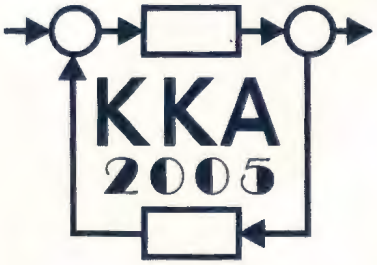
XV Krajowa Konferencja Automatyki

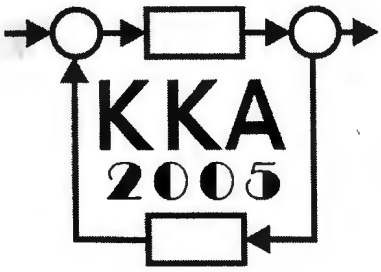
Tom II



Redaktorzy:
Zdzisław Bubnicki
Roman Kulikowski
Janusz Kacprzyk

XV Krajowa Konferencja Automatyki

Tom II



Redaktorzy:
Zdzisław BUBNICKI
Roman KULIKOWSKI
Janusz KACPRZYK

ORGANIZATOR
Komitet Automatyki i Robotyki Polskiej Akademii Nauk
Instytut Badań Systemowych Polskiej Akademii Nauk
WSPÓŁORGANIZATORZY
Politechnika Warszawska
Przemysłowy Instytut Automatyki i Pomiarów
Polskie Stowarzyszenie Pomiarów, Automatyki i Robotyki

ORGANIZATOR

Komitet Automatyki i Robotyki Polskiej Akademii Nauk
Instytut Badań Systemowych Polskiej Akademii Nauk

WSPÓŁORGANIZATORZY

Politechnika Warszawska
Przemysłowy Instytut Automatyki i Pomiarów
Polskie Stowarzyszenie Pomiarów, Automatyki i Robotyki

KOMITET PROGRAMOWY

Przewodniczący	Zdzisław BUBNICKI
Zastępca Przewodniczącego	Roman KULIKOWSKI

CZŁONKOWIE

Stanisław BAŃKA	Michał BIAŁKO
Mikołaj BUSŁOWICZ	Władysław FINDEISEN
Ryszard GESSING	Henryk GÓRECKI
Jakub GUTENBAUM	Jerzy JÓZEFCZYK
Stanisław KACZANOWSKI	Tadeusz KACZOREK
Janusz KACPRZYK	Jerzy KLAMKA
Józef KORBICZ	Zbigniew KOWALSKI
Krzysztof KOZŁOWSKI	Juliusz L. KULIKOWSKI
Krzysztof KUŹMIŃSKI	Kazimierz MALANOWSKI
Krzysztof MALINOWSKI	Wojciech MITKOWSKI
Antoni NIEDERLIŃSKI	Władysław PEŁCZEWSKI
Tadeusz PUCHAŁKA	Leszek RUTKOWSKI
Stanisław SKOCZOWSKI	Roman SŁOWIŃSKI
Jerzy ŚWIĄTEK	Andrzej ŚWIERNIAK
Ryszard TADEUSIEWICZ	Piotr TATJEWSKI
Krzysztof TCHOŃ	Leszek TRYBUS
Jan WĘGLARZ	Andrzej P. WIERZBICKI

KOMITET ORGANIZACYJNY

Przewodniczący	Roman KULIKOWSKI
Zastępcy Przewodniczącego	Janusz KACPRZYK
	Stanisław KACZANOWSKI
	Tadeusz KACZOREK
	Krzysztof MALINOWSKI
Członkowie	Roman OSTROWSKI
	Tadeusz PUCHAŁKA
	Dariusz WAGNER
Sekretarze naukowi	Jan STUDZIŃSKI
	Jan W. OWSIŃSKI

ISBN 83-89475-01-4

Copyright © Instytut Badań Systemowych Polskiej Akademii Nauk
All rights reserved

Druk: ARGRAF, Warszawa

STEROWANIE
I TECHNIKA KOMPUTEROWA

ZASTOSOWANIE GRY SYMULACYJNEJ DO ANALIZY BEZPIECZEŃSTWA SYSTEMÓW INFORMATYCZNYCH

Ireneusz J. JÓŹWIAK*, Wojciech LASKOWSKI*

* Politechnika Wrocławska, Instytut Informatyki Stosowanej
ul. Wybrzeże Wyspiańskiego 27, 50-370 Wrocław,
e-mail:ireneusz.jozwiak@pwr.wroc.pl; w.laskowski@wop.pl

