ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫ
әл-Фараби атындағы Қазақ ұлттық университетінің

ХАБАРЛАРЫ

ИЗВЕСТИЯ

НАЦИОНАЛЬНОЙ АКАДЕМИИ НАУК
РЕСПУБЛИКИ КАЗАХСТАН
Казахский национальный университет
имени аль-Фараби

NEWS

OF THE ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN
al-Farabi Kazakh National University

SERIES
PHYSICO-MATHEMATICAL

1 (341)

JANUARY – MARCH 2022

PUBLISHED SINCE JANUARY 1963

PUBLISHED 4 TIMES A YEAR

ALMATY, NAS RK

NAS RK is pleased to announce that News of NAS RK. Series physico-mathematical 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 News of NAS RK. Series of chemistry and technologies in the Emerging Sources Citation Index demonstrates our dedication to providing the most relevant and influential content of chemical sciences to our community.

Қазақстан Республикасы Ұлттық ғылым академиясы «ҚР ҰҒА Хабарлары. Физика және информатика сериясы» 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. Webof Science зерттеушілер, авторлар, баспашылар мен мекемелерге контент тереңдігі мен сапасын усынады. ҚР ҰҒА Хабарлары. Химия және технология сериясы Emerging Sources Citation Index-ке енуі біздің қоғамдастық үшін ең өзекті және беделді химиялық ғылымдар бойынша контентке адалдығымызды білдіреді.

НАН РК сообщает, что научный журнал «Известия НАН РК. Серия физика и информационные технологии» 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 Известия НАН РК в Emerging Sources Citation Index демонстрирует нашу приверженность к наиболее актуальному и влиятельному контенту по химическим наукам для нашего сообщества.

«ҚР ҰҒА Хабарлары. Физика-математикалық сериясы».
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

Меншіктеуші: «Қазақстан Республикасының Ұлттық ғылым академиясы» РҚБ (Алматы қ.). Қазақстан Республикасының Ақпарат және қоғамдық даму министрлігінің Ақпарат комитетінде 14.02.2018 ж. берілген **No 16906-Ж** мерзімдік басылым тіркеуіне қойылу туралы куәлік.
Тақырыптық бағыты: *физика және ақпараттық коммуникациялық технологиялар сериясы.*
Қазіргі уақытта: *«ақпараттық технологиялар»бағыты бойынша ҚР БҒМ БҒСБК ұсынған журналдар тізіміне енді.*
Мерзімділігі: *жылына 4 рет.*
Тиражы: *300 дана.*
Редакцияның мекен-жайы: *050010, Алматы қ., Шевченко көш., 28, 219 бөл., тел.: 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

Типографияның мекен-жайы: «Аруна» ЖК, Алматы қ., Мұратбаев көш., 75.

«Известия НАН РК. Серия физика-математическая».
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

Собственник: *Республиканское общественное объединение «Национальная академия наук Республики Казахстан» (г. Алматы).*
Свидетельство о постановке на учет периодического печатного издания в Комитете информации Министерства информации и общественного развития Республики Казахстан **No 16906-Ж** выданное 14.02.2018 г.
Тематическая направленность: *серия физика и информационные коммуникационные технологии.*
В настоящее время: *вошел в список журналов, рекомендованных ККСОН МОН РК по направлению «информационные коммуникационные технологии».*
Периодичность: *4 раз в год.*
Тираж: *300 экземпляров.*
Адрес редакции: *050010, г. Алматы, ул. Шевченко, 28, оф. 219, тел.: 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

Адрес типографии: ИП «Аруна», г. Алматы, ул. Муратбаева, 75.

News of the National Academy of Sciences of the Republic of Kazakhstan.
Series physico-mathematical.
ISSN 2518-1726 (Online),
ISSN 1991-346X (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 Social Development of the Republic of Kazakhstan **No. 16906-Ж,** issued 14.02.2018
Thematic scope: *series physics and information technology.*
Currently: *included in the list of journals recommended by the CCSES MES RK in the direction of «information and communication technologies».*
Periodicity: *4 times a year.*
Circulation: *300 copies.*
Editorial address: *28, Shevchenko str., of. 219, Almaty, 050010, tel. 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

Address of printing house: ST «Aruna», 75, Muratbayev str, Almaty.

NEWS
OF THE NATIONAL ACADEMY OF SCIENCES OF THE REPUBLIC OF KAZAKHSTAN
PHYSICO-MATHEMATICAL SERIES
ISSN 1991-346X
Volume 1, Number 341 (2022), 17–25 https://doi.org/10.32014/2022.2518-1726.112

IRSTI 81.93.29
UDC 621.39:004.05

Zh. Avkurova[1]*, B. Abduraimova[2], S. Gnatyuk[3], L.M. Kydyralina[4]

[1]Karaganda Industrial University, Temirtau, Kazakhstan;
[2]L.N. Gumilyov, Nur-Sultan, Kazakhstan;
[3]National Aviation University, Kyiv, Ukraine;
[4]NAO "ShakarimUniversity in Semey", Semey, Kazakhstan.
E-mail: *zhadyra.avkurova.83@mail.ru*

MODEL OF PARA METERS FOR EARLY DETECTION OF APT ATTACKS AND IDENTIFICATION OF SECURITY INTRUDERS IN CYBERSPACE

Abstract. Detection of attacks in information and communication systems and networks is an important and complex task in the field of information security. It is especially important to effectively identify threats to the critical infrastructure of the state. There are many approaches that are based either on signature analysis or anomaly detection. But there is no universal approach for early detection of targeted attacks and identification of violators, since the nature of cyberspace is heterogeneous and poorly formalized - not all parameters of cyberspace can be measured quantitatively and monitor their change over a certain period of time. In this regard, the article developed a model of host and network parameters, the processing of which will make it possible to detect an ART attack in cyberspace at an early stage. In addition, the model allows you to develop a system for determining the category of the intruder, and this will make it possible to predict the nature of the intruder's actions, potential targets in the system and possible damage. Also, the article provides an abstract model of the violator, which will allow classifying potential violators for a more detailed formalization of their actions in relation to the object of protection. The next step is to develop a system of decision rules based on clear and fuzzy logic. The results obtained are important in the context of the further creation of a modern system for detecting and preventing intrusions in information and communication systems and networks.

Key words: information security, cracker bot, host parameters, intruder identification, APT attack detection, targeted attacks, cyberspace monitoring.

