BULLETIN OF NATIONAL ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN
ISSN 1991-3494
Volume 5, Number 387 (2020), 16 – 24 **https://doi.org/10.32014/2020.2518-1467.138**

UDC 621.39:004.05
IRSTI 81.93.29

Nazym Zhumangaliyeva[1], Aliya Doszhanova[2], Anna Korchenko[3], Svitlana Kazmirchuk[3], Zhadyra Avkurova[4], Dauriya Zhaxygulova[5]

[1]Satbayev University, Almaty, Kazakhstan;
[2]Almaty University of Power Engineering and Telecommunications, Kazakhstan;
[3]Department of Information Technology Security, National Aviation, Kiev, Ukraine;
[4]L. N. Gumilyov Eurasian National University, Nur-Sultan, Kazakhstan;
[5]Shakarim State University of Semey, Kazakhstan.
E-mail: nazym_k.81@mail.ru, d_alia.81@mail.ru, annakor@ukr.net,
sv.kazmirchuk@gmail.com, zhadyra.avkurova.83@mail.ru, daurija_zd@mail.ru

METHOD OF LINGUISTIC VARIABLE STANDARDS FORMATION FOR HONEYPOT CLASSIFICATION

Abstract. Nowadays, one of the relevant areas that is developing in the field of information security is associated with the use of Honeypot (virtual lures, online traps), and the selection of criteria for determination of the most effective Honeypot and their further classification is an urgent task. There are presented the main products in which virtual lures technology is implemented. Often they are used to study the behavior, approaches and methods that an unauthorized party uses for unauthorized access to information system resources. Online traps can imitate any resource, but more often they look like real production servers and workstations. There are known a number of fairly effective developments that are used to solve the problems of identifying attacks on the information systems resources, which are based on the fuzzy sets apparatus. They showed the effectiveness of using the appropriate mathematical apparatus, the use of which, for example, to formalize the approach for the formation of a set of criteria, will improve the process of determining the most effective Honeypot. For this purpose, there have been proposed criteria that characterize online traps, with the use of which there has been developed a method of linguistic variable standards formation for choosing the most effective Honeypot. The method is based on the formation of a set of Honeypot, subsets of characteristics and identifier values of linguistic estimates of Honeypot characteristics, a base and derivative frequency matrix, as well as on the construction of fuzzy terms and standard fuzzy numbers with their visualization. This will allow further classification and selection of them osteffective virtual lures.

Key words: honeypot classification, online traps classification, virtual lures, fuzzy standards, linguistic standards formation method, intrusion detection systems.

The rapid development of information systems (IS) and technologies affects all areas of society. A significant number of modern public and private enterprises use IS to manage production processes, to support decision making, to find the necessary data, and etc. Along with this, there is increasing the amount of IS vulnerabilities and threats, and therefore, there is a need in specialized security tools to ensure their normal operation and to prevent intrusions. It should be noted that one of the current areas that is actively developing in the field of information security is associated with the use of Honeypot (virtual lures, online traps). The purpose of the operation of such lures is to be attacked or scanned by an unauthorized party (UNP) in order to study the protection strategy, to determine the range of their means by which attacks on real security objects can be conducted. Honeypot and methods used to their implementation are different, for example, it is a specially developed integrated network or one single emulated network service, the main task of which is to attract UNP attention [1]. Therefore, the selection of criteria for determining the most effective Honeypot and their further classification is an urgent task.

$$VS_{DTKИ} = \left\| vs_{DTKИq} \right\| = \left\| vs_{DTKИ1}, vs_{DTKИ2}, vs_{DTKИ3} \right\| = \left\| \bigcup_{q=1}^{3} \sum_{s=1}^{3} f_{DTKИsq} \right\| = \left\| 8,8,10 \right\|, (q = \overline{1,3}).$$

Then, taking into account (16) in [21,22] from $VS_{DTKУН}, VS_{DTKИП}, VS_{DTKСД}, VS_{DTKП}$, and $VS_{DTKИ}$ define the maximum element $vsm_{DTKУН} = \bigvee_{q=1}^{3} vs_{DTKУНq} = vs_{DTKУН1} \vee vs_{DTKУН2} \vee$ $vs_{DTKУН3} = 6 \vee 9 \vee 4 = vsm_{DTKУН} = 9,\ vsm_{DTKИП} = \bigvee_{q=1}^{3} vs_{DTKИПq} = vs_{DTKИП1} \vee vs_{DTKИП2} \vee$ $vs_{DTKИП3} = 6 \vee 5 \vee 5 = vsm_{DTKИП} = 6,\ vsm_{DTKСД} = \bigvee_{q=1}^{3} vs_{DTKСДq} = vs_{DTKСД1} \vee vs_{DTKСД2} \vee$ $vs_{DTKСД3} = 7 \vee 14 \vee 9 = vsm_{DTKСД} = 14,\ vsm_{DTKП} = \bigvee_{q=1}^{3} vs_{DTKПq} = vs_{DTKП1} \vee vs_{DTKП2} \vee$ $vs_{DTKП3} = 7 \vee 7 \vee 5 = vsm_{DTKП} = 7$ and $vsm_{DTKИ} = \bigvee_{q=1}^{3} vs_{DTKИq} = vs_{DTKИ1} \vee vs_{DTKИ2} \vee$ $vs_{DTKИ3} = 8 \vee 8 \vee 10 = vsm_{DTKИ} = 10.$ and according to (17) in [21,22] we obtain a derivative frequency

matrix, $F'_{DTKУН} = (vsm_{DTKУН} / vsm_{DTKУНq}) F_{DTKУН} = \begin{Vmatrix} 3,33 & 2 & 0 \\ 0,67 & 6 & 0 \\ 0 & 1 & 1,78 \end{Vmatrix}$,

$$F'_{DTKИП} = (vsm_{DTKИП} / vsm_{DTKИПq}) F_{DTKИП} = \begin{Vmatrix} 4 & 0,83 & 0 \\ 2 & 2,5 & 0,83 \\ 0 & 0,83 & 3,33 \end{Vmatrix},$$

$$F'_{DTKСД} = (vsm_{DTKСД} / vsm_{DTKСДq}) F_{DTKСД} =$$

$$\begin{Vmatrix} 2,5 & 3 & 0 \\ 1 & 7 & 0,64 \\ 0 & 4 & 5,14 \end{Vmatrix},\ F'_{DTKП} = (vsm_{DTKП} / vsm_{DTKПq}) F_{DTKП} = \begin{Vmatrix} 6 & 1 & 0 \\ 1 & 5 & 1,43 \\ 0 & 1 & 2,14 \end{Vmatrix},$$

$$F'_{DTKИ} = (vsm_{DTKИ} / vsm_{DTKИq}) F_{DTKИ} = \begin{Vmatrix} 5,6 & 0,8 & 0 \\ 0,8 & 4,8 & 2 \\ 0 & 0,8 & 8 \end{Vmatrix}.$$

