DOI: https://doi.org/10.15276/hait.07.2024.20
UDC 004.891.2

An expert system of recommendations for combating cyber threats using CVSS metrics and game theory

Maksym V. Mishchenko[1)]
ORCID: https://orcid.org/0000-0001-9769-9759; it144111@stu.cn.ua
Mariia S. Dorosh[1)]
ORCID: https://orcid.org/0000-0001-6537-8957; mariyaya5536@gmail.com. Scopus Author ID: 56912183600
[1)] Chernihiv Polytechnic National University, 95, Shevchenko Str. Chernihiv, 14035, Ukraine

ABSTRACT

This study is focused on the creation of an expert system for generating recommendations on cyber security. The developed expert system uses a game-theoretic model as a inference engine to transform expert knowledge into recommendations for end-users, who may be chief IT security officers (CISOs), system administrators, or cyber security engineers. Expert knowledge is presented in the form of an estimate of the base group of CVSS metrics - Common Vulnerability Score System, for each type of attack and adjusted values of CVSS in the case that the counterattack strategy is applied. Given a set of attacks and a base of expert attack knowledge, the system generates a game matrix of zero-sum game with a cybercriminal and a cyberdefense expert as players. The inference engine of the expert system is a game-theoretic model responsible for solving the game using the Brown-Robinson iterative method and generating cyber protection recommendations. An experiment was conducted on the convergence of the Brown-Robinson algorithm on the 2022 vulnerability dataset from the Cybersecurity and Infrastructure Security Agency database, as a result of which it was determined that the convergence of the algorithm for solving the matrix game is achieved at a number of iterations of 1000. As a result of the work, expert system was designed and implemented along with the Web interface, which provides input by experts of CVSS level assessments of collected threats, threats countermeasures and output of recommendations for combating cyber threats.

Keywords: Expert system; cybersecurity; game theory; Brown-Robinson method; CVSS

For citation: **Mishchenko M. V., Doros M. S. "An expert system of recommendations for combating cyber threats using CVSS metrics and game theory".** ***Herald of Advanced Information Technology.*** **2024; Vol.7 No.3: 284–295. DOI: https://doi.org/10.15276/hait.07.2024.20**

I. INTRODUCTION

Cyber security plays a key role in the modern world, and must be ensured in many spheres of life - in social spheres, in production, in offices and for personal use. While for personal use it is usually limited to the installation of special antivirus software, to ensure cyber protection of organizations of various sizes, a separate role of a specialist or department for cyber protection is allocated.

There are 3 main types of cyber security systems – IPS, IDS and SIEM [1]. IPS systems work automatically, without human intervention and are aimed at the fastest neutralization of any threats detected by this system. This approach has risks of false positives, but its advantage is the speed of response. IDS systems, in turn, generate an extensive report on possible threats and enable a specialist to make decisions on their elimination. SIEM systems offer functionality that is a combination of the functionality of IPS and IDS systems – they provide security reports to the user, and at the same time, they have the functionality of neutralizing cyber threats. Systems that combine the functionality of IPS, IDS and SIEM systems are quite popular and are an important link in building the topology of home and corporate networks.

To facilitate the work of these specialists, as well as to increase the effectiveness of protection against cyber attacks, an expert system can be applied, which, based on expert knowledge, will issue recommendations on cyber protection.

An expert system is a software tool that uses the knowledge of experts in a certain subject area to emulate the reasoning process of a human expert [2]. The architecture of the expert system includes a knowledge base of experts, an inference engine, an explanation module, and a user interface that provides a set of recommendations generated by the inference engine [3] .

A game-theoretic model can act as an inference engine of the expert system, and, based on expert assessments, could formulate the optimal strategies of cyber criminals and the corresponding strategies of cyber defense experts. The advantage of using gametheoretic models is their low resource consumption and ease of implementation, compared to engines built on fuzzy inference systems or neural networks.

Thus, the goal of our research is to create an expert system that will combine parts of the functionality of the IDS and SIEM systems – to provide reports on detected and predicted threats, and to supplement this functionality by calculating the probability of using different attack strategies by a cybercriminal and defense strategies by a cyber security specialist, using game theory models. Based on the obtained optimal game strategies, recommendations for the use of strategies for countering existing and potential cyber threats are provided for cyber security specialists.

To achieve the goal of the research, the following tasks were set: formulate the architecture of the expert system; select a game-theoretic model for the inference engine of the expert system; determine the optimal parameter values for the game-theoretic model; determine cyber threat assessment system used by experts; implement expert system.

The structure of the article is structured as follows: in section 2, existing research on the application of expert systems and game theory models in cyber security was analyzed. In Chapter 3, an overview of CVSS metrics and a description of game theory models, which will be used as a driver for the generation of conclusions of the expert system, were made. Chapter 4 contains the architecture of the created expert system and the obtained results. Chapter 5 presents conclusions regarding the obtained results.

II. ANALYSIS OF LITERATURE

The use of expert systems in the field of cyber security is a problem that is being actively researched. For example, Iqbal H. Sarker et al. [4] in their work investigated the aspects of creating expert systems for cyber defense based on artificial intelligence. In the course of the research, the author distinguished two main types of expert systems: systems using neural networks and systems using ontologies – conceptual models that represent something that exists in a certain domain of knowledge. In the case of cyber security, such ontologies as threat, vulnerability, attack, impact, and control were highlighted. In the study, the expert system was presented as a set of 3 components: the expert's knowledge base in the form *IF <incident> – THEN <consequent>*; a user interface for entering incident-specific action requests and output drivers that apply the expert's knowledge base to the user's queries and output suggested actions.

Churu, Matida, et al. [5] proposed an expert system for cyber threat analysis based on a fuzzy inference system in their study. The input data of the system were metrics PC to Server ping time, PC-to-PC ping time, and Download time. To test the system, the authors deployed a local network and simulated cyberattacks using Kali Linux. As a result, the authors came to the conclusion that with the growth of PC-to-server time, PC-to-PC time and download time, the risks of cyber threats for the investigated network also increase.

As an example of expert systems using neural networks, we can cite the DeNNeS model presented in the work of Samaneh Mahdavifar and Ali A. Ghorbani [6]. The authors proposed an architecture based on deriving rules from a trained Deep Neural Network model to replace the knowledge base of an expert system. The authors validated the created model on the UCI phishing websites dataset and the Android malware dataset, obtaining 97.5 % accuracy and a false positive rate of 1.8 %.

The CVSS metric is a standard that is researched, improved, and applied in various fields. For example, in his work D.T. Vasireddy et al. [7] proposed the prediction of the CVSS metric value for vulnerabilities in power supply systems using the Doc2Vec model and neural networks. The authors vectorize the text description of the vulnerability and perform regression analysis of the vectorized text. The developed method improves CVSS by replacing the need for manual calculation of the metric value by experts.

Maghrabi, L. et al. [8] in their work developed a methodology for improving strategies for eliminating cyber vulnerabilities by finding Nash equilibrium for a matrix game, the players of which are a cyber-criminal and a cyber-defender. To calculate the values of the objective function, the authors used the Confidentiality, Integrity and Availability metrics of the CVSS standard.

Zhang, S. et al. [9] conducted a study of the most error-prone CVSS metrics by analyzing identical or sufficiently similar entries in the National Vulnerability Database that have sufficiently distant CVSS values. This made it possible to reveal the most problematic CVSS metrics.

