POLITECHNIKA WARSZAWSKA

Wydział Zarządzania

STRESZCZENIE ROZPRAWY DOKTORSKIEJ

mgr inż. Michał Wiśniewski

Zarządzanie sytuacyjne bezpieczeństwem infrastruktury krytycznej

Promotor

Prof. dr hab. inż. Tadeusz Krupa

Warszawa 2018

Streszczenie

W rozprawie została podjęta problematyka zarządzania bezpieczeństwem infrastruktury krytycznej (IK) z perspektywy podmiotów odpowiedzialnych za jej bezpieczeństwo, sprowadzona do opracowania integralnego modelu bezpieczeństwa infrastruktury krytycznej (IM-BIK) i bazującej na nim metodyki zarządzania sytuacyjnego bezpieczeństwem infrastruktury krytycznej (ZS-BIK). Zaproponowane rozwiązania przedstawiają sposób postępowania w obszarze odwzorowania charakterystyki IK, umożliwiającej wygenerowanie scenariuszy zdarzeń niekorzystnych (SZN), oszacowanie ryzyka związanego z zagrożeniami, na które podatna jest rozpatrywana IK oraz sformułowania i rozwiązania problemu decyzyjnego wskazującego zestaw zabezpieczeń eliminujący lub redukujących ryzyko do wymaganego poziomu.

W rozprawie opracowano program realizacji badań w konwencji poziomów gotowości technologicznej (PGT). Ze względu na dostępność danych dotyczących IK założono, że osiągnięty zostanie piąty PGT oznaczający zweryfikowanie opracowanych rozwiązań w warunkach zbliżonych do rzeczywistych.

W ramach prac nad IM-BIK oraz metodyką ZS-BIK przeprowadzono badania dostępnej literatury z obszaru zarządzania bezpieczeństwem IK, co pozwoliło na rozpoznanie barier, utrudniających współdziałanie podmiotów odpowiedzialnych za bezpieczeństwo IK, do których zaliczono rozbieżności definicji ochrony IK, brak standardu określania charakterystyki IK oraz brak metodyki zarządzania bezpieczeństwem IK.

Analiza aktów normatywnych, strategii, programów, norm oraz metodyk oceny ryzyka na rzecz zarządzania kryzysowego pozwoliła na ustalenie wzorcowych etapów postępowania dla metodyki ZS-BIK takich jak: powołanie zespołu analitycznego, określenie progów bezpieczeństwa funkcjonalności IK, odwzorowanie charakterystyk IK, wygenerowanie SZN, sformułowanie problemu decyzyjnego, szacowanie ryzyka oraz wdrożenie zabezpieczeń. Etapy metodyki ZS-BIK wskazują na bazowe elementy IM-BIK tj. możliwość: odwzorowania charakterystyki IK, generowania SZN, formułowania problemu decyzyjnego, szacowania ryzyka.

W rezultacie ustalenia składowych IM-BIK przeanalizowano istniejące metody wykorzystywane do: określania charakterystyki rozpatrywanego obiektu, formułowania

scenariuszy zdarzeń, szacowania ryzyka i rozwiązywania problemów decyzyjnych. Na podstawie dokonanej oceny wskazano rozwiązania bazowe dla elementów IM-BIK.

W obszarze IM-BIK zaproponowano model sytuacji IK, opracowany na podstawie modelu sytuacji Kłykowa, który integruje dane wymagane do określenia charakterystyki IK dotyczące: zasobów, funkcjonalności, zagrożeń, i zabezpieczeń. Model sytuacji IK warunkuje możliwość wykonania metod IM-BIK: szacowania ryzyka – wykorzystującej dostosowany do modelu sytuacji IK wzór na ryzyko, generowania SZN – wykorzystującej twierdzenie Bayesa oraz formułowania problemu decyzyjnego – wykorzystującej metodę analizy powiązanych obszarów decyzyjnych.

W odpowiedzi na potrzeby podmiotów odpowiedzialnych za bezpieczeństwo IK i uwzględniając wnioski z analizy metodyk oceny ryzyka na potrzeby zarządzania kryzysowego, opracowano metodykę ZS-BIK, której dopełnieniem są procedury jej realizacji dla przypadku płaskiego i hierarchicznego problemu decyzyjnego.