The creation of fuzzy terms and standard FN. Stage 5–the creation of fuzzy terms and standard FN.Firslty, according to (22) in [21,22] let form the subset of fuzzy terms $\mathbf{T_{DTKУН}}$, $\mathbf{T_{DTKИП}}$, $\mathbf{T_{DTKСД}}$, $\mathbf{T_{DTKП}}$, $\mathbf{T_{DTKИ}}$ if $n = 1$ (i.e. for Honeypotwith ID $H_{DTK} = DTK$), $m_1 = 5$, $r_1 = r_2 = r_3 = r_4 = r_5 = 3$.

$$\{\bigcup_{i=1}^{1} \mathbf{T_i}\} = \{\bigcup_{i=1}^{n} \{\bigcup_{j=1}^{m_i} \mathbf{T_{ij}}\}\} = \{\bigcup_{i=1}^{n} \{\bigcup_{j=1}^{m_i} \{\bigcup_{s=1}^{r_j} \underset{\sim}{T}_{ijs}\}\}\} = \{\{\underset{\sim}{T}_{DTKУН1}, \underset{\sim}{T}_{DTKУН2}, \underset{\sim}{T}_{DTKУН3}\},\ \{\underset{\sim}{T}_{DTKИП1}, \underset{\sim}{T}_{DTKИП2}, \underset{\sim}{T}_{DTKИП3}\},$$

$$\{\underset{\sim}{T}_{DTKСД1}, \underset{\sim}{T}_{DTKСД2}, \underset{\sim}{T}_{DTKСД3}\}, \{\underset{\sim}{T}_{DTKП1}, \underset{\sim}{T}_{DTKП2}, \underset{\sim}{T}_{DTKП3}\}, \{\underset{\sim}{T}_{DTKИ1}, \underset{\sim}{T}_{DTKИ2}, \underset{\sim}{T}_{DTKИ3}\}\} =$$

$$\{\{\underset{\sim}{ПР}_{DTKУН}, \underset{\sim}{СР}_{DTKУН}, \underset{\sim}{СЛ}_{DTKУН}\},\ \{\underset{\sim}{ПР}_{DTKИП}, \underset{\sim}{СР}_{DTKИП}, \underset{\sim}{СЛ}_{DTKИП}\},\ \{\underset{\sim}{ОГ}_{DTKСД}, \underset{\sim}{ПМ}_{DTKСД}, \underset{\sim}{РР}_{DTKСД}\},$$

$\{\underset{\sim}{ОГ}_{DTKП}, \underset{\sim}{ПМ}_{DTKП}, \underset{\sim}{РР}_{DTKП}\},\ \{\underset{\sim}{Н}_{DTKИ}, \underset{\sim}{СР}_{DTKИ}, \underset{\sim}{В}_{DTKИ}\}\}$.According to (23) in [21], [22] on corresponding lines of $F'_{DTKУН}$, $F'_{DTKИП}$, $F'_{DTKСД}$, $F'_{DTKП}$ and $F'_{DTKИ}$ let create construct the vectors of maximum i.e.

$$FM_{DTKУН} = \|fm_{DTKУНs}\| = \|fm_{DTKУН1}, fm_{DTKУН2}, fm_{DTKУН3}\| = \|3,33; 6; 1,78\|,\ FM_{DTKИП} = \|fm_{DTKИПs}\| =$$

$$\|fm_{DTKИП1}, fm_{DTKИП2}, fm_{DTKИП3}\| = \|4; 2,5; 3,33\|,\ FM_{DTKСД} = \|fm_{DTKСДs}\| =$$

$$\|fm_{DTKСД1}, fm_{DTKСД2}, fm_{DTKСД3}\| = \|2,5; 7; 5,14\|,\ FM_{DTKП} = \|fm_{DTKПs}\| =$$

$$\|fm_{DTKП1}, fm_{DTKП2}, fm_{DTKП3}\| = \|6; 5; 2,14\|,\ FM_{DTKИ} = \|fm_{DTKИs}\| =$$

$$\|fm_{DTKИ1}, fm_{DTKИ2}, fm_{DTKИ3}\| = \|5,6; 4,8; 8\|.$$

On the basis of $FM_{DTKУН}, FM_{DTKИП}, FM_{DTKСД}, FM_{DTKП}$ and $FM_{DTKИ}$ according to the expression (24) in [21,22] let form matrices of membership function:

$$M_{DTKУН} = \left\| \mu_{DTKУНsq} \right\| = \left\| \begin{matrix} 1 & 0,33 & 0 \\ 0,2 & 1 & 0 \\ 0 & 0,17 & 1 \end{matrix} \right\|,$$

$$M_{DTKИП} = \left\| \mu_{DTKИПsq} \right\| = \left\| \begin{matrix} 1 & 0,33 & 0 \\ 0,5 & 1 & 0,25 \\ 0 & 0,33 & 1 \end{matrix} \right\|, \; M_{DTKСД} = \left\| \mu_{DTKСДsq} \right\| = \left\| \begin{matrix} 1 & 0,43 & 0 \\ 0,4 & 1 & 0,12 \\ 0 & 0,57 & 1 \end{matrix} \right\|,$$

$$M_{DTKП} = \left\| \mu_{DTKПsq} \right\| = \left\| \begin{matrix} 1 & 0,2 & 0 \\ 0,17 & 1 & 0,67 \\ 0 & 0,2 & 1 \end{matrix} \right\|, \; M_{DTKИ} = \left\| \mu_{DTKИsq} \right\| = \left\| \begin{matrix} 1 & 0,17 & 0 \\ 0,14 & 1 & 0,25 \\ 0 & 0,17 & 1 \end{matrix} \right\|,$$

where $\mu_{DTKУНsq} = f'_{DTKУНsq} / fm_{DTKУНs}$, $(s,q = \overline{1,3})$, $\mu_{DTKИПsq} = f'_{DTKИПsq} / fm_{DTKИПs}$, $(s,q = \overline{1,3})$, $\mu_{DTKСДsq} = f'_{DTKСДsq} / fm_{DTKСДs}$, $(s,q = \overline{1,3})$, $\mu_{DTKПsq} = f'_{DTKПsq} / fm_{DTKПs}$, $(s,q = \overline{1,3})$, $\mu_{DTKИsq} = f'_{DTKИsq} / fm_{DTKИs}$, $(s,q = \overline{1,3})$.