In their review, Cuong, Do et al. [10] cited and examined a wide range of studies related to the application of game theory to cyber security challenges. The studied works were grouped according to the game model and the problem to be solved using game theory. In particular, works were presented in which the protection of privacy, protection of cyber-physical systems [11], [12], protection against DoS and DDoS attacks and others are investigated using game theory models.

Sayed, M. A. et al. [13] in their work use a two-player zero-sum game to solve the problem of placing “honeypot” traps in the network in such a way as to protect the most important assets. The authors pay attention to zero-day attacks because such attacks are able to bypass existing traps. As a result, the authors developed and confirmed the effectiveness of using a game-theoretic approach against zero-day attacks.

Major, M. et al. [14] apply game theory to investigate cyberattacks in which a cyberattacker uses deceptive strategies to distract a cyberdefense and at the same time a cyberdefense specialist uses decoys to hide and protect real hosts. The authors proposed a model with multiple game trees to determine and evaluate the strategies of each player using implicit knowledge about the game structure and payoffs.

Another example of the application of game theory to cyber security problems is the work of Ullah, F. et al. [15], in which researchers proposed an improved IDS for detecting cyberattacks on IoT devices and validated it using a game-theoretic approach. The authors have developed a framework according to which a game is created, the players of which are a cyber-criminal and a cyber-defender. In the case of finding Nash equilibrium, robustness and effectiveness of different detection methods against different types of attacks are considered to be achieved.

Gill, K. S. et al. [16] proposed to apply game theory to the evaluation of cyber attacker’s and cyber defender’s strategies for cloud environments. In their work, the authors calculate the Nash equilibrium using a graphical method. As a result, the authors achieved an increase in the detection rate and a decrease in the false positive rate.

In contrast to existing studies, we propose the application of game theory to create an expert system for generating recommendations for countering cyberattacks that are detected or predicted by modules using malicious file classification models [17], detection of network traffic anomalies using Chaos Theory and EWMA statistics, and a threat prediction module using Bayesian trees, which were developed in our previous studies [18].

Our study proposes to populate the knowledge base by assigning CVSS level and countermeasure strategies to a fixed set of cyber threats that are fed into the database from the attack detection and prediction modules developed in our previous studies.

Among the novelty elements of our proposed expert system is the use of the Brown-Robinson iterative method of fictitious playing to solve a strategic antagonistic game, the actors of which are a cyber criminal and a cyber defense specialist.

III. MATERIAL AND METHODS

In our proposed expert system, the knowledge base of experts is filled by determining the CVSS indicator for a certain attack and possible countermeasures to the attack in the form of communication <*attack*>-<*mitigation*>-<*cvss*>. Common Vulnerability Scoring System (CVSS) – an open standard of the cyber security industry, created to assess the severity of computer system vulnerabilities [19]. The latest CVSS 4.0 specification consists of 4 groups of metrics: Base, Threat, Environmental and Supplemental. The groups and their corresponding metrics are presented in Fig. 1.

According to the new specification, the overall value of CVSS is calculated by creating a text vector:

$$CVSS:4.0/<metric\_name>:<metric\_value>, \tag{1}$$

where *metric_name* is metric name, *metric_value* is metric value.

The value of CVSS can be from 0 to 10, where 10 is the maximum measure of the danger of a cyber attack.

For example, text vector *CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:H* - describes DDoS attack on local network and consists of metrics: Attack Vector (AV): Network (N), Attack Complexity (AC): Low (L), Attack Requirements (AT): None (N), Privileges Required (PR): None (N), User Interaction (UI): None (N), Confidentiality (VC): None (N), Integrity (VI): None (N), Availability (VA): High (H); Subsequent system impact metrics: Confidentiality (SC): None (N), Integrity (SI): None (N), Availability (SA): High (H). The corresponding attack has a value of CVSS=9.3, which corresponds to a critical threat level. Table 1 shows the value of CVSS metrics for the threats investigated in the work and adjusted metrics if cyber defense strategies were used.

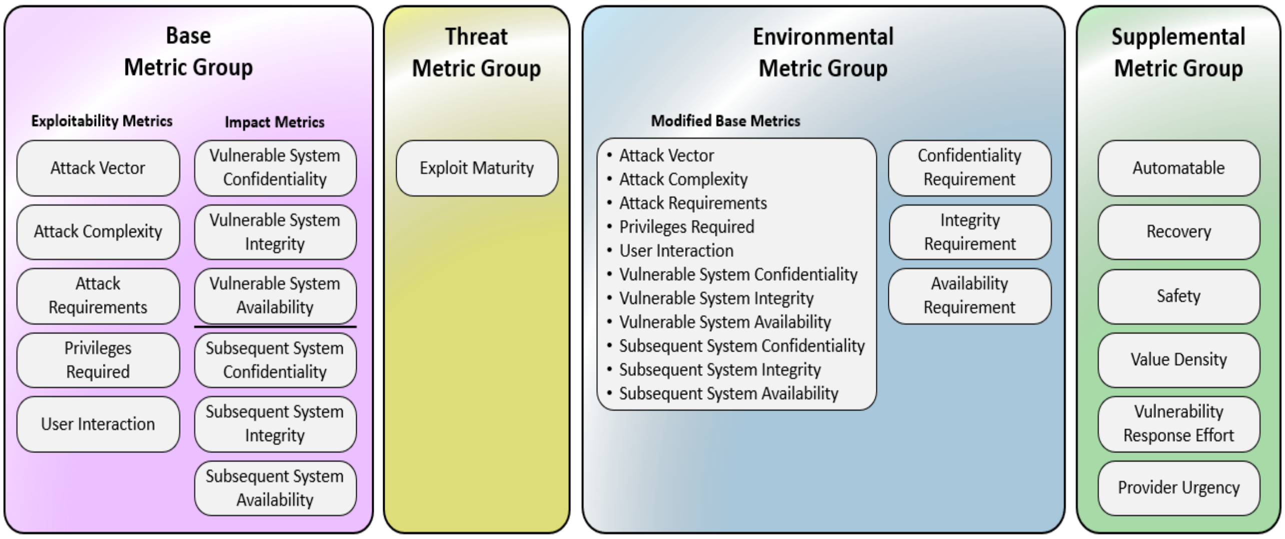

Base Metric Group
Exploitability Metrics
Impact Metrics
Attack Vector
Attack Complexity
Attack Requirements
Privileges Required
User Interaction
Vulnerable System Confidentiality
Vulnerable System Integrity
Vulnerable System Availability
Subsequent System Confidentiality
Subsequent System Integrity
Subsequent System Availability
Threat Metric Group
Exploit Maturity
Environmental Metric Group
Modified Base Metrics
• Attack Vector
• Attack Complexity
• Attack Requirements
• Privileges Required
• User Interaction
• Vulnerable System Confidentiality
• Vulnerable System Integrity
• Vulnerable System Availability
• Subsequent System Confidentiality
• Subsequent System Integrity
• Subsequent System Availability
Confidentiality Requirement
Integrity Requirement
Availability Requirement
Supplemental Metric Group
Automatable
Recovery
Safety
Value Density
Vulnerability Response Effort
Provider Urgency

Fig. 1. **Groups and metrics of the standard CVSS 4.0**

Source: **compiled by the [19]**

Table 1. **CVSS metrics for investigated cyber threats and strategies of combating cyber threats**

