

ISSN 2518-1467 (Online),
ISSN 1991-3494 (Print)

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫНЫҢ

Х А Б А Р Ш Ы С Ы

ВЕСТНИК

НАЦИОНАЛЬНОЙ АКАДЕМИИ НАУК
РЕСПУБЛИКИ КАЗАХСТАН

THE BULLETIN

THE NATIONAL ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN

PUBLISHED SINCE 1944

5

SEPTEMBER – OCTOBER 2020

ALMATY, NAS RK

NAS RK is pleased to announce that Bulletin of NAS RK scientific journal has been accepted for indexing in the Emerging Sources Citation Index, a new edition of Web of Science. Content in this index is under consideration by Clarivate Analytics to be accepted in the Science Citation Index Expanded, the Social Sciences Citation Index, and the Arts & Humanities Citation Index. The quality and depth of content Web of Science offers to researchers, authors, publishers, and institutions sets it apart from other research databases. The inclusion of Bulletin of NAS RK in the Emerging Sources Citation Index demonstrates our dedication to providing the most relevant and influential multidiscipline content to our community.

Қазақстан Республикасы Ұлттық ғылым академиясы "ҚР ҰҒА Хабаршысы" ғылыми журналының Web of Science-тің жаңаланған нұсқасы Emerging Sources Citation Index-те индекстелуге қабылданғанын хабарлайды. Бұл индекстелу барысында Clarivate Analytics компаниясы журналды одан әрі the Science Citation Index Expanded, the Social Sciences Citation Index және the Arts & Humanities Citation Index-ке қабылдау мәселесін қарастыруда. Web of Science зерттеушілер, авторлар, баспашылар мен мекемелерге контент тереңдігі мен сапасын ұсынады. ҚР ҰҒА Хабаршысының Emerging Sources Citation Index-ке енуі біздің қоғамдастық үшін ең өзекті және беделді мультидисциплинарлы контентке адалдығымызды білдіреді.

НАН РК сообщает, что научный журнал «Вестник НАН РК» был принят для индексирования в Emerging Sources Citation Index, обновленной версии Web of Science. Содержание в этом индексировании находится в стадии рассмотрения компанией Clarivate Analytics для дальнейшего принятия журнала в the Science Citation Index Expanded, the Social Sciences Citation Index и the Arts & Humanities Citation Index. Web of Science предлагает качество и глубину контента для исследователей, авторов, издателей и учреждений. Включение Вестника НАН РК в Emerging Sources Citation Index демонстрирует нашу приверженность к наиболее актуальному и влиятельному мультидисциплинарному контенту для нашего сообщества.

Б а с р е д а к т о р ы

х.ғ.д., проф., ҚР ҰҒА академигі

М.Ж. Жұрынов

Р е д а к ц и я а л қ а с ы:

Абиев Р.Ш. проф. (Ресей)
Абылкасымова А.Е. проф., академик (Қазақстан)
Аврамов К.В. проф. (Украина)
Аппель Юрген проф. (Германия)
Баймұқанов Д.А. проф., академик (Қазақстан)
Баймұратов У.Б. проф., академик (Қазақстан)
Байтанаев Б.А. проф., академик (Қазақстан)
Байтулин И.О. проф., академик (Қазақстан)
Банас Иозеф проф. (Польша)
Берсимбаев Р.И. проф., академик (Қазақстан)
Велесько С. проф. (Германия)
Велихов Е.П. проф., РҒА академигі (Ресей)
Кабульдинов З.Е. проф. (Қазақстан)
Қажыбек Е.З. проф., корр.-мүшесі (Қазақстан)
Қалимолдаев М.Н. проф., академик (Қазақстан), бас ред. орынбасары
Қамзабекұлы Д. проф., академик (Қазақстан)
Қойгелдиев М.К. проф., академик (Қазақстан)
Лупашку Ф. проф., корр.-мүшесі (Молдова)
Мохд Хасан Селамат проф. (Малайзия)
Новак Изабелла проф. (Польша)
Огарь Н.П. проф., корр.-мүшесі (Қазақстан)
Полещук О.Х. проф. (Ресей)
Поняев А.И. проф. (Ресей)
Сагиян А.С. проф., академик (Армения)
Таймагамбетов Ж.К. проф., академик (Қазақстан)
Хрипунов Г.С. проф. (Украина)
Шәукенова З.К. проф., корр.-мүшесі (Қазақстан)
Юлдашбаев Ю.А. проф., РҒА академигі (Ресей)
Якубова М.М. проф., академик (Тәжікстан)

«Қазақстан Республикасы Ұлттық ғылым академиясының Хабаршысы».

ISSN 2518-1467 (Online),

ISSN 1991-3494 (Print)

Меншіктенуші: «Қазақстан Республикасының Ұлттық ғылым академиясы»РҚБ (Алматы қ.).

Қазақстан Республикасының Ақпарат және коммуникациялар министрлігінің Ақпарат комитетінде 12.02.2018 ж. берілген № 16895-Ж мерзімдік басылым тіркеуіне қойылу туралы куәлік.

Тақырыптық бағыты: *іргелі ғылымдар саласындағы жаңа жетістіктер нәтижелерін жария ету.*

Мерзімділігі: жылына 6 рет.

Тиражы: 2000 дана.

Редакцияның мекенжайы: 050010, Алматы қ., Шевченко көш., 28, 219 бөл., 220, тел.: 272-13-19, 272-13-18,
<http://www.bulletin-science.kz/index.php/en/>

© Қазақстан Республикасының Ұлттық ғылым академиясы, 2020

Типографияның мекенжайы: «NurNaz GRACE», Алматы қ., Рысқұлов көш., 103.