Streszczenie: Prezentowany artykuł dotyczy zagadnień związanych z bezpieczeństwem teleinformatycznym. Zaprezentowano koncepcję wykorzystania gry symulacyjnej do badania bezpieczeństwa systemów informatycznych. Przedstawione zostały elementy teoriogrowego modelu, który znalazł zastosowanie w prowadzonych badaniach. Zamieszono krótki przegląd literatury, stanowiącej punkt wyjścia dla podjętych badań. Z uwagi na uniwersalność prezentowanych rozwiązań, gra symulacyjna może być stosowana do badania bezpieczeństwa oraz niezawodności złożonych komputerowych systemów sterowania i automatyki.

Słowa kluczowe: Bezpieczeństwo teleinformatyczne, modele teoriogrowe, gra symulacyjna.

1. WPROWADZENIE

W dziedzinie bezpieczeństwa teleinformatycznego mamy bez wątpienia do czynienia z sytuacjami konfliktowymi. Zgodnie z definicją konfliktu (np. Słownik Języka Polskiego PWN), jest to „zjawisko wyrażające sprzeczność interesów, spór, zatarg, kolizję". Wspomniane zjawisko zachodzi w momencie, gdy przeciwstawiają się cele i działania, co najmniej dwóch stron – uczestników konfliktu. Wydaje się, iż problematyka bezpieczeństwa teleinformatycznego może być analizowana właśnie poprzez pryzmat terminologii i narzędzi związanych z sytuacjami konfliktowymi.
Poszukując języka, który w sposób formalny wyraziłby zależności zachodzące w rozpatrywanych sytuacjach, należy zwrócić się w stronę teorii gier. Podejście teoriogrowe, prezentujące modele i analizy w kontekście bezpieczeństwa, spotykane jest w szeregu publikacji. Dostępne opracowania można podzielić, na co najmniej trzy grupy:

1. prace prezentujące rozważania w kontekście systemów wykrywania włamań np. [2],[3]
2. prace poruszające zagadnienia bezpieczeństwa sieci mobilnych (bezprzewodowych) [1], [17]
3 prace o charakterze militarnym (m.in. poruszające zagadnienia wojny informacyjnej), [4],[5], [6], [7], [8].

Inny podział prowadzi do klasyfikacji publikacji według przyjętych modeli teorii gier, np. niekooperacyjna gra o sumie niezerowej [9], [13], gra stochastyczna [16], gra kooperacyjna [2].

Cytowane prace pozwalają nakreślić ramy problematyki, w której umiejscowione zostają prezentowane w niniejszej publikacji rozważania.
Ogólne wnioski z przeglądu literatury przedstawiają się następująco:

1. teoria gier pozwala na modelowanie wybranych aspektów bezpieczeństwa teleinformatycznego,
2. w dostępnej literaturze prezentowane modele i wyniki prac mają charakter teoretyczny, słabo podkreśla się możliwości ich praktycznego wykorzystania,
3. zauważalny jest brak narzędzi w postaci np. komputerowych gier symulacyjnych, za pomocą których możliwe byłoby zweryfikowanie modeli teoriogrowych na drodze symulacji interaktywnej.

2. ELEMENTY TEORII GIER

2.1. Notacja i definicje

Dwuosobowa gra w postaci normalnej (strategicznej) o sumie zerowej, określona jest poprzez trójkę (X,Y,A), gdzie
X – niepusty zbiór strategii gracza I
Y – niepusty zbiór strategii gracza II
A – funkcja wypłaty, przyjmująca wartości ze zbioru liczb rzeczywistych.
Skończona, dwuosobowa gra w formie strategicznej (X,Y,A) jest określana jako gra macierzowa, z uwagi na fakt, iż funkcja wypłaty może być przedstawiona jako macierz. Przyjmując zbiory strategii w postaci $X=\{x_1,x_2,\ldots,x_m\}$ oraz $Y=\{y_1,y_2,\ldots,y_n\}$, macierz A może być określona jako:

$$A=\begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \ldots & & \ldots \\ a_{mi} & \ldots & a_{mn} \end{pmatrix}$$

Wybór wierszy macierzy A odpowiada wybraniu strategii przez gracza I, zaś wybór kolumn – wybraniu strategii przez gracza II.

