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

N E W S

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

SERIES
PHYSICO-MATHEMATICAL

6 (340)

NOVEMBER – DECEMBER 2021

PUBLISHED SINCE JANUARY 1963

PUBLISHED 6 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. Физикалық-математикалық 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 физико-математическая» 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: *математика, информатика, механика, физика, ғарыштық зерттеулер, астрономия, ионосфера.*
Мерзімділігі: жылына 6 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: *математика, информатика, механика, физика, космические исследования, астрономия, ионосфера.*
Периодичность: 6 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. Physical-mathematical series.
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: *mathematics, computer science, mechanics, physics, space research, astronomy, ionosphere.*
Periodicity: 6 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.

ИНФОРМАТИКА

NEWS
OF THE NATIONAL ACADEMY OF SCIENCES OF THE REPUBLIC OF KAZAKHSTAN
PHYSICO-MATHEMATICAL SERIES
ISSN 1991-346X
Volume 6, Number 340 (2021), 42–47 https://doi.org/10.32014/2021.2518-1726.100

UDC 004.056.53
IRSTI81.93.29

Baisholan N.[1*], Turdalyuly M.[2], Baisholanova K.S.[1], Kubayev K.E.[1], Tungyshbayev M.T.[3]

[1]Al-Farabi Kazakh National University, Almaty, Kazakhstan;
[2] Kazakh National ResearchTechnical University K.I. Satbayev, Almaty, Kazakhstan;
[3] Zhambyl Zhabayev Lyceum 161, Almaty, Kazakhstan.
E-mail**:** baisholan@gmail.com

SOFTWARE AND MATHEMATICAL SUPPORT FOR ATTACK PREDICTION IN INFORMATION SECURITY EVENTS

Abstract. The importance of information that directly affects business processes in a company, the vulnerability of opportunities to penetrate its database management system, the abundance of IP address lists, and attacks on web applications using SQL querying require information security measures. Phishing and social engineering are the most common lyseenat tacks in financial institutions, insurance industries, and online payment systems that become sources of information security attack techniques.

This article discusses the need to detect attacks in real-time management of information security events and identify anomalies to prevent any attacks. Authors pay attention to the predictive process as one of the management functions. Information security management also considers incidents as unexpected events that can compromise information security.

Here management is considered - the only way to prevent anomalies, the result of which could lead to incidents, is its prediction. The anomaly prediction process analyses the capabilities of the software and mathematical software equipment.

The possibility of incident management and detection in real time by SIEM (Security information and event management) as information security automation equipment is outlined. The measures for detecting incidents, methods of their investigation and prevention in case of detection are analysed.

An anomaly observed in network traffic may indicate the presence of an attack or technical failure. Regression metrics, trends can be used in determining it. The nature of the models used in detecting anomalies in the data flow in a time series network is given. The results of predetermined anomalies will help management to make the right decision.

Key words: network anomaly, networkincident, network attack, SIEM system, DLP system, Irwin model, prediction models.

Introduction. The internal structure of any institution in the digital market includes an important information infrastructure and consists of a large amount of corporate data. In general, the information contained in the company has become its trade secret and has become the most important value in increasing potential revenues in the present or future, preventing unjustified losses, maintaining its position in the market of goods and services or bringing other commercial benefits to the company. Thus, there was a need to protect such information or data.

Important sources of information in an institution can include, for example, the contents of internal financial documents, starting with the personal data of employees. All this can be caused by threats from external or internal parties – the actions of intruders or the administrator of the system with functional capabilities, or the vulnerability of the security system. Threats can occur intentionally or accidentally. Its consequences lead to downtime of the entire institution, starting with the cessation of service activities.

Intentional threats include theft or deliberate destruction, while accidental threats include actions such as loss or damage of the information carrier, and unintentional transfer of information to anunauthorized person. Social engineering techniques, which are currently considered to be the human factor, are also one of the most effective methods of attacking information security threats.

However, it can be noted that recently the following phenomena have been observed in the information security system of large institutions:

- targeted attacks on the infrastructure of Information systems;
- the consequences of phishing attacks and social engineering, which are more common in the banking and insurance sectors, online payment systems;
- real-time data leaks caused by internal intruders;
- data leakage from trusted specialists: network and Information System Administrators, engineers;
- leakage of data from databases in external supervision organizations;
- internal fraudulent actions by employees when buying and selling [1].

Incident management is one of the most important information security management measures described in international and domestic standards. Its quality management provides ample opportunity for the prevention of attacks in information security events. There are now quite several types of regulations in international practice governing incident management [2-6].