Г л а в н ы й р е д а к т о р
д.х.н., проф. академик НАН РК
М.Ж. Журинов

Р е д а к ц и о н н а я к о л л е г и я:

Абиев Р.Ш. проф. (Россия)
Абылкасымова А.Е. проф., академик (Казахстан)
Аврамов К.В. проф. (Украина)
Апель Юрген проф. (Германия)
Баймуканов Д.А. проф., академик (Казахстан)
Баймуратов У.Б. проф., академик (Казахстан)
Байтанаев Б.А. проф., академик (Казахстан)
Байтулин И.О. проф., академик (Казахстан)
Банас Иозеф проф. (Польша)
Берсимбаев Р.И. проф., академик (Казахстан)
Велесько С. проф. (Германия)
Велихов Е.П. проф., академик РАН (Россия)
Кабульдинов З.Е. проф. (Казахстан)
Кажыбек Е.З. проф., чл.-корр. (Казахстан)
Калимолдаев М.Н. академик (Казахстан), зам. гл. ред.
Камзабекулы Д. проф., академик (Казахстан)
Койгельдиев М.К. проф., академик (Казахстан)
Лунашку Ф. проф., чл.-корр. (Молдова)
Мохд Хасан Селамат проф. (Малайзия)
Новак Изабелла проф. (Польша)
Огарь Н.П. проф., чл.-корр. (Казахстан)
Полещук О.Х. проф. (Россия)
Поняев А.И. проф. (Россия)
Сагьян А.С. проф., академик (Армения)
Таймагамбетов Ж.К. проф., академик (Казахстан)
Хрипунов Г.С. проф. (Украина)
Шаукенова З.К. проф., чл.-корр. (Казахстан)
Юлдашбаев Ю.А. проф., академик РАН (Россия)
Якубова М.М. проф., академик (Таджикистан)

«Вестник Национальной академии наук Республики Казахстан».

ISSN 2518-1467 (Online),

ISSN 1991-3494 (Print)

Собственник: РОО «Национальная академия наук Республики Казахстан» (г. Алматы).

Свидетельство о постановке на учет периодического печатного издания в Комитете информации Министерства информации и коммуникаций и Республики Казахстан № **16895-Ж**, выданное 12.02.2018 г.

Тематическая направленность: *публикация результатов новых достижений в области фундаментальных наук.*

Периодичность: 6 раз в год.

Тираж: 2000 экземпляров.

Адрес редакции: 050010, г. Алматы, ул. Шевченко, 28, ком. 219, 220, тел. 272-13-19, 272-13-18.

<http://www.bulletin-science.kz/index.php/en/>

© Национальная академия наук Республики Казахстан, 2020

Адрес типографии: «NurNazGRACE», г. Алматы, ул. Рыскулова, 103.

Editor in chief

doctor of chemistry, professor, academician of NAS RK

M.Zh. Zhurinov

Editorial board:

Abiyev R.Sh. prof. (Russia)
Abylkasymova A.E. prof., academician (Kazakhstan)
Avramov K.V. prof. (Ukraine)
Appel Jurgen, prof. (Germany)
Baimukanov D.A. prof., academician (Kazakhstan)
Baimuratov U.B. prof., academician (Kazakhstan)
Baitanaev B.A. prof., academician (Kazakhstan)
Baitullin I.O. prof., academician (Kazakhstan)
Joseph Banas, prof. (Poland)
Bersimbayev R.I. prof., academician (Kazakhstan)
Velesco S., prof. (Germany)
Velikhov Ye.P. prof., academician of RAS (Russia)
Kabuldinov Z.E. prof. (Kazakhstan)
Kazhybek E.Z. prof., corr. member. (Kazakhstan)
Kalimoldayev M.N. prof., academician (Kazakhstan), deputy editor in chief
Kamzabekuly D. prof., academician (Kazakhstan)
Koigeldiev M.K. prof., academician (Kazakhstan)
Lupashku F. prof., corr. member (Moldova)
Mohd Hassan Selamat, prof. (Malaysia)
Nowak Isabella, prof. (Poland)
Ogar N.P. prof., corr. member (Kazakhstan)
Poleshchuk O.Kh. prof. (Russia)
Ponyaev A.I. prof. (Russia)
Sagiyani A.S. prof., academician (Armenia)
Tajmagambetov Zh.K. prof., academician (Kazakhstan)
Khripunov G.S. prof. (Ukraine)
Shaukenova Z.K. prof., corr. member. (Kazakhstan)
Yuldashbayev Y.A., prof., academician of RAS (Russia)
Yakubova M.M. prof., academician (Tadjikistan)

Bulletin of the National Academy of Sciences of the Republic of Kazakhstan.

ISSN 2518-1467 (Online),

ISSN 1991-3494 (Print)

Owner: RPA "National Academy of Sciences of the Republic of Kazakhstan" (Almaty).

The certificate of registration of a periodical printed publication in the Committee of information of the Ministry of Information and Communications of the Republic of Kazakhstan No. **16895-Ж**, issued on 12.02.2018.

Thematic focus: *publication of the results of new achievements in the field of basic sciences.*

Periodicity: 6 times a year.

Circulation: 2000 copies.

Editorial address: 28, Shevchenko str., of. 219, 220, Almaty, 050010, tel. 272-13-19, 272-13-18,

<http://www.bulletin-science.kz/index.php/en/>

© National Academy of Sciences of the Republic of Kazakhstan, 2020

Address of printing house: «NurNaz GRACE», 103, Ryskulov str, Almaty.