W przypadku rozpatrywania gry o sumie dowolnej (niezerowej), funkcja wypłaty określona jest za pomocą dwóch funkcji o wartościach ze zbioru liczb rzeczywistych: $u_1(x,y)$ oraz $u_2(x,y)$. Macierz wypłat staję się macierzą uporządkowanych dwójek (x,y). Alternatywą dla takiego zapisu, jest przedstawienie wypłat za pomocą dwóch macierzy A i B, prezentujących wypłaty gracy I i II odpowiednio.

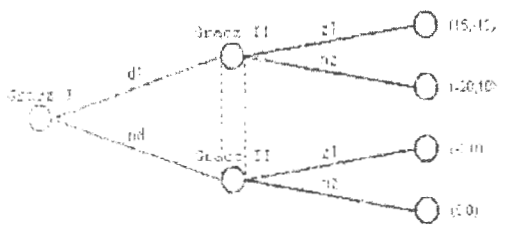
Rozważane strategie, określa się mianem strategii czystych. Strategie czyste związane są z dokonywanie konkretnych, czytelnych wyborów, w odróżnieniu od strategii mieszanych, gdzie wybór uzależniany jest od prawdopodobieństwa podjęcia określonych działań przez stronę przeciwną.
W prezentowanym przykładzie zastosowanie znalazło pojęcie strategii mieszanych z uwagi na fakt, iż takie podejście jest bliższe rzeczywistości.
Reprezentacją gry w postaci rozszerzonej jest drzewo decyzyjne (dendryt). W niniejszym opracowaniu, zdecydowano się nie przytaczać formalnej definicji gry w postaci ekstensywnej, ograniczając się do praktycznego przykładu.
Przyjmijmy, ze danych jest zbiór znanych zagrożeń $Z = \{z_1, z_2, \ldots\ldots, z_m\}$ oraz zbiór mechanizmów (środków) zabezpieczeń $D = \{d_1, d_2, \ldots\ldots, d_n\}$. Dla uproszczenia i potrzeb dalszych rozważań, przyjmijmy, ze zbiór $Z = \{z_1\}$ oraz zbiór $D = \{d_1\}$. Gracz I (defensywny) wybiera działania ze zbioru D, zaś gracz II (ofensywny) wybiera działania ze zbioru Z.

2.2. Model teoriogrowy

Uwzględniając przyjętą notację i założenia, zostanie przedstawiony model elementarnej sytuacji konfliktowej w dziedzinie bezpieczeństwa teleinformatycznego.

Rozpatrywana jest następująca rzeczywista sytuacja: gracz defensywny (gracz I) staje przed wyborem zainstalowania np. oprogramowania antywirusowego w systemie bądź też nie instalowania takiego oprogramowania. Natomiast strona zorientowana na działania destrukcyjne (gracz II) może wprowadzić do systemu oprogramowanie złośliwe (pod dowolną postacią, np konia trojańskiego, lub wirusa), bądź też nie robić nic w tym zakresie.

Reprezentacja decyzji graczy, wyrażona w postaci formy rozszerzonej gry jest przedstawiona na rys. 1. .



Rys. 1. Gra w postaci ekstensywnej. Opracowanie własne.

Analizowana sytuacja konfliktowa, może być przedstawiona w postaci strategicznej (rys. 2), zakładając ogólne wartości funkcji wypłaty.

	z1	nz
d1	$\alpha_s, -\beta_d$	$-\alpha_f, 0$
nd	$-\alpha_a, \beta_h$	0,0

Rys. 2. Gra w postaci normalnej (macierz wypłat). Opracowanie własne.

Poszczególne wartości macierzy prezentowanej na rys. 2, mają następujące znaczenie:

α_s - wypłata (zysk) gracza. I w przypadku, gdy wdrożono skuteczny mechanizm zabezpieczeń

β_d - koszt nieskutecznego ataku na system informatyczny (strata gracza II)

α_f - koszt zabezpieczenie, zabezpieczeń przypadku braku działań destrukcyjnyc (koszt wdrożenia zabezpieczeń)

α_a - koszt poniesiony przez gracza I w przypadku skutecznego ataku na system (strata gracza I)