According to the obtained data, $\mu_{DTKУНsq}, \mu_{DTKИПsq}, \mu_{DTKСДsq}, \mu_{DTKПsq}, \mu_{DTKИsq}$ and calculated by the expression (26) in [21,22] $x_{DTKУНsq}, x_{DTKИПsq}, x_{DTKСДsq}, x_{DTKПsq}, x_{DTKИsq}$ let define sets of fuzzy terms according to (25) in [21,22] $\underset{\sim}{T}_{DTKУНs} = \{ \mu_{DTKУНs1} / x_{DTKУНs1}, \mu_{DTKУНs2} / x_{DTKУНs2}, \mu_{DTKУНs3} / x_{DTKУНs3} \}$, $(s,q = \overline{1,3})$, where according to (26) in [21,22] $X_{DTKУНsq} = N^{max}_{DTKУНq} / N^{max}_{DTKУНr}$, $(q = \overline{1,3})$ or $\{\bigcup_{q=1}^{3} X_{DTKУНsq}\} = \{0,03;0,19;1\}$, $\underset{\sim}{T}_{DTKИПs} = \{\mu_{DTKИПs1} / x_{DTKИПs1}, \mu_{DTKИПs2} / x_{DTKИПs2}, \mu_{DTKИПs3} / x_{DTKИПs3}\}$, $(s,q = \overline{1,3})$, where according to (26) in [21,22] $X_{DTKИПsq} = N^{max}_{DTKИПq} / N^{max}_{DTKИПr}$, $(q = \overline{1,3})$ or $\{\bigcup_{q=1}^{3} X_{DTKИПsq}\} = \{0,2;0,6;1\}$, $\underset{\sim}{T}_{DTKСДs} = \{ \mu_{DTKСДs1} / x_{DTKСДs1}, \mu_{DTKСДs2} / x_{DTKСДs2}, \mu_{DTKСДs3} / x_{DTKСДs3} \}$, $(s,q = \overline{1,3})$, where according to (26) in [21,22] $X_{DTKСДsq} = N^{max}_{DTKСДq} / N^{max}_{DTKСДr}$, $(q = \overline{1,3})$ or $\{\bigcup_{q=1}^{3} X_{DTKСДsq}\} = \{0,2;0,6;1\}$, $\underset{\sim}{T}_{DTKПs} = \{ \mu_{DTKПs1} / x_{DTKПs1}, \mu_{DTKПs2} / x_{DTKПs2}, \mu_{DTKПs3} / x_{DTKПs3} \}$, $(s,q = \overline{1,3})$, where according to (26) in [21,22] $X_{DTKПsq} = N^{max}_{DTKПq} / N^{max}_{DTKПr}$, $(q = \overline{1,3})$ or $\{\bigcup_{q=1}^{3} X_{DTKПsq}\} = \{0,006;0,25;1\}$, $\underset{\sim}{T}_{DTKИs} = \{ \mu_{DTKИs1} / x_{DTKИs1}, \mu_{DTKИs2} / x_{DTKИs2}, \mu_{DTKИs3} / x_{DTKИs3} \}$, $(s,q = \overline{1,3})$, where according to (26) in [21,22] $X_{DTKИsq} = N^{max}_{DTKИq} / N^{max}_{DTKИr}$, $(q = \overline{1,3})$ or $\{\bigcup_{q=1}^{3} X_{DTKИsq}\} = \{0,05;0,1;1\}$.

Therefore, the resulting members of the subset $\mathbf{T_{DTKУН}}, \mathbf{T_{DTKИП}}, \mathbf{T_{DTKСД}}, \mathbf{T_{DTKП}}, \mathbf{T_{DTKИ}}$ (numerical form), respectively, are the reflection of the members of the subset $\mathbf{LE_{DTKУН}}, \mathbf{LE_{DTKИП}}, \mathbf{LE_{DTKСД}}, \mathbf{LE_{DTKП}}, \mathbf{LE_{DTKИ}}$ (linguistic form) and are presented in the following form:

$\underset{\sim}{T}_{DTKУН1} = \underset{\sim}{ПР}_{DTKУН1} = \{1/0,03; 0,33/0,19; 0/1\}$; $\underset{\sim}{T}_{DTKУН2} = \underset{\sim}{СР}_{DTKУН2} = \{0,2/0,03; 1/0,19; 0/1\}$;

$\underset{\sim}{T}_{DTKУН3} = \underset{\sim}{СЛ}_{DTKУН3} = \{0/0,03; 0,17/0,19; 1/1\}$, $\underset{\sim}{T}_{DTKИП1} = \underset{\sim}{ПР}_{DTKИП1} = \{1/0,2; 0,33/0,6; 0/1\}$;

$\underset{\sim}{T}_{DTKИП2} = \underset{\sim}{CP}_{DTKИП2} = \{0,5/0,2; 1/0,6; 0,25/1\}$; $\underset{\sim}{T}_{DTKИП3} = \underset{\sim}{CЛ}_{DTKИП3} = \{0/0,2; 0,33/0,6; 1/1\}$,
$\underset{\sim}{T}_{DTKCД1} = \underset{\sim}{OГ}_{DTKCД1} = \{1/0,2; 0,43/0,6; 0/1\}$; $\underset{\sim}{T}_{DTKCД2} = \underset{\sim}{ПМ}_{DTKCД2} = \{0,4/0,2; 1/0,6; 0,12/1\}$;
$\underset{\sim}{T}_{DTKCД3} = \underset{\sim}{PP}_{DTKCД3} = \{0/0,2; 0,57/0,6; 1/1\}$, $\underset{\sim}{T}_{DTKП1} = \underset{\sim}{OГ}_{DTKП1} = \{1/0,006; 0,2/0,25; 0/1\}$;
$\underset{\sim}{T}_{DTKП2} = \underset{\sim}{ПМ}_{DTKП2} = \{0,17/0,006; 1/0,25; 0,67/1\}$; $\underset{\sim}{T}_{DTKП3} = \underset{\sim}{PP}_{DTKП3} = \{0/0,006; 0,2/0,25; 1/1\}$,
$\underset{\sim}{T}_{DTKИ1} = \underset{\sim}{H}_{DTKИ1} = \{1/0,05; 0,17/0,1; 0/1\}$; $\underset{\sim}{T}_{DTKИ2} = \underset{\sim}{CP}_{DTKИ2} = \{0,14/0,05; 1/0,1; 0,25/1\}$;

$$\underset{\sim}{T}_{DTKИ3} = \underset{\sim}{B}_{DTKИ3} = \{0/0,05; 0,17/0,1; 1/1\}.$$

