ona z etapów, które obejmują identyfikację zasobów informacyjnych, zagrożeń, oszacowanie skutków utraty zasobów oraz ocenę ryzyka. Uwypuklonym jest jak ważnym jest zachowanie poufności, integralności i dostępności informacji, a także przeciwdziałanie szkodom poprzez odpowiednie środki ochrony.

Czwarty rozdział omawia różne działania mające na celu utrzymanie zakładanego poziomu bezpieczeństwa informacji. Obejmuje to przeglądy ryzyk, nadzór i kontrolę zgodności z dokumentacją bezpieczeństwa, monitorowanie bezpieczeństwa w czasie rzeczywistym, informowanie o pojawiającym się ryzyku i aktualizowanie zabezpieczeń oraz uświadamianie i szkolenie pracowników. Określona zostanie możliwość aplikacji proponowanej metody. Wszystkie te działania są istotne dla zapewnienia trwałego i skutecznego bezpieczeństwa informacji w systemie.

W trakcie badań nad proponowaną metodą oceny bezpieczeństwa przeprowadzono konsultacje z ekspertami (Audytorami udzielającymi akredytacji systemów), interesariuszami (Kierownikami Jednostek Organizacyjnych przetwarzających informacje wrażliwe, Administratorami systemów, Inspektorami Bezpieczeństwa Teleinformatycznego, Kierownikami Kancelarii Tajnych oraz Kancelarii Kryptograficznych, Użytkownikami). Dzięki temu uzyskano różnorodne perspektywy i cenne doświadczenia.

Damian Kacpiewicz
16.05.2024