β_h - wypłata (zysk) gracza II w przypadku, gdy atak zakończył się powodzeniem

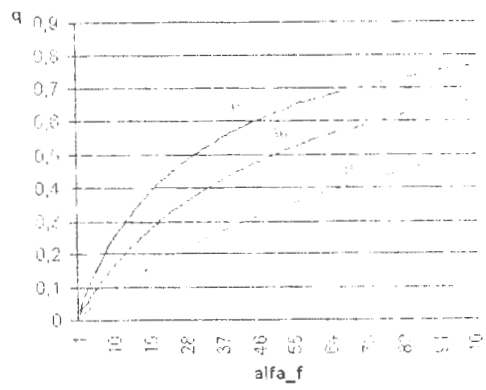
Gracz I, działając racjonalnie, powinien uzależnić swoją wypłatę od oszacowanych prawdopodobieństw podejmowania konkretnych akcji przez gracza II (czyli oczekiwana wypłata gracza I jest wyrażona poprzez rozkład prawdopodobieństwa na zbiorze strategii gracza II).
Niech p oznacza prawdopodobieństwo wyboru strategii d_1 przez gracza I, zaś q – prawdopodobieństwo wyboru strategii z_1 przez gracza II.
Decydują się na konkretne działania gracz I powinien rozważyć następującą zależność:

$$\alpha_s q - \alpha_f (1-q) = -\alpha_a q \qquad (1)$$

co w praktyce oznacza uzależnienie otrzymanej wypłaty od decyzji gracza II.
Z równania (1) otrzymujemy:

$$q = \frac{\alpha_f}{\alpha_f + \alpha_s + \alpha_a} \qquad (2)$$

Wartość α_f oznacza koszt poniesiony przez gracza I w przypadku, gdy zabezpieczenia zostały wdrożone, ale brak jest działań ze strony intruza. Może być, zatem interpretowana jako koszt wdrożenia mechanizmu d_1. Zależność (2) przedstawiona graficznie na rys. 3, pozwala zauważyć następującą prawidłowość: wraz ze wzrostem kosztu zabezpieczeń, rośnie prawdopodobieństwo zaatakowanie systemu. Odpowiada to sytuacji w której intruz przekonany jest, iż kosztowne zabezpieczenia racjonalny gracz defensywny będzie wdrażał z pewną ostrożnością i niechętnie.



Rys. 3 Prawdopodobieństwo podejmowania działań przez gracza II w zależności od wartości funkcji współczynnika α_f przy różnych wartościach zysków gracza I. Opracowanie własne.

Przebieg zależności zilustrowano dla trzech przypadków, przy rosnących wartościach składnika $\alpha_a + \alpha_s$ (czyli sumy wartości bezwzględnej zysków i strat gracza I). Przyjęto następujące wartości: 30, 50 i 100, które można interpretować jako rzeczywista wartość systemy dla strony zabezpieczającej. Widzimy, że w momencie, gdy rośnie koszt zabezpieczeń, przy dużej wartości $\alpha_a + \alpha_s$ prawdopodobieństwo zaatakowania systemu wykazuje charakter malejący. W tym przypadku zysk lub/i strata może wyrażona w postaci dóbr ekonomicznych, a także może oznaczać reputację gracza I. Prezentowane rozważania ilustrują intuicyjnie dostrzegalną, ale nie zawsze właściwie interpretowaną i rozumianą, zależność pomiędzy skutkami elementarnych decyzji w zakresie wdrażania zabezpieczeń zasobów informacyjnych. Pozwalają spojrzeć na problematykę zabezpieczeń nieco z innej perspektywy.

Powtarzając powyższe rozumowanie w odniesieniu do gracza II, jego wypłata uzależniona od decyzji gracza I może być opisana za pomocą zależności:

$$p = \frac{\beta_h}{\beta_h + \beta_d} \qquad (3)$$

Otrzymana ten sposób uporządkowana para wartości prawdopodobieństw (p, q), odpowiada sytuacji równowagi w grze niekoopracyjnej [18]. W ogólnym przypadku, znajdowanie punktu równowagi nawet prostych gier dwuosobowych jest problemem złożonym obliczeniowo, a poszukiwanie efektywnych algorytmów wyznaczających równowagę, jest stale otwartym problemem badawczym.