**Nazym Zhumangaliyeva¹, Aliya Doszhanova², Anna Korchenko³,
Svitlana Kazmirchuk³, Zhadyra Avkurova⁴, Dauriya Zhaxygulova⁵**

¹Satbayev University, Almaty, Kazakhstan;

²Almaty University of Power Engineering and Telecommunications, Kazakhstan;

³Department of Information Technology Security, National Aviation, Kiev, Ukraine;

⁴L. N. Gumilyov Eurasian National University, Nur-Sultan, Kazakhstan;

⁵Shakarim 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.

$$VS_{DTKH} = \|vS_{DTKHq}\| = \|vS_{DTKH1}, vS_{DTKH2}, vS_{DTKH3}\| = \left\| \bigcup_{q=1}^3 \sum_{s=1}^3 f_{DTKHsq} \right\| = \|8, 8, 10\|, (q = \overline{1, 3}).$$

Then, taking into account (16) in [21,22] from $VS_{DTKVH}, VS_{DTKHP}, VS_{DTKCD}, VS_{DTKPI},$ and VS_{DTKHI} define the maximum element $vsm_{DTKVH} = \bigvee_{q=1}^3 vs_{DTKVHq} = vs_{DTKVH1} \vee vs_{DTKVH2} \vee vs_{DTKVH3} = 6 \vee 9 \vee 4 = vsm_{DTKVH} = 9,$ $vsm_{DTKHP} = \bigvee_{q=1}^3 vs_{DTKHPq} = vs_{DTKHP1} \vee vs_{DTKHP2} \vee vs_{DTKHP3} = 6 \vee 5 \vee 5 = vsm_{DTKHP} = 6,$ $vsm_{DTKCD} = \bigvee_{q=1}^3 vs_{DTKCDq} = vs_{DTKCD1} \vee vs_{DTKCD2} \vee vs_{DTKCD3} = 7 \vee 14 \vee 9 = vsm_{DTKCD} = 14,$ $vsm_{DTKPI} = \bigvee_{q=1}^3 vs_{DTKPIq} = vs_{DTKPI1} \vee vs_{DTKPI2} \vee vs_{DTKPI3} = 7 \vee 7 \vee 5 = vsm_{DTKPI} = 7$ and $vsm_{DTKHI} = \bigvee_{q=1}^3 vs_{DTKHIq} = vs_{DTKHI1} \vee vs_{DTKHI2} \vee vs_{DTKHI3} = 8 \vee 8 \vee 10 = vsm_{DTKHI} = 10.$ and according to (17) in [21,22] we obtain a derivative frequency

$$\text{matrix, } F'_{DTKVH} = (vsm_{DTKVH} / vsm_{DTKVHq})F_{DTKVH} = \begin{vmatrix} 3,33 & 2 & 0 \\ 0,67 & 6 & 0 \\ 0 & 1 & 1,78 \end{vmatrix},$$

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

$$F'_{DTKCD} = (vsm_{DTKCD} / vsm_{DTKCDq})F_{DTKCD} = \begin{vmatrix} 2,5 & 3 & 0 \\ 1 & 7 & 0,64 \\ 0 & 4 & 5,14 \end{vmatrix}, F'_{DTKPI} = (vsm_{DTKPI} / vsm_{DTKPIq})F_{DTKPI} = \begin{vmatrix} 6 & 1 & 0 \\ 1 & 5 & 1,43 \\ 0 & 1 & 2,14 \end{vmatrix},$$

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

The creation of fuzzy terms and standard FN. Stage 5—the creation of fuzzy terms and standard FN. Firstly, according to (22) in [21,22] let form the subset of fuzzy terms $T_{DTKVH}, T_{DTKHP}, T_{DTKCD}, T_{DTKPI}, T_{DTKHI}$ if $n = 1$ (i.e. for HoneyPot with ID $H_{DTK} = DTK$), $m_1 = 5, r_1 = r_2 = r_3 = r_4 = r_5 = 3$.

$$\{\bigcup_{i=1}^1 T_i\} = \{\bigcup_{i=1}^n \{\bigcup_{j=1}^{m_i} T_{ij}\}\} = \{\bigcup_{i=1}^n \{\bigcup_{j=1}^{m_i} \{\bigcup_{s=1}^{r_j} T_{ijs}\}\}\} = \{\{T_{DTKVH1}, T_{DTKVH2}, T_{DTKVH3}\}, \{T_{DTKHP1}, T_{DTKHP2}, T_{DTKHP3}\},$$

$$\{T_{DTKCD1}, T_{DTKCD2}, T_{DTKCD3}\}, \{T_{DTKPI1}, T_{DTKPI2}, T_{DTKPI3}\}, \{T_{DTKHI1}, T_{DTKHI2}, T_{DTKHI3}\}\} =$$

$$\{\{\underline{PP}_{DTKVH}, \underline{CP}_{DTKVH}, \underline{CL}_{DTKVH}\}, \{\underline{PP}_{DTKHP}, \underline{CP}_{DTKHP}, \underline{CL}_{DTKHP}\}, \{\underline{OG}_{DTKCD}, \underline{PM}_{DTKCD}, \underline{PP}_{DTKCD}\},$$

$\{\underline{OG}_{DTKPI}, \underline{PM}_{DTKPI}, \underline{PP}_{DTKPI}\}, \{\underline{H}_{DTKHI}, \underline{CP}_{DTKHI}, \underline{B}_{DTKHI}\}\}$. According to (23) in [21], [22] on corresponding lines of $F'_{DTKVH}, F'_{DTKHP}, F'_{DTKCD}, F'_{DTKPI}$ and F'_{DTKHI} let create construct the vectors of maximum i.e.

$$FM_{DTKVH} = \|fm_{DTKVHs}\| = \|fm_{DTKVH1}, fm_{DTKVH2}, fm_{DTKVH3}\| = \|3,33; 6; 1,78\|, FM_{DTKHP} = \|fm_{DTKHPs}\| =$$

$$\|fm_{DTKHP1}, fm_{DTKHP2}, fm_{DTKHP3}\| = \|4; 2,5; 3,33\|, FM_{DTKCD} = \|fm_{DTKCDs}\| =$$

$$\|fm_{DTKCD1}, fm_{DTKCD2}, fm_{DTKCD3}\| = \|2,5; 7; 5,14\|, FM_{DTKPI} = \|fm_{DTKPIs}\| =$$

$$\|fm_{DTKPI1}, fm_{DTKPI2}, fm_{DTKPI3}\| = \|6; 5; 2,14\|, FM_{DTKHI} = \|fm_{DTKHis}\| =$$