Ж.С. Авкурова[1*], Б.К. Абдураимова[2], Б. Гнатюк[3], Л.М. Қыдыралина[4]

[1]Қарағанды индустриялық университеті, Теміртау, Қазақстан;
[2]Л.Н.Гумилев Атындағы ЕҰУ, Нұрсұлтан, Қазақстан;
[3]Ұлттық авиация университеті, Киев, Украина;
4»Семей қаласының Шәкәрім атындағы университеті», Семей, Қазақстан.
E-mail: *zhadyra.avkurova.83@mail.ru*

АРТ-ШАБУЫЛДАРДЫ ЕРТЕ АНЫҚТАУҒА ЖӘНЕ КИБЕРКЕҢІСТІКТЕГІ ҚАУІПСІЗДІК БҰЗУШЫЛАРЫН АНЫҚТАУҒА АРНАЛҒАН ПАРАМЕТРЛЕР МОДЕЛІ

Аннотация. Ақпараттық-коммуникациялық жүйелер мен желілердегі шабуылдарды анықтау ақпараттық қауіпсіздік саласындағы маңызды және күрделі міндет болып табылады. Мемлекеттің сындарлы инфрақұрылымы объектілеріне төнетін қауіптерді тиімді анықтау аса маңызды. Қолтаңбаны талдауға немесе ауытқуларды анықтауға негізделген көптеген тәсілдер бар. Бірақ мақсатты шабуылдарды ерте анықтаудың және бұзушыларды анықтау үшін әмбебап тәсіл жоқ, өйткені киберкеңістіктің табиғаты гетерогенді және нашар рәсімделген - киберкеңістіктің барлық

параметрлерін сандық түрде өлшеуге және олардың өзгеруін белгілі бір уақыт аралығында бақылауға болмайды. Осыған байланысты мақалада киберкеңістіктегі APT-шабуылды ерте кезеңде анықтауға мүмкіндік беретін хост және желі параметрлерінің моделі әзірленді. Сонымен қатар, модель бұзушының санатын анықтау үшін жүйені құруға мүмкіндік береді, бұл бұзушының іс-әрекетінің сипатын, жүйеде ықтимал мақсаттарды және ықтимал залалды болжауға мүмкіндік береді. Сондай-ақ, мақалада құқық бұзушының дерексіз моделі келтірілген, бұл қорғаныс объектісіне қатысты олардың әрекеттерін егжей-тегжейлі ресімдеу үшін ықтимал құқық бұзушыларды жіктеуге мүмкіндік береді. Келесі қадам-нақты және анық емес логика негізінде шешуші ережелер жүйесін дамыту. Алынған нәтижелер ақпараттық-коммуникациялық жүйелер мен желілердегі шабуылдарды анықтау және алдын-алудың заманауи жүйесін одан әрі құру тұрғысынан маңызды болып табылады.

Түйін сөздер: ақпараттық қауіпсіздік, крекер-бот, хост параметрлері, зиянкестерді анықтау, APT шабуылын анықтау, мақсатты шабуылдар, киберкеңістік мониторингі.

Ж.С.Авкурова[1*], Б.К. Абдураимова[2], С. Гнатюк[3], Л.М. Кыдыралина[4]

[1]Карагандинский индустрияльный университет, Темиртау, Казахстан;
[2]ЕНУ им.Л.Н.Гумилева, Нур-Султан, Казахстан;
[3]Национальный авиационный университет, Киев, Украина;
[4]НАО «Университет имени Шакарима города Семей», Семей, Казахстан.
E-mail: *zhadyra.avkurova.83@mail.ru*

МОДЕЛЬ ПАРАМЕТРОВ ДЛЯ РАННЕГО ВЫЯВЛЕНИЯ APT-АТАК И ИДЕНТИФИКАЦИИ НАРУШИТЕЛЕЙ БЕЗОПАСНОСТИ В КИБЕРПРОСТРАНСТВЕ

Аннотация. Выявление атак в информационно-коммуникационных системах и сетях является важной и сложной задачей в области информационной безопасности. Особенно важно эффективно выявлять угрозы объектам критической инфраструктуры государства. Существует много подходов, которые базируются или на сигнатурном анализе, или же на выявлении аномалий. Но не существует универсального подхода для раннего выявления целевых атак и идентификации нарушителей, так как природа киберпространства является неоднородной и слабоформализованной - не все параметры киберпространства можно измерить количественно и мониторить их изменение на протяжении некоторого периода времени. В связи с этим, в статье разработана модель хостовых и сетевых параметров, обработка которых позволит выявить на ранней стадии APT-атаку в киберпространстве. Кроме этого, модель позволить разработать систему для определения категории нарушителя, а это даст возможность прогнозировать характер действий нарушителя, потенциальные цели в системе и возможный ущерб. Также в статье приведена абстрактная модель нарушителя, что позволит классифицировать потенциальных нарушителей для более детальной формализации их действий по отношению к объекту защиты. Следующим шагом является разработка системы решающих правил на базе четкой и нечеткой логики. Полученные результаты важны в контексте дальнейшего создания современной системы выявления и предотвращения вторжений в информационно-коммуникационных системах и сетях.

Ключевые слова: информационная безопасности, бот-взломщик, хостовые параметры, идентификации нарушителей, выявления APT-атак, целевые атаки, мониторинг киберпространства.

Introduction. The development of information technologies gives rise to new types of information security threats, among which the intrusion into computer systems and networks occupies the main place. To effectively counter this threat, early detection systems and intruder detection systems (IDS) are being developed, which make it possible to reveal the fact of an intrusion into the system and to identify it. Many of these modern systems use honeypot technology [1]. Particularly relevant is the early detection of targeted attacks (APT), the task of which is to detect important information on the user's device and use it in the interests of intruders (cybercriminals).

Research analysis and problem statement. A typical IDS should perform the following main functions [2]: monitor and analyze the activity of IS users; fix system configurations and vulnerabilities; evaluate the integrity of critical system files and data files; recognize patterns of activity that reflect known attacks; conduct statistical analysis to detect abnormal behavior; recognize violations of the security policy by the

user of the system. The tasks that are solved by the IDS can be divided into global and local. Global tasks - recognition of an intruder (Hp) and a legitimate user - the solution of this problem includes the following stages [2-4]: data collection, filtering, behavior classification - the process of Hp recognition itself, a report and system response. As can be seen from the main functions and tasks of the IDS, one of the most important aspects of their functioning is not only fixing the fact of violation of IS protection, but also its recognition (identification) - this will help to more effectively respond to the incident and to implement the appropriate countermeasures. The aim of the work is to develop a model of parameters for detecting APT attacks and identifying intruders.

The main part of the research. Under Hp, in general, it is possible to consider a person or a group of persons who, as a result of intentional or unintentional actions, ensure the implementation of information security threats. In [5] the following definition is given - this is a subject whose actions violate the security of information in a computer system. In each specific case, based on the information processing technology, it is necessary to develop a model of Hp, which should be adequate to the real Hp for this IS. Hp model is an abstract formalized or non-formalized description of Hp's actions, which reflects its practical and theoretical capabilities, a priori knowledge, time and place of action, etc. Hp model should determine the possible aim of Hp and its gradation according to the degree of danger to IS, the category of persons, from which there may be Hp, assumptions about the qualifications of Hp, assumptions about the nature of his actions. Regarding IS, Hp can be internal (from among IS personnel) or external (unauthorized persons). There are three main motives of Hp: irresponsibility, selfish interest, self-affirmation. All Hp can be classified as follows: according to the level of knowledge about IS, according to the level of possibilities (used by the method and means), according to the time of action, according to the place of action, etc. However, for effective identification of Hp, the IDS must «know» a set of key parameters. Let us define the main parameters, the changes of which must be monitored for effective identification of Hp, based on the abstract model of the intruder.