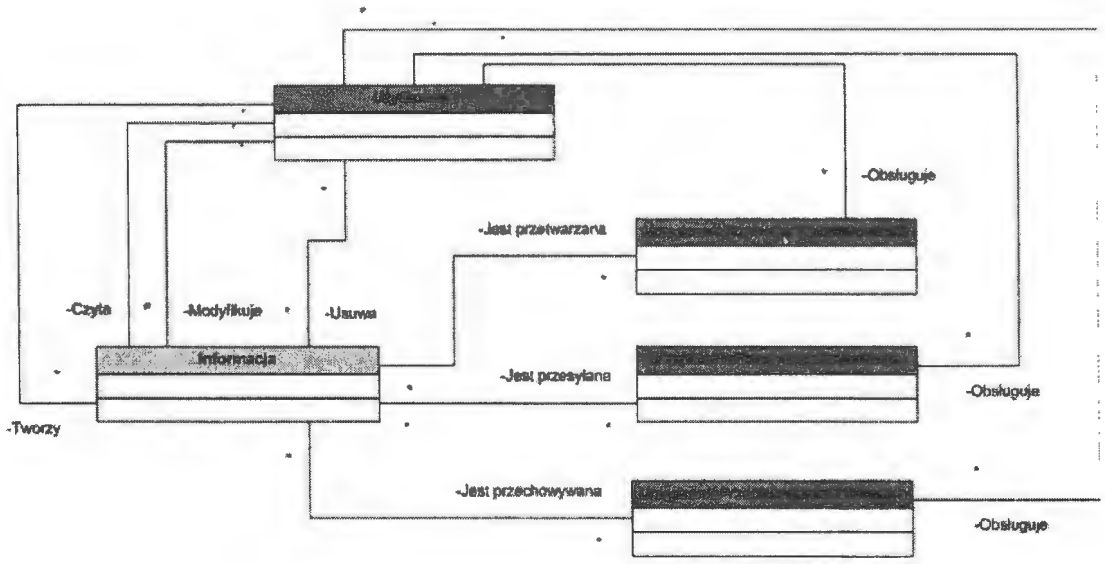
Opis i analiza zjawisk związanych z bezpieczeństwem teleinformatycznym za pomocą metod formalnych stanowi pierwszy krok konstruowania narzędzia w postaci komputerowej gry symulacyjnej. Z oczywistych względów, niemożliwe jest wierne uchwycenie wszystkich aspektów bezpieczeństwa w postaci modeli teorii gier. Dlatego też, racjonalnym postępowaniem jest dokonanie rozbicia problemów bezpieczeństwa na drodze procesu badawczego – analizy na składniki podstawowe. Rzecz jasna, elementarność tych składników jest umowna a zaliczenie ich w ten poczet ma charakter subiektywny. Niemniej jednak – zdaniem autorów – pozwala na dokonanie głębszej analizy zagadnień związanych z bezpieczeństwem teleinformatycznym, a ponadto przyczynia się do uchwycenia tych aspektów, które wydają się najistotniejsze z punktu widzenia projektowania gry symulacyjnej. Wyodrębnione w ten sposób elementy układają się w strukturę o charakterze cyklicznym, obejmującym takie etapy, jak: zabezpieczanie, wykrywanie oraz reagowanie [12], [15]. Dzięki takiemu podejściu, możliwe jest sformułowanie następującej tezy. **bezpieczeństwo teleinformatyczne jest procesem.** Procesem, który rozkłada się w czasie. Nie jest aktem jednorazowym,ani tym bardziej gotowym produktem. Proces ten generuje szereg sytuacji konfliktowych, np. od prostych typu wdrożyć zabezpieczenia, itd. nie, po złożone, takie jak ekonomiczna analiza wdrażania kompletnej polityki bezpieczeństwa.