$$\|fm_{DTKHI1}, fm_{DTKHI2}, fm_{DTKHI3}\| = \|5,6; 4,8; 8\|.$$

On the basis of FM_{DTKVH} , FM_{DTKHP} , FM_{DTKCD} , FM_{DTKPI} and FM_{DTKHI} according to the expression (24) in [21,22] let form matrices of membership function:

$$M_{DTKVH} = \|\mu_{DTKVHsq}\| = \begin{vmatrix} 1 & 0,33 & 0 \\ 0,2 & 1 & 0 \\ 0 & 0,17 & 1 \end{vmatrix},$$

$$M_{DTKHP} = \|\mu_{DTKHPsq}\| = \begin{vmatrix} 1 & 0,33 & 0 \\ 0,5 & 1 & 0,25 \\ 0 & 0,33 & 1 \end{vmatrix}, M_{DTKCD} = \|\mu_{DTKCDsq}\| = \begin{vmatrix} 1 & 0,43 & 0 \\ 0,4 & 1 & 0,12 \\ 0 & 0,57 & 1 \end{vmatrix},$$

$$M_{DTKPI} = \|\mu_{DTKPIsq}\| = \begin{vmatrix} 1 & 0,2 & 0 \\ 0,17 & 1 & 0,67 \\ 0 & 0,2 & 1 \end{vmatrix}, M_{DTKHI} = \|\mu_{DTKHIsq}\| = \begin{vmatrix} 1 & 0,17 & 0 \\ 0,14 & 1 & 0,25 \\ 0 & 0,17 & 1 \end{vmatrix},$$

where $\mu_{DTKVHsq} = f_{DTKVHsq} / fm_{DTKVHs}$, $(s, q = \overline{1,3})$, $\mu_{DTKHPsq} = f_{DTKHPsq} / fm_{DTKHPs}$, $(s, q = \overline{1,3})$, $\mu_{DTKCDsq} = f_{DTKCDsq} / fm_{DTKCDs}$, $(s, q = \overline{1,3})$, $\mu_{DTKPIsq} = f_{DTKPIsq} / fm_{DTKPIs}$, $(s, q = \overline{1,3})$, $\mu_{DTKHIsq} = f_{DTKHIsq} / fm_{DTKHIs}$, $(s, q = \overline{1,3})$.

According to the obtained data, $\mu_{DTKVHsq}$, $\mu_{DTKHPsq}$, $\mu_{DTKCDsq}$, $\mu_{DTKPIsq}$, $\mu_{DTKHIsq}$ and calculated by the expression (26) in [21,22] $x_{DTKVHsq}$, $x_{DTKHPsq}$, $x_{DTKCDsq}$, $x_{DTKPIsq}$, $x_{DTKHIsq}$ let define sets of fuzzy terms according to (25) in [21,22] $T_{DTKVHs} = \{\mu_{DTKVHs1} / x_{DTKVHs1}, \mu_{DTKVHs2} / x_{DTKVHs2}, \mu_{DTKVHs3} / x_{DTKVHs3}\}$, $(s, q = \overline{1,3})$, where according to (26) in [21,22] $X_{DTKVHsq} = N_{DTKVHq}^{max} / N_{DTKVHr}^{max}$, $(q = \overline{1,3})$ or $\{\bigcup_{q=1}^3 X_{DTKVHsq}\} = \{0,03; 0,19; 1\}$, $T_{DTKHPs} = \{\mu_{DTKHPs1} / x_{DTKHPs1}, \mu_{DTKHPs2} / x_{DTKHPs2}, \mu_{DTKHPs3} / x_{DTKHPs3}\}$, $(s, q = \overline{1,3})$, where according to (26) in [21,22] $X_{DTKHPsq} = N_{DTKHPq}^{max} / N_{DTKHPr}^{max}$, $(q = \overline{1,3})$ or $\{\bigcup_{q=1}^3 X_{DTKHPsq}\} = \{0,2; 0,6; 1\}$, $T_{DTKCDs} = \{\mu_{DTKCDs1} / x_{DTKCDs1}, \mu_{DTKCDs2} / x_{DTKCDs2}, \mu_{DTKCDs3} / x_{DTKCDs3}\}$, $(s, q = \overline{1,3})$, where according to (26) in [21,22] $X_{DTKCDsq} = N_{DTKCDq}^{max} / N_{DTKCDr}^{max}$, $(q = \overline{1,3})$ or $\{\bigcup_{q=1}^3 X_{DTKCDsq}\} = \{0,2; 0,6; 1\}$, $T_{DTKPIs} = \{\mu_{DTKPIs1} / x_{DTKPIs1}, \mu_{DTKPIs2} / x_{DTKPIs2}, \mu_{DTKPIs3} / x_{DTKPIs3}\}$, $(s, q = \overline{1,3})$, where according to (26) in [21,22] $X_{DTKPIsq} = N_{DTKPIq}^{max} / N_{DTKPIr}^{max}$, $(q = \overline{1,3})$ or $\{\bigcup_{q=1}^3 X_{DTKPIsq}\} = \{0,006; 0,25; 1\}$, $T_{DTKHIs} = \{\mu_{DTKHIs1} / x_{DTKHIs1}, \mu_{DTKHIs2} / x_{DTKHIs2}, \mu_{DTKHIs3} / x_{DTKHIs3}\}$, $(s, q = \overline{1,3})$, where according to (26) in [21,22] $X_{DTKHIsq} = N_{DTKHIsq}^{max} / N_{DTKHIsr}^{max}$, $(q = \overline{1,3})$ or $\{\bigcup_{q=1}^3 X_{DTKHIsq}\} = \{0,05; 0,1; 1\}$.