Then, secondly, according to (29) in [21,22] let form standard FN $\mathbf{T^e_{DTKУН}} \subseteq \mathbf{T^e}$, $\mathbf{T^e_{DTKИП}} \subseteq \mathbf{T^e}$, $\mathbf{T^e_{DTKCД}} \subseteq \mathbf{T^e}$, $\mathbf{T^e_{DTKП}} \subseteq \mathbf{T^e}$, $\mathbf{T^e_{DTKИ}} \subseteq \mathbf{T^e}$:

$$\mathbf{T^e_{DTKУН}} = \{\bigcup_{s=1}^{3} \underset{\sim}{T}^e_{DTKУНs}\} = \{\underset{\sim}{T}^e_{DTKУН1}, \underset{\sim}{T}^e_{DTKУН2}, \underset{\sim}{T}^e_{DTKУН3}\} = \{\underset{\sim}{ПP}^e_{DTKУН1}, \underset{\sim}{CP}^e_{DTKУН2}, \underset{\sim}{CЛ}^e_{DTKУН3}\},\ (s = \overline{1,3}),$$

$$\mathbf{T^e_{DTKИП}} = \{\bigcup_{s=1}^{3} \underset{\sim}{T}^e_{DTKИПs}\} = \{\underset{\sim}{T}^e_{DTKИП1}, \underset{\sim}{T}^e_{DTKИП2}, \underset{\sim}{T}^e_{DTKИП3}\} = \{\underset{\sim}{ПP}^e_{DTKИП1}, \underset{\sim}{CP}^e_{DTKИП2}, \underset{\sim}{CЛ}^e_{DTKИП3}\},\ (s = \overline{1,3}),$$

$$\mathbf{T^e_{DTKCД}} = \{\bigcup_{s=1}^{3} \underset{\sim}{T}^e_{DTKCДs}\} = \{\underset{\sim}{T}^e_{DTKCД1}, \underset{\sim}{T}^e_{DTKCД2}, \underset{\sim}{T}^e_{DTKCД3}\} = \{\underset{\sim}{OГ}^e_{DTKCД1}, \underset{\sim}{ПМ}^e_{DTKCД2}, \underset{\sim}{PP}^e_{DTKCД3}\},\ (s = \overline{1,3}),$$

$$\mathbf{T^e_{DTKП}} = \{\bigcup_{s=1}^{3} \underset{\sim}{T}^e_{DTKПs}\} = \{\underset{\sim}{T}^e_{DTKП1}, \underset{\sim}{T}^e_{DTKП2}, \underset{\sim}{T}^e_{DTKП3}\} = \{\underset{\sim}{OГ}^e_{DTKП1}, \underset{\sim}{ПМ}^e_{DTKП2}, \underset{\sim}{PP}^e_{DTKП3}\},\ (s = \overline{1,3}),$$

$$\mathbf{T^e_{DTKИ}} = \{\bigcup_{s=1}^{3} \underset{\sim}{T}^e_{DTKИs}\} = \{\underset{\sim}{T}^e_{DTKИ1}, \underset{\sim}{T}^e_{DTKИ2}, \underset{\sim}{T}^e_{DTKИ3}\} = \{\underset{\sim}{H}^e_{DTKИ1}, \underset{\sim}{CP}^e_{DTKИ2}, \underset{\sim}{B}^e_{DTKИ3}\},\ (s = \overline{1,3}),$$

where: the members of a subset $\mathbf{T^e_{DTKУН}}$ =– $\underset{\sim}{ПP}^e_{DTKУН1}$, $\underset{\sim}{CP}^e_{DTKУН2}$, $\underset{\sim}{CЛ}^e_{DTKУН3}$; $\mathbf{T^e_{DTKИП}}$ – $\underset{\sim}{ПP}^e_{DTKИП1}$, $\underset{\sim}{CP}^e_{DTKИП2}$, $\underset{\sim}{CЛ}^e_{DTKИП3}$; $\mathbf{T^e_{DTKCД}}$ – $\{\underset{\sim}{OГ}^e_{DTKCД1}, \underset{\sim}{ПМ}^e_{DTKCД2}, \underset{\sim}{PP}^e_{DTKCД3}\}$; $\mathbf{T^e_{DTKП}}$ – $\underset{\sim}{OГ}^e_{DTKП1}$, $\underset{\sim}{ПМ}^e_{DTKП2}$, $\underset{\sim}{PP}^e_{DTKП3}$; $\mathbf{T^e_{DTKИ}}$ – $\{\underset{\sim}{H}^e_{DTKИ1}, \underset{\sim}{CP}^e_{DTKИ2}, \underset{\sim}{B}^e_{DTKИ3}\}$ are standard FN. Next, let convert the fuzzy terms $\underset{\sim}{ПP}^e_{DTKУН1}, \underset{\sim}{CP}^e_{DTKУН2}, \underset{\sim}{CЛ}^e_{DTKУН3}$ in such a way, that for all $\underset{\sim}{T}_{DTKУНs}$ the relation order is fair, i.e. $\forall x_{DTKУНsq} : x_{DTKУНsq} < x_{DTKУНsq+1}$, $(q = \overline{1,3})$ (according to the step 1, stage 5 in [21,22]). If we use the specific values obtained in the example above as components of such terms, then for them such relation will be true. So, for example, for $\underset{\sim}{ПP}^e_{DTKУН1}$ it is $x_{DTKУН1} < x_{DTKУН2} < x_{DTKУН3} = 0,03 < 0,19 < 1$. Also, the relation for all other given standard FN will be similarly true.