3. GRA SYMULACYJNA

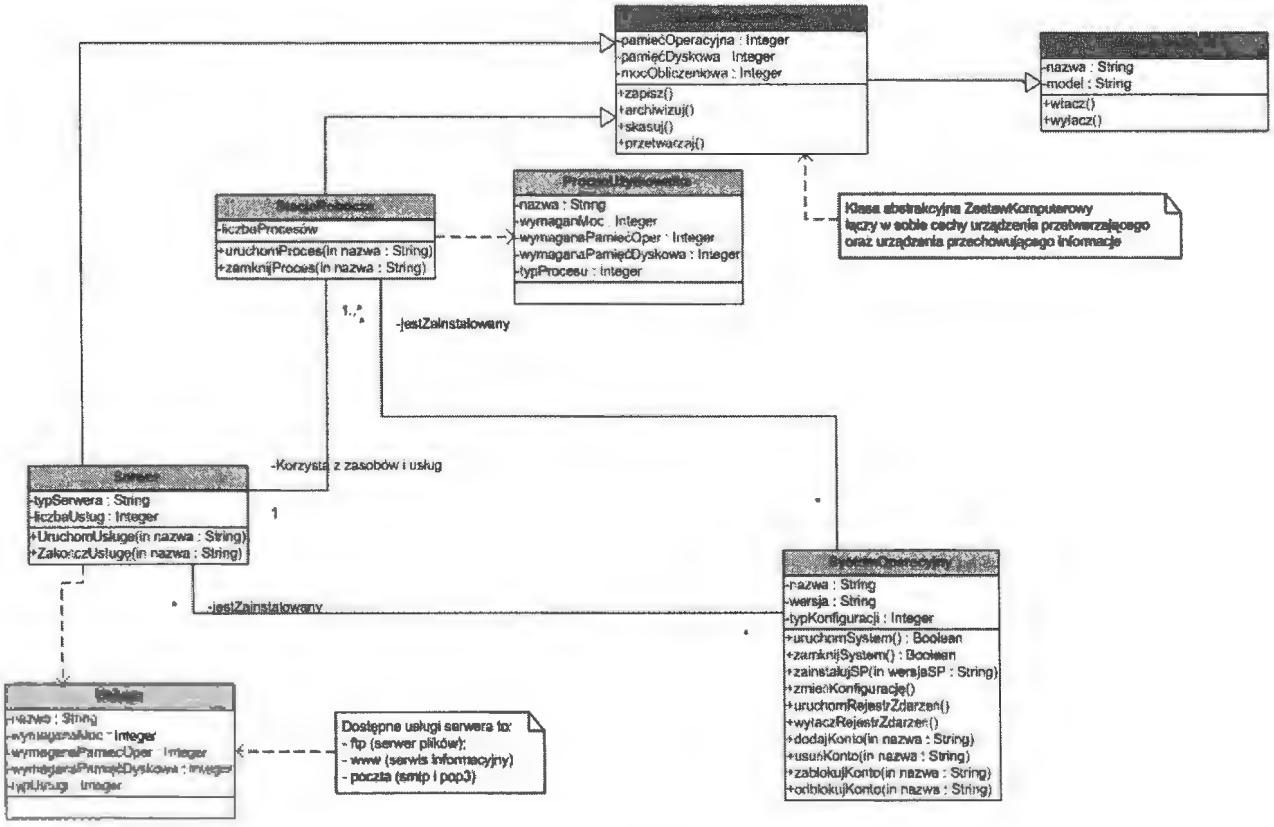
Gra symulacyjna jest końcowym produktem prowadzonych badań. Przeznaczona jest dla szerokiego kręgu odbiorców: od zwykłych użytkowników zainteresowanych problematyka bezpieczeństwa, poprzez administratorów systemów, bezpieczeństwa (oficerów bezpieczeństwa) po decydentów w firmach, instytucjach, czy organizacjach. Zaadresowanie projektowanego narzędzia do tak szerokiego kręgu odbiorców możliwe jest z uwagi na otwartość i elastyczności rozwiązań zastosowanych w projekcie. Gra symulacyjna jest narzędziem realizującym symulacyjną metodę badania bezpieczeństwa teleinformatycznego. Na metodę tą, składają się następujące elementy.

1. Określenie obszaru problematyki, czyli przegląd aktualnych zagadnień bezpieczeństwa teleinformatycznego, przegląd współczesnych zagrożeń i metod im przeciwdziałania (np. [11], [12] lub [16]) i w wyniku otrzymanie listy obiektów i zdarzeń elementarnych.
2. Przyjęcie języka formalnego opisu zjawisk zachodzących w sferze bezpieczeństwa teleinformatycznego (np. [11]) i analiza zależności pomiędzy elementami systemu bezpieczeństwa teleinformatycznego za pomocą modeli matematycznych.
3. Przełożenie modeli matematycznych na język notacji obiektowej (UML): zaproponowanie diagramów klas, przypadków użycia oraz sekwencji.
4. Implementacja gry symulacyjnej.
5. Weryfikacja przyjętych modeli na drodze symulacji interaktywnej. Analiza wybranych strategii zabezpieczeń za pomocą gry symulacyjnej.