Cyber threat name	CVSS text vector	CVSS value	Strategy of combating cyber threat	CVSS text vector, if strategy of combating cyber threat is applied	CVSS value, if strategy of combating cyber threat is applied
DDoS attack	CVSS:4.0/AV:N/ AC:L/AT:N/PR:N/ UI:N/VC:N/VI:N/ VA:H/SC:N/SI:N/SA:H	9.3	Block attackers IP addresses [ip addresses range]	CVSS:4.0/AV:N/ AC:L/AT:N/PR:N/UI:N /VC:N/VI:N/VA:N/SC:N/SI:N/SA:N	0
PE Trojan virus	CVSS:4.0/AV:L/AC:L/AT:P/PR:N/UI:P/VC:H/VI:H/VA:H/SC:L/SI:L/SA:L	7.3	Users cybersecurity training	CVSS:4.0/AV:L/AC:H/AT:P/PR:H/UI:A/VC:H/VI:H/ VA:H/SC:L/SI:L/SA:L	5.4
PE adware virus	CVSS:4.0/AV:L/AC:L/AT:P/PR:N/UI:A/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N	5.7	Use CCleaner program on the host <host IP>	CVSS:4.0/AV:L/AC:L/AT:P/PR:N/UI:A/VC:N/VI:H/ VA:H/SC:N/SI:L/SA:L	1.8
ELF Lightaidra virus	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:L/VI:N/VA:H/SC:L/SI:N/SA:H	8.3	Block and remove file <filename>, blacklist IP <source ip> where file downloaded	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/ VA:N/SC:N/SI:N/SA:N	0

Source: **compiled by the authors**

The CVSS text vector evaluation algorithm is not publicly available, but the official website [20] presents a calculator that calculates the CVSS value for a text vector and can be used by experts. In our study, experts are asked to rate the level of CVSS by a basic group of metrics.

The proposed expert system processes the input data by constructing a game matrix used to solve the zero-sum game in normal form. The players are a cybercriminal and a cyber security specialist. For each player, his strategy is represented as a vector, where each element of the vector corresponds to the value of CVSS, in case of choosing a certain strategy - cyber attack or cyber defense. The elements of the game matrix are represented by the corresponding CVSS value. However, if a certain cyber attack can be completely neutralized by an appropriate cyber defense strategy, this will be considered a loss for the cyber criminal, so the corresponding CVSS value in the matrix will be counted with a minus sign. It is the cybercriminal's job to maximize CVSS for an attack strategy, the cyber defense expert's job is to minimize this value.

The cyber specialist sets an initial CVSS value for the attack that is valid if no countermeasures have been taken. The cyber specialist can then determine countermeasures and an appropriate adjusted CVSS value. The CVSS value for the threat-countermeasure match that was not determined by the specialist is set to the initial CVSS value.

Thus, the game will be defined as a system of sets:

$$G = \left\langle 2, \{S_i\}_{i\in\{1,2\}}, \{H_i\}_{i\in\{1,2\}} \right\rangle, \qquad (2)$$

where S_i is strategy of player i, represented by cyber-attack or cyber combat ; H_i is payoff of the player i,that is CVSS score is a positive value means the cybercriminal wins, and a negative value means the cyber security specialist wins.

As a method of solving the matrix game, we will use the Brown-Robinson iterative method of fictitious playing [21]. The Brown-Robinson iterative method consists in finding mixed strategies for each of the players by fictitiously playing the game repeatedly.

The algorithm begins with the first player choosing his maximin strategy. In response, the second player plays the strategy that brings him the least loss. In subsequent iterations, each player chooses strategies according to the previous strategy played by the opposite player. The mixed strategies of each player are calculated by calculating the frequency of use of each of the strategies.

IV. ARCHITECTURE AND RESULTS

The created expert system generates recommendations according to the solution of the matrix game. In Fig. 2 schematically depicts the method of forming recommendations for the application of optimal strategies for cyber protection in the expert system.

The first step in the cyber defense recommendation process is to find a solution to the matrix game in pure strategies. Searching for the lowest value of the game $\underline{V} = \max_i \min_j a_{ij}$ upper value of the game $\overline{V} = \min_j \max_i a_{ij}$ and saddle point $\overline{V} = \underline{V}$. If saddle point is found, then the solution for the game is (x_{i_0}, y_{j_0}), which pair of optimal pure strategies is. If saddle point doesn’t exist, it is necessary to find a solution in the mixed strategies.

To find a solution to the game in mixed strategies, the Brown-Robinson agorithm algorithm is used.

The formation of recommendations for the application of cyber defense strategies depends on the solution of the matrix game. If a solution in pure strategies has been obtained, then the cyber security expert's pure optimal strategy will be recommended for use. If the game has a solution in mixed strategies, the strategies of the cyber defense expert are recommended for use with a priority determined by sorting the probability of their use.

Recommendations are made according to the decreasing priority of the application of certain strategies of protection against cyberattacks.

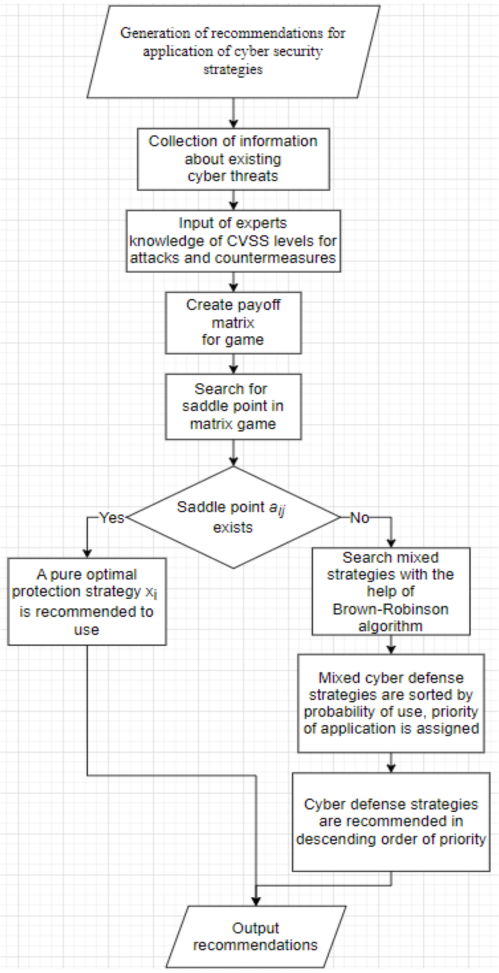

Generation of recommendations for application of cyber security strategies
Collection of information about existing cyber threats
Input of experts knowledge of CVSS levels for attacks and countermeasures
Create payoff matrix for game
Search for saddle point in matrix game
Saddle point a_{ij} exists
Yes
No
A pure optimal protection strategy x_i is recommended to use
Search mixed strategies with the help of Brown-Robinson algorithm
Mixed cyber defense strategies are sorted by probability of use, priority of application is assigned
Cyber defense strategies are recommended in descending order of priority
Output recommendations

Fig. 2. **The method of forming recommendations for the application of optimal strategies for cyber protection in the expert system**

Source: **compiled by the authors**

In our work, we analyze identified threats to computer networks, the nodes of which can be personal computers, routers, firewalls, etc. This was reflected in the types of attacks and counterattack strategies in the training dataset that was chosen for our study.