Determining the specific values of the characteristics of possible Hp is largely subjective. The HP model, created taking into account the peculiarities of a specific subject area and information processing technology, can be represented by listing several options for its type. Each type of Hp must be characterized by the values of the parameters given above. As the analysis of the models of potential actions of Hp in IS has shown [3-8], Hp can be classified according to the following criteria:

1. Regarding IS: a) internal, including system users, personnel serving technical facilities, managers of various levels of the job hierarchy, employees of the software development and maintenance department, technical personnel serving the premises; b) external, which include representatives of organizations interacting on the life support of the institution, representatives of competing institutions or persons acting on their instructions, visitors, persons who accidentally or intentionally violate the access control, any persons outside the controlled area, and etc.

2. According to the reasons of intrusion: a) irresponsibility of the person; i) persons with a selfish interest; c) persons seeking to assert themselves.

3. According to the level of knowledge about IS: a) knows the functional features of the system; b) has a high level of knowledge in the field of programming, design and operation of the system; c) has a high level of knowledge and experience with the technical means of the system.

4. According to the time of action: a) during the functioning of the system; b) during the period of inactivity of the system components; c) both during the functioning of the system and during the period of inactivity of the system components.

5. According to the level of capabilities: a) using undercover methods of mastering information; b) using passive means; c) using only standard means and disadvantages of the security system to overcome it; d) using methods and means of active influence.

6. According to the place of action: a) without access to the controlled area; b) from a controlled area without access to the premises; c) indoors, but without access to the technical means of the system; d) from the workstations of the end users of the system; e) with access to the data zone; f) with access to the system security control area.

In general, in the context of this work, it is advisable to divide Hp into classes, and those, in turn, will be divided into categories. Based on the nature of Hp itself, it is worth highlighting both main classes: Hp-man (HpM) and Hp-robot (or Hp-bot, HpB). According to the capabilities, motives and nature of actions, the HpM includes four categories: burglar, cracker, spammer and disinformer. Likewise, HpB has categories such as spam bot and cracker bot. The presentation of these categories within the framework of

the standard intruder model is given in Table. 1. One of the central concepts in the field of Hp information security is a **hacker** (English hacker, from to hack - to hack, shred) - an extremely qualified IT specialist, a person who understands the very depths of computer systems. At first, hackers were called programmers who corrected errors in software in some quick and not always elegant (in the context of the programming style used in the program and its general structure, interface design) or in a professional way. Now hackers are very often identified with computer crackers (English cracker, from to crack - to crack, break), but this use of the word "hacker" is incorrect. Sometimes this term is used to refer to specialists in general - in the context that they possess very detailed knowledge in any matters or have rather non-standard and constructive thinking. Since its inception in the form of a computer term (1960s), it has acquired new, often different meanings. Thus, a hacker is too general concept and the paper proposes to divide it into such categories as burglar and cracker [9].

In this research, the category of **burglar** will be understood as Hp, which, using mainly scripts written with his own hand, breaks the IS protection and violates the confidentiality of information stored in it, mostly without useful purposes. His attack ends at the moment of breaking the IS protection, and in the IS itself, he usually does not make any changes and modifications (unlike a cracker).

Cracker - a type of computer cracker: 1) a person who breaks into security systems (in particular software protection) 2) a person who creates or modifies so-called cracks; 3) a person who breaks into computer games, software, etc. In practice, the general term «computer burglar» or «hacker» is also used, which is also not correct. Crackers deliberately result in crack, in the vast majority of cases the cracker does not have the source code of the program, so the program is studied by a combination of a disassembler and a debugger using special utilities. Crackers' motives are predominantly selfish. In this paper, we will assume that the main difference between a burglar and a cracker is that the cracker makes certain modifications in the system, not limited only to cracking or obtaining the necessary information.

A spammer is an Hp that spreads spam by attacking IS with it. Spam (English spam) - sending commercial and other advertisements or other types of messages (information) to persons who have not expressed a desire to receive them. In addition to mail spam itself, there are other types of attacks that can be carried out in a similar way, namely DoS and DDoS attacks - mass mailing on behalf of another person in order to cause a negative attitude towards him, mailing letters containing computer viruses (for their initial distribution), phishing and the like. Thus, in our classification, the spammer category also includes Hps who organize DoS and DDoS attacks, as well as those involved in computer fraud - phishing (since their methods of constructing attacks are practically the same).

The last category of HpM is a **disinformer** - this is a special type of Hp, which in its characteristics is close to a hacker or cracker, but has one feature - the purpose of his attacks is to violate the integrity and reliability (sometimes availability) of information stored in the IS.

A robot, or a bot, as well as an Internet bot (English bot, abbreviated from English robot) is a special program that performs automatically and (or) according to a given schedule any actions through the same interfaces as a regular user. When discussing computer programs, the term is used primarily in relation to the Internet. Usually bots are designed to do repetitive work as fast as possible (obviously much beyond human capabilities).

Bots are also used in conditions where a better response is required compared to human capabilities (for example, game bots, bots for Internet auctions, etc.) or, less often, for imitating human actions (for example, chat bots, etc.). A harmful manifestation of bots is their use to coordinate network attacks on computers, for example, DDoS and DoS attacks through a botnet. Internet bots can be used for Click fraud. Recently, bots used in games of the MMORPG genre have become massive. Spambots are used to spread information (usually advertising content) across various network resources.

Categories in the standard Hp model — Table 1

Category	Regarding IS	Motive	Knowledge level	Opportunity level	Time of action	Place of action
Burglar	External	Self-affirmation	Possess a high level of knowledge in the field of computing and programming, design and operation of IS	Use methods and means of active influence on IS	Both during the functioning of the IS, and during the period of activity of the components of the IS	Without gaining access to the controlled territory of the organization
Cracker	External / Internal	Selfish motive				
Spammer	External	Selfish motive	Possess information about the functional features of the IS, know how to use standard tools			
Disinformer	External / Internal	Selfish motive				

Let us distinguish both categories in this class: spam-bots and burglar-bots.

Spam-bots are similar to the spammer's HpM, but perform their actions automatically. The main harmful actions of bots in this category are spam-bots that collect E-mail addresses from contact forms and guest books; programs that loaded the Internet channel with a stream of unnecessary information (usually of an advertising nature); sites that collect information on harmless sites for use in automatically generated doorways (special HTML pages designed for high positioning in search engines for a specific keyword) DoS and DDoS attacks, etc.

The second category includes **botnets** and **zombie computers**. In essence, they contain the characteristics of hackers and crackers, and are organized in a completely automatic manner. A botnet (English botnet, comes from the words robot and network) is a computer network consisting of a number of hosts running bots - autonomous software. Most often, a bot as part of a botnet is a program that is secretly installed on a victim's device and allows an attacker to perform certain actions using the resources of an infected computer. They are usually used for illegal activities - sending spam, brute-force attacks on a remote system, DoS attacks, and etc.