Gra symulacyjna jest narzędziem inżynierskim, które powstaje na podbudowie teoretycznej przyjmującej teorię gier za język formalny wykorzystywanych modeli matematycznych. Zagadnienia bezpieczeństwa teleinformatycznego nieodłącznie związane są z analizą ludzkich zachowań, z powstawaniem sytuacji konfliktowych, dlatego też, teoria gier wydaje się być w tym kontekście narzędziem nieodzownym.

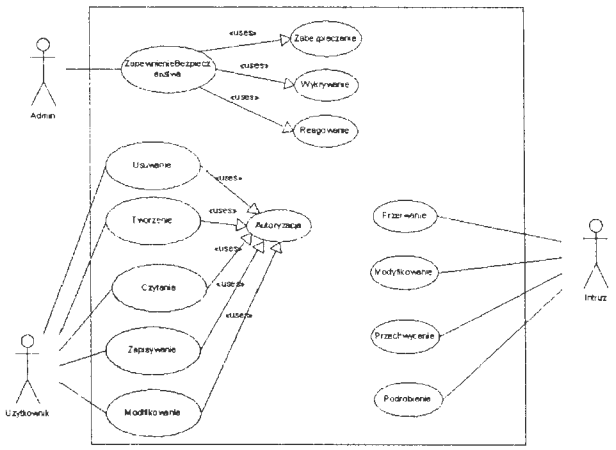


Rys. 4. Elementy systemu informatycznego – zapis w języku UML. Opracowanie własne.



Rys. 5. Elementy diagramu klas projektowanej gry symulacyjnej. Opracowanie własne.

Analizowane zagadnienia związane z bezpieczeństwem teleinformatycznym zostały wyrażone w postaci notacji UML, która jest przełożeniem języka formalnego na potrzeby projektanta gry symulacyjnej.
Typowy system teleinformatyczny, może być przedstawiony za pomocą modelu przedstawionego na rys. 4 ..
Punktem wyjścia wszelkich rozważań, jest zdefiniowanie i przyjęcie określonej listy obiektów i zdarzeń elementarnych, które posłużą do generowania struktur systemów teleinformatycznych oraz analizy zdarzeń związanych z bezpieczeństwem.
Obiekty elementarne, najwygodniej jest przedstawić w postaci diagramu klas UML (rys. 5)
Poszukując właściwej terminologii w odniesieniu do czynności wykonywanych przez strony konfliktu informacyjnego (np. hackera i administratora) należy rozważyć istniejące w literaturze przedmiotu propozycje, np. [10]. W prowadzonych badaniach przyjęto właśnie tą terminologię, która jest wykorzystywana np. przez CERT (Computer Emergency Response Team). Zachowanie graczy w tym może być opisane za pomocą diagramu przypadków użycia rys. 6.



Rys. 6. Elementy diagramu przypadków użycia w kontekście bezpieczeństwa teleinformatycznego.

Język UML pozwala na wyrażenie najważniejszych zagadnień bezpieczeństwa teleinformatycznego, z pominięciem szczegółów zbędnych w danym kontekście. Cechuje go precyzyjność. Za pomocą graficznych symboli pozwala zilustrować obiekty systemu oraz związki zachodzące pomiędzy nimi.
Przypadki użycia, w swoim standardowym zastosowaniu, opisują to, co projektowany system ma robić lub, co istniejący system robi. W zakresie systemów bezpieczeństwa (czy też zjawisk związanych z bezpieczeństwem teleinformatycznym), przypadki użycia służą do zamodelowania różnych sposobów interakcji użytkowników (graczy defensywnych i ofensywnych) z systemem informatycznym.

4. PODSUMOWANIE

W artykule zaprezentowano ideę konstruowania i zastosowania gry symulacyjnej do badania bezpieczeństwa teleinformatycznego. Zarysowano ogólny obszar problematyki. Zaprezentowano wybrane elementy modelu matematycznego w postaci prostej gry dwuosobowej oraz przykładowe modele wyrażone w języku UML. Prezentowane wątki stanowią element projektu, związanego z realizacją komputerowej gry symulacyjnej, dla potrzeb badania bezpieczeństwa teleinformatycznego.
Podkreślić należy, iż dość złożonym zadaniem jest określenie dobrych (z inżynierskiego oraz menedżerskiego punktu widzenia) miar bezpieczeństwa, podatności, czy w ogólności: wiarygodności danego sytemu. Czynnikiem, który najskuteczniej przemawia do decydentów jest aspekt finansowy (ekonomiczny). Dlatego przyjęcie miar mających odniesienie ekonomiczne wydaje się być działaniem mającym racjonalne uzasadnienie. A w związku z tym, metody, narzędzia i modele akceptowalne z punktu widzenia analiz ekonomicznych, mogą być stosowane na gruncie bezpieczeństwa teleinformatycznego.
Spodziewa się, iż narzędzie takie dostarczy odpowiedzi na pytanie, w których elementach systemu teleinformatycznego wskazane jest zastosowanie mechanizmów automatyzujących zarządzanie, czy sterowanie bezpieczeństwem

