One of the pressing areas that is developing in the field of information security is associated with the use of Honeypots (virtual decoys, online traps), and the selection of criteria for determining the most effective Honeypots and their further classification is an urgent task. The main products that implement virtual decoy technologies are presented. They are often used to study the behavior, approaches and methods that an unauthorized party uses to gain unauthorized access to information system resources. Online hooks can simulate any resource, but more often they look like real production servers and workstations. A number of fairly effective developments are known that are used to solve the problems of detecting attacks on information system resources, which are based on the apparatus of fuzzy sets. They showed the effectiveness of the appropriate mathematical apparatus, the use of which, for example, to formalize the approach to the formation of a set of reference values that will improve the process of determining the most effective Honeypots. For this purpose, many characteristics have been formed (installation and configuration process, usage and support process, data collection, logging level, simulation level, interaction level) that determine the properties of online traps. These characteristics became the basis for developing a method for the formation of standards of linguistic variables for further selection of the most effective Honeypots. The method is based on the formation of a Honeypots set, subsets of characteristics and identifier values of linguistic estimates of the Honeypot characteristics, a base and derived frequency matrix, as well as on the construction of fuzzy terms and reference fuzzy numbers with their visualization. This will allow classifying and selecting the most effective virtual baits in the future

Keywords: honeypot classification, virtual decoys, fuzzy standards, method of forming linguistic standards

UDC 004.056.53(045)
DOI: 10.15587/1729-4061.2021.225346

DEVELOPMENT OF A METHOD FOR CONSTRUCTING LINGUISTIC STANDARDS FOR MULTI-CRITERIA ASSESSMENT OF HONEYPOT EFFICIENCY

A. Korchenko
Doctor of Technical Sciences, Associate Professor
Department of Information Technology Security*
V. Breslavskyi
Deputy Head of Department
Ukrainian State Centre of Radio Frequencies
Peremohy ave., 151, Kyiv, Ukraine, 03179
S. Yevseiev
Doctor of Technical Sciences, Professor
Department of Cyber Security and Information Technology
Simon Kuznets Kharkiv National University of Economics
Nauky ave., 9-A, Kharkiv, Ukraine, 61166
E-mail: serhii.yevseiev@hneu.net
N. Zhumangalieva
Satbayev University
Satpaev str., 22a, Almaty, Republic of Kazakhstan, 050013
T. K. Zhurgenov Kazakh National Academy of Arts
Panfilova str., 127, Almaty, Republic of Kazakhstan, 050013
A. Zvarych
PhD
Central Scientific Research Institute of Armament and
Military Equipment of the Armed Forces of Ukraine
Povitroflotsky ave., 28b, Kyiv, Ukraine, 03049
S. Kazmirchuk
Doctor of Technical Sciences, Associate Professor
Department of Computerized Information Protection Systems*
O. Kurchenko
PhD, Associate Professor, Senior Researcher
Department of Programming and Computer Equipment
Taras Shevchenko National University of Kyiv
Volodymyrska str., 60, Kyiv, Ukraine, 01033
O. Laptiev
Doctor of Technical Sciences, Senior Researcher
Department of Information and Cybersecurity Systems
Institute of Information Protection State University of Telecommunications
Solomenska str., 7, Kyiv, Ukraine, 03110
O. Sievierinov
PhD, Associate Professor
Department of Information Technologies Security
Kharkiv National University of Radio Electronics
Nauky ave., 14, Kharkiv, Ukraine, 61166
S. Tkachuk
PhD, Associate Professor
Department of Military Training
Vinnytsia National Technical University
Khmelnytske shose str., 95, Vinnytsia, Ukraine, 21000
*National Aviation University
Liubomyra Huzara ave., 1, Kyiv, Ukraine, 03058

Received date 20.11.2020
Accepted date 20.01.2021
Published date 26.02.2021

1. Introduction

The rapid development of information systems (IS) and technology affects all areas of society. A significant number of modern public and private enterprises use IS to manage production processes, support decision-making, search for the necessary data, etc. This provides them with a number of advantages associated with increased productivity and mo-

bility of workers, high efficiency of access to information and services, as well as the ability to remotely manage resources and processes.

Also, in recent years, there has been a significant increase in the amount of information accumulated, stored and processed using computer systems. At the same time, the concentration of information for various purposes and belonging in common databases, as well as a sharp expansion of the range of users with direct access to IS resources, give rise to the problem of ensuring their protection against various kinds of intrusions. The increasing complexity of hardware and software and the existing shortcomings of modern information technologies lead to the improvement of intrusions on IS resources.

Along with this, the number of vulnerabilities and threats to IS is increasing, and therefore, to ensure their normal functioning and prevent intrusions, specialized security tools are needed. It should be noted that one of the topical areas that is actively developing in the field of information security is associated with the use of Honeypots (virtual decoys, online traps). The purpose of such decoys is to be attacked or scanned by an unauthorized party (UAP) to study the defense strategy, to determine the range of their means by which strikes can be applied to real security objects. Honeypots and methods used to implement them are varied, for example, it is a specially deployed integral network or a single emulated network service, the main task of which is to attract the UAP's attention [1]. Therefore, the selection of characteristics and the formation of the corresponding criteria for determining the most effective Honeypots and their further classification is an urgent task.

2. Literature review and problem statement

The technology of virtual baits is based on developments [2, 3], and is also implemented in products such as: Deception Toolkit (DTK) (California, USA), CyberCop Sting (USA) and BackOfficer Friendly (USA) [4, 5]. Its development and expansion of the scope are associated with the Honeynet Project (the project includes dozens of operating branches around the world: Brazil, Indonesia, Greece, India, Mexico, Iran, Australia, Ireland, and many in the United States) [6]. Given [4–9], Honeypot has become a tool that has its own architecture, tools, and scope. Often, decoys were used to study the behavior, approaches, and methods that the UAP used. However, in recent years there have been various uses for the Honeypot. They can simulate any resource, but more often the decoys look like real production servers and workstations. Some of them can be used, for example, in corporate networks for: collecting information, wasting the time and resources of attackers [10], reducing spam activity [11], deceiving intruders [12], analyzing the activities of hackers when hacking a system [13], and identifying images (signatures) of attacks [14, 15]. The main thing when creating a Honeypot is registering the start of an attack and a system break.

The work [16] describes a Micro-Honeypot implementation that aims to use browser fingerprint technology to track a web attacker. The exploitation process showed that Micro-Honeypot can collect more information and track intruders. [17] also proposes the development of practical client-side honeypots based on a virtual environment that can assist users in building and installing their own Honeypots. In [18], a threat analysis method is considered aimed at evaluating trap log data to determine the behavior of attackers when searching for attack patterns. In [19], it is proposed to group a number of decoys into one Honeynet and use it to collect, research, and evaluate data. The research [20] is aimed at identifying methods for implementing traps to detect the activity of ransomware. Also, in the course of the study, the threshold values of quantities used to counter cyber attacks were determined. [21] shows how highly interoperable Honeypots can be improved by providing them with special functions for reverse engineering in order to efficiently analyze captured malicious objects. The work [22] is aimed at investigating the integration of the capabilities of active and passive decoys to create a common set of malicious programs. In [23], spy decoys are considered that search the network for various documents and other intelligence information. They became the basis for the proposed set of tools that assess the degree of interest in the specified data. In [24], a dynamic addressing system Honeypot is proposed for detecting access to an unassigned address. This enables port scan detection through coordinated interaction between different honeypots. In [25], the methodology of automatic creation and dynamic updating of the Honey net Project is investigated. This provides additional functionality to enhance the capabilities of the IDS.