Therefore, the resulting members of the subset T_{DTKVH} , T_{DTKHP} , T_{DTKCD} , T_{DTKPI} , T_{DTKHI} (numerical form), respectively, are the reflection of the members of the subset LE_{DTKVH} , LE_{DTKHP} , LE_{DTKCD} , LE_{DTKPI} , LE_{DTKHI} (linguistic form) and are presented in the following form:

$$\begin{aligned} T_{DTKVH1} &= \underline{PP}_{DTKVH1} = \{1 / 0,03; 0,33 / 0,19; 0 / 1\}; T_{DTKVH2} = \underline{CP}_{DTKVH2} = \{0,2 / 0,03; 1 / 0,19; 0 / 1\}; \\ T_{DTKVH3} &= \underline{CJ}_{DTKVH3} = \{0 / 0,03; 0,17 / 0,19; 1 / 1\}; T_{DTKHP1} = \underline{PP}_{DTKHP1} = \{1 / 0,2; 0,33 / 0,6; 0 / 1\}; \end{aligned}$$

$$\begin{aligned} \underline{T}_{DTK\Pi\Pi 2} &= \underline{CP}_{DTK\Pi\Pi 2} = \{0,5 / 0,2; 1 / 0,6; 0,25 / 1\}; \underline{T}_{DTK\Pi\Pi 3} = \underline{CJ}_{DTK\Pi\Pi 3} = \{0 / 0,2; 0,33 / 0,6; 1 / 1\}, \\ \underline{T}_{DTKCD 1} &= \underline{OG}_{DTKCD 1} = \{1 / 0,2; 0,43 / 0,6; 0 / 1\}; \underline{T}_{DTKCD 2} = \underline{PM}_{DTKCD 2} = \{0,4 / 0,2; 1 / 0,6; 0,12 / 1\}; \\ \underline{T}_{DTKCD 3} &= \underline{PP}_{DTKCD 3} = \{0 / 0,2; 0,57 / 0,6; 1 / 1\}; \underline{T}_{DTK\Pi 1} = \underline{OG}_{DTK\Pi 1} = \{1 / 0,006; 0,2 / 0,25; 0 / 1\}; \\ \underline{T}_{DTK\Pi 2} &= \underline{PM}_{DTK\Pi 2} = \{0,17 / 0,006; 1 / 0,25; 0,67 / 1\}; \underline{T}_{DTK\Pi 3} = \underline{PP}_{DTK\Pi 3} = \{0 / 0,006; 0,2 / 0,25; 1 / 1\}, \\ \underline{T}_{DTK\Pi 1} &= \underline{H}_{DTK\Pi 1} = \{1 / 0,05; 0,17 / 0,1; 0 / 1\}; \underline{T}_{DTK\Pi 2} = \underline{CP}_{DTK\Pi 2} = \{0,14 / 0,05; 1 / 0,1; 0,25 / 1\}; \\ \underline{T}_{DTK\Pi 3} &= \underline{B}_{DTK\Pi 3} = \{0 / 0,05; 0,17 / 0,1; 1 / 1\}. \end{aligned}$$

Then, secondly, according to (29) in [21,22] let form standard FN $\mathbf{T}_{DTK\Pi\Pi}^e \subseteq \mathbf{T}^e$, $\mathbf{T}_{DTK\Pi\Pi}^e \subseteq \mathbf{T}^e$, $\mathbf{T}_{DTKCD}^e \subseteq \mathbf{T}^e$, $\mathbf{T}_{DTK\Pi}^e \subseteq \mathbf{T}^e$, $\mathbf{T}_{DTK\Pi}^e \subseteq \mathbf{T}^e$:

$$\begin{aligned} \mathbf{T}_{DTK\Pi\Pi}^e &= \left\{ \bigcup_{s=1}^3 \underline{T}_{DTK\Pi\Pi s}^e \right\} = \left\{ \underline{T}_{DTK\Pi\Pi 1}^e, \underline{T}_{DTK\Pi\Pi 2}^e, \underline{T}_{DTK\Pi\Pi 3}^e \right\} = \left\{ \underline{PP}_{DTK\Pi\Pi 1}^e, \underline{CP}_{DTK\Pi\Pi 2}^e, \underline{CJ}_{DTK\Pi\Pi 3}^e \right\}, (s = \overline{1,3}), \\ \mathbf{T}_{DTKCD}^e &= \left\{ \bigcup_{s=1}^3 \underline{T}_{DTKCD s}^e \right\} = \left\{ \underline{T}_{DTKCD 1}^e, \underline{T}_{DTKCD 2}^e, \underline{T}_{DTKCD 3}^e \right\} = \left\{ \underline{OG}_{DTKCD 1}^e, \underline{PM}_{DTKCD 2}^e, \underline{PP}_{DTKCD 3}^e \right\}, (s = \overline{1,3}), \\ \mathbf{T}_{DTK\Pi}^e &= \left\{ \bigcup_{s=1}^3 \underline{T}_{DTK\Pi s}^e \right\} = \left\{ \underline{T}_{DTK\Pi 1}^e, \underline{T}_{DTK\Pi 2}^e, \underline{T}_{DTK\Pi 3}^e \right\} = \left\{ \underline{OG}_{DTK\Pi 1}^e, \underline{PM}_{DTK\Pi 2}^e, \underline{PP}_{DTK\Pi 3}^e \right\}, (s = \overline{1,3}), \\ \mathbf{T}_{DTK\Pi}^e &= \left\{ \bigcup_{s=1}^3 \underline{T}_{DTK\Pi s}^e \right\} = \left\{ \underline{T}_{DTK\Pi 1}^e, \underline{T}_{DTK\Pi 2}^e, \underline{T}_{DTK\Pi 3}^e \right\} = \left\{ \underline{H}_{DTK\Pi 1}^e, \underline{CP}_{DTK\Pi 2}^e, \underline{B}_{DTK\Pi 3}^e \right\}, (s = \overline{1,3}), \end{aligned}$$