Further, according to the step 2 of the stage 5 in [21,22] we will carry out the absorption procedure for each $\underset{\sim}{T}_{DTKУНs}$. Since the condition U_1 and U_2 is not satisfied for any of FN, the absorption operation is not carried out. Therefore, the standard FN will remain unchanged, and the formed intermediate terms will have the form: $\underset{\sim}{T}'_{D\ \ У} = \underset{\sim}{T}_{\ \ H} = \underset{\sim}{ПP}_{K} = \{1/0;$ $\underset{\sim}{T}'_{DTKУН2} = \underset{\sim}{T}_{DTKУН2} = \underset{\sim}{CP}_{DTKУН2} = \{0,2/0,03; 1/0,19; 0/1\}$; $\underset{\sim}{T}'_{DTKУН3} = \underset{\sim}{T}_{DTKУН3} = \underset{\sim}{CЛ}_{DTKУН3} = \{0/0,03; 0,17/0,19; 1/1\}$. According to the step 3 of the stage 5 in [21], during the implementation of the second step in the expression (28) for a set of intermediate terms $\underset{\sim}{ПP}^e_{DTKУН1}$ $\exists \underset{\sim}{T}_{DTKУН1} : \{0/x^{min}_{DTKУН1}\} \in \varnothing$ (i.e. $\mu_{DTKУН1} = 1 \neq 0$), and for $\underset{\sim}{CЛ}^e_{DTKУН3}$ $\exists \underset{\sim}{T}_{DTKУН3} : \{0/x^{max}_{DTKУН3}\} \in \varnothing$ (i.e. $\mu_{DTKУН3} = 1 \neq 0$), then the formation of the subsets $\underset{\sim}{T}^e_{DTKУН1}$ and $\underset{\sim}{T}^e_{DTKУН3}$ will be carried out by expanding $\underset{\sim}{T}^e_{DTKУН1}$ and

$\underset{\sim}{T}^{e}_{ДТКУН3}$ (see (28) in [21]) through the introduction of additional $\mu_{ДТКУН1\beta\text{-}1} / x_{ДТКУН1\beta\text{-}1} = 0/0{,}03$, and $\mu_{ДТКУН3r_j\text{-}\gamma+2} / x_{ДТКУН3r_j\text{-}\gamma+2} = 0/1$ respectively, after that in the FN there is carried out rein doxing of the components starting from the first one.With this in mind, a set of intermediate terms for $\underset{\sim}{ПР}^{e}_{ДТКУН1}$ will have the following form $\underset{\sim}{T}'_{ДТКУНs} = \underset{\sim}{ПР}'_{ДТКУН1} = \{\mu_{ДТКУН1} / x_{ДТКУН1}, \mu_{ДТКУН2} / x_{ДТКУН2}, \mu_{ДТКУН3} / x_{ДТКУН3}, \mu_{ДТКУН4} / x_{ДТКУН4}\} = \{0/\ 0{,}03; 1/0{,}03; 0{,}33/0{,}19; 0/1\}$, where $\mu_{ДТКУН1\beta\text{-}1} = 0$. In a simil arway, weobtain intermediate terms for $\underset{\sim}{СР}^{e}_{ДТКИП2}$ and $\underset{\sim}{СЛ}^{e}_{ДТКУН3}$, where $\mu_{ДТКУН2\beta\text{-}1} = \mu_{ДТКУН3r_j\text{-}\gamma+2} = 0$. Thus, the components of the subset of standards $\underset{\sim}{T}^{e}_{ДТКУН1}$ according to (29) in [21] will be defined as $\mu^{e}_{ДТКУН1} / x^{e}_{ДТКУН1} = 0/0{,}03$, $\mu^{e}_{ДТКУН2} / x^{e}_{ДТКУН2} = 1/0{,}03$, $\mu^{e}_{ДТКУН3} / x^{e}_{ДТКУН3} = 0{,}33/0{,}19$, $\mu^{e}_{ДТКУН4} / x^{e}_{ДТКУН4} = 0/1$ and similarly for $\underset{\sim}{T}^{e}_{ДТКУН2}$, $\underset{\sim}{T}^{e}_{ДТКУН3}$.

Then according to (29) in [21] for $\underset{\sim}{ПР}'_{ДТКУН1}, \underset{\sim}{СР}'_{ДТКУН2}, \underset{\sim}{СЛ}'_{ДТКУН3}$ let form the standard values, i.e.:

$\underset{\sim}{T}^{e}_{ДТКУН1} = \underset{\sim}{ПР}^{e}_{ДТКУН1} = \{0/0{,}03; 1/0{,}03; 0{,}33/0{,}19; 0/1\}$; $\underset{\sim}{T}^{e}_{ДТКУН2} = \underset{\sim}{СР}^{e}_{ДТКУН2} = \{0/0{,}03; 0{,}2/0{,}03; 1/0{,}19; 0/1\}$; $\underset{\sim}{T}^{e}_{ДТКУН3} = \underset{\sim}{СЛ}^{e}_{ДТКУН3} = \{0/0{,}03; 0{,}17/0{,}19; 1/1; 0/1\}$.Also, by analogy, the following standard values are formed: $\underset{\sim}{T}^{e}_{ДТКИП1} = \underset{\sim}{ПР}^{e}_{ДТКИП1} = \{0/0{,}2; 1/0{,}2; 0{,}33/0{,}6; 0/1\}$; $\underset{\sim}{T}^{e}_{ДТКИП2} = \underset{\sim}{СР}^{e}_{ДТКИП2} = \{0/0{,}2; 0{,}5/0{,}2; 1/0{,}6; 0{,}25/1; 0/1\}$;

$$\underset{\sim}{T}^{e}_{ДТКИП3} = \underset{\sim}{СЛ}^{e}_{ДТКИП3} = \{0/0{,}2; 0{,}33/0{,}6; 1/1; 0/1\}, \underset{\sim}{T}^{e}_{ДТКСД1} = \underset{\sim}{ОГ}^{e}_{ДТКСД1} =$$

$$\{0/0{,}2; 1/0{,}2; 0{,}43/0{,}6; 0/1\}; \underset{\sim}{T}^{e}_{ДТКСД2} = \underset{\sim}{ПМ}^{e}_{ДТКСД2} = \{0/0{,}2; 0{,}4/0{,}2; 1/0{,}6; 0{,}12/1; 0/1\};$$

$$\underset{\sim}{T}^{e}_{ДТКСД3} = \underset{\sim}{РР}^{e}_{ДТКСД3} = \{0/0{,}2; 0{,}57/0{,}6; 1/1; 0/1\}, \underset{\sim}{T}^{e}_{ДТКП1} = \underset{\sim}{ОГ}^{e}_{ДТКП1} =$$