However, the papers [16–25] do not show the necessary characteristics by which in the future it is possible to select the most effective Honeypots and carry out their classification to solve the corresponding security problems.

Taking into account [15, 26, 27], virtual baits are divided into low (for example, BackOfficer Friendly (BOF) (USA), Specter, DTK, LaBrea (Switzerland), medium (for example, Honeyd, Honeypot Manager (HM) (Michigan, USA), Nepenthes, Multipot, Mwcollect (USA) and high level of interaction (for example, ManTrap, Argos, Minos (USA)).

In [15, 26, 28], criteria for the characteristics (characteristic features of the classification) of the Honeypot are proposed: "Installation and configuration process", "Usage and support process", "Data collection", "Logging level", "Simulation level" and "Interaction level", which can be displayed by the corresponding linguistic variables. To construct the corresponding reference fuzzy numbers (FN), it is necessary to enter a common interval of numerical characteristics that determine the values (criteria) of linguistic variables ("SIMPLE" – (S), "MEDIUM" – (M), "COMPLEX" – (C), "LIMITED" – (LM), "VARIABLE" – (V), "EXTENDED" – (E), "LOW" – (LO), "HIGH" – (H)) of specific terms (Table 1). Before constructing the standards of linguistic variables, we will reveal each of the criteria.

"Installation and configuration process" (IC) – characterizes the time and effort involved in installing and configuring Honeypot. The more complex the Honeypot is and the more extensive the tasks that are assigned to it, the more significant this parameter is. The increasing functionality that is presented to the attacker requires the installation and configuration of more services and the ability to process more commands. The simple installation process does not include the requirements for configuring or setting additional parameters for the Honeypot tool. Medium – requires setting a limited number of parameters (for example, selecting a simulated service option) for the correct operation of the tool, complex – requires a fairly detailed setting (usually associated with installation), setting a large number of additional operating parameters [26].

Table 1

Generalized classification for Honeypot evaluation

Specifications	Honeypot											
	DTK	Specter	BOF	LaBrea	Honeyd	HM	Nepenthes	Multipot	Mwcollect	ManTrap	Argos	Minos
Installation and configuration process	S	S	S	S	M	M	S	M	S	C	C	C
Usage and support process	M	M	S	S	M	M	M	M	M	C	M	C
Data collection	LM	LM	LM	LM	V	LM	V	V	V	E	S	E
Logging level	LO	M	LO	LO	M	H	M	M	M	H	H	M
Simulation level	LO	M	LO	LO	H	M	M	LO	M	H	H	H
Interaction level	LO	LO	LO	LO	M	M	M	M	M	H	H	H

The IC process is characterized by an integral indicator, which takes into account the number of actions (user commands) to install the Honeypot and the time spent on this process, i.e. $I=C\times T$, where I – integral indicator, C – number of actions (commands), T – time spent on installation. Considering that to install a low, medium and high interaction Honeypot, it is needed to complete up to 4, 5 to 7, and 8 to 12 steps, respectively, the time costs will be up to 3, from 4 to 10 and from 11 to 30 minutes. Let's define the upper limit of the integral indicator as 360.

"Usage and support process" (US) – describes the time and effort to use and support the Honeypot after the installation and configuration process. It follows from this that the higher the functionality of the Honeypot, the more difficult it is to use, and the more time and effort it takes to support it. A simple process of usage and support means the minimum amount of time required to support the tool, as well as ease of use (for example, to use it correctly, you just need to start the program). The middle level adds additional steps to the usage process aimed at configuring the Honeypot in the process of functioning, the need for administrator participation to correct behavior, etc. The complex level includes the necessary actions in the use and subsequent support of the tool (for example, updating the software, restoring the environment for further research after the interaction has been made) [26].

The US process is determined by the number of actions of the user (operator) per unit of time. So, for a Honeypot with a low interaction level, this is on average 1–2 actions per minute, medium – from 3 to 6, and high – from 6 to 10. Thus, we set 10 user actions per minute as the upper limit of this characteristic.

Data collection (DC) is the amount of data that the Honeypot can collect about an attacker and his activity. If the Honeypot is a specially prepared operating system, then a lot of data about the attacker and his actions can be collected. If the Honeypot is an imitation of some system service, the amount of data is reduced. The latter is an example of simple data collection. Variable data collection characterizes Honeypot tools, where there are additional settings for the selection of collected events. Advanced data collection implies a strong interaction Honeypot [26].

The value of DC is characterized by the indicator of the diversity of the collected data, that is, by their categories. Based on this, we will introduce the following intervals for the formation of criteria: 0–4 – for low-level Honeypots, 5–12 – for medium-level honeypots, and 13–20 – for high-level Honeypots.

"Logging level" (L) – characterizes the level of detail with which the logging will be performed. The higher the logging level, the more detailed the program log records are. The low level of logging is determined by the low level of detail of the collected data. As a rule, this level is possessed by means of Honeypot of weak interaction, when only the IP address of the source of communication and data originating from the attacker are logged. The medium level of logging can include the protocol of both sides of the interaction, as well as additional data (for example, the specific time of data arrival, interaction identifiers, etc.). Strong interaction Honeypots have a high level of logging, when a tool takes on the responsibility of logging all events that occur in the system during interaction [26].

The value of L is determined by the amount of data that is recorded in the memory of the virtual decoy. Since Microsoft recommends that the event log in 64-bit Windows Server is limited to 16 MB of memory, it is advisable to take this value as the upper limit of the specified intervals. Thus, we get the following intervals for low-, medium- and high-level honeypots – 0–100 KB, 101–4,000 KB and 4,001–16,000 KB, respectively.

"Simulation level" (S) – characterizes the degree of service simulation. A simple level of simulation implies an almost complete lack of support for the functionality of the simulated service (for example, the ability to display only a greeting message when connecting). The medium level implies a fairly detailed simulation of the service, taking into account the peculiarities of its operation. The high level of simulation presupposes the full implementation of all the functionality of the service (in fact, it is approaching the emulation of the service). When using real operating systems, the level of simulation is high. This characteristic also includes the level of simulation of behavior in response to an attack attempt [26].

It is advisable to determine the "I" value based on the number of simulated services. At the same time, we will take into account that the Windows OS in working order has an average of 60 to 100 simultaneously running services, including system services. So, for low-, medium- and high-level honeypots – 0–5, 6–10 and 11–100 simulated services, respectively.

"Interaction level" (IL) is a measure that allows characterizing the Honeypot in relation to the breadth of the field of UAP activity, i.e. the higher the level of interaction, the more critical information about the attacker can be obtained. But the more the UAP's capabilities are provided, the more damage it can cause.

In turn, online traps are divided into low-, medium- and high-level interactions. Each of these types of Honeypots provides a specific functionality or level of interaction between the UAP and the system, and developers usually define this metric.