To evaluate the convergence of the Brown-Robinson algorithm and determine the optimal number of iterations of the game, a dataset [22] with analyzed vulnerabilities for 2022 based on the reports of the CISA – Cybersecurity and Infrastructure Security Agency was downloaded. The dataset contains a list of vulnerabilities, the CVSS level assigned to them, and recommendations for countering these vulnerabilities. Duplicate and dominant strategies were removed from the dataset, strategies description were shortened, resulting in a matrix containing 42 cyberattacks and 10 countermeasures. Part of the game matrix of size 9 by 10 is shown in Table 2.

An experiment was conducted to investigate the convergence of the average game value *V* obtained for the number of iterations from 10 to 3000 with a step of 10 - a total of 300 draws. We obtained the result shown in Fig. 3. From the graph, we can see a tendency towards the convergence of the average value of the winnings.

After 1000 iterations, it is possible to note a decrease in the fluctuation of the average value of *V* in the range from 5.8 to 6.0, which indicates the feasibility of using the indicator of 1000 iterations to solve the given matrix game.

Based on the results of 300 draws of the game with different number of iterations, the strategies from the dataset that were most often used by cyber criminals and cyber security specialists were analyzed. The graph of the frequency of the use of strategies is shown in Fig. 4 and Fig. 5, respectively.

Table 2. **Part of the payoff matrix, generated based on vulnerabilities 2022 dataset of the CISA**

Attack/Defence	Apply June 2022 updates for Windows	Apply updates per vendor instructtions	Update Adobe Acrobat and Reader or Delete Adobe Flash Player	Update or Disconnect device	Upgrade Apache Log4j to 2.15+	Upgrade Confluence server to 7.18.1	Impacted product is end-of-life and should be disconnected	Multiple impacted products are end-of-life and should be disconnected	Patch D-Link KEV entry CVE-2018-6530	Upgrade product from version 6 to 7
“Sigred” - microsoft windows domain name system (dns) server remote code execution	-10.0	10.0	-10.0	-10.0	-10.0	-10.0	-10.0	-10.0	-10.0	-10.0
Adobe acrobat and reader, flash player unspecified	-9.2	-9.2	9.2	-9.2	-9.2	-9.2	-9.2	-9.2	-9.2	-9.2
Adobe flash player and air integer overflow	-9.8	-9.8	-9.8	-9.8	-9.8	-9.8	-9.8	9.8	-9.8	-9.8
Adobe flash player arbitrary code execution	-9.8	-9.8	-9.8	-9.8	-9.8	-9.8	9.8	-9.8	-9.8	-9.8
Apache log4j2 remote code execution	-10.0	-10.0	-10.0	-10.0	10.0	-10.0	-10.0	-10.0	-10.0	-10.0
Atlassian confluence server and data center remote code execution	-9.2	-9.2	-9.2	-9.2	-9.2	9.2	-9.2	-9.2	-9.2	-9.2
Checkbox survey deserialization of untrusted data	-9.8	-9.8	-9.8	-9.8	-9.8	-9.8	-9.8	-9.8	-9.8	9.8
D-link multiple routers os command injection	-9.2	-9.2	-9.2	-9.2	-9.2	-9.2	-9.2	-9.2	9.2	-9.2
Netgear multiple devices exposure of sensitive information	-9.2	-9.2	-9.2	9.2	-9.2	-9.2	-9.2	-9.2	-9.2	-9.2

Source: **compiled by the authors**

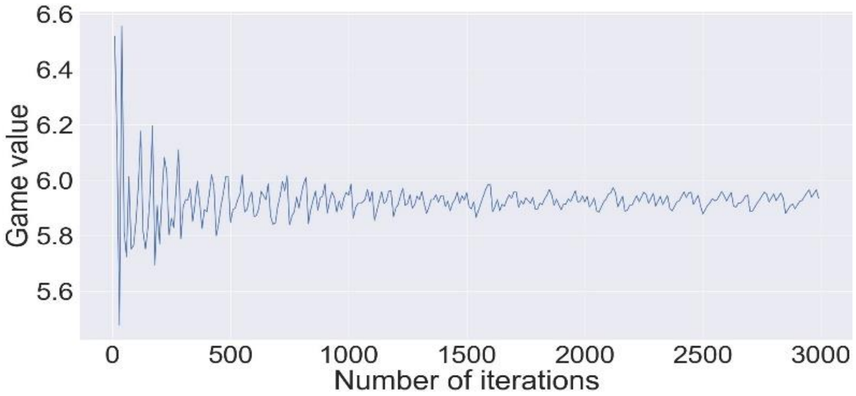


Fig. 3. **The convergence of Brown-Robinson algorithm, showing mean value of the game V depending on number of iterations with the use of CISA dataset**

***Source:* compiled by the authors**

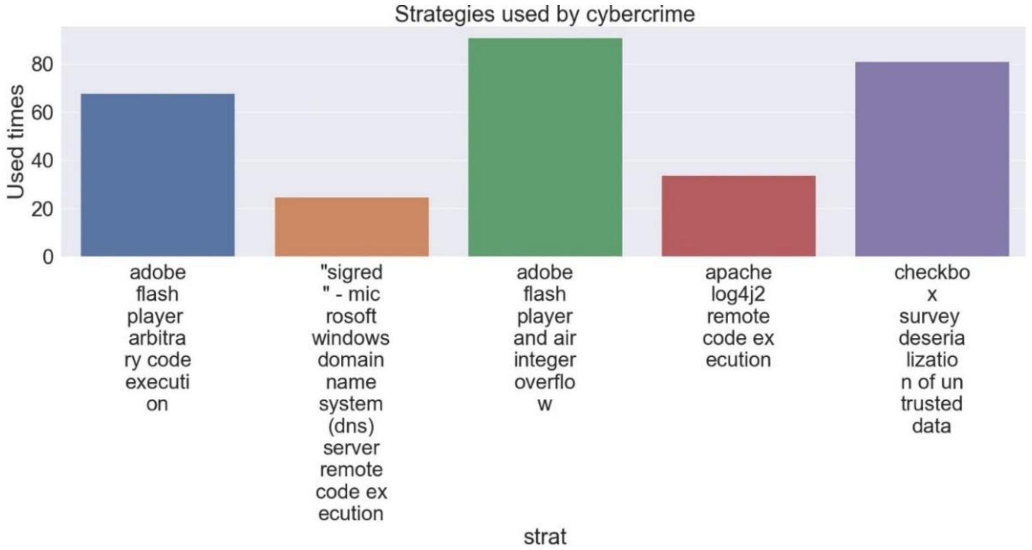


Fig. 4. **Strategies used by cybercrime based on the 300 draws of the game with CISA dataset**