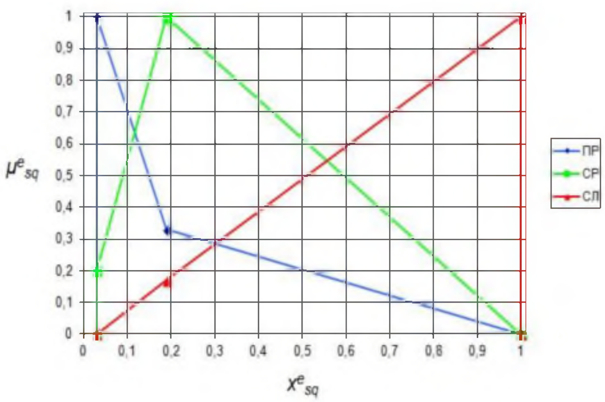
$$\{0/0{,}006; 1/0{,}006; 0{,}2/0{,}25; 0/1\}; \underset{\sim}{T}^{e}_{ДТКП2} = \underset{\sim}{ПМ}^{e}_{ДТКП2} =$$

$$\{0/0{,}006; 0{,}17/0{,}006; 1/0{,}25; 0{,}67/1; 0/1\}; \underset{\sim}{T}^{e}_{ДТКП3} = \underset{\sim}{РР}^{e}_{ДТКП3} = \{0/0{,}006; 0{,}2/0{,}25; 1/1; 0/1\},$$

$$\underset{\sim}{T}^{e}_{ДТКИ1} = \underset{\sim}{Н}^{e}_{ДТКИ1} = \{0/0{,}05; 1/0{,}05; 0{,}17/0{,}1; 0/1\}; \underset{\sim}{T}^{e}_{ДТКИ2} = \underset{\sim}{СР}^{e}_{ДТКИ2} =$$

$$\{0/0{,}05; 0{,}14/0{,}05; 1/0{,}1; 0{,}25/1; 0/1\}; \underset{\sim}{T}^{e}_{ДТКИ3} = \underset{\sim}{В}^{e}_{ДТКИ3} = \{0/0{,}05; 0{,}17/0{,}1; 1/1; 0/1\}.$$

The visualization of standard FN. Stage 6 – the visualization of standard FN. For a subset of standards $\mathbf{T}^{e}_{ДТКУН}$, $\mathbf{T}^{e}_{ДТКИП}$, $\mathbf{T}^{e}_{ДТКСД}$, $\mathbf{T}^{e}_{ДТКП}$ and $\mathbf{T}^{e}_{ДТКИ}$ taking into account the obtained specific values, it is possible to realize their graphical interpretation (see figure 1-4) using the corresponding FN standards.



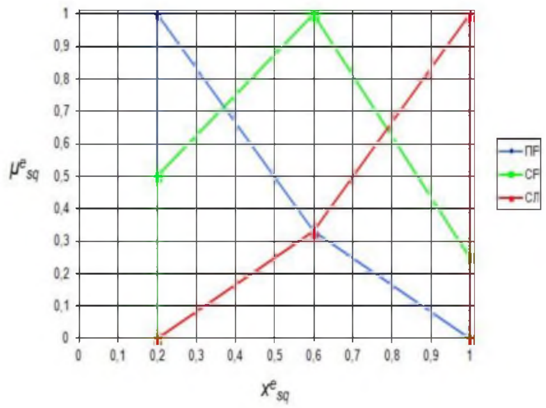


Figure 1 – Linguistic standards for $T^{e}_{ДТКУН}$

Figure 2 – Linguistic standards for $T^{e}_{ДТКНП}$

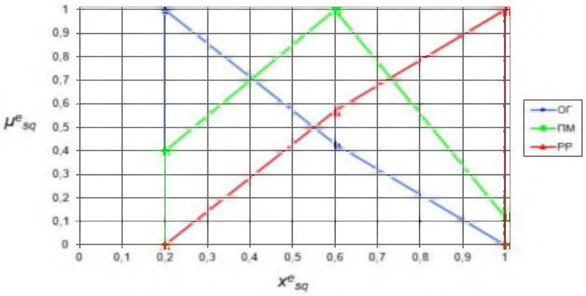


Figure 3 – Linguistic standards for $T^{e}_{ДТКСД}$

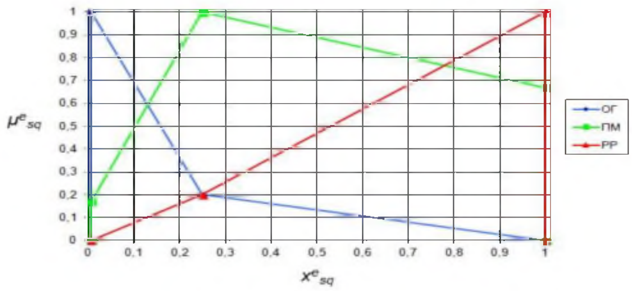


Figure 4 – Linguistic standards for $T^{e}_{ДТКП}$

Conclusions. Based on certain values of IC, US, DC, L, S, and their formed standard values, it is possible to classify further and to select the most effective Honeypot. For this, it is necessary, by analogy with [1, 23-25], to determine the current estimates of the values relative to the standard values created in the work, as well as to form the necessary set of rules which allow to obtain the final result.

Н. К. Жумангалиева[1], А. А. Досжанова[2], А. А. Корченко[3], С. В. Казмирчук[3], Ж. Авкурова[4], Д. Д. Жаксыгулова[5]

[1]Satbayev University, Алматы, Қазақстан;
[2]Алматы Энергетика және байланыс университеті, Алматы, Қазақстан;
[3]Ұлттық авиациалық университет, Украина, Киев;
[4]Л. Н. Гумилев атындағы Еуразия ұлттық университеті, Нұр-Сұлтан, Қазақстан;
[5]Семей қаласының Шәкәрім атындағы мемлекеттік университеті, Қазақстан

HONEYPOT ЖІКТЕУГЕ АРНАЛҒАН ЛИНГВИСТИКАЛЫҚ АЙНЫМАЛЫ СТАНДАРТТАРДЫ ҚАЛЫПТАСТЫРУ ТӘСІЛІ

Аннотация. Қазіргі уақытта ақпараттық қауіпсіздік саласында дамып келе жатқан маңызды бағыттың бірі – Honeypot (виртуалды еліктіру, онлайн тұзақтар) қолдануға, сонымен қатар ең тиімді Honeypot анықтау және оларды одан әрі жіктеу өлшемдерін таңдауға байланысты. Мақалада виртуалды тұзаққа түсіру технологиясы іске асырылатын негізгі өнімдер ұсынылған. Honeypot көбінесе рұқсат етілмеген жағдайда, ақпараттық жүйе ресурстарына рұқсатсыз қол жеткізу үшін қолданатын тәсілдер мен әдістерді зерттеу үшін қолданылады. Желілік тұзақтар кез-келген ресурстарға еліктей алады, алайда көбінесе олар нақты өндірістік серверлер мен жұмыс станциялары секілді көрінеді. Нақты емес жиынтық аппарат негізінде ақпараттық жүйе ресурстарына жасалған шабуылды анықтау мәселелерін шешу үшін қолданылатын бірқатар тиімді әзірлемелер белгілі. Олар тиісті математикалық аппаратты қолдану тиімділігін көрсетті әрі қолдану барысында, мысалы, критерий жиынтығын жасау тәсілін қалыптастырады және ең тиімді Honeypot анықтау үдерісін жақсартады. Осы мақсатта интернеттегі еліктіру үдерісін сипаттайтын критерийлер ұсынылды, тиімді Honeypot таңдау үшін тілдік айнымалы стандарттар қалыптастыру әдісі жасалды.