In [29], an analysis of the existing risk assessment systems was carried out, on the basis of which a set of parameters was formed that allow performing the corresponding assessments in the field of information security. So, for example, for the values characterizing the probability (P), frequency (F), costs and losses (L), danger (D), the construction of reference values of linguistic variables, displayed by graphic models in the form of rectangular and trapezoidal fuzzy numbers (FN), is carried out. This process is implemented on the basis of expert data displayed at intervals on the x-axis and is used to assess the risks that affect various security characteristics of information systems resources. This approach can be effectively used when building information security management systems on a risk-based basis and the initial data of an expert in the form of sets of intervals characterizing the formed set of parameters. The resulting models, for example, cannot be used to construct linguistic standards for multicriteria assessment of honeypot efficiency or to detect cyber attacks, as well as use the initial data presented in the form of frequencies of the expert judgments about possible values formed by the set of parameters for evaluating online traps.

The work [30] discusses the formation of linguistic variables used to construct tools aimed at identifying processes associated with unauthorized scanning of computer system ports. Based on the analysis of well-known developments, for example, for values characterizing the number of virtual channels (NVC) and the age of virtual channels (AVC), the construction of reference values of linguistic variables is carried out, displayed by the corresponding graphic models. This approach can be effectively used to identify scanning utilities when building intrusion detection systems based on the use of statistical input data generated as a result of processing the expert judgments regarding the generated set of parameters. The linguistic standards obtained in [30], graphically displayed by normal unimodal convex discrete nonparametric FN, cannot, for example, be used to implement the estimation processes associated with honeypots or information risks.

The work [1] considers the formation of linguistic variables used to build tools aimed at detecting DDoS attacks and spoofing on information system resources. Taking into account the relevant analysis, for example, for values characterizing the number of simultaneous server connections (SSC), the speed of processing requests from clients (SPR), the delay between requests from one user(DBR), the number of packets with the same sender and recipient address (NPSA), the construction of reference values of linguistic variables is carried out, displayed (by analogy with [30]) by the corresponding graphic models. This approach can be effectively used to expand the functionality of intrusion detection systems by identifying cyber attacks associated with DDos and spoofing in the m-dimensional heterogeneous parametric environment. The disadvantage of this study is isomorphic with the work [30].

The analysis of monographic studies related to the construction of fuzzy standards [1, 29, 30] showed that the existing approaches are effective in the implementation of measurements associated with assessing information security risks and identifying various types of cyberattacks, but cannot be directly used for multicriteria assessment of Honeypot efficiency.

3. The aim and objectives of the study

The aim of the study is to develop a method for constructing linguistic standards for multicriteria assessment of the effectiveness of online traps based on the experience and judgments of experts describing the properties of a Honeypot relative to the values of a given set of characteristics. In the future, this will make it possible to use the obtained standards for the classification and selection of the most effective virtual baits.

To achieve the aim, the following objectives were set:

– to analyze the existing characteristics of modern Honeypots to form appropriate criteria for their evaluation;

– to develop a method for constructing linguistic standards for multicriteria assessment of Honeypot efficiency.

4. Analysis of the existing characteristics of modern Honeypots to form appropriate criteria for their assessment

The developments [2–14, 16–25], which are based on Honeypot technologies, are focused on solving various security problems. But in order to select the most effective of them for solving the corresponding problems, it is necessary to determine a set of criteria by which traps can be classified. In [15, 26, 28], a number of quantities (IC, US, DC, L, S, I) are proposed, the generalization of which is shown in Fig. 1. They can be used to make a choice (assessment, measurement), but for this it is necessary to form the corresponding reference values of linguistic quantities that are not defined in these studies.

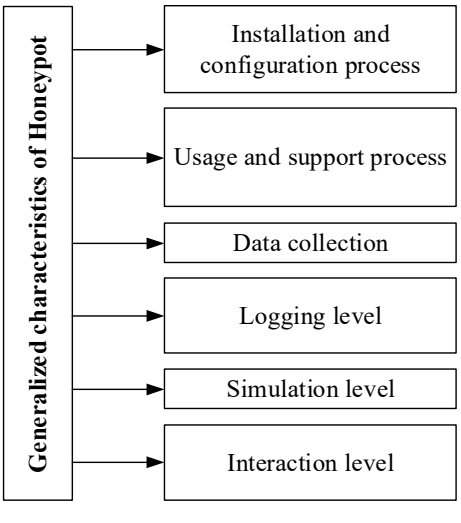

Fig. 1. Generalized characteristics used to build standards for further classification and evaluation of the Honeypot

It should be noted that there are quite effective developments [1, 29, 30] used to solve the problems of risk

assessment and identifying attacks on information system resources, which are based on the theory of fuzzy sets. This approach has shown the effectiveness of using the appropriate mathematical apparatus, for example, to formalize the approach to the construction of fuzzy (linguistic) standards. In the future, this will make it possible to select and classify Honeypots in order to use them to solve the set tasks of information protection.

5. Development of a method for constructing linguistic standards for multicriteria assessment of Honeypot efficiency

The proposed method for constructing linguistic standards is partially based on the method of linguistic terms using statistical data [30], as well as on the method of forming linguistic standards for intrusion detection systems [1, 31, 32]. Taking this into account, we define six basic stages of the method implementation [33–36]:

– stage 1 – formation of a set of Honeypots;

– stage 2 – formation of subsets of Honeypot characteristics;

– stage 3 – formation of subsets of identifier values of linguistic estimates of Honeypot characteristics;

– stage 4 – formation of the base and derived frequency matrix;

– stage 5 – construction of fuzzy terms and reference FN [33];

– stage 6 – visualization of reference FN [33].

Thus, the main stages have been formed, the implementation process of which will form the basis of the developed method. Further, in the specified sequence, we describe the essence of the implementation of each of the stages.

Next, we will describe each of the stages.

Stage 1 – formation of a set of Honeypots. Let's introduce the set of possible Honeypots H represented as

$$\mathbf{H}=\left\{\bigcup_{i=1}^{n}H_i\right\}=\{H_1,H_2,...,H_n\},\ \ (i=\overline{1,n}), \tag{1}$$

where n – number of possible Honeypots.

For example, for i=12 according to (1), the set H can be represented as:

$$\mathbf{H}=\left\{\bigcup_{i=1}^{12}H_i\right\}=\{H_1,H_2,...,H_{12}\}=$$
$$\begin{Bmatrix}H_{DTK},H_S,H_{BOF},H_{LB},H_H,H_{HM},\\H_N,H_{Mp},H_{Mw},H_{MT},H_A,H_M\end{Bmatrix}, \tag{2}$$

where H_{DTK}=DTK, H_S=Specter, H_{BOF}=BOF, H_{LB}=LaBrea, H_H=Honeyd, H_{HM}=HM, H_N=Nepenthes, H_{Mp}=Multipot, H_{Mw}=Mwcollect, H_{MT}=ManTrap, H_A=Argos and H_M=Minos, respectively, are the mapping of Honeypots of various developers used in practice, which are presented in Table 1 "DTK (*DTK*)" (for i=1), "Specter (*S*)" (for i=2), "BOF (*BOF*)" (for i=3), "LaBrea (*LB*)" (for i=4), "Honeyd (*H*)" (for i=5), "HM (*HM*)" (for i=6), "Nepenthes (*N*)" (for i=7), "Multipot (*Mp*)" (for i=8), "Mwcollect (*Mw*)" (for i=9), "ManTrap (*MT*)" (for i=10), "Argos (*A*)" (for i=11) and "Minos (*M*)" (for i=12).