***Source*: compiled by the authors**

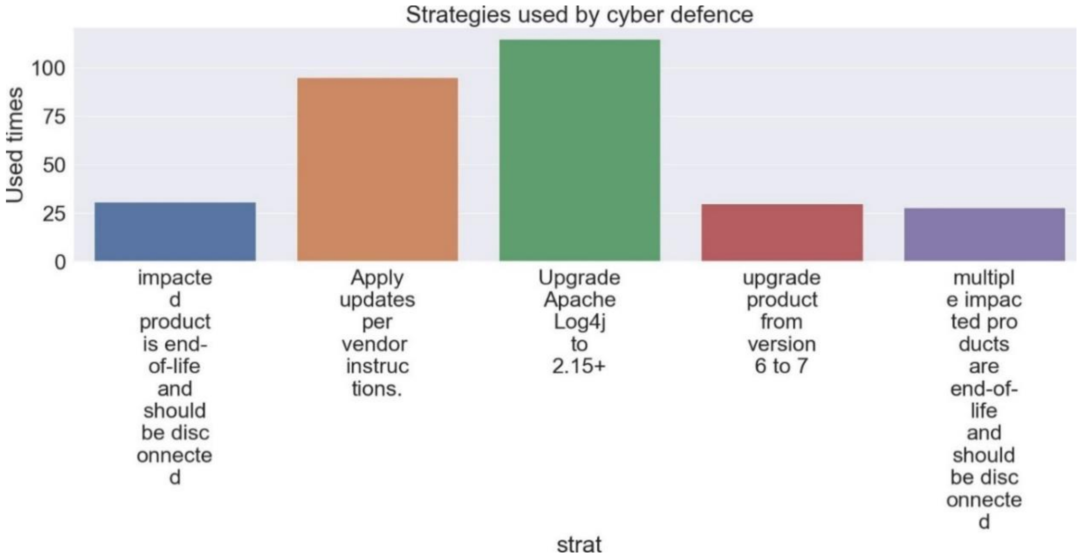


Fig. 5. **Strategies used by cyber defence based on the 300 draws of the game with CISA dataset**

***Source:* compiled by the authors**

From Fig. 4, we can see that 3 cyber attack strategies were most often used: “adobe flash player and air integer overflow”, “checkbox survey deserializtion of untrusted data” and “adobe flash player arbitrary code execution”.

From the graph of used cyber defense strategies, shown in Fig. 5, we can see that 2 of the five strategies were used more often than others, namely: "apply updates per vendor instructions" and "Upgrade Apache Log4j to 2.15+". During the research, the architecture of the expert system was developed, which is shown in Figure 6. The developed architecture includes three subsystems: Network Analysis system, Expert system, and Information Security Management System.

The actors of the system are the cyber security expert and the Chief Information Security Officer – CISO. The Cyber Security Expert is responsible for populating the knowledge base of the Expert System subsystem, and the CISO is responsible for applying cybersecurity strategies to the Network Analysis System subsystem.

Network Analysis System includes a local network and a proxy server through which traffic from the local network to the Internet passes and is analyzed.

The Network Analysis System also includes cyber threat detection and prediction modules developed in our previous research and includes:

– malware classification module for Linux ELF and Windows Portable Executable files;

– abnormal network traffic detection module using Chaos Theory and the Lyapunov coefficient;

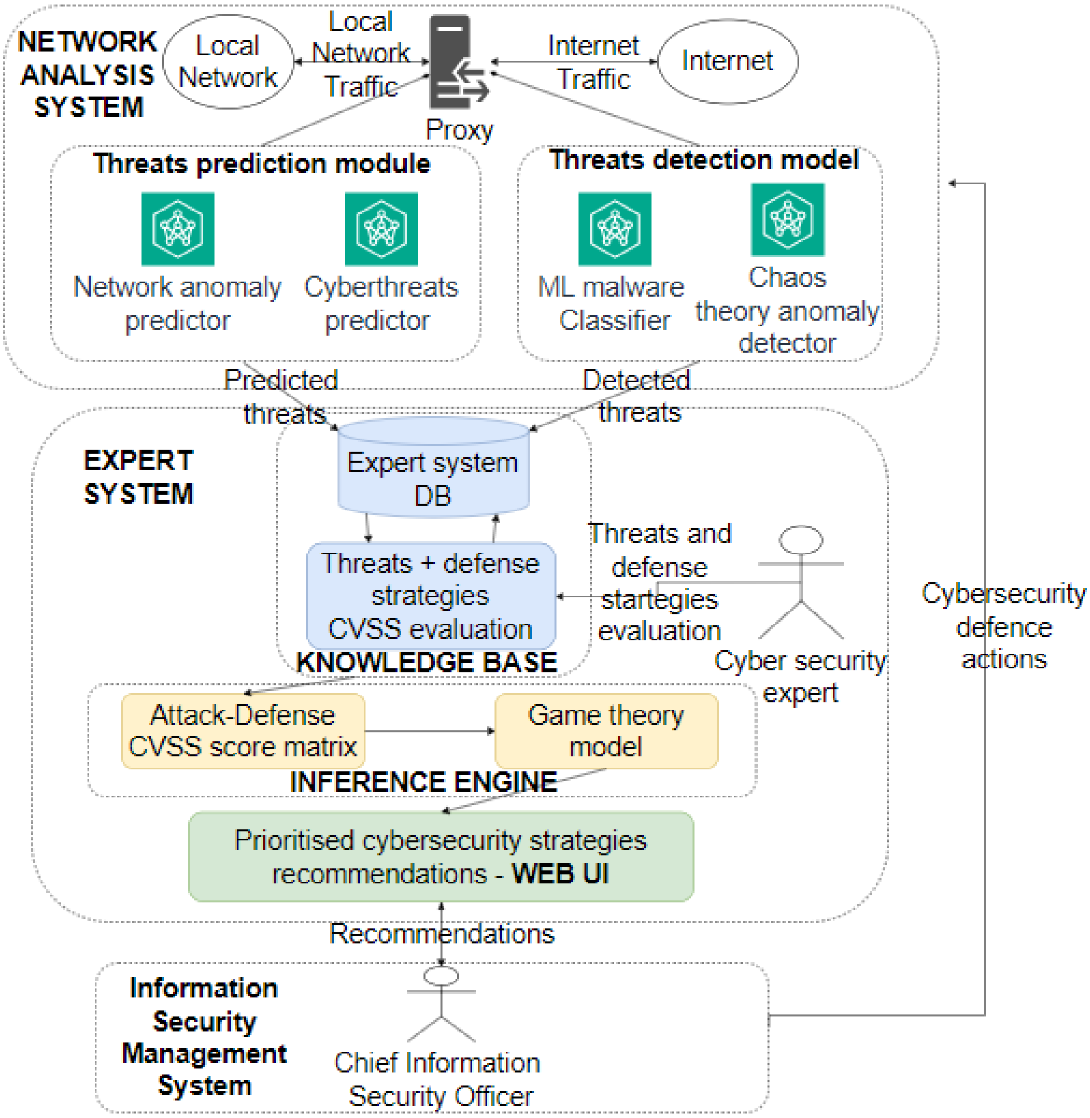

NETWORK ANALYSIS SYSTEM
Local Network
Local Network Traffic
Proxy
Internet Traffic
Internet
Threats prediction module
Network anomaly predictor
Cyberthreats predictor
Threats detection model
ML malware Classifier
Chaos theory anomaly detector
Predicted threats
Detected threats
EXPERT SYSTEM
Expert system DB
Threats + defense strategies CVSS evaluation
KNOWLEDGE BASE
Threats and defense startegies evaluation
Cyber security expert
Cybersecurity defence actions
Attack-Defense CVSS score matrix
Game theory model
INFERENCE ENGINE
Prioritised cybersecurity strategies recommendations - WEB UI
Recommendations
Information Security Management System
Chief Information Security Officer

Fig. 6. **Architecture for the Expert System of recommendations for combating cyber threats using CVSS metrics and game theory**
Source: **compiled by the authors**

– abnormal traffic detection and prediction module using EWMA statistics and ARIMA models;

– threat prediction module using Bayesian decision trees.