To recognize Hp, you need to compare its profile (that is, his activity in IS) with the profile of each of the categories of the general Hp model. The IDES model uses profiles to characterize the expected performance of a computing system. The parameters of the computing system activity used to construct the profile may vary depending on the type of IS activity that is being monitored. Parameters for identification are divided into two types: host (Table 2) and network (Table 3), the characteristics of which are described below. In most cases, the common types of information found in profiles at the host level are [1]:

1) Lognin activity. For a user or a system, profiles can represent the typical number of logins at a specific time period during the day, the earliest expected login time, the estimated maximum login duration, and etc. Practice has shown that such parameters are most typical for most computing operating environments. For example, in some operating environments, it is abnormal for users to login to the system at 4 AM, while in others it may be considered normal.

2) Runtime parameters. Profiles can also be set based on the intended use of the resources that a particular computing system needs to support. These profiles typically include statistics on the use of CPU time, memory, and other resources. This is another parameter that is usually regular and predictable. In a clerical report runtime, for example, a program that is called that takes more than 10 minutes of CPU time should be considered abnormal, while in a scientific operating environment it may be quite normal. The execution parameters in the Hp detection system provide a means of possibly repelling this type of malicious activity.

3) Access to files. You can create profiles for the frequency of reading and writing specific files, the number of times that read or write requests for specific files are denied, and profiles for other file access parameters. This setting may be less predictable, but certain files may be marked as inaccessible to regular users. For example, if a regular user tries to write something to a password file, this could be considered abnormal behavior. In most operating environments, copying a password file should be considered a suspicious activity. Depending on the types of suspected attacks, the following audit methods can be proposed for a IDS host, given in the works of the NIDES system developers [2]:

a) Login audit - collects data about who, when and how logged on to the system. In this case, it is advisable to record: the name of the user logged into the system; the name of the terminal or remote host from which the system was logged in; user login and logout time.

b) process audit - collects data about which system services were used. In this case, it is advisable to record: the conditions for the execution (for example, whether the superuser rights are used) of the process; the return value of the process on termination; username and group name, terminal from which the process is started; process call time; time spent in user mode; time spent in kernel mode; total execution time; average used memory; the number of characters processed; the number of read-written blocks of information; the name of the command to start the process.

4) Audit of errors and administrative information data.

Host parameters

Similarly, our system must monitor certain parameters of the IS activity, that are given in table. 2, fix them and identify Hp.

Host parameters for Hp identification and their characteristics Table 2

Parameter	Fuzziness	HpM				HpB	
		Disinformer	Spammer	Cracker	Hacker	Spam-bot	Burglar-bots
UID	-	+	-	+	+	-	+
Tlog	+	With a certain probability depending on the time of day	-	With a certain probability depending on the time of day	With a certain probability depending on the time of dayv	-	With a certain probability depending on the time of day
Nlog	+	Above average	-	Above average	Above average	-	High
TSlog	+	Above average	-	Above average	Above average	-	Above average
I	+	Within normal limits	Within normal limits	Within normal limits	Within normal limits	Above normal limits	Above normal limits
CPU	+	Above normal limits	Above normal limits	Above normal limits	Above normal limits	Above normal limits	Above normal limits
MUse	+	Above normal limits	Above normal limits	Above normal limits	Above normal limits	Above normal limits	Above normal limits
NEF	+	Not within normal limits	-	Not within normal limits	Not within normal limits	-	Not within normal limits
AtEF	-	Scripts and PHP scripts	PHP- scripts	Executable files	Scripts	PHP- scripts	Scripts
NEr	+	Above normal limits	Above normal limits	Above normal limits	Above normal limits	Above normal limits	Above normal limits
RTPr/F	+	Different from normal time	Different from normal time	Different from normal time	Different from normal time	Different from normal time	Different from normal time
UPr	-	Present	Present	Present	Present	Present	Present
TrFin	-	Present	Present	Present	Mostly absent	Present	Mostly absent
ModF	-	Present	Absent	Present	Mostly present	Absent	Mostly present
TrFout	-	Absent	Absent	Mostly present	Present	Absent	Present
KS	-	Fixed	Fixed	Fixed	Fixed	not fixed	not fixed

Let's consider in more detail the model of the host parameters, which will actually be the basis for further research:

1) Login username (UID). A list of users (logins) who are allowed to use the IS resources (i.e., are authorized) must be defined and stored in the IDS database or honeypot, on the basis of which this system is created. Any other usernames that are not included in this list are considered unauthorized and their appearance indicates an unauthorized entry into the system. This parameter is clear since the occurrence of an unusual login clearly indicates Hp. However, spammers, spam bots and bloodhound bots usually do not require authorization in the system, and therefore it is mostly impossible to determine the fact of penetration into the system by this parameter.

2) Login time (Tlog). The parameter is based on the fact that the activity of the IS and users of these systems depends on the time of day. Usually, a lot of user activity when logging into the system is manifested in the daytime, less - at night, but other statistics are possible, which is determined by the mode of operation of the organization to which the IS belong. The nature of this parameter is unclear, because it is impossible to unambiguously draw a conclusion about the illegal activity of Hp. So in organizations with a working time from 08:00 to 16:00, the probability that a user who logged in is Hp is the lowest at 08:00 and increases over time, reaching a maximum in hours after 16:00. However, it should be noted that in the concept of honeypot technologies, this parameter loses its weight somewhat, since any activity on them is considered malicious.

3) Frequency of login requests (Nlog). It is clear that a high frequency of login requests will be observed when the system is attacked by bots (in particular, burglar bots, since spammers do not require login). HpM is also distinguished by an increased frequency of requests as a result of attempts to bypass the protection and the theoretical assumption that it does not have a legitimate username and password, so it will have to make at least several attempts. Moreover, the greater the number of attempts, the more probability that Hp is really trying to enter the IS. It is clear that this parameter is also fuzzy.

4) Time spent on logging in (TSlog). A parameter that is closely related to the previous one. The time spent by Hp is, in most cases, longer than the time spent by the legitimate user. But it is indistinct, since it does not allow for an unambiguous identification.

5) Intensity of action (I). It means the number of any user actions, including logging in/out of the system, transferring, modifying, copying files, starting/stopping processes, etc. per unit of time. The intensity may not differ in HpM and in a legitimate user, however, in bots it is much higher, therefore, it is most essential for identifying and distinguishing between human-robot categories. Although a significant excess of the norm indicates the activity of unauthorized automatic systems-Hp (bots), however, I is an indistinct parameter, since the normal value of the intensity indicator is very difficult to determine.