Thus, sets of Honeypots are formed – *DTK*, *S*, *BOF*, *LB*, *H*, *HM*, *N*, *Mp*, *Mw*, *MT*, *A*, *M*, which can be used to form a subset of Honeypot characteristics.

Stage 2 – formation of subsets of Honeypot characteristics. Each Honeypot is described by certain characteristics, and the construction of the subset CH_{ij} is carried out based on the set of all possible characteristics of the Honeypot CH_i

$$CH_i=\left\{\bigcup_{j=1}^{m_i}CH_{ij}\right\}=\{CH_{i1},CH_{i2},...,CH_{im_i}\},\ \left(j=\overline{1,m_i}\right), \tag{3}$$

where m_i – number of such characteristics.

For example, for j=5, according to (3), the set CH can be represented as:

$$CH=\left\{\bigcup_{v=1}^{5}CH_v\right\}=\{CH_1,CH_2,...,CH_5\}=$$
$$=\{CH_{IC},CH_{US},CH_{DC},CH_L,CH_S\}, \tag{4}$$

where CH_1=CH_{IC}="IC", CH_2=CH_{US}="US", CH_3=CH_{DC}= ="DC", CH_4=CH_L="L" and CH_5=CH_S="S", respectively, are such characteristics of Honeypot as: IC – "Installation and configuration" (for j=1), US – "Usage and support" (for j=2), DC – "Data collection" (for j=3), L – "Logging" (for j=4), and S – "Simulation" (for j=5).

At this stage, subsets of Honeypot characteristics are formed, such as IC, US, DC, L, S, which are the basis for the formation of subsets of identifier values for linguistic estimates of Honeypot characteristics.

Stage 3 – formation of subsets of identifier values of linguistic estimates of Honeypot characteristics. Construction of the subset LEH_i is based on the set of all possible Honeypot values LEH represented as

$$LEH=\left\{\bigcup_{l=1}^{c}LEH_l\right\}=\{LEH_1,LEH_2,...,LEH_c\},\ \left(l=\overline{1,c}\right), \tag{5}$$

which represent the judgments used by the expert to characterize the state of the Honeypot when they are observed in a certain environment, and c – is the number of such ID.

For example, for c=8 according to (5), the set LEH can be represented as:

$$LEH=\left\{\bigcup_{l=1}^{8}LEH_l\right\}=\{LEH_1,LEH_2,...,LEH_8\}=$$
$$=\begin{Bmatrix}LEH_S,LEH_M,LEH_C,LEH_{LM},\\LEH_V,LEH_E,LEH_{LO},LEH_H\end{Bmatrix},$$
$$\{\text{"S", "M", "C", "LM", "V", "E", "LO", "H"}\}, \tag{6}$$

where LEH_1=LEH_S="S", LEH_2=LEH_M="M", LEH_3=LEH_C= ="C", LEH_4=LEH_{LM}="LM", LEH_5=LEH_V="V", LEH_6= =LEH_E="E", LEH_7=LEH_{LO}="LO" and LEH_8=LEH_H="H", respectively, are the IDs of such values of the linguistic assessments of the expert as "SIMPLE" (for l=1), "MEDIUM" (for l=2), "COMPLEX" (for l=3), "LIMITED" (for l=4), "VARIABLE" (for l=5), "EXTENDED" (for l=6), "LOW" (for l=7) and "HIGH" (for l=8), which are presented in Table 1.

For example, taking into account the generated set of Honeypot (1), a subset of its characteristics (3) and subsets of identifier values of linguistic estimates of Honeypot characteristics (5), as well as, by analogy with stage 1, ex-

pressions (7) in [31, 32] for n=1 for Honeypot HP_1=HP_{DTK}= =DTK, m_1=5, r_1=r_2=r_3=r_4=r_5=3, we form

$$\left\{\bigcup_{i=1}^{1} LE_1\right\}=\left\{\bigcup_{i=1}^{1}\left\{\bigcup_{j=1}^{m_i} LE_{ij}\right\}\right\}=\left\{\bigcup_{i=1}^{1}\left\{\bigcup_{j=1}^{m_i}\left\{\bigcup_{k=1}^{r_j} LE_{ijk}\right\}\right\}\right\}=$$

$$=\begin{Bmatrix}\{LE_{DTKICS1},LE_{DTKIC2},LE_{DTKIC3}\},\\ \{LE_{DTKUS1},LE_{DTKUS2},LE_{DTKUS3}\},\\ \{LE_{DTKDC1},LE_{DTKDC2},LE_{DTKDC3}\},\\ \{LE_{DTKL1},LE_{DTKL2},LE_{DTKL3}\},\\ \{LE_{DTKS1},LE_{DTKS2},LE_{DTKS3}\}\end{Bmatrix}=$$

$$=\begin{Bmatrix}\{\text{"S","M","C"}\},\{\text{"S","M","V"}\},\\ \{\text{"LM","V","E"}\},\\ \{\text{"LM","V","E"}\},\{\text{"LO","M","H"}\}\end{Bmatrix}, \quad (7)$$

where DTK – "Deception Toolkit", and LE_{DTKIC1}=*"S"*, LE_{DTKIC2}=*"M"*, LE_{DTKIC3}=*"C"*, LE_{DTKUS1}=*"V"*, LE_{DTKUS2}=*"M"*, LE_{DTKUS3}=*"C"*,LE_{DTKDC1}=*"LM"*,LE_{DTKDC2}=*"V"*,LE_{DTKDC3}=*"E"*, LE_{DTKL1}=*"LM"*, LE_{DTKL2}=*"V"*, LE_{DTKL3}=*"E"*, LE_{DTKS1}=*"LO"*, LE_{DTKS2}=*"M"*, LE_{DTKS3}=*"H"*, respectively, are the IDs of such linguistic expert assessments that reflect the characteristics of the Honeypot, such as IC, US, DC, L and S.

Thus, subsets of identifier values of linguistic estimates of Honeypot characteristics IC, US, DC, L, S are formed, which will allow constructing basic and derived frequency matrices.

Stage 4 – formation of the base and derived frequency matrix. This stage is implemented by analogy with stage 2 in [31, 32]. The first is to generate a basic frequency matrix. To do this, construct a subset of interval IDs $N_{ij}\ (j=\overline{1,m_i})$ ((12) in [31, 32]), characterizing the Honeypot with ID HP_1= =HP_{DTK}=DTK, on the domain of which the expert carries out linguistic assessment with respect to the parameter values P_{DTKIC}, P_{DTKUS}, P_{DTKDC}, P_{DTKL} and P_{DTKS}.