The expert system receives data about cyber threats from the Network Analysis System, and stores them in the PostgreSQL relational database. The database stores information about detected and predicted cyber attacks, CVSS scores for attacks given by experts and countermeasures strategies for each type of attack.

The threat list is updated in real-time by attack detection and prediction modules. During system initialization, experts evaluate a given set of attacks and determine a given set of defense strategies. During the operation of the system, it may be possible to adjust expert knowledge in accordance with the change of attack detection and prediction modules - expanding the list of threats that can be detected and predicted. The expert system's inference engine includes a game matrix formed by combining information about detected and predicted cyber threats and CVSS-level expert knowledge for threats and counter-threat strategies.

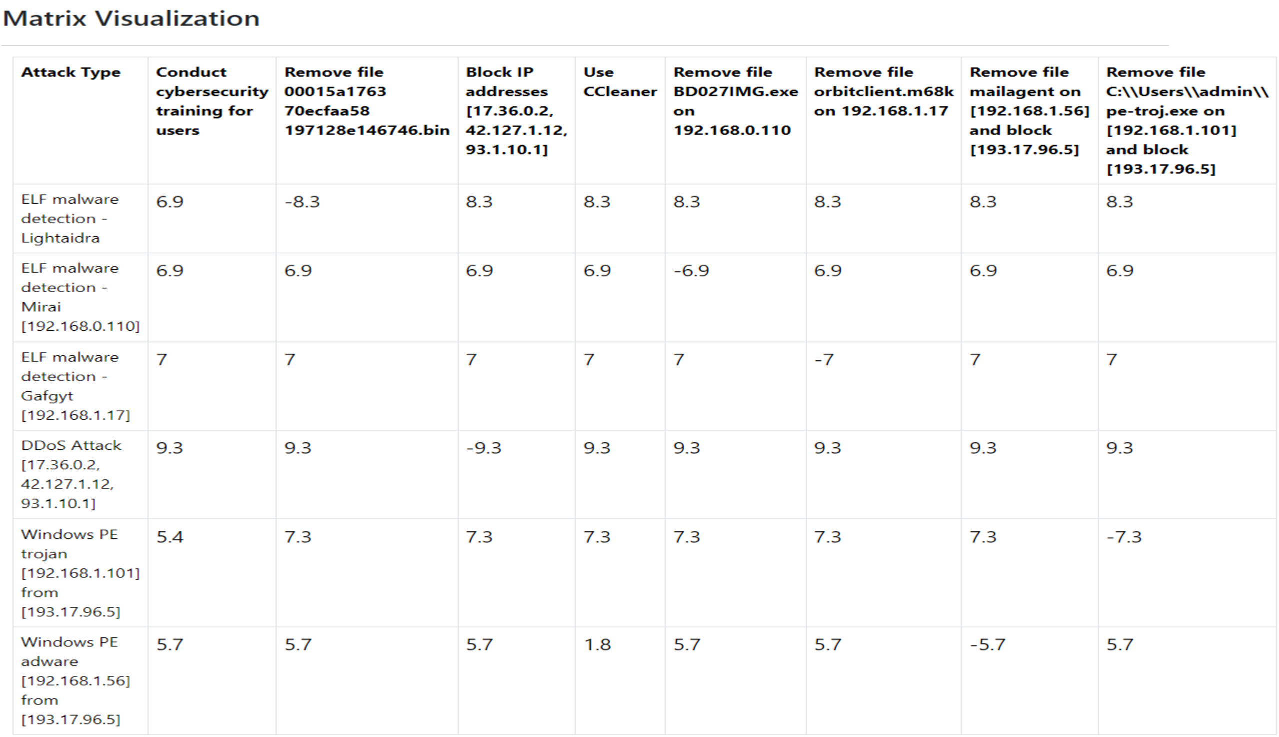
A game-theoretic model aimed at solving the matrix game and obtaining optimal strategies for a cybercriminal and a cyber defense specialist is used to draw conclusions from the formed game matrix.

System Web user interface is shown on Fig. 7 and Fig. 8. The user interface is a web application that provides recommendations for the application of cyber defense strategies. The web application interface consists of two web pages.

The first page displays the formed matrix of the game, and allows you to understand all possible strategies and gains from their application. The second page displays an explanation of the obtained optimal strategies and recommendations for the use of strategies by the system user, sorted by priority.

The generated recommendations are sent to the Information Security Management System, where the Chief Information Security Officer (CISO), acting as the end user of the system, makes decisions on the application of certain cyber protection strategies. The CISO can apply strategies to specific local network nodes, to the network as a whole, or to other entities and actors that are part of the Network Analysis System.

The developed expert system is updated in real time. The generation of the payment matrix of the game and recommendations for the application of cyber protection strategies occurs in the event of a change in the knowledge base of experts or when new detected or predicted cyber threats are received.

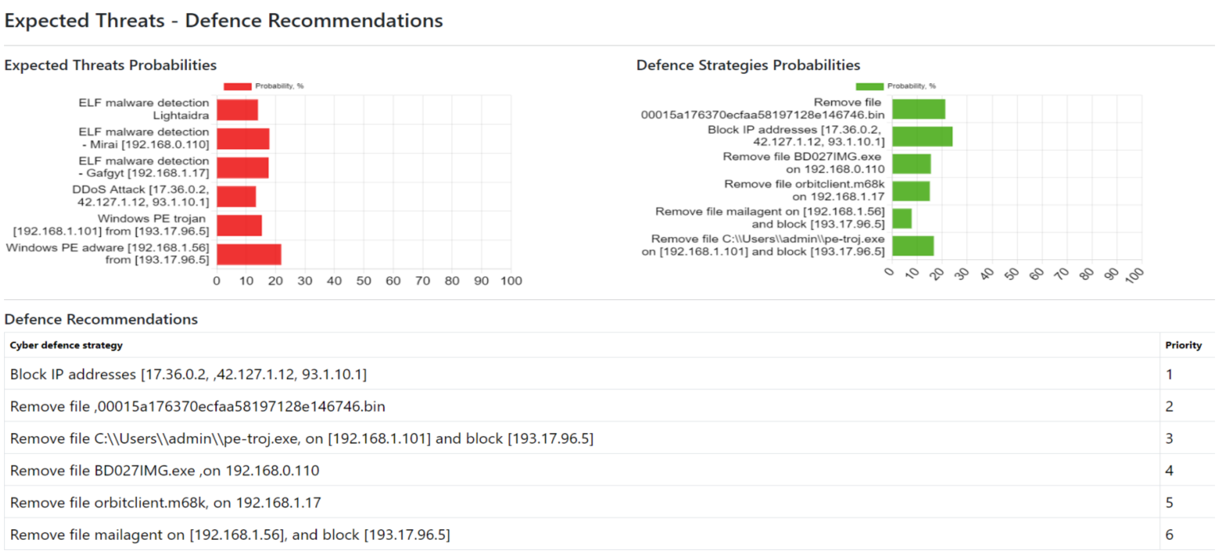


Matrix Visualization

Attack Type	Conduct cybersecurity training for users	Remove file 00015a1763 70ecfaa58 197128e146746.bin	Block IP addresses [17.36.0.2, 42.127.1.12, 93.1.10.1]	Use CCleaner	Remove file BD027IMG.exe on 192.168.0.110	Remove file orbitclient.m68k on 192.168.1.17	Remove file mailagent on [192.168.1.56] and block [193.17.96.5]	Remove file C:\\Users\\admin\\ pe-troj.exe on [192.168.1.101] and block [193.17.96.5]
ELF malware detection - Lightaidra	6.9	-8.3	8.3	8.3	8.3	8.3	8.3	8.3
ELF malware detection - Mirai [192.168.0.110]	6.9	6.9	6.9	6.9	-6.9	6.9	6.9	6.9
ELF malware detection - Gafgyt [192.168.1.17]	7	7	7	7	7	-7	7	7
DDoS Attack [17.36.0.2, 42.127.1.12, 93.1.10.1]	9.3	9.3	-9.3	9.3	9.3	9.3	9.3	9.3
Windows PE trojan [192.168.1.101] from [193.17.96.5]	5.4	7.3	7.3	7.3	7.3	7.3	7.3	-7.3
Windows PE adware [192.168.1.56] from [193.17.96.5]	5.7	5.7	5.7	1.8	5.7	5.7	-5.7	5.7