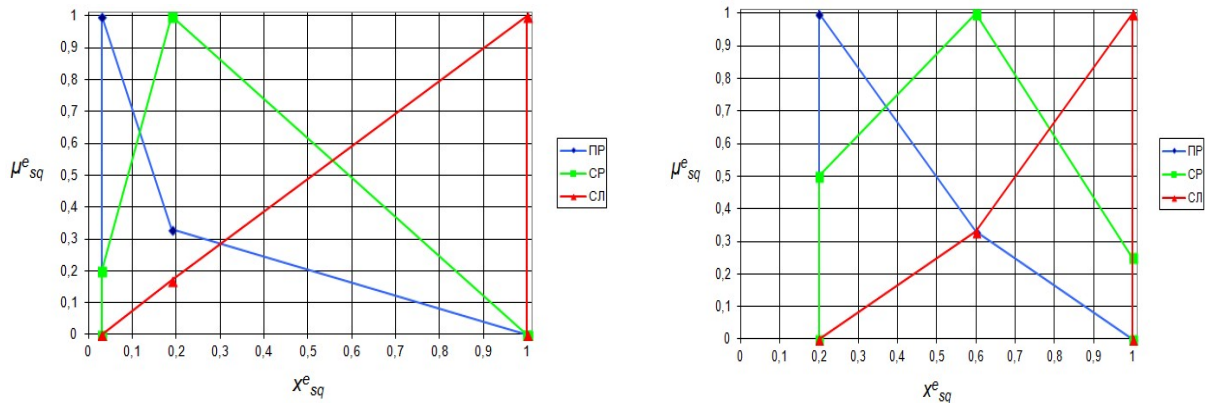
where: the members of a subset $\mathbf{T}_{DTK\Pi\Pi}^e = - \underline{PP}_{DTK\Pi\Pi 1}^e, \underline{CP}_{DTK\Pi\Pi 2}^e, \underline{CJ}_{DTK\Pi\Pi 3}^e$; $\mathbf{T}_{DTKCD}^e = - \underline{OG}_{DTKCD 1}^e, \underline{PM}_{DTKCD 2}^e, \underline{PP}_{DTKCD 3}^e$; $\mathbf{T}_{DTK\Pi}^e = - \underline{OG}_{DTK\Pi 1}^e, \underline{PM}_{DTK\Pi 2}^e, \underline{PP}_{DTK\Pi 3}^e$; $\mathbf{T}_{DTK\Pi}^e = - \left\{ \underline{H}_{DTK\Pi 1}^e, \underline{CP}_{DTK\Pi 2}^e, \underline{B}_{DTK\Pi 3}^e \right\}$ are standard FN. Next, let convert the fuzzy terms $\underline{PP}_{DTK\Pi\Pi 1}^e, \underline{CP}_{DTK\Pi\Pi 2}^e, \underline{CJ}_{DTK\Pi\Pi 3}^e$ in such a way, that for all $\underline{T}_{DTK\Pi\Pi s}^e$ the relation order is fair, i.e. $\forall x_{DTK\Pi\Pi s q} : x_{DTK\Pi\Pi s q} < x_{DTK\Pi\Pi s q+1}$, ($q = \overline{1,3}$) (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 $\underline{PP}_{DTK\Pi\Pi 1}^e$ it is $x_{DTK\Pi\Pi 1} < x_{DTK\Pi\Pi 2} < x_{DTK\Pi\Pi 3} = 0,03 < 0,19 < 1$. Also, the relation for all other given standard FN will be similarly true.

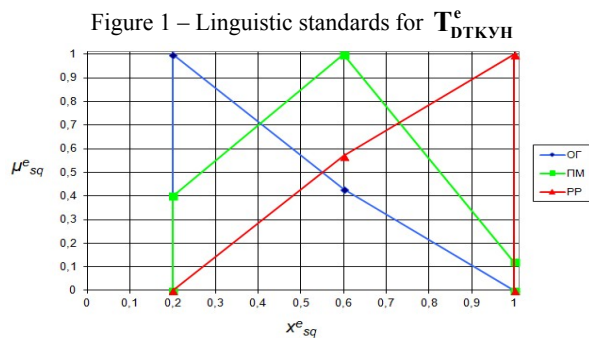
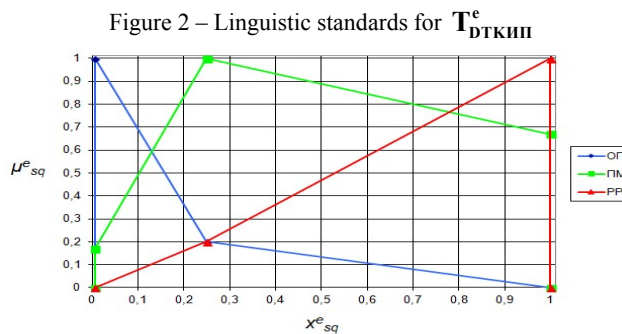
Further, according to the step 2 of the stage 5 in [21,22] we will carry out the absorption procedure for each $\underline{T}_{DTK\Pi\Pi s}^e$. Since the condition U_1 and U_2 is not satisfied for any of FN, the absorption operation is not carried out. Therefore, the standard FN will remain unchanged, and the formed intermediate terms will have the form: $\underline{T}'_{DTK\Pi\Pi 1} = \underline{T}_{DTK\Pi\Pi 1} = \underline{PP}_{DTK\Pi\Pi 1} = \{1 / 0,03; 0,33 / 0,19; 0 / 1\}$; $\underline{T}'_{DTK\Pi\Pi 2} = \underline{T}_{DTK\Pi\Pi 2} = \underline{CP}_{DTK\Pi\Pi 2} = \{0,2 / 0,03; 1 / 0,19; 0 / 1\}$; $\underline{T}'_{DTK\Pi\Pi 3} = \underline{T}_{DTK\Pi\Pi 3} = \underline{CJ}_{DTK\Pi\Pi 3} = \{0 / 0,03; 0,17 / 0,19; 1 / 1\}$. 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 $\underline{PP}_{DTK\Pi\Pi 1}^e \exists \underline{T}_{DTK\Pi\Pi 1}^e : \{0 / x_{DTK\Pi\Pi 1}^{min}\} \in \emptyset$ (i.e. $\mu_{DTK\Pi\Pi 1} = 1 \neq 0$), and for $\underline{CJ}_{DTK\Pi\Pi 3}^e \exists \underline{T}_{DTK\Pi\Pi 3}^e : \{0 / x_{DTK\Pi\Pi 3}^{max}\} \in \emptyset$ (i.e. $\mu_{DTK\Pi\Pi 3} = 1 \neq 0$), then the formation of the subsets $\underline{T}_{DTK\Pi\Pi 1}^e$ and $\underline{T}_{DTK\Pi\Pi 3}^e$ will be carried out by expanding $\underline{T}_{DTK\Pi\Pi 1}^e$ and