6) Processor time / processor load (CPU). Since the number of active processes on honeypot systems should be minimal, any increase in load is a sign of Hp activity in the system. In real ISs, the probability that the activity caused by Hp is somewhat lower, and, of course, the normal value of the processor time is higher. However, this parameter can still be effectively used to identify the fact of a violation in intrusion detection and sleep detection systems. Since it is impossible to give an unambiguous answer about Hp for this parameter, primarily due to the possible activity of viruses, the processor CPU is an indistinct parameter.

7) The amount of loaded RAM (MUse). Similar in content to the previous one and also fuzzy.

8) Number of executable files (NEF). Also included in the group of fuzzy parameters. The fact of an attacker's actions on this parameter is determined by a deviation from the norm. So, in each organization, in accordance with the security policy and job responsibilities, each legitimate user can use certain files at a given moment, and the simultaneous use of several files at once is practically excluded. This allows to identify both external and internal Hp, but with a certain probability.

9) The type of files used during the attack (AtEF). If a recently changed or created file was noticed, which is identified as a script, then we are dealing with a hacker, a person who is highly computer literate and capable of further breaking systems with the help of the script we discovered. If the seen file is an executable file, then according to the definition "... the result of the cracker's work is ... a modified ("cracked" or "broken") program with the required functionality" we can judge that the person who broke the server's protection is a cracker. Finally, the case when we find a PHP script clearly speaks of a hacker working on the Internet. According to modern research, the largest number among the considered categories of cybercriminals, DDoS attackers and spammers. The disinformer can use several types of files, mainly scripts and PHP scripts. Since the result of applying the parameter gives an unambiguous answer about the presence of Hp and its class, the parameter is clear.

10) Number of failures and errors (NEr). This option is fuzzy because failures es and errors can occur during both logged in and Hp. However, with frequent repetition of failures or errors, we can conclude with a certain degree of probability that the system has been attacked. This group includes a wide range of events, from authorization errors to failures in the execution of certain processes or files. With the active work of Hp, regardless of its class and category, the failure rate will be slightly higher. It should also be noted that it is quite possible that when determining HpM, this frequency will be even higher.

11) Process/file execution time (RTPr/F). Examining the statistics of the work of IS of various enterprises and organizations, it is easy to notice that, depending on the specifics of the work, the time spent on performing a certain operation is approximately the same for the same type of IS and their tasks. Honeypot systems run primarily system processes, that is, those that keep the honeypot itself running, or administrator processes that run at a specific time for a specific period. Thus, when identifying such processes, it can be concluded that the Hp system was attacked. Since this state of affairs can be caused by the negligence of the employee, the conclusion is ambiguous and, accordingly, the parameter is fuzzy.

12) Unnatural processes (UPr). According to the concept of IDS and honeypot systems in the IS, continuous monitoring of the running processes must be carried out. So, over the course of the system's operation, so-called system snapshots can be formed, recording all activity on the host, or lists of processes and their characteristics that have been launched are created. In the event that an unusual process appears in the operation of the IS, that is, one that has not been launched at all for a long time or has been launched a limited number of times, our IDS immediately notes the fact of the appearance of Hp. Since in this case the probability of correct raising of the alarm is practically equal to «1», the parameter can be classified as clear.

13) Transferring a file to the system (TrFin), modifying files (ModF), copying/transferring files from the system (TrFout) is a group of clear parameters. Any actions with files inherent in each attack, but those

actions that prevail during the attack determine the class and category of Hp. For example, in a spam attack, the transfer of files to the system is usually noted, but their change or transfer from the system is mostly absent. Other categories of Hp are identified similarly.

14) Pressing the keyboard keys (KS). To detect attacks, this technology uses monitoring by pressing the user on the keyboard keys. The basic idea is that the sequence of user clicks sets the attack pattern. The disadvantage of this approach is the lack of a sufficiently reliable mechanism for intercepting work with the keyboard without the support of the operating system, as well as a large number of possible variants of presenting the same attack. In addition, without a semantic keystroke analyzer, various kinds of command aliases can easily destroy this technology. Because it analyzes keystrokes, automated attacks that result from the execution of malicious programs may also go undetected. But this fact is most useful for us in the process of identifying Hp and is attributed to the class of people or robots. This parameter is unambiguous, therefore it is also assigned to the clear group.

Network parameters. Network IDS, presented in table. 3, work with network traffic and detect attacks related to low-level impact on network protocols, and can detect attacks on multiple hosts on the network. Network IDS is created on the basis of an intelligent traffic analyzer that processes each data frame passing through it in order to search for prohibited signatures in it, indicating attacks. Network data, network traffic is received from a network adapter operating in a promiscuous mode (that is, receiving all packets on the network).

Network parameters for Hp identification and their characteristics Table 3

Parameter	Fuzziness	HpM				HpB	
		Disinformer	Spammer	Cracker	Hacker	Spam-bot	Burglar-bot
ARP-request	-	Does not match the allowed	Does not match the allowed	Does not match the allowed	Does not match the allowed	Does not match the allowed	Does not match the allowed
IP-fragmet	-	Does not match the allowed	Does not match the allowed	Does not match the allowed	Does not match the allowed	Does not match the allowed	Does not match the allowed
ICMP-message	-	Does not match the allowed	Does not match the allowed	Does not match the allowed	Does not match the allowed	Does not match the allowed	Does not match the allowed
TCP-packet	-	Does not match the allowed	Does not match the allowed	Does not match the allowed	Does not match the allowed	Does not match the allowed	Does not match the allowed

Let's list the audit data that must be collected to detect remote attacks, with the characteristics of the TCP/IP protocol family [2]:

ARP request is monitored according to the following parameters: source IP address; source hardware address; the network interface that restricts the ARP request.

IP fragment: source address; receiver address; protocol field; offset field; length; header length; MF bit; identification.

ICMP message: source IP address; receiver IP address; ICMP field type; ICMP identifier; ICMP sequence number.

TCP packet: source IP address; receiver IP address; source TCP port; receiver TCP port; bit of TCP code.

All of the listed network parameters, with the correct configuration of the interworking policy, clearly indicate an attack, and therefore belong to the group of clear ones [10]. The parameters described in the work (both network and host) form a tuple of identification and identification of Hp:

DIO = < UID, Tlog, Nlog, TSlog, I, CPU, MUse, NEF, AtEF, NEr, RTPr/F, UPr, TrFin, ModF, TrFout, KS, ARP, IP, ICMP, TCP >.

The value of the elements (or rather, their change) of this tuple allow to reveal the fact of penetration of Hp into the IS (to identify an APT attack), as well as the type of Hp: for HpM - burglar, spammer, disinformer and cracker, and for HpB – burglar-bot and spam-bot. To use this tuple in the process of identifying an intruder, in particular its fuzzy components, it is necessary to construct models of standards of parameters necessary for the functioning of the IDS in a not clear defined, poorly formalized environment, which today is cyberspace.

Conclusions. In this work, a model of parameters (host and network) has been created for early detection of APT attacks and identification of a clear definition of the type of intruder - that is, HpM or HpB). Formalization of such parameters allows us to take into account the peculiarities of attacks on IS and increase the effectiveness of preventive measures, rapid response tools and information protection systems.