Fig. 7. **Web interface of the expert system. The page with the payoff matrix, that is used by the inference engine**

***Source:* compiled by the authors**



Expected Threats - Defence Recommendations

Expected Threats Probabilities

Probability, %
ELF malware detection Lightaidra
ELF malware detection - Mirai [192.168.0.110]
ELF malware detection - Gafgyt [192.168.1.17]
DDoS Attack [17.36.0.2, 42.127.1.12, 93.1.10.1]
Windows PE trojan [192.168.1.101] from [193.17.96.5]
Windows PE adware [192.168.1.56] from [193.17.96.5]
0
10
20
30
40
50
60
70
80
90
100

Defence Strategies Probabilities

Probability, %
Remove file 00015a176370ecfaa58197128e146746.bin
Block IP addresses [17.36.0.2, 42.127.1.12, 93.1.10.1]
Remove file BD027IMG.exe on 192.168.0.110
Remove file orbitclient.m68k on 192.168.1.17
Remove file mailagent on [192.168.1.56] and block [193.17.96.5]
Remove file C:\\\Users\\admin\\pe-troj.exe on [192.168.1.101] and block [193.17.96.5]
0
10
20
30
40
50
60
70
80
90
100

Defence Recommendations

Cyber defence strategy	**Priority**
Block IP addresses [17.36.0.2, ,42.127.1.12, 93.1.10.1]	1
Remove file ,00015a176370ecfaa58197128e146746.bin	2
Remove file C:\\Users\\admin\\pe-troj.exe, on [192.168.1.101] and block [193.17.96.5]	3
Remove file BD027IMG.exe ,on 192.168.0.110	4
Remove file orbitclient.m68k, on 192.168.1.17	5
Remove file mailagent on [192.168.1.56], and block [193.17.96.5]	6

Fig. 8. **Web interface of the expert system. Web page with the expected threats probabilities and defense recommendations.**
Source: **compiled by the authors**

CONCLUSIONS

The proposed expert system provides cyber defense recommendations based on expert knowledge of CVSS threat levels by solving a zero-sum matrix adversarial game. In the course of the study, an experimental verification of the convergence of the Brown-Robinson method of solving the matrix game was carried out using the Cybersecurity and Infrastructure Security Agency dataset. It was determined that the optimal number of iterations, which is necessary to obtain convergence of results, is 1000 iterations.

As a result of the conducted research, an architecture consisting of the Network Analysis System, Information Security Management System and Expert System was developed. The interface of the Expert System subsystem was implemented as a web application. The novelty of the developed system is the application of the CVSS basic group metric for expert based assessments and the use of an Brown-Robinson algorithm to solve strategic zero-sum games.

As a future work, it is planned to integrate the expert system with the corporate network and validate it in real time, using the simulation of various types of cyber attacks.

REFERENCES

1. Miller, J. "IDS vs IPS vs SIEM: what you should know". 2020. – Available from: https://www.bitlyft.com/resources/ids-vs-ips-vs-siem.

2. Hu, S. D. "Expert systems for software engineers and managers". *Springer New York, NY*. 2013. DOI: https://doi.org/10.1007/978-1-4613-1065-5.

3. Liebowitz, J. "The handbook of applied expert systems". *Taylor & Francis Group*. 2019. DOI: https://doi.org/10.1201/9780138736654.

4. Sarker, I. & Furhad, M. & Nowrozy, R. "AI-Driven cybersecurity: An overview, security intelligence modeling and research directions. SN computer science". 2021; 2 (3): 173, https://www.scopus.com/record/display.uri?eid=2-s2.0-85131828113&origin=resultslist. DOI: https://doi.org/10.1007/s42979-021-00557-0.

5. Churu, M. & Blaauw, D. & Watson, B. "A review and analysis of cybersecurity threats and vulnerabilities, by development of a fuzzy rule-based expert system". *Communications in Computer and Information Science.* 2069 CCIS. 2024. p. 151–168, https://www.scopus.com/record/display.uri?eid=2-s2.0-85192174410&origin=resultslist. DOI: https://doi.org/10.1007/978-3-031-57639-3_7.

6. Mahdavifar, S. & Ghorbani, A. "DeNNeS: deep embedded neural network expert system for detecting cyber attacks". *Neural Computing and Applications*. 2020; 32 (18): 14753–14780. DOI: https://doi.org/10.1007/s00521-020-04830-w.

7. Vasireddy, D. T., Dale, D. S. & Li, Q. “CVSS base score prediction using an optimized machine learning scheme”. *2023 Resilience Week (RWS)*. National Harbor, MD, USA, 2023, https://www.scopus.com/record/display.uri?eid=2-s2.0-85176130718&origin=resultslist. DOI: https://doi.org/10.1109/RWS58133.2023.10284627.

8. Maghrabi, L. & Pfluegel, E. & al-Fagih, L. & Graf, R. & Settanni, G. & Skopik, F. “Improved software vulnerability patching techniques using CVSS and game theory”. *2017 International Conference on Cyber Security And Protection Of Digital Services (Cyber Security)*. London, UK. 2017. p. 1–6. https://www.scopus.com/record/display.uri?eid=2-s2.0-85039968160&origin=resultslist. DOI: https://doi.org/10.1109/CyberSecPODS.2017.8074856.

9. Zhang, S., Cai, M., Zhang, M., Zhao L. & de Carnavalet, X. d. C. “The flaw within: Identifying CVSS score discrepancies in the NVD”. *IEEE International Conference on Cloud Computing Technology and Science (CloudCom)*. Naples, Italy. 2023. p. 185–192, https://www.scopus.com/record/display.uri?eid=2-s2.0-85189624842&origin=resultslist. DOI: https://doi.org/10.1109/CloudCom59040.2023.00039.

10. Cuong, D., Tran, N. Hong, C. S., Kamhoua, C., Kwiat, K., Blasch, E., Ren, S., Pissinou, N. & Iyengar, S. “Game theory for cyber security and privacy”. *ACM Computing Surveys*. 2017; 50 (2), https://www.scopus.com/record/display.uri?eid=2-s2.0-85019898776&origin=resultslist. DOI: https://doi.org/10.1145/3057268.

11. Zhu, Q. & Başar, T. “Game-theoretic methods for robustness, security, and resilience of cyberphysical control systems: Games-in-Games principle for optimal cross-layer resilient control systems”. *Control Systems, IEEE*. 2015; 35: 46–65, https://www.scopus.com/record/display.uri?eid=2-s2.0-84921497384&origin=resultslist. DOI: https://doi.org/10.1109/MCS.2014.2364710.