W eksperymentach obliczeniowych weryfikujących metodykę ZS-BIK dla przypadków płaskich i hierarchicznych problemów decyzyjnych wykorzystano dane charakteryzujące rafinerię PKN ORLEN sp. S.A. Wyniki eksperymentów potwierdziły użyteczność metodyki ZS-BIK w obszarze: określania charakterystyki IK, generowania SZN na podstawie modeli IK, formułowania problemu decyzyjnego i wskazania zbioru zabezpieczeń, szacowania poziomu ryzyka utraty funkcjonalności przed i po zastosowaniu dodatkowych zabezpieczeń, wdrożenia zabezpieczeń.

Słowa kluczowe

planowanie cywilne, zarządzanie kryzysowe, podejście sytuacyjne, bezpieczeństwo, infrastruktura krytyczna, funkcjonalność infrastruktury krytycznej, szacowanie ryzyka, próg bezpieczeństwa, kanon infrastruktury krytycznej, sytuacja infrastruktury krytycznej, integralny model bezpieczeństwa infrastruktury krytycznej, metodyka zarządzania sytuacyjnego bezpieczeństwem infrastruktury krytycznej, problem decyzyjny, scenariusz zdarzenia niekorzystnego

Summary

Presented thesis reveals a detailed analysis of the security management of the critical infrastructure (CI) from the perspective of entities responsible for its security, essential for the development of an integral model of critical infrastructure safety (IMCIS) and evolution of the situational management of critical infrastructure safety (SMCIS) methodology based on IMCIS. Proposed solutions show a novel and proper way of proceeding in the area of CI characteristics mapping, what allows for the generation of unfavorable events scenarios (UES) and assessment of the risk associated with the threats on which the CI is prone to. Moreover, it provides information about the formulation and solving of the decision problem indicating a set of protections utilized for the risk elimination and/or reduction to the required level.

For chosen results indicated in this dissertation, a program for the implementation of tests was prepared, in the convention of technological readiness levels. Due to the availability of the data regarding CI, it was assumed that the fifth level of technological readiness will be achieved, meaning that the verification of the solutions developed in such conditions is close to reality.

As part of the research performed on IMCIS and SMCIS, literature survey regarding critical infrastructure security management area was also conducted. As a result, the hampering barriers in subjects' cooperation which are responsible of CI safety were determined. They include: discrepancy in the definition of IC security, lack of standards to describe CI characteristic and deficiency in methodology of CI safety management.

The analysis of normative acts, strategies, programs, standards and risk assessment techniques for crisis management allowed for setting up an exemplary process steps for the SMCIS methodology, i.e. establishment of an analytical team, defining security thresholds of CI functions, CI characteristics mapping, generation of UES, formulation of a decision problem, risk estimation and security implementation. Stages of the SMCIS mimic the basic elements of IMCIS system, i.e. the possibility of CI characteristics projection, generation of UES, formulation of a decision problem or risk assessment.

In order to define IMCIS components, the existing/available methods used for the determination of the characteristics of the considered object, event scenarios formulations, risk estimation and solve decision problems were deeply analyzed. Based on the performed assessment, the basic solutions for IMCIS elements were indicated.

In the case of IMCIS, CI situation model was proposed and developed on the basis of the Kłykow situation theory, which integrates all the data required for the determination of CI characteristics regarding: resources, functionality, threats and security. The CI situation model gives the possibility of implementation of the ICISM methods such as: risk estimation – utilizing the risk model adapted to the model of CI situation, generation of UES – involving the Bayes theorem and the formulation of a decision problem - using the method for analysis of interconnected decision areas.

Taking into consideration subjects' needs/requirements responsible for CI safety as well as conclusions obtained from the analysis/assessment of the risk for crisis management, the SMCIS has been developed and updated with procedures for its implementation for the case of flat and hierarchical decision problems.

To verify the SMCIS methodology, the computational experiments for flat and hierarchical decision problems were conducted utilizing the data used for characterization of PKN ORLEN refinery Inc. Obtained results fully confirmed accurateness of SMCIS model in terms of: determination of CI characterization, generation of UES based on CI models, formulation of a decision problem and identification of a security set, estimation of the level of risk of functionality loss before and after applying additional safeguards, security implementation.

Key words

civil planning, crisis management, situational approach, security, critical infrastructure, functionality of critical infrastructure, risk assessment, security threshold, canon of critical infrastructure, situation of critical infrastructure, integral model of critical infrastructure security, methodology situational management of critical infrastructure safety, decision problem, adverse event scenario