Бұл әдіс Honeypot жиынтығын, Honeypot сипаттамаларының ішкі жиынтығын, жиілік матрицаларының базалық және туынды жиынтығын қалыптастыруға, сондай-ақ оларды визуализациялай отырып нақты емес терминдер мен стандартты анық емес сандарды құруға негізделген. Бұл ең тиімді виртуалды тұзақты одан әрі жіктеуге және таңдауға мүмкіндік береді.

Ақпараттық жүйелер (АЖ) мен технологиялардың қарқынды дамуы қоғам өмірінің барлық салаларына әсер етеді. Қазіргі заманғы мемлекеттік және жеке кәсіпорындардың белгілі бір мөлшері өндірістік үдерістерді басқару, шешім қабылдауды қолдау, қажетті деректерді іздеу және т.б. үшін пайдаланады.

Ақпараттық қауіпсіздік саласында белсенді дамып келе жатқан өзекті бағыттардың Honeypot (виртуалды еліктіру, онлайн тұзақтар) қолдануға байланысты екенін атап өткен жөн. Мұндай тұзақты қолға түсіру жұмысының мақсаты қорғаныс стратегиясын зерделеу, нақты қауіпсіздік нысандарына шабуыл жасалуы ықтимал құралдарының ауқымын анықтау мақсатында рұқсат етілмеген тарап (UNP) шабуылы немесе сканерлеуі болып саналады.

Honeypot және оларды жүзеге асыруда қолданылатын әдістер әртүрлі, мысалы, арнайы әзірленген интеграцияланған желі немесе негізгі міндеті UNP назарын аудару болып саналатын бірден бір эмуляцияланған желі қызметін атаймыз. Сондықтан ең тиімді жағын анықтау үшін өлшемдерді таңдау және оларды одан әрі жіктеу өзекті мәселе болып есептеледі.

Түйін сөздер: еліктіру классификациясы, онлайн-тұзақ классификациясы, виртуалды еліктіргіш, анық емес стандарттар, тілдік стандарттарды қалыптастыру әдісі, басып кіруді анықтау жүйесі.

Н. К. Жумангалиева[1], А. А. Досжанова[2], А. А. Корченко[3], С. В. Казмирчук[3], Ж. Авкурова[4], Д. Д. Жаксыгулова[5]

[1]Satbayev University, Алматы, Казахстан;
[2]Алматинский университет энергетики и связи, Казахстан;
[3]Национальный авиационный университет, Украина, Киев;
[4]Евразийский национальный университет им. Л. Н. Гумилева, Нур-Султан, Казахстан;
[5]Государственный университет им. Шакарима города Семей, Казахстан

СПОСОБ ФОРМИРОВАНИЯ ЛИНГВИСТИЧЕСКИХ ПЕРЕМЕННЫХ СТАНДАРТОВ ДЛЯ КЛАССИФИКАЦИИ HONEYPOT

Аннотация. В настоящее время одна из важных областей, которая развивается в области информационной безопасности, связана с использованием Honeypot (виртуальные приманки, онлайн-ловушки), а также выбором критериев для определения наиболее эффективного Honeypot и их дальнейшей классификации. Представлены основные продукты, в которых реализована технология виртуальных приманок. Honeypot они используются для изучения поведения, подходов и методов, которые несанкционированная сторона использует для несанкционированного доступа к ресурсам информационной системы. Сетевые ловушки могут имитировать любой ресурс, но чаще всего они выглядят как реальные рабочие серверы и рабочие станции. Известен ряд достаточно эффективных разработок, которые используются для решения задач идентификации атак на ресурсы информационных систем, основанных на аппарате нечетких множеств. Они показали эффективность использования соответствующего математического аппарата, использование которого, например, формализует подход к формированию набора критериев, позволит улучшить процесс определения наиболее эффективного Honeypot. Для этой цели были предложены критерии, которые характеризуют онлайн-ловушки, с помощью которых был разработан метод формирования стандартов языковых переменных для выбора наиболее эффективного Honeypot. Метод основан на формировании набора Honeypot, подмножеств характеристик и значений идентификаторов лингвистических оценок характеристик Honeypot, базовой и производной частотных матриц, а также на построении нечетких терминов и стандартных нечетких чисел с их визуализацией. Это позволит провести дальнейшую классификацию и отбор наиболее эффективных виртуальных приманок.

Стремительное развитие информационных систем (ИС) и технологий затрагивает все сферы жизни общества. Значительное число современных государственных и частных предприятий используют его для управления производственными процессами, поддержки принятия решений, поиска необходимых данных и т.д. Наряду с этим увеличивается количество уязвимостей и угроз ИС, а значит, возникает необходимость в специализированных средствах безопасности для обеспечения их нормального функционирования и предотвращения вторжений. Следует отметить, что одно из актуальных направлений, которое активно развивается в сфере информационной безопасности, связано с использованием медоносных горшочков (виртуальных приманок, онлайн-ловушек). Целью работы таких приманок является атака или сканирование неавторизованной стороной (УНП) с целью изучения стратегии защиты, определения диапазона их средств, с помощью которых могут проводиться атаки на реальные объекты безопасности. Honeypot и методы, используемые для их реализации, различны, например, это специально разработанная интегрированная сеть или один единственный эмулируемый сетевой сервис, основной задачей которого является привлечение внимания UNP [1]. Поэтому выбор критериев для определения наиболее эффективных медоносов и их дальнейшая классификация является актуальной задачей.

Ключевые слова: классификация приманок, классификация онлайн-ловушек, виртуальные приманки, нечеткие стандарты, метод формирования языковых стандартов, системы обнаружения вторжений.