12. Wang, K. & Du, M. & Yang, D. & Zhu, C. & Shen, J. & Zhang, Y. “Game-Theory-based active defense for intrusion detection in cyber-physical embedded systems”. *ACM Transactions on Embedded Computing Systems*. 2016; 16: 1–21, https://www.scopus.com/record/display.uri?eid=2-s2.0-84992213754&origin=resultslist. DOI: https://doi.org/10.1145/2886100.

13. Sayed, M. A., Anwar, A. H., Kiekintveld, C., Bosansky, B. & Kamhoua, C. “Cyber Deception Against Zero-Day Attacks: A Game Theoretic Approach”. *In: Fang, F., Xu, H., Hayel, Y. (eds) Decision and Game Theory for Security. GameSec. Lecture Notes in Computer Science. Springer, Cham*. 2022; 13727: 44–63, https://www.scopus.com/record/display.uri?eid=2-s2.0-85151145797&origin=resultslist . DOI: https://doi.org/10.1007/978-3-031-26369-9_3.

14. Major, M., Fugate, S., Mauger, J. & Ferguson-Walter, K.”Creating cyber deception games”. *In: IEEE First International Conference on Cognitive Machine Intelligence (CogMI)*. Los Angeles, CA, USA. 2019. p. 102–111, https://www.scopus.com/record/display.uri?eid=2-s2.0-85081278794&origin=resultslist. DOI: https://doi.org/10.1109/CogMI48466.2019.00023.

15. Ullah, F., Turab, A., Ullah, S., Cacciagrano, D. & Zhao, Y. “Enhanced network intrusion detection system for internet of things security using multimodal big data representation with transfer learning and game theory”. *Sensors*. 2024; 24: 4152, https://www.scopus.com/record/display.uri?eid=2-s2.0-85198342880&origin=resultslist. DOI: https://doi.org/10.3390/s24134152.

16. Gill, K. S., Saxena S. & Sharma, A. “NCGTM: A Noncooperative game-theoretic model to assist IDS in cloud environment”. *In IEEE Transactions on Industrial Informatics*. 2024; 20 (3): 3124–3132, https://www.scopus.com/record/display.uri?eid=2-s2.0-85168260535&origin=resultslist. DOI: https://doi.org/10.1109/TII.2023.3300452.

17. Grebennyk, A., Trunova, O., Kazimir, V. & Mishchenko. M. “Detection and forecasting of the threat level for a corporate computer network. technical sciences and technologies”. *Technical sciences and technologies*. 2020; (2 (20)): 175–185. DOI: https://doi.org/10.25140/2411-5363-2020-2(20)-175-185.

18. Mishchenko, M. & Dorosh, M. “Semantic analysis and classifi- cation of malware for UNIX-like operating systems with the use of machine learning methods”. *Applied Aspects of Information Technology*. 2022; 5: 371–386. DOI: https://doi.org/10.15276/aait.05.2022.25.

19. “Common Vulnerability Scoring System: Specification Document”. 2024. – Available from: https://www.first.org/cvss/specification-document.

20. “Common Vulnerability Scoring System Version 4.0 Calculator”. 2024. – Available from: https://www.first.org/cvss/calculator/4.0.

21. Akyar, E. & Akyar, H. & Duzce, S. “Brown–Robinson method for interval matrix games”. *Soft Comput*. 2011; 15: 2057–2064. DOI: https://doi.org/10.1007/s00500-011-0703-6.

22. “Cybersecurity Risk (2022 CISA Vulnerability)”. – Available from: https://www.kaggle.com/datasets/thedevastator/exploring-cybersecurity-risk-via-2022-cisa-vulne.

Conflicts of Interest: the authors declare no conflict of interest

Received 26.06.2024
Received after revision 30.08.2024
Accepted 16.09.2024

DOI: https://doi.org/10.15276/hait.07.2024.20
УДК 004.891.2

Експертна система рекомендацій з протидії кіберзагрозам з використанням метрик CVSS та теорії ігор

Міщенко Максим Валерійович [1)]
ORCID: https://orcid.org/0000-0001-9769-9759; it144111@stu.cn.ua
Дорош Марія Сергіївна [1)]
ORCID: https://orcid.org/0000-0001-6537-8957; mariyaya5536@gmail.com. Scopus Author ID: 56912183600
[1)] Національний університет «Чернігівська політехніка» вул. Шевченка, 95. Чернігів, 14035, Україна

АНОТАЦІЯ

Дане дослідження зосереджене на створенні експертної системи генерації рекомендацій з кібербезпеки. Розроблена експертна система використовує теоретико-ігрову модель у якості рушія для перетворення еспертних знань у рекомендації для кінцевих користувачів, якими можуть бути керівники відділу ІТ-безпеки (CISO), системні адсміністратори або інженери з кіберзахисту. Експертні знання представлені у вигляді оцінки базової групи метрик CVSS – Common Vulnerability Score System, для кожного типу атаки та коригованих значень CVSS у разі, якщо застосовано вектор протидії атаці. Отримавши набір атак та базу експертних знань про атаки, система генерує матричну антагоністичну гру з нульовою сумою, гравцями якої виступають кіберзлочинець та експерт з кіберзахисту. Рушієм експертної системи виступає теоретико-ігрова модель, що відповідає за вирішення гри ітераційним методом Брауна-Робінсон та генерації рекомендацій з кіберзахисту. Було проведено експеримент зі збіжності алгоритму Брауна-Робінсон на датасеті вразливостей за 2022 рік з бази даних Cybersecurity and Infrastructure Security Agency, в результаті чого було визначено, що збіжність алгоритму вирішення матричної гри досягається на кількості ітерацій в 1000. У результаті проведеної роботи було розроблено архітектуру експертної системи та її інтерфейс у вигляді веб-застосунку, що забезпечує ввід експертами оцінок рівня CVSS зібраних загроз та протидій загрозам та вивід рекомендацій з протидії кіберзагрозам, згенерованих експертною системою.

Ключові слова: експертна система; кіберзахист; теорія Ігор; метод Брауна-Робінсон; CVSS

ABOUT THE AUTHORS

Maksym V. Mishchenko - Postgraduate, Information Technology and Software Engineering Department. Chernihiv Polytechnic National University, 95, Shevchenko Str. Chernihiv, 14035, Ukraine
ORCID: https://orcid.org/0000-0001-9769-9759; it144111@stu.cn.ua
Research field: Cybersecurity; machine learning; operating systems; software engineering

Міщенко Максим Валерійович - аспірант, кафедра Інформаційних технологій та програмної інженерії. Національний університет «Чернігівська політехніка», вул. Шевченка, 95. Чернігів, 14035, Україна

Mariia S. Dorosh - Doctor of Engineering Sciences, Professor, Information Technology and Software Engineering Department, Chernihiv Polytechnic National University, 95, Shevchenko Str. Chernihiv, 14035, Ukraine
ORCID: https://orcid.org/0000-0001-6537-8957; mariyaya5536@gmail.com. Scopus Author ID: 56912183600
Research field: Modeling and design of intelligent systems; knowledge management; convergence of project management systems; human factor in information security systems of organizations and projects

Дорош Марія Сергіївна - доктор технічних наук, професор кафедри Інформаційних технологій та програмної інженерії. Національний університет «Чернігівська політехніка», вул. Шевченка, 95. Чернігів, 14035, Україна