For n=1, $m_1$5, r_1=r_2=r_3=r_4=r_5=3, we get

$$\left\{\bigcup_{i=1}^{1} N_i\right\}=\left\{\bigcup_{i=1}^{1}\left\{\bigcup_{j=1}^{m_i} N_{ij}\right\}\right\}=\left\{\bigcup_{i=1}^{1}\left\{\bigcup_{j=1}^{m_i}\left\{\bigcup_{k=1}^{r_j} N_{ijk}\right\}\right\}\right\}=$$

$$=\begin{Bmatrix}\{N_{DTKIC1},N_{DTKIC2},N_{DTKIC3}\},\\ \{N_{DTKUS1},N_{DTKUS2},N_{DTKUS3}\},\\ \{N_{DTKDC1},N_{DTKDC2},N_{DTKDC3}\},\\ \{N_{DTKL1},N_{DTKL2},N_{DTKL3}\},\\ \{N_{DTKS1},N_{DTKS2},N_{DTKS3}\}\end{Bmatrix}. \quad (8)$$

Taking into account the elements of the subsets LE_{ij} and NE_{ij} on the basis of the generalized table (Table 1 in [31, 32]), we construct the current estimates (Tables 2–6) for the elements of the subsets,

$$LE_{DTKICk}\left(r_1=3,k=\overline{1,3}\right),\ \ N_{DTKICk},$$

i. e.

$$N_{DTKIC1}=\left[N^{\min}_{DTKIC1};N^{\max}_{DTKIC1}\right]\Leftrightarrow[0;12],$$

$$N_{DTKIC2}=\left[N^{\min}_{DTKIC2};N^{\max}_{DTKIC2}\right]\Leftrightarrow[13;70],$$

$$N_{DTKIC3}=\left[N^{\min}_{DTKIC3};N^{\max}_{DTKIC3}\right]\Leftrightarrow[71;360],$$

$$LE_{DTKUSk}\left(r_2=3,k=\overline{1,3}\right),\ \ N_{DTKUSk},$$

i.e.

$$N_{DTKUS1}=\left[N^{\min}_{DTKUS1};N^{\max}_{DTKUS1}\right]\Leftrightarrow[0;2],,$$

$$N_{DTKUS2}=\left[N^{\min}_{DTKUS2};N^{\max}_{DTKUS2}\right]\Leftrightarrow[2;6],$$

$$N_{DTKUS3}=\left[N^{\min}_{DTKUS3};N^{\max}_{DTKUS3}\right]\Leftrightarrow[6;10],$$

$$LE_{DTKDCk}\left(r_3=3,k=\overline{1,3}\right),\ \ N_{DTKDCk},$$

i.e.

$$N_{DTKDC1}=\left[N^{\min}_{DTKDC1};N^{\max}_{DTKDC1}\right]\Leftrightarrow[0;4],$$

$$N_{DTKDC2}=\left[N^{\min}_{DTKDC2};N^{\max}_{DTKDC2}\right]\Leftrightarrow[5;12],$$

$$N_{DTKDC3}=\left[N^{\min}_{DTKDC3};N^{\max}_{DTKDC3}\right]\Leftrightarrow[13;20];$$

and

$$LE_{DTKLk}\left(r_3=3,k=\overline{1,3}\right),\ \ N_{DTKLk},$$

i.e.

$$N_{DTKL1}=\left[N^{\min}_{DTKL1};N^{\max}_{DTKL1}\right]\Leftrightarrow[0;100],$$

$$N_{DTKL2}=\left[N^{\min}_{DTKL2};N^{\max}_{DTKL2}\right]\Leftrightarrow[101;4,000],$$

$$N_{DTKL3}=\left[N^{\min}_{DTKL3};N^{\max}_{DTKL3}\right]\Leftrightarrow[4,001;16,000];$$

and

$$LE_{DTKSk}\ \left(r_3=3,k=\overline{1,3}\right),\ \ N_{DTKSk},$$

i. e.

$$N_{DTKS1}=\left[N^{\min}_{DTKS1};N^{\max}_{DTKS1}\right]\Leftrightarrow[0;5],$$

$$N_{DTKS2}=\left[N^{\min}_{DTKS2};N^{\max}_{DTKS2}\right]\Leftrightarrow[6;10],$$

$$N_{DTKS3}=\left[N^{\min}_{DTKS3};N^{\max}_{DTKS3}\right]\Leftrightarrow[11;100].$$

Table 2

Current estimates LE_{DTKIC}

LE_{DTKIC}	N_{DTKIC}		
	N_{DTKIC1}	N_{DTKIC2}	N_{DTKIC3}
"S"	5	2	0
"M"	1	6	0
"C"	0	1	4

Table 3

Current estimates LE_{DTKUS}

LE_{DTKUS}	N_{DTKUS}		
	N_{DTKUS1}	N_{DTKUS2}	N_{DTKUS3}
"S"	4	1	0
"M"	2	3	1
"C"	0	1	4

Table 4

Current estimates LE_{DTKDC}

LE_{DTKDC}	N_{DTKDC}		
	N_{DTKDC1}	N_{DTKDC2}	N_{DTKDC3}
"LM"	5	3	0
"V"	2	7	1
"E"	0	4	8

Table 5

Current estimates LE_{DTKL}

LE_{DTKL}	N_{DTKL}		
	LE_{DTKL1}	LE_{DTKL2}	LE_{DTKL3}
"LM"	6	1	0
"V"	1	5	2
"E"	0	1	3

Table 6

Current estimates LE_{DTKS}

LE_{DTKS}	N_{DTKS}		
	N_{DTKS1}	N_{DTKS2}	N_{DTKS3}
"LO"	7	1	0
"M"	1	6	2
"H"	0	1	8

Further, taking into account the data in Tables 2–6 and expressions (13) in [31, 32], we form the frequency matrices at $n=1,\ m_1=1,5,\ s,q=\overline{1,r_1},\ s,q=\overline{1,r_2},\ s,q=\overline{1,r_3},\ s,q=\overline{1,r_4},\ s,q=\overline{1,r_5}$

$$F_{11}=F_{DTKIC}=\left\|f_{11sq}\right\|=\begin{vmatrix} f_{1111} & f_{1112} & f_{1113} \\ f_{1121} & f_{1122} & f_{1123} \\ f_{1131} & f_{1132} & f_{1133} \end{vmatrix}=\begin{vmatrix} 5 & 2 & 0 \\ 1 & 6 & 0 \\ 0 & 1 & 4 \end{vmatrix},$$

$$F_{12}=F_{DTKUS}=\left\|f_{12sq}\right\|=\begin{vmatrix} f_{1211} & f_{1212} & f_{1213} \\ f_{1221} & f_{1222} & f_{1223} \\ f_{1231} & f_{1232} & f_{1233} \end{vmatrix}=\begin{vmatrix} 4 & 1 & 0 \\ 2 & 3 & 1 \\ 0 & 1 & 4 \end{vmatrix},$$

$$F_{13}=F_{DTKDC}=\left\|f_{13sq}\right\|=\begin{vmatrix} f_{1311} & f_{1312} & f_{1313} \\ f_{1321} & f_{1322} & f_{1323} \\ f_{1331} & f_{1332} & f_{1333} \end{vmatrix}=\begin{vmatrix} 5 & 3 & 0 \\ 2 & 7 & 1 \\ 0 & 4 & 8 \end{vmatrix},$$

$$F_{14}=F_{DTKL}=\left\|f_{14sq}\right\|=\begin{vmatrix} f_{1411} & f_{1412} & f_{1413} \\ f_{1421} & f_{1422} & f_{1423} \\ f_{1431} & f_{1432} & f_{1433} \end{vmatrix}=\begin{vmatrix} 6 & 1 & 0 \\ 1 & 5 & 2 \\ 0 & 1 & 3 \end{vmatrix},$$

and

$$F_{15}=F_{DTKS}=\left\|f_{15sq}\right\|=\begin{vmatrix} f_{1511} & f_{1512} & f_{1513} \\ f_{1521} & f_{1522} & f_{1523} \\ f_{1531} & f_{1532} & f_{1533} \end{vmatrix}=\begin{vmatrix} 7 & 1 & 0 \\ 1 & 6 & 2 \\ 0 & 1 & 8 \end{vmatrix}.$$