$T_{\sim_{DTKVH3}}^e$ (see (28) in [21]) through the introduction of additional $\mu_{DTKVH1\beta-1} / x_{DTKVH1\beta-1} = 0 / 0,03$, and $\mu_{DTKVH3r_j-\gamma+2} / x_{DTKVH3r_j-\gamma+2} = 0 / 1$ 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 $\widetilde{PP}^e_{DTKVHI}$ will have the following form $T'_{\sim_{DTKVHs}} = \widetilde{PP}'_{DTKVHI} = \{ \mu_{DTKVH1} / x_{DTKVH1}, \mu_{DTKVH2} / x_{DTKVH2}, \mu_{DTKVH3} / x_{DTKVH3}, \mu_{DTKVH4} / x_{DTKVH4} \} = \{ 0 / 0,03; 1 / 0,03; 0,33 / 0,19; 0 / 1 \}$, where $\mu_{DTKVH1\beta-1} = 0$. In a simil arway, weobtain intermediate terms for $\widetilde{CP}^e_{DTKIII2}$ and $\widetilde{CJ}^e_{DTKVH3}$, where $\mu_{DTKVH2\beta-1} = \mu_{DTKVH3r_j-\gamma+2} = 0$. Thus, the components of the subset of standards $T^e_{\sim_{DTKVHI}}$ according to (29) in [21] will be defined as $\mu^e_{DTKVH1} / x^e_{DTKVH1} = 0 / 0,03$, $\mu^e_{DTKVH2} / x^e_{DTKVH2} = 1 / 0,03$, $\mu^e_{DTKVH3} / x^e_{DTKVH3} = 0,33 / 0,19$, $\mu^e_{DTKVH4} / x^e_{DTKVH4} = 0 / 1$ and similarly for $T^e_{\sim_{DTKVH2}}$, $T^e_{\sim_{DTKVH3}}$.

Then according to (29) in [21] for \widetilde{PP}'_{DTKVHI} , \widetilde{CP}'_{DTKVH2} , \widetilde{CJ}'_{DTKVH3} let form the standard values, i.e.:
 $T^e_{\sim_{DTKVHI}} = \widetilde{PP}^e_{DTKVHI} = \{ 0 / 0,03; 1 / 0,03; 0,33 / 0,19; 0 / 1 \}$; $T^e_{\sim_{DTKVH2}} = \widetilde{CP}^e_{DTKVH2} = \{ 0 / 0,03; 0,2 / 0,03; 1 / 0,19; 0 / 1 \}$; $T^e_{\sim_{DTKVH3}} = \widetilde{CJ}^e_{DTKVH3} = \{ 0 / 0,03; 0,17 / 0,19; 1 / 1; 0 / 1 \}$. Also, by analogy, the following standard values are formed: $T^e_{\sim_{DTKIII1}} = \widetilde{PP}^e_{DTKIII1} = \{ 0 / 0,2; 1 / 0,2; 0,33 / 0,6; 0 / 1 \}$; $T^e_{\sim_{DTKIII2}} = \widetilde{CP}^e_{DTKIII2} = \{ 0 / 0,2; 0,5 / 0,2; 1 / 0,6; 0,25 / 1; 0 / 1 \}$; $T^e_{\sim_{DTKIII3}} = \widetilde{CJ}^e_{DTKIII3} = \{ 0 / 0,2; 0,33 / 0,6; 1 / 1; 0 / 1 \}$; $T^e_{\sim_{DTKCD1}} = \widetilde{OJ}^e_{DTKCD1} = \{ 0 / 0,2; 1 / 0,2; 0,43 / 0,6; 0 / 1 \}$; $T^e_{\sim_{DTKCD2}} = \widetilde{PM}^e_{DTKCD2} = \{ 0 / 0,2; 0,4 / 0,2; 1 / 0,6; 0,12 / 1; 0 / 1 \}$; $T^e_{\sim_{DTKCD3}} = \widetilde{PP}^e_{DTKCD3} = \{ 0 / 0,2; 0,57 / 0,6; 1 / 1; 0 / 1 \}$; $T^e_{\sim_{DTKPI1}} = \widetilde{OJ}^e_{DTKPI1} = \{ 0 / 0,006; 1 / 0,006; 0,2 / 0,25; 0 / 1 \}$; $T^e_{\sim_{DTKPI2}} = \widetilde{PM}^e_{DTKPI2} = \{ 0 / 0,006; 0,17 / 0,006; 1 / 0,25; 0,67 / 1; 0 / 1 \}$; $T^e_{\sim_{DTKPI3}} = \widetilde{PP}^e_{DTKPI3} = \{ 0 / 0,006; 0,2 / 0,25; 1 / 1; 0 / 1 \}$, $T^e_{\sim_{DTKII1}} = \widetilde{H}^e_{DTKII1} = \{ 0 / 0,05; 1 / 0,05; 0,17 / 0,1; 0 / 1 \}$; $T^e_{\sim_{DTKII2}} = \widetilde{CP}^e_{DTKII2} = \{ 0 / 0,05; 0,14 / 0,05; 1 / 0,1; 0,25 / 1; 0 / 1 \}$; $T^e_{\sim_{DTKII3}} = \widetilde{B}^e_{DTKII3} = \{ 0 / 0,05; 0,17 / 0,1; 1 / 1; 0 / 1 \}$.