The results obtained can serve as a basis for building an effective system for early detection of APT attacks and identification of intruders in cyberspace based on honeypot technology.

In further work, it is planned to construct models of standards and logical rules for detecting using the preset model of parameters for early detection of APT attacks and identification of the type of intruder.

Information about authors:

Avkurova Zhadyra – Karaganda Industrial University, Temirtau, Kazakhstan, *zhadyra.avkurova.83@mail.ru*, *https://orcid.org/0000-0002-2836-0919*;

Abduraimova Bayan – Associate Professor ENU L.N.Gumilyov, Nur-Sultan, Kazakhstan, abduraimova_bk@enu.kz;

Sergiy Gnatyuk – National Aviation University, Kyiv, Ukraine, *sergio.gnatyuk@gmail.com*;

Kydyralina Lazat Muktarovna – NAO "ShakarimUniversity in Semey", Semey, Kazakhstan, *lazat_75@mail.ru*.

REFERENCES

[1] Zh. Avkurova, B. Abduraimova, S. Gnatyuk, A. Gizun / Analysis of modern attack detection systems based on virtual bait technologies // No.6(142) Bulletin of KazNITU, pp. 654-659, November, 2020.

[2] Court S.S. The structure of intruder detection systems [Electronic resource]: article/S.S. Court. - Access mode: http://www.ssl.stu.neva.ru/sam/

[3] Denning D.E. An Intrusion-Detection Model / Dorothy E. Denning // IEEE Transactions On Software Engineering. - February 1987. - Vol. SE-13, No. 2. - P. 222-232.

[4] M. Zaliskyi, R. Odarchenko, Yu. Petrova. A. Chaplits, Method of traffic monitoring for DDoS attacks detection in e-health systems and networks, CEUR Workshop Proceedings, Vol. 2255, pp. 193-204, 2018.

[5] Wang S.S.K. Anomalous payload-based network intrusion detection / S.S.K. Wang // Proceedings of the 7th International Symposium on Recent Advances in Intrusion Detection. - Sophia Antipolis, 2004.

[6] Z. Hassan, R. Odarchenko, A. Zaman, M. Shah, Detection of Distributed Denial of Service Attacks Using Snort Rules in Cloud Computing & Remote Control Systems, Proceedings of the 2018 IEEE 5th International Conference on Methods and Systems of Navigation and Motion Control, October 16-18, 2018. Kyiv, Ukraine, pp. 283-288.

[7] M. Du and K. Wang, «An SDN-Enabled Pseudo-Honeypot Strategy for Distributed Denial of Service Attacks in Industrial Internet of Things,» in IEEE Transactions on Industrial Informatics, vol. 16, no. 1, pp. 648-657, Jan. 2020.

[8] Hacker [Electronic resource]: Encyclopedic Dictionary of the Hacker. - Access mode: http://www.catb.org/ ~esr/jargon/html/H/hacker.html.

[9] Hu Z., Odarchenko R., Gnatyuk S., Zaliskyi M., Chaplits A., Bondar S., Borovik V. Statistical techniques for detecting cyberattacks on computer networks based on an analysis of abnormal traffic behavior, International Journal of Computer Network and Information Security, Volume 12, Issue 6, pp. 1-13, 2020.

[10] Akhmetov B.B., Lakhno V.A., Adranova A.B., Kydyralina L.M., Pliska L.D. Analysis of mathematical models of investment strategies in the university on cyber security systems. //Bulletin of National academy of sciences of the Republic of Kazakhstan.- Almaty. - 2020. – V. 1. – Num. 383 (2020). – P. 128 – 139. https://doi.org/10.32014/2020.2518-1467.16.

[11] Usatova O.A., ZHumabekova A.T., Metson E., Karyukin V.I., Ilesova B.E., Types of threats to information resources and their identification using machine learning methods//newsof the national academy of sciences of the republic of kazakhstanphysico-mathematical seriesissn 1991-346X Volume 6, Number 340 (2021), 48–58 https://doi.org/10.32014/2021.2518-1726.101.

[12] J. Tang, M. Xu, S. Fu and K. Huang, "A scheduling optimization technique based on reuse in spark to defend against apt attack," in Tsinghua Science and Technology, vol. 23, no. 5, pp. 550-560, Oct. 2018, doi: 10.26599/TST.2018.9010022.

[13] Yegneswaran V. An architecture for generating semantic-aware signatures / V. Yegneswaran, J.T. Giffin, S.J. Paul Barford // Proceedings of the 14th USENIX Security Symposium, 2005. – P. 97-112.

[14] Honeypot Technology, Part 1: Purpose of the Honeypot. [Electr. resource] - Access mode: http://www.securitylab.ru/analytics/275420.php.

[15] Honeypot technology. Part 2: Honeypot Classification. [Electr. resource] - Access mode: http://www.securitylab.ru/analytics/275775.php.

[16] Honeypot technology. Part 3: Overview of Existing Honeypots. [Electr. resource] - Access mode: http://www.securitylab.ru/contest/283103.php.

СОДЕРЖАНИЕ

ИНФОРМАТИКА

Ж.С. Абдимуратов, В.И. Дмитриченко, М.А. Джетписов, Е.Н. Жагыпаров
АДАПТАЦИЯ ЗАЩИТЫ РЕЛЕ ЭЛЕКТРОДВИГАТЕЛЯ ПРИ ПРОЕКТИРОВАНИИ ЦИФРОВЫХ ПОДСТАНЦИЙ В РЕСПУБЛИКЕ КАЗАХСТАН. 6

Ж.С. Авкурова, Б.К. Абдураимова, С. Гнатюк, Л.М. Кыдыралина
МОДЕЛЬ ПАРАМЕТРОВ ДЛЯ РАННЕГО ВЫЯВЛЕНИЯ APT-АТАК И ИДЕНТИФИКАЦИИ НАРУШИТЕЛЕЙ БЕЗОПАСНОСТИ В КИБЕРПРОСТРАНСТВЕ. 17

Т.С. Байшоланов, Ж.М. Алимжанова, Н. Байшолан, К.Е. Кубаев, К.С. Байшоланова
ОЦЕНКА СТОЙКОСТИ КРИПТОГРАФИЧЕСКИХ ШИФРОВ С ПОМОЩЬЮ АНАЛИЗА ШИФРТЕКСТОВ.... 26

Ж.С. Есенгалиева, К.Н. Касылкасова, А.О. Касылкасова
АНАЛИЗ МЕДИЦИНСКИХ ПРИЛОЖЕНИЙ, СОЗДАННЫХ СПЕЦИАЛЬНО ДЛЯ БОРЬБЫ С COVID-19. 34

Ж.С. Иксебаева, К. Жетписов, Ж.М. Муратова
РАЗРАБОТКА КОНЦЕПТУАЛЬНОЙ МОДЕЛИ АВТОМАТИЧЕСКОЙ ПРОВЕРКИ ТЕХНИЧЕСКОЙ ДОКУМЕНТАЦИИ. 43