Further, the second, to form the derivative of the frequency matrix, at $n=1$, $m_1=5$, we construct from the corresponding columns of matrices F_{DTKIC}, F_{DTKUS}, F_{DTKDC}, F_{DTKL} and F_{DTKS} taking into account expression (15) in [31, 32], the vectors of the sums

$$VS_{DTKIC}=\left\|vs_{DTKICq}\right\|=$$
$$=\left\|vs_{DTKIC1},vs_{DTKIC2},vs_{DTKIC3}\right\|=\ \left(q=\overline{1,3}\right),$$
$$=\left\|\bigcup_{q=1}^{3}\sum_{s=1}^{3}f_{DTKICsq}\right\|=\|6,9,4\|,$$

$$VS_{DTKUS}=\left\|vs_{DTKUSq}\right\|=$$
$$=\left\|vs_{DTKUS1},vs_{DTKUS2},vs_{DTKUS3}\right\|=\ \left(q=\overline{1,3}\right),$$
$$=\left\|\bigcup_{q=1}^{3}\sum_{s=1}^{3}f_{DTKUSsq}\right\|=\|6,5,5\|,$$

$$VS_{DTKDC}=\left\|vs_{DTKDCq}\right\|=$$
$$=\left\|vs_{DTKDC1},vs_{DTKDC2},vs_{DTKDC3}\right\|=\ \left(q=\overline{1,3}\right),$$
$$=\left\|\bigcup_{q=1}^{3}\sum_{s=1}^{3}f_{DTKDCsq}\right\|=\|7,14,9\|,$$

$$VS_{DTKL}=\left\|vs_{DTKLq}\right\|=$$
$$=\left\|vs_{DTKL1},vs_{DTKL2},vs_{DTKL3}\right\|=\ \left(q=\overline{1,3}\right),$$
$$=\left\|\bigcup_{q=1}^{3}\sum_{s=1}^{3}f_{DTKLsq}\right\|=\|7,7,5\|,$$

and

$$VS_{DTKS}=\left\|vs_{DTKSq}\right\|=$$
$$=\left\|vs_{DTKS1},vs_{DTKS2},vs_{DTKS3}\right\|=\ \left(q=\overline{1,3}\right).$$
$$=\left\|\bigcup_{q=1}^{3}\sum_{s=1}^{3}f_{DTKSsq}\right\|=\|8,8,10\|,$$

Then, taking into account (16) in [31, 32] from VS_{DTKIC}, VS_{DTKUS}, VS_{DTKDC}, VS_{DTKL} и VS_{DTKS}, we define the maximum element

$$vsm_{DTKIC}=\bigvee_{q=1}^{3}vs_{DTKICq}=$$
$$=vs_{DTKIC1}\vee vs_{DTKIC2}\vee vs_{DTKIC3}=$$
$$=6\vee 9\vee 4=vsm_{DTKIC}=9,$$

$$vsm_{DTKUS}=\bigvee_{q=1}^{3}vs_{DTKUSq}=$$
$$=vs_{DTKUS1}\vee vs_{DTKUS2}\vee vs_{DTKUS3}=$$
$$=6\vee 5\vee 5=vsm_{DTKUS}=6,$$

$$vsm_{DTKDC}=\bigvee_{q=1}^{3}vs_{DTKDCq}=$$
$$=vs_{DTKDC1}\vee vs_{DTKDC2}\vee vs_{DTKDC3}=$$
$$=7\vee 14\vee 9=vsm_{DTKDC}=14,$$

$$vsm_{DTKL}=\bigvee_{q=1}^{3}vs_{DTKLq}=$$
$$=vs_{DTKL1}\vee vs_{DTKL2}\vee vs_{DTKL3}=$$
$$=7\vee 7\vee 5=vsm_{DTKL}=7,$$

and

$$vsm_{DTKS} = \bigvee_{q=1}^{3} vs_{DTKSq} =$$
$$= vs_{DTKS1} \vee vs_{DTKS2} \vee vs_{DTKS3} =$$
$$= 8 \vee 8 \vee 10 = vsm_{DTKS} = 10,$$

and according to (17) in [31, 32], we obtain the derived frequency matrix,

$$F'_{DTKIC} = \left(vsm_{DTKIC} \,/\, vsm_{DTKICq}\right) F_{DTKIC} =$$
$$= \begin{Vmatrix} 3.33 & 2 & 0 \\ 0.67 & 6 & 0 \\ 0 & 1 & 1.78 \end{Vmatrix},$$

$$F'_{DTKUS} = \left(vsm_{DTKUS} \,/\, vsm_{DTKUSq}\right) F_{DTKUS} =$$
$$= \begin{Vmatrix} 4 & 0.83 & 0 \\ 2 & 2.5 & 0.83 \\ 0 & 0.83 & 3.33 \end{Vmatrix},$$

$$F'_{DTKDC} = \left(vsm_{DTKDC} \,/\, vsm_{DTKDCq}\right) F_{DTKDC} =$$
$$= \begin{Vmatrix} 2.5 & 3 & 0 \\ 1 & 7 & 0.64 \\ 0 & 4 & 5.14 \end{Vmatrix},$$

$$F'_{DTKL} = \left(vsm_{DTKL} \,/\, vsm_{DTKLq}\right) F_{DTKL} =$$
$$= \begin{Vmatrix} 6 & 1 & 0 \\ 1 & 5 & 1.43 \\ 0 & 1 & 2.14 \end{Vmatrix},$$

$$F'_{DTKS} = \left(vsm_{DTKS} \,/\, vsm_{DTKSq}\right) F_{DTKS} =$$
$$= \begin{Vmatrix} 5.6 & 0,8 & 0 \\ 0.8 & 4.8 & 2 \\ 0 & 0.8 & 8 \end{Vmatrix}.$$

At this stage, the base and derived frequency matrices are formed, which will make it possible to create fuzzy terms and reference FN, as well as to visualize them.

6. Discussion of the results of studying the process of constructing fuzzy terms and reference FN

Based on the analysis, a set of characteristics have been formed, which can be used to evaluate various Honeypot systems. For this, a method has been developed that, based on the stages of forming the Honeypot sets (expression (2) of stage 1), subsets of their characteristics (expression (3) of stage 2) and identifier values of linguistic estimates of such characteristics (expression (5) of stage 3), as well as the base and derived frequency matrix (taking into account the data of Tables 2–6 of stage 4) allows constructing the corresponding standards of linguistic variables for the generated characteristics that determine the properties of online traps.