Materials and methods. The response to information security incidents is developed taking into account the functional characteristics of the institution, the nature of its activities. The course of information security incident management in modern institutions, according to Pisarenko [7]: reception of the information on incident; reception of the additional information connected with the revealed incident; the analysis of occurred, localisation of incident and timely, operative application of measures against it; revealing of the reasons of incident, incident and an identification of responsible persons and, if necessary, carrying out of investigatory actions; such processes as carrying out of corrective and preventive actions. The incident management procedure is developed as part of the information security management system as a whole and is enforced by appropriate regulations. The frequent recurrence of incidents occurring in the process of information security in the team is also the basis for describing the quality indicators of the security system itselfand warns of possible attacks. Its prevention or avoidance is therefore one of the relevant business processes. In incident management, for example, it is most effective to detect incidents in a timely manner (Table 1).

Table 1. Measures required to identify incidents

Measures to identify incidents	
Organisational measures	Technical measures
1. Planning processes for dealing with information security incidents at the institution. 2. Establishing procedures for responding to information security incidents. 3. Monitoring the implementation of the incident response processes. 4.Planning, monitoring and coordinating the joint activities of the different levels of information security incident response team (Information Security Incident Response Team (ISIRT)). 5. Analysis of the results of incident response. 6. Conducting an annual audit. 7. Formulation of proposals for IT management decisions based on incident response results. Proposals for improvement and monitoring of incident management processes.	1. Study of event logs in the system, collection, processing and analysis of events from various sources. 2.Detection and fixation of internal and external attacks, violations of security measures in real time. 3. Monitor information input/output devices and do not leave them unattended. 4.Monitor user activities and user identification system. 5. Review, present and take action to investigate information security incidents.

There fore, considering that such information security incidents or specific types of security threats include virus infections, phishing spreads (stratifications), attempts of unauthorized access to confidential data, errors and failures in the operation of the information system, fraud with financial data or surprises in the means of information protection, there are systems that help to prevent or detect them in real time. SIEM (Security information and event management), for example, is one of them. SIEM, by enhancing information security, detects and identifies abnormal attacks, reporting them to the user.

The SIEM system collects data on the overall status of the information system and its security from various sources and transmits it to the user within a single interface. Its main purpose is to prevent information security threats. For this purpose, it analyses events on the basis of which it draws conclusions and implements countermeasures. Another property is that it stores the collected data in a structured manner. This means that in the event of an incident it will be possible to present it as evidence. SIEM provides real-time management of the information system, allowing it to respond to incidents until the situation becomes more complex. It cannot make decisions on its own and does not offer any protective measures. It saves time and helps in the direction in which to work. It is better to be clear that the foundation of SIEM is statistics and mathematics [8].

In addition, SIEM performs important tasks such as investigating information security incidents, taking an asset inventory and controlling the protection of information resources. It can also be used in an on-premises or cloud environment. Typically, the list of activities for a pilot project is distributed according to the objectives for further application of the SIEM system in the institution, as shown in Table 2.

Table 2. List of popular tasks for MaxPatrol SIEM pilot implementation (share of projects)*

№	Types of measures	Share in the project
1	Collection, storage and processing of information security events	100%
2	Inventory and analysis of the configuration of information assets	91%
3	Detection and investigation of information security incidents	86%
4	Support for new sources of information security events	73%
5	Monitoring of system performance in the context of a specific IT infrastructure	68%
6	Control over the protection of information resources	64%
7	Creating reports	64%
8	Laying out the network diagram (topology)	45%

* Created based on the materials of © Positive Technologies [9].

SIEM uses correlation to link data and define patterns when an incident is detected. In addition, its main tasks include data collection and normalization, reporting, visualization, data storage, search and analysis and reporting.

And for enterprises using DLP, IDS, IDM, integration with a SIEM system enables a significant increase in the functionality of each of these elements. [10]. This is illustrated, for example, by capabilities of StaffCop, a system formed by merging SIEM and DLP systems, as well as the function of its deviation detector. The solutions of this system on the market are very diverse. A different solution may be appropriate for each case.

Real-time observation of the state of linear deviations (anomalies) starts with observation of some security indicators. By summing up these indicators, it is possible to predict what values they will have at which point. For this purpose, it is better to use prediction points at small intervals when analysing time series. From data streams in multi-threaded networks, it is possible to observe repeated outliers over a period of time.

Several prediction models can also be used for the accuracy of the prediction value. In the method proposed by A. V. Girik [11], the finding of deviations from the indicators of the observed object by time series was given. Here, a «normal functionalisation profile» is formed for the selected indicator through its previous values or through previously known patterns, i.e. the nature of the indicator in the absence of deviations. If new indicators are observed for which deviation values from a given indicator are determined, they constitute warnings about these observed deviations. The deviation values obtained are not included in the updated normal profile and are taken into account in the parametric establishment of deviations.