В.А. Лахно, Б.С. Ахметов, М.Б. Ыдырышбаева, Ш. Сагындыкова
ПРИМЕНЕНИЕ СЕТИ БАЙЕСА СО СКРЫТЫМИ ВЕРШИНАМИ В СЕКТОРАЛЬНЫХ СППР ДЛЯ ЗАДАЧ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ. 50

О.Ж. Мамырбаев, Д.О. Оралбекова, К. Алимхан, M. Othman, Б. Жумажанов
ПРИМЕНЕНИЕ ГИБРИДНОЙ ИНТЕГРАЛЬНОЙ МОДЕЛИ ДЛЯ РАСПОЗНАВАНИЯ КАЗАХСКОЙ РЕЧИ. 58

А.Р. Оразаева, Д.А. Тусупов, С.В. Павлов, Г.Б. Абдикеримова
ЭФФЕКТИВНОСТЬ ОБРАБОТКИ БИОМЕДИЦИНСКИХ ИЗОБРАЖЕНИЙ РАКА МОЛОЧНОЙ ЖЕЛЕЗЫ С ИСПОЛЬЗОВАНИЕМ ФИЛЬТРОВ. 69

Ж.М. Ташенова, Э.Н. Нурлыбаева, Ж.К. Абдугулова, Ш.А. Аманжолова
МЕТОДЫ БЕЗОПАСНОСТИ И ШИФРОВАНИЯ В ОБЛАЧНОЙ СИСТЕМЕ. 77

О.А. Усатова, А.Ш. Баракова
АНАЛИЗСОВРЕМЕННЫХСИСТЕМЗАЩИТЫВЕБ-РЕСУРСОВ. 88

Г.С. Ыбытаева, Н.Ф. Хайрова, К.Ж. Мухсина, Б.Ж. Жумажанов
ОБЗОР ПРОБЛЕМ ИСПОЛЬЗОВАНИЯ И ФОРМИРОВАНИЯ ЛИНГВИСТИЧЕСКИХ ОНТОЛОГИЙ. 96

К.С. Чежимбаева, М.Ж. Батырова
ИЗУЧЕНИЕ ВЛИЯНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА НА СЕТЬ ПЕРЕДАЧИ ДАННЫХ (IOT) ДЛЯ МОДЕЛИРОВАНИЯ УМНОГО ДОМА. 107

ФИЗИКА

Г.Б. Абдраманова, О. Имамбек, А.М. Надир, М.Б. Мырзабаева
УПРУГОЕ РАССЕЯНИЕ ПРОТОНОВ НА ЯДРЕ ^{3}He ПРИ ПРОМЕЖУТОЧНЫХ ЭНЕРГИЯХ.....117

А.Е. Амантаева, Г.Р. Сүбебекова, А.Т. Агишев, С.А. Хохлов
ОПРЕДЕЛЕНИЕ ФУНДАМЕНТАЛЬНЫХ ПАРАМЕТРОВ КАТАКЛИЗМИЧЕСКОЙ ПЕРЕМЕННОЙЗВЕЗДЫ ПРОМЕЖУТОЧНОГО ПЕРИОДА V1239 HERCULES.....124

Т.Н. Исмагамбетова, М.Т. Габдуллин, Т.С. Рамазанов
СТРУКТУРНЫЕ И ТЕРМОДИНАМИЧЕСКИЕ СВОЙСТВА ДВУХКОМПОНЕНТНОЙ ПЛОТНОЙ ВОДОРОДНОЙ ПЛАЗМЫ. 131

МАЗМҰНЫ

ИНФОРМАТИКА

Ж.С. Абдимуратов, В.И. Дмитриченко, М.А. Джетписов, Е.Н. Жагыпаров
ҚАЗАҚСТАН РЕСПУБЛИКАСЫНДАҒЫ ЦИФРЛЫҚ ҚОСАЛҚЫ СТАНЦИЯЛАРДЫ ЖОБАЛАУ КЕЗІНДЕ ҚОЗҒАЛТҚЫШТЫҢ РЕЛЕЛІК ҚОРҒАНЫСЫН БЕЙІМДЕУ 6

Ж.С. Авкурова, Б.К. Абдураимова, Б. Гнатюк, Л.М. Қыдыралина
АРТ-ШАБУЫЛДАРДЫ ЕРТЕ АНЫҚТАУҒА ЖӘНЕ КИБЕРКЕҢІСТІКТЕГІ ҚАУІПСІЗДІК БҰЗУШЫЛАРЫН АНЫҚТАУҒА АРНАЛҒАН ПАРАМЕТРЛЕР МОДЕЛІ. 17

Т.С. Байшоланов, Ж.М. Алимжанова, Н. Байшолан, К.Е. Кубаев, К.С. Байшоланова
ШИФРМӘТІНДІ ТАЛДАУ АРҚЫЛЫ КРИПТОГРАФИЯЛЫҚ ШИФРЛАРДЫҢ ТҰРАҚТЫЛЫҒЫН БАҒАЛАУ 26

Ж.С. Есенгалиева, К.Н. Касылкасова, А.О. Касылкасова
COVID-19-БЕН КҮРЕСУ ҮШІН АРНАЙЫ ЖАСАЛҒАН МЕДИЦИНАЛЫҚ ҚОСЫМШАЛАРДЫ ТАЛДАУ..... 34

Ж.С. Иксебаева, К. Жетписов, Ж.М. Муратова
ТЕХНИКАЛЫҚ ҚҰЖАТТАМАНЫ АВТОМАТТЫ ТҮРДЕ ТЕКСЕРУДІҢ ТҰЖЫРЫМДАМАЛЫҚ МОДЕЛІН ӘЗІРЛЕУ 43

В.А. Лахно, Б.С. Ахметов, М.Б. Ыдырышбаева, Ш. Сагындыкова
КИБЕРҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ ҮШІН СЕКТОРАЛДЫ ШҚҚЖ - ДЕ ЖАСЫРЫН ТӨБЕЛЕРІ БАР БАЙЕС ЖЕЛІСІН ҚОЛДАНУ 50

О.Ж. Мамырбаев, Д.О. Оралбекова, Қ. Әлімхан, M. Othman, Б. Жумажанов
ҚАЗАҚША СӨЙЛЕУДІ ТАНУ ҮШІН ГИБРИДТІ ИНТЕГРАЛДЫҚ МОДЕЛЬДЕРДІ ҚОЛДАНУ 58

А.Р. Оразаева, Д.А. Тусупов, С.В. Павлов, Г.Б. Абдикеримова
СҮТ БЕЗІ ҚАТЕРЛІ ІСІГІНІҢ БИОМЕДИЦИНАЛЫҚ КЕСКІНДЕРІН СҮЗГІЛЕРДІ ПАЙДАЛАНА ОТЫРЫП ӨҢДЕУ ТИІМДІЛІГІ. 69