At stage 5, a number of subsets of fuzzy terms T_{DTKIC}, T_{DTKUS}, T_{DTKDC}, T_{DTKL}, T_{DTKS}, vectors of maxima FM_{DTKIC}, FM_{DTKUS}, FM_{DTKDC}, FM_{DTKL}, FM_{DTKS} and matrices of membership functions M_{DTKIC}, M_{DTKUS}, M_{DTKDC}, M_{DTKL}, M_{DTKS} are formed. Using matrices, reference FNs were obtained T^e_{DTKIC}, T^e_{DTKUS}, T^e_{DTKDC}, T^e_{DTKL}, T^e_{DTKS} and the reference values are formed on their basis, which allow visualizing the corresponding reference FN. The construction of a graphical model of reference FNs (Fig. 2–6) was carried out using Microsoft Excel 2016 tools for Windows 10. The following symbols are used in the figures: μ^e_{sq} $\left(\mu^e_{sq} = \overline{0,1}\right)$ – reference FN membership function, tabulated with a step 0,1, x^e_{sq} $\left(x^e_{sq} = \overline{0,1}\right)$ – membership function value calculated to the third decimal place.

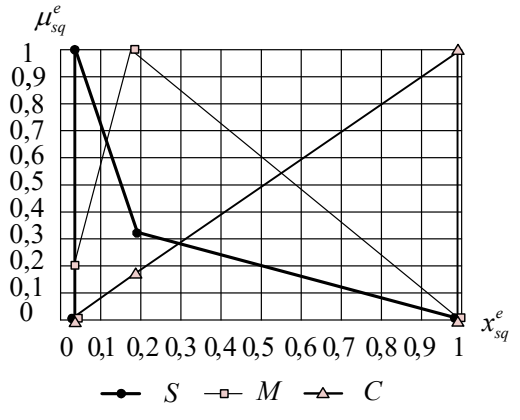

Fig. 2. Linguistic standards for T^e_{DTKIC}

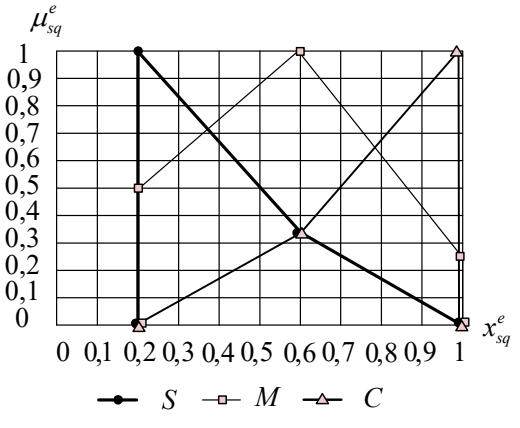

Fig. 3. Linguistic standards for T^e_{DTKUS}

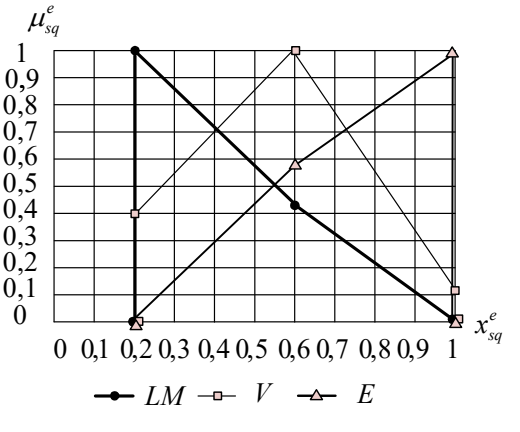

Fig. 4. Linguistic standards for T^e_{DTKDC}

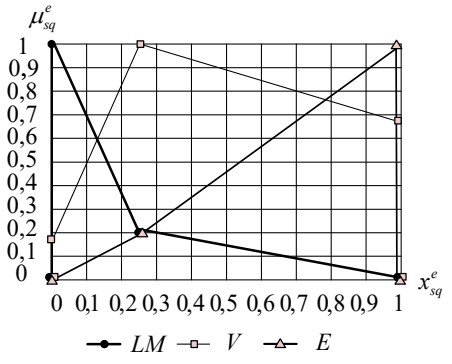

Fig. 5. Linguistic standards for T^e_{DTKL}

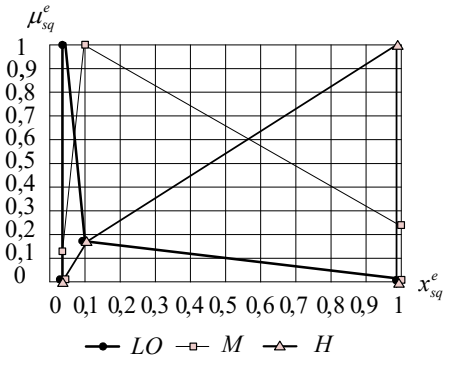

Fig. 6. Linguistic standards for T^e_{DTKS}

Thus, the proposed method, in contrast to the well-known methods for constructing standards of parameters [1, 29, 30], cannot be used, for example, to implement risk assessment or identify cyber attacks, but provides new opportunities for evaluating online traps based on the frequency of expert judgments (expert assessment) relative to the formed new set of values. This allows expanding the existing capabilities of the mathematical apparatus of the theory of fuzzy sets, allowing to form standards of linguistic variables, which can later be used to classify, evaluate and select the most effective Honeypots used to solve the set information security problems.

7. Conclusions

1. Based on the analysis, a set of characteristics (installation and configuration process, usage and support process, data collection, logging level, simulation level, interaction level), as well as Honeypot systems were formed, characterized by a set of criteria for which, by creating an appropriate method, new linguistic standards can be built used to evaluate and select online traps.

2. A method has been developed for constructing linguistic standards for multicriteria estimation of Honeypot efficiency by means of forming a set of Honeypots, subsets of Honeypot characteristics, subsets of identifier values for linguistic estimates of Honeypot characteristics, base and derived frequency matrix, fuzzy terms and reference FNs, as well as visualization of reference FNs. This provides a new opportunity for evaluating online traps based on the frequency of expert judgments (expert assessment) regarding the generated new set of values. The generated standards of linguistic variables can then be used to classify, evaluate and select the most effective Honeypots used to solve the assigned information security problems.

Acknowledgments

The paper was prepared using the results of research carried out by the Scientific School of Cybersecurity of the National Aviation University at the Department of Information Technology Security (Kyiv, Ukraine).