AN APPLICATION OF SIMULATION GAME TO IT SECURITY ANALYSIS

Abstract: The paper presents chosen elements of simulation game for IT security analysis purpose. Elements of game theoretical model have been presented as a framework for the simulation game. Basic elements of IT systems and events connected with security have been presented using UML notation.

Literatura

[1] Agah A., Das S.K., Basu K. (2004) A game theory based approach for security in wireless sensor networks. *Proceedings of IEEE International Performance Computing and Communications Conference.* 259- 263..

[2] Alpcan T., Basar T. (2003) A game theoretic approach to decision and analysis in network intrusion detection. *IEEE Conference on Decision and Control,* 2595-2600.

[3] Alpcan T., Basar T. (2004) A game theoretic analysis of intrusion detection in access control systems, *Proceedings. IEEE Conference on Decision and Control,* 1568-1573

[4] Browne R. (2000) Defensive information warfare with non-localizable command and control. New Jersey Computer and Communications (http://citeseer.ist.psu.edu/485272.html)

[5] Brynielson J. (2004) Game-theoretic reasoning in command and control, *15th Mini-EURO Conference: Managing Uncertainty in Decision Support Models*

[6] Burke D. (1999) Towards a game theory model of information warfare, Master Thesis, Airforce Institute of Technology, Air University

[7] Hamilton S.N., Miller W.L. Ott A. (2002) The role of game theory in information warfare, *Proceedings of 4th Information Survivability Workshop*

[8] Hamilton S.N., Miller W.L. Ott A. (2002) Challenges in applying game theory to the domain of information warfare. *Procedings of 4th Information Survivability Workshop*

[9] Hespanha J., Bohacek S. (2001) Preliminary Results in Routing Games. *Proceedings of the 2001 American Control Conference*, vol. 3, 1904-1909,

[10] Howard J.D., Longstaff T.A. (1998) A Common Language for Computer Security Incidents, SANDIA Report, SAND98-8667 (http://www.cert.org)

[11] Jóźwiak I., Laskowski W., Zych J. (2004) Towards a simulation model of computer systems security. *Proceedings of the 10th IEEE International Conference on Methods and Models in Automation and Robotics.*

[12] Jóźwiak I., Laskowski W. (2003) Kierunki rozwoju metod i technik zabezpieczeń systemów komputerowych. *Diagnostyka procesów przemysłowych. VI Krajowa konferencja naukowo-techniczna.*

[13] Kelly F. (1999) Mathematical modeling of the Internet. *Proceedings of 4th International Congress on Industrial and Applied Mathematics*, 105-116

[14] Kodialam M., Lakshman T.V. (2003) Detecting Network Intrusion via Sampling: A Game Theoretic Approach. *Proceedings of The 22nd Annual Joint Conference of the IEEE Computer and Communications Societies*, San Francisco. USA

[15] Laskowski W. (2005) Ochrona informacji w systemach teleinformatycznych – współczesne trendy i zagrożenia. *Przegląd Telekomunikacyjny i Wiadomości Telekomunikacyjne*, 1, 12 – 17.

[16] Lye K., Wing J. (2002) Game strategies in network security. *In Proceedings of 15th IEEE Computer Security Foundations Workshop*, Copenhagen, Denmark 2002 (Technical Report CMU-CS-02-136, Carnegie Mellon University)

[17] Michardi P., Molva R. (2002) Game theoretic analysis of security in mobile ad hoc networks. Research report No. RR-02-070, Institut Telcom, France

[18] Owen G. *Teoria gier.* (1975) PWN, Warszawa.

Instytut Badań Systemowych
Polskiej Akademii Nauk

ISBN 83-89475-01-4