The visualization of standard FN. Stage 6 – the visualization of standard FN. For a subset of standards T^e_{DTKVH} , T^e_{DTKIII} , T^e_{DTKCD} , T^e_{DTKPI} and T^e_{DTKII} 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 3 – Linguistic standards for T_{DTKCD}^e Figure 4 – Linguistic standards for T_{DTKHP}^e

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. Жумангалиева¹, А. А. Досжанова², А. А. Корченко³,
С. В. Казмирчук³, Ж. Авкурова⁴, Д. Д. Жаксыгулова⁵

¹Satbayev University, Алматы, Қазақстан;

²Алматы Энергетика және байланыс университеті, Алматы, Қазақстан;

³Ұлттық авиациялық университет, Украина, Киев;

⁴Л. Н. Гумилев атындағы Еуразия ұлттық университеті, Нұр-Сұлтан, Қазақстан;

⁵Семей 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.

Honeyrot 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. Жумангалиева¹, А. А. Досжанова², А. А. Корченко³,
С. В. Казмирчук³, Ж. Авкурова⁴, Д. Д. Жаксыгулова⁵

¹Satbayev University, Алматы, Қазақстан;

²Алматинский университет энергетика и связи, Қазақстан;

³Национальный авиационный университет, Украина, Киев;

⁴Евразийский национальный университет им. Л. Н. Гумилева, Нур-Султан, Қазақстан;

⁵Государственный университет им. Шакарима города Семей, Қазақстан

СПОСОБ ФОРМИРОВАНИЯ ЛИНГВИСТИЧЕСКИХ ПЕРЕМЕННЫХ СТАНДАРТОВ ДЛЯ КЛАССИФИКАЦИИ HONEYROT

Аннотация. В настоящее время одна из важных областей, которая развивается в области информационной безопасности, связана с использованием Honeyrot (виртуальные приманки, онлайн-ловушки), а также выбором критериев для определения наиболее эффективного Honeyrot и их дальнейшей классификации. Представлены основные продукты, в которых реализована технология виртуальных приманок. Honeyrot 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 Honeyrot. Для этой цели были предложены критерии, которые характеризуют онлайн-ловушки, с помощью которых был разработан метод формирования стандартов языковых переменных для выбора наиболее эффективного Honeyrot. Метод основан на формировании набора Honeyrot, подмножеств характеристик и значений идентификаторов лингвистических оценок характеристик Honeyrot, 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. Honeyrot 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 медоносных 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 intrusion detection for networks / M. Roesch. LISA'99 Systems Administration Conference, 1999.
- [10] LaBrea: «Sticky» Honeypot and 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 // Zahistinformacii, 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] Honeypots lure on a hacker. [Electr. resource] - Access mode: <https://docplayer.ru/54222428-Honeypots-primanka-nahakera.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 in computer 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, Kiev, 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., Zhumangaliyeva 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, Klos-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>

**Publication Ethics and Publication Malpractice
in the journals of the National Academy of Sciences of the Republic of Kazakhstan**

For information on Ethics in publishing and Ethical guidelines for journal publication see <http://www.elsevier.com/publishingethics> and <http://www.elsevier.com/journal-authors/ethics>.

Submission of an article to the National Academy of Sciences of the Republic of Kazakhstan implies that the described work has not been published previously (except in the form of an abstract or as part of a published lecture or academic thesis or as an electronic preprint, see <http://www.elsevier.com/postingpolicy>), that it is not under consideration for publication elsewhere, that its publication is approved by all authors and tacitly or explicitly by the responsible authorities where the work was carried out, and that, if accepted, it will not be published elsewhere in the same form, in English or in any other language, including electronically without the written consent of the copyright-holder. In particular, translations into English of papers already published in another language are not accepted.

No other forms of scientific misconduct are allowed, such as plagiarism, falsification, fraudulent data, incorrect interpretation of other works, incorrect citations, etc. The National Academy of Sciences of the Republic of Kazakhstan follows the Code of Conduct of the Committee on Publication Ethics (COPE), and follows the COPE Flowcharts for Resolving Cases of Suspected Misconduct (http://publicationethics.org/files/u2/New_Code.pdf). To verify originality, your article may be checked by the Cross Check originality detection service <http://www.elsevier.com/editors/plagdetect>.

The authors are obliged to participate in peer review process and be ready to provide corrections, clarifications, retractions and apologies when needed. All authors of a paper should have significantly contributed to the research.

The reviewers should provide objective judgments and should point out relevant published works which are not yet cited. Reviewed articles should be treated confidentially. The reviewers will be chosen in such a way that there is no conflict of interests with respect to the research, the authors and/or the research funders.

The editors have complete responsibility and authority to reject or accept a paper, and they will only accept a paper when reasonably certain. They will preserve anonymity of reviewers and promote publication of corrections, clarifications, retractions and apologies when needed. The acceptance of a paper automatically implies the copyright transfer to the National Academy of Sciences of the Republic of Kazakhstan.

The Editorial Board of the National Academy of Sciences of the Republic of Kazakhstan will monitor and safeguard publishing ethics.

Правила оформления статьи для публикации в журнале смотреть на сайте:

www.nauka-nanrk.kz

ISSN 2518-1467 (Online), ISSN 1991-3494 (Print)

<http://www.bulletin-science.kz/index.php/en/>

Редакторы *М. С. Ахметова, Д. С. Аленов, А. Ахметова*
Верстка на компьютере *Д. А. Абдрахимовой*

Подписано в печать 14.10.2020.
Формат 60x881/8. Бумага офсетная. Печать – ризограф.
21 п.л. Тираж 500. Заказ 5.