Information about authors:

Zhumangaliyeva Nazym, PhD student, Satbayev University, Almaty, Kazakhstan; nazym_k.81@mail.ru; https://orcid.org/0000-0003-1130-3405

Doszhanova Aliya, PhD, Associate professor, Almaty University of Power Engineering and Telecommunications, Almaty, Kazakhstan; d_alia.81@mail.ru; https://orcid.org/0000-0002-6932-6282

Korchenko Anna, candidate of technical Sciences, associate Professor, National aviation University, Department of information technology Security, Kiev, Ukraine; annakor@ukr.net; https://orcid.org/0000-0003-0016-1966

Kazmirchuk Svitlana, Dr Eng (Information security), Head of Computerised Information Security Systems Academic Department, National Aviation University, Kyiv, Ukraine; sv.kazmirchuk@gmail.com; https://orcid.org/0000-0001-6083-251X

Avkurova Zhadyra, PhD student L.N. Gumilyov Eurasian National University, Nur-Sultan, Kazakhstan; zhadyra.avkurova.83@mail.ru; https://orcid.org/0000-0002-0706-6075

Zhaxygulova Dauriya, Senior Lecturer, Shakarim State University of Semey, Kazakhstan; daurija_zd@mail.ru; https://orcid.org/0000-0002-2347-9857

REFERENCES

[1] Korchenko Anna. Methods of Identifying Anomalous States for Intrusion Detection Systems. Monograph, Kiev, CP “Komprint”, 2019. 361 p. (in Ukr.).

[2] Stoll C. Cuckoo’s Egg / C. Stoll. NY : Pocket, 1990. 356 p.

[3] Cheswick B. An Evening with Berferd In Which a Cracker is Lured, Endured, and Studied / B. Cheswick. NY: Management Analytics and Others, 1995. 147 p.

[4] Spitzner L. Honeypots: Tracking Hackers / L. Spitzner. NY : Addison-Wesley Professional, 2002. 480 p.

[5] Provos N. Virtual Honeypots: From Botnet Tracking to Intrusion Detection. NY : Addison-Wesley Professional, 2007. 440 p.

[6] Honeynet Project Blog [Electr. resource]: (Blog) // The Honeynet Project. Access mode: http://www.honeynet.org (17.07.2019).

[7] A Framework for Deception / Cohen F., Lambert D., Preston C., Berry N., Stewart C., Thomas E. Tech. Report, 2001.

[8] Balas E., Viecco C. Towards a Third Generation Data Capture Architecture for Honeynets // Workshop on Information Assurance and Security US Military Academy, West Point, NY. IEEE, 2005.

[9] Roesch M. Snort – lightweight instrusion detection for networks / M. Roesch. LISA'99 Systems Admistration Conference, 1999.

[10] LaBrea: «Sticky» Honeypotand IDS [Electr. resource]: (Labrea Tarpit Project) // Labrea. Access mode: http://labrea.sourceforge.net (25.07.2019).

[11] Hammer R. Enhancing IDS using, Tiny Honeypot / R. Hammer. SANS Institute, 2006.

[12] TheDeceptionToolkit [Electr. resource]: (The Deception Toolkit Home Page and Mailing List) // Fred Cohen & Associates. Access mode: http://www.all.net/dtk/dtk.html (04.08.2019).

[13] Diebold P. A Honeypot Architecture for Detecting and Analyzing Unknown Network Attacks / P. Diebold, A. Hess, G. Schafer // In Proc. Of 14th Kommunikation in Verteilen Systemen 2005. Kaiserslautern: Technische Universitat Berlin, 2005.

[14] Bugubayeva R.O., Tapenova G.S. (2019) Regulatory aspects of public administration system of higher education in the republic of kazakhstan // Bulletin of national academy of sciences of the Republic of Kazakhstan. ISSN 2224-5294 Vol. 1, N 323 (2019). P.151-160. https://doi.org/10.32014/2019.2224-5294.24 (in Eng.).

[15] Thakar U., Varma S., Ramani A. 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, 2005.

[16] Gnatyuk S., Volyanska V., Karpenko S., Advanced virtual lure systems based on honeypot technology // Zahistinformacіï, 2012. Vol. 14, N 3. P. 107-115 (in Ukr.).

[17] Honeypot Technology. Part 2: Honeypot Classification. [Electr. resource] - Access mode: http://www.securitylab.ru/analytics/275775.php (04.09.2019).

[18] Honeypotslureon a hacker. [Electr. resource] - Access mode: https://docplayer.ru/54222428-Honeypots-primanka-na-hakera.html (12.09.2019).

[19] Akkaya D. Honeypots in Network Security / Deniz Akkaya, Fabien Thalgott. Kalmar : Linnaeus University, 2010. 39 p.

[20] V. Kotenko M.V. Stepashkin. Deception systems for protection of information resources incomputer networks // SPIIRAS Proceeding. Issue 2, Vol. 1. SPb.: SPIIRAS, 2004.

[21] Korchenko A.G. The development of information protection systems based on the fuzzy sets // The theory and practical solutions, Kuev, 2006. 320 p. (in Russ.).

[22] Korchenko A.A. The method of linguistic standards formation for intrusion detection systems / Korchenko A.A. // Zakhist Information. 2014. Vol. 16, N 1. P. 5-12 (in Russ.).

[23] Improved method for the formation of linguistic standards for of intrusion detection systems / Akhmetov B., Korchenko A., Akhmetova S., Zhumangalieva N. // Journal of Theoretical and Applied Information Technology. 2016. Vol.87, N 2. P. 221-232.

[24] Zhumangaliyeva Nazym, Korchenko Anna, Doszhanova Aliya, Shaikhanova Aigul, Shangytbayeva Gulmira, Avkurova Zhadyra / Detection environment formation method for anomaly detection systems // Journal of Theoretical and Applied Information Technology, 2019. Vol.97, N 16. P. 4239-4250.

[25] Karpinski Mikolaj, Poland, Korchenko Anna, Vikulov Pavlo, Ukraine, Kochan Roman. The Etalon Models of Linguistic Variables for Sniffing-Attack Detection // Proceedings of the 2017 IEEE 9th International Conference on «Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications» (IDAACS'2017), Romania, Bucharest, September 21-23, 2017: Vol. 1. P. 258-264.

[26] Korchenko Anna, Warwas Kornel, Kłos-Witkowska Aleksandra. The Tupel Model of Basic Components' Set Formation for Cyberattacks // Proceedings of the 2015 IEEE 8th International Conference on «Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications» (IDAACS'2015), Warsaw, Poland, September 24-26, 2015. Vol. 1. P. 478-483.

[27] Zhumangaliyeva Nazym, Doszhanova Aliya, Korchenko Anna. Algorithmic and software support for the formation of parameter standards for the cyber attacks detection systems // Bulletin of National Academy of Sciences of The Republic Of Kazakhstan. Vol. 6, N 382 (2019), 6-23. ISSN 1991-3494. UDC 621.39:004.05 IRSTI 81.93.2. https://doi.org/10.32014/2019.2518-1467.14