References

1. Korchenko, A. (2019). Metody identyfikatsii anomalnykh staniv dlia system vyiavlennia vtorhnen. Kyiv, 361.
2. Stoll, C. (1990). Cuckoo's Egg. NY: Pocket, 356.
3. Cheswick, B. (1995). An Evening with Berferd In Which a Cracker is Lured, Endured, and Studied. NY: Management Analytics and Others, 147.
4. Spitzner, L. (2002). Honeypots: Tracking Hackers. NY: Addison-Wesley Professional, 480.
5. Provos, N., Holz, T. (2007). Virtual Honeypots: From Botnet Tracking to Intrusion Detection. NY: Addison-Wesley Professional, 440.
6. Honeynet Project. Blog. Available at: http://www.honeynet.org
7. Cohen, F., Lambert, D., Preston, C., Berry, N., Stewart, C., Thomas, E. (2001). A Framework for Deception. Tech. Report.
8. Balas, E., Viecco, C. (2005). Towards a third generation data capture architecture for honeynets. Proceedings from the Sixth Annual IEEE Systems, Man and Cybernetics (SMC) Information Assurance Workshop, 2005. doi: https://doi.org/10.1109/iaw.2005.1495929
9. Roesch, M. (1999). Snort – lightweight intrusion detection for networks. Proceedings of LISA '99: 13th Systems Administration Conference, 229–238.
10. LaBrea: «Sticky» Honeypot and IDS. Available at: http://labrea.sourceforge.net
11. Hammer, R. (2006). Enhancing IDS using, Tiny Honeypot. SANS Institute.
12. The Deception Toolkit Home Page and Mailing List. The Deception Toolkit. Available at: http://www.all.net/dtk/dtk.html
13. Baykara, M., Daş, R. (2015). A Survey on Potential Applications of Honeypot Technology in Intrusion Detection Systems. International Journal of Computer Networks and Applications (IJCNA), 2 (5), 203–211.
14. Thakar, U., Varma, S., Ramani, A. (2005). HoneyAnalyzer – Analysis and Extraction of Intrusion Detection Patterns & Signatures Using Honeypot. The Second International Conference on Innovations in Information Technology (IIT'05). – Indore: Institute of Technology and Science.

15. Hnatiuk, S., Volianska, V., Karpenko, S. (2012). Modern virtual decoy systems based on honeypot technology. Ukrainian Information Security Research Journal, 14 (3 (56)), 107–115. doi: https://doi.org/10.18372/2410-7840.14.3398
16. Jia, Z., Cui, X., Liu, Q., Wang, X., Liu, C. (2018). Micro-Honeypot: Using Browser Fingerprinting to Track Attackers. 2018 IEEE Third International Conference on Data Science in Cyberspace (DSC), 197–204. doi: http://doi.org/10.1109/DSC.2018.00036
17. Park, J.-H., Choi, J.-W., Song, J.-S. (2016). How to Design Practical Client Honeypots Based on Virtual Environment. 2016 11th Asia Joint Conference on Information Security (AsiaJCIS), 67–73. doi: http://doi.org/10.1109/AsiaJCIS.2016.19
18. Almohannadi, H., Awan, I., Hamar, J. A., Cullen, A., Disso, J. P., Armitage, L. (2018). Cyber Threat Intelligence from Honeypot Data Using Elasticsearch. 2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA), 900–906. doi: http://doi.org/10.1109/AINA.2018.00132
19. Fraunholz, D., Zimmermann, M., Hafner, A., Schotten, H. D. (2017). Data Mining in Long-Term Honeypot Data. 2017 IEEE International Conference on Data Mining Workshops (ICDMW), 649–656. doi: http://doi.org/10.1109/ICDMW.2017.92
20. Moore, C. (2016). Detecting Ransomware with Honeypot Techniques. 2016 Cybersecurity and Cyberforensics Conference (CCC), 77–81. doi: http://doi.org/10.1109/CCC.2016.14
21. Bombardieri, M., Castano, S., Curcio, F., Furfaro, A., Karatza, H. D. (2016). Honeypot-Powered Malware Reverse Engineering. 2016 IEEE International Conference on Cloud Engineering Workshop (IC2EW), 65–69. doi: http://doi.org/10.1109/IC2EW.2016.16
22. Lin, Y.-D., Lee, C.-Y., Wu, Y.-S., Ho, P.-H., Wang, F.-Y., Tsai, Y.-L. (2014). Active versus Passive Malware Collection. Computer, 47 (4), 59–65. doi: http://doi.org/10.1109/MC.2013.226
23. Henderson, B., Mckenna, S., Rowe, N. (2018). Web Honeypots for Spies. 2018 International Conference on Computational Science and Computational Intelligence (CSCI), 1–6. doi: http://doi.org/10.1109/CSCI46756.2018.00009
24. Kishimoto, K., Ohira, K., Yamaguchi, Y., Yamaki, H., Takakura, H. (2012). An Adaptive Honeypot System to Capture IPv6 Address Scans. 2012 International Conference on Cyber Security. doi: https://doi.org/10.1109/cybersecurity.2012.28
25. Hecker, C., Hay, B. (2013). Automated Honeynet Deployment for Dynamic Network Environment. 2013 46th Hawaii International Conference on System Sciences. doi: https://doi.org/10.1109/hicss.2013.110
26. Tehnologiya Honeypot. Chast' 2: Klassifikatsiya Honeypot. Available at: https://www.securitylab.ru/analytics/275775.php
27. Honeypots primanka na hakera. Available at: https://docplayer.ru/54222428-Honeypots-primanka-na-hakera.html
28. Kotenko, I. V., Stepashkin, M. V. (2014). Deception systems for protection of information resources in computer networks. SPIIRAS Proceedings, 1 (2), 211. doi: https://doi.org/10.15622/sp.2.16
29. Korchenko, O. H., Kazmirchuk, S. V., Akhmetov, B. B. (2017). Prykladni systemy otsiniuvannia ryzykiv informatsiynoi bezpeky. Kyiv, 435.
30. Korchenko, A. G. (2006). The development of information protection systems based on the fuzzy sets. The theory and practical solutions. Kyiv, 320.
31. Korchenko, A. A. (2014). Metod formirovaniya lingvisticheskih etalonov dlya sistem vyyavleniya vtorzheniy. Zakhyst informatsiyi, 16 (1), 5–12.
32. Akhmetov, B., Korchenko, A., Akhmetova, S., Zhumangalieva, N. (2016). Improved method for the formation of linguistic standards for of intrusion detection systems. Journal of Theoretical and Applied Information Technology, 87 (2), 221–232.
33. Zhumangaliyeva, N., Doszhanova, A., Korchenko, A., Kazmirchuk, S., Avkurova, Z., Zhaxygulova, D. (2020). Method of linguistic variable standards formation for honeypot classification. Bulletin of national academy of sciences of the republic of Kazakhstan, 5 (387), 16–24. doi: https://doi.org/10.32014/2020.2518-1467.138
34. Zhumangaliyeva, N., Korchenko, A., Doszhanova, A., Shaikhanova, A., Zhadyra, S. G. A. (2019). Detection environment formation method for anomaly detection systems. Journal of Theoretical and Applied Information Technology, 97 (16), 4239–4250.
35. Karpinski, M., Korchenko, A., Vikulov, P., Kochan, R., Balyk, A., Kozak, R. (2017). The etalon models of linguistic variables for sniffing-attack detection. 2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS). doi: https://doi.org/10.1109/idaacs.2017.8095087
36. Korchenko, A., Warwas, K., Klos-Witkowska, A. (2015). The tupel model of basic components' set formation for cyberattacks. 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS). doi: https://doi.org/10.1109/idaacs.2015.7340782