Ж.М. Ташенова, Э.Н. Нурлыбаева, Ж.К. Абдугулова, Ш.А. Аманжолова
БҰЛТТЫҚ ЖҮЙЕДЕГІ ҚАУІПСІЗДІК ЖӘНЕ ШИФРЛАУ ӘДІСТЕРІ. 77

О.А. Усатова, А.Ш. Баракова
ҚАЗІРГІ ЗАМАНҒЫ ВЕБ-РЕСУРСТАРДЫ ҚОРҒАУ ЖҮЙЕЛЕРІН ТАЛДАУ 88

Г.С. Ыбытаева, Н.Ф. Хайрова, К.Ж. Мухсина, Б.Ж. Жумажанов
ЛИНГВИСТИКАЛЫҚ ОНТОЛОГИЯНЫ ҚОЛДАНУ ЖӘНЕ ҚАЛЫПТАСТЫРУ МӘСЕЛЕЛЕРІНЕ ШОЛУ.....96

К.С. Чежимбаева, М.Ж. Батырова
АҚЫЛДЫ ҮЙДІ МОДЕЛЬДЕУ ҮШІН ДЕРЕКТЕР ЖЕЛІСІНЕ (IOT) ЖАСАНДЫ ИНТЕЛЛЕКТ ӘСЕРІН ЗЕРТТЕУ.....107

ФИЗИКА

Г.Б. Абдраманова, О. Имамбек, Ә.М. Нәдір, М.Б. Мырзабаева
АРАЛЫҚ ЭНЕРГИЯЛАРДАҒЫ ПРОТОНДАРДЫҢ ^{3}He ЯДРОСЫНАН СЕРПІМДІ ШАШЫРАУЫ. 117

А.Е. Амантаева, Г.Р. Сүбебекова, А.Т. Агишев, С.А. Хохлов
АРАЛЫҚ ПЕРИОДТАҒЫ V 1239 HERCULES КАТАКЛИЗМАЛЫҚ АЙНЫМАЛЫ ЖҰЛДЫЗЫНЫҢ ІРГЕЛІ ПАРАМЕТРЛЕРІН АНЫҚТАУ 124

Т.Н. Исмагамбетова, М.Т. Габдуллин, Т.С. Рамазанов
ЕКІ КОМПОНЕНТТІ ТЫҒЫЗ СУТЕГІ ПЛАЗМАСЫНЫҢ ҚҰРЫЛЫМДЫҚ ЖӘНЕ ТЕРМОДИНАМИКАЛЫҚ ҚАСИЕТТЕРІ. 131

CONTENTS

COMPUTER SCIENCE

Zh.S. Abdimuratov, V.I. Dmitrichenko, M.A. Jetpisov,Y.N. Zhagyparov
ADAPTATION OF ELECTRIC MOTOR RELAY PROTECTION WHEN DESIGNING DIGITAL SUBSTATIONS IN THE REPUBLIC OF KAZAKHSTAN 6

Zh. Avkurova, B. Abduraimova , S. Gnatyuk, L.M. Kydyralina
MODEL OF PARA METERS FOR EARLY DETECTION OF APT ATTACKS AND IDENTIFICATION OF SECURITY INTRUDERS IN CYBERSPACE. 17

T.S. Baisholanov, Zh.M. Alimzhanova, N. Baisholan, K.E. Kubayev, K.S. Baisholanova
EVALUATION OF THE STRENGTH OF CRYPTOGRAPHIC CIPHERS USING CIPHERTEXT ANALYSIS. 26

Zh. Yessengaliyeva, K. Kassylkassova, A. Kassylkassova
ANALYSIS OF MEDICAL APPLICATIONS DESIGNED SPECIFICALLY TO COMBAT COVID-19. 34

Zh.S. Ixebayeva, K. Jetpisov, Zh.M. Muratova
DEVELOPMENT OF A CONCEPTUAL MODEL FOR AUTOMATIC VERIFICATION OF TECHNICAL DOCUMENTATION. 43

V.A. Lakhno, B.S. Akhmetov, M.B. Ydyryshbayeva, Sh. Sagyndykova
APPLICATION OF A BAYESIAN NETWORK WITH HIDDEN VERTICES IN SECTORAL DSS FOR CYBERSECURITY TASKS. 50

O.Zh. Mamyrbayev, D.O. Oralbekova, K. Alimhan, M. Othman, B. Zhumazhanov
APPLICATION OF HYBRID END TO END MODELS FOR KAZAKH SPEECH RECOGNITION. 58

A.R. Orazayeva, J.A. Tussupov, S.V. Pavlov , G.B. Abdikerimova
EFFICIENCY OF PROCESSING BIOMEDICAL IMAGES OF BREAST CANCER USING FILTERS. 69

Zh. Tashenova, E. Nurlybaeva, Zh. Abdugulova, Sh. Amanzholova
CLOUD SECURITY AND ENCRYPTION METHODS. 77

O.A. Ussatova, A.Sh. Barakova
ANALYSIS OF MODERN WEB RESOURCE PROTECTION SYSTEMS. 88

G.S. Ybytayeva, N.F. Khairova, K.Zh. Mukhsina, B.Zh. Zhumazhanov
PROBLEMS OF USING AND FORMING LINGUISTIC ONTOLOGIES: AN OVERVIEW 96

K.S. Chezimbayeva, M.Z. Batyrova
STUDYING THE IMPACT OF ARTIFICIAL INTELLIGENCE ON THE DATA NETWORK (IOT) FOR SIMULATION OF A SMART HOME. 107

PHYSICS

G.B. Abdramanova, O. Imambek, F.B. Belisarova
ELASTIC PROTON SCATTERING BY ^{3}He NUCLEI AT INTERMEDIATE ENERGIES. 117

A.E. Amantayeva, G.R. Subebekova, A.T. Agishev, S.A. Khokhlov
DETERMINATION OF THE FUNDAMENTAL PARAMETERS OF CATACLYSMIC
VARIABLE PERIOD GAP STAR V1239 HERCULES. 124

T.N. Ismagambetova, M.T. Gabdullin, T.S. Ramazanov
STRUCTURAL AND THERMODYNAMIC PROPERTIES OF A TWO-COMPONENT
DENSE HYDROGEN PLASMA. 131

Publication Ethics and Publication Malpracticein
the journals of the National Academy of Sciences of the Republic of Kazakhstan

For information on Ethics in publishing and Ethicalguidelines 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 otherlanguage, 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 сайтах:

www:nauka-nanrk.kz

http://physics-mathematics.kz/index.php/en/archive

ISSN2518-1726 (Online),
ISSN 1991-346X (Print)

Редакторы: *М.С. Ахметова, А. Ботанқызы, Д.С. Аленов, Р.Ж. Мрзабаева*
Верстка на компьютере *Г.Д.Жадыранова*

Подписано в печать 10.03.2022.
Формат 60x881/8. Бумага офсетная. Печать –ризограф.
9,0 п.л. Тираж 300. Заказ 1.

Национальная академия наук РК
050010, Алматы, ул. Шевченко, 28, т. 272-13-19