It is known that the forecast value can be short-term and long-term. In short-term forecasting, processes are mapped through these time series. If there are sometimes deviations in the time series under study, this prevents the actual forecast from being obtained. Also an outlier observed in network traffic, for example, may indicate the presence of an attack or a technical failure. It can be defined as a time series $\{ y_t | \, t = 2, \dots k\}$ using Irwin's method [12]:

$$\lambda_t = \frac{|y_t - y_{t-1}|}{\delta_y}, t \in \overline{[2, k]}, \quad (1)$$

where

$$\delta_y = \sqrt{\frac{1}{k-1}} \sum_{t=1}^{k} (y_t - \bar{y}); \; \bar{y} = \frac{1}{k} \sum_{t=1}^{k} y_t. \quad (2)$$

In this (1) equality $\lambda_2, \lambda_3, \ldots \lambda_N$ if the values are compared with and exceed the values of the Irwin criterion table, the corresponding values of the level of the series are considered to be outliers. But this approach also has its disadvantages.

In Irwin's method, outliers (emissions) include only extreme values, and this is not always the case when looking for outliers.

The degree of accuracy of a time series model, which is the result of modelling the process of finding outliers, indicates its quality. Indicators that assess the quality of a forecast model include regression indices such as coefficient of determination, Theil's disparity, ME, MAE, MPE, MAPE, SMAPE, SSE, MSE, RMSE, regression trends AR, ARMA, ARIMA, FARIMA, etc. [13].

For example, the analysis of A. V. Girik showed that multiplicative three-dimensional Winters model from Holt, Brown, Theil-Wage, Winters models is a flexible and versatile model [11].

In addition, network anomaly detection, cloud analysis [14], and traffic monitoring [15] methods are widely used in detecting anomalies in the data flow in a time series network. The choice of these methods is influenced by quantities such as data type, length, outlier value, model description, etc.

Results and its discussion. The management of information security incidents is influenced by the availability of sufficient statistical data for a qualitative output of the prediction result, the ability of models to clearly characterise the subject area, the degree of automation of its solution, etc. Therefore, existing computing hardware and prediction approaches have a wide range.

SIEM is also the appropriate equipment for the users because the process of such activities is performed more efficiently by an automated system than in traditional forecasting processing. It can be used to monitor a distributed network infrastructure with a large number of users and devices for financial facilities, and to record and identify incidents. By integrating SIEM and DLP, a company's level of information security is increased manifold. SIEM also determines the behaviour of deviations and the way information is accessed, as well as assessing the content of cyber incidents. Combining these two products allows each of them to work much more effectively.

Conclusion. This paper analyses the hardware used to detect or predict real-time information security incidents and anomalies in a network.

In conclusion, if there is financial capability to detect and predict network anomalies for information security, using SIEM systems described as software or using mathematical prediction models also provides great opportunities for timely defect detection and timely decision making.

Байшолан Н.[1]*, Тұрдалыұлы М.[2], Байшоланова Қ.С.[1], Кубаев Қ.Е.[1], Тунгушбаев М.Т.[3]

[1]Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан;
[2]Қ.И. Сәтпаев атындағы Қазақ ұлттық зерттеу техникалық университеті. Алматы Қазақстан;
Жамбыл Жабаев атындағы 161 лицей, Алматы, Қазақстан.
E-mail**:** baisholan@gmail.com

АҚПАРАТТЫҚ ҚАУІПСІЗДІК ОҚИҒАЛАРЫНДАҒЫ ШАБУЫЛДАРДЫ БОЛЖАУДЫ БАҒДАРЛАМАЛЫҚ ЖӘНЕ МАТЕМАТИКАЛЫҚ ҚАМТАМАСЫЗ ЕТУ

Аннотация. Компаниядағы бизнес-процесстерге тікелей әсер ететін ақпараттың маңыздылығы, ондағы деректер қорын басқару жүйесіне енуге мүмкіндіктердің осалдығы, IP-адрестер тізімінің көптігі, SQL-запрос көмегімен веб-қосымшаларға жасалатын шабуылдар ақпараттық қауіпсіздік шараларын талап етеді. Әсіресе қаржы ұйымдарымен сақтандыру салаларында, онлайн төлем жүйелерінде жиірек байқалатын фишингтік шабуылдар мен әлеуметтік инженерия да ақпараттық қауіпсіздікке төнетін шабуыл әдістерінің көзіне айналды.

Мақалада нақты уақыт режиміндегі ақпараттық қауіпсіздік оқиғаларын басқаруда шабуылдарды анықтап, олардың алдын алуда аномалияларды (ауытқу) анықтау керектігі қаралады. Сол үшін басқарудың бір функциясы ретіндегі – болжау процесіне көңіл бөлінеді. Ақпаратты қорғаудың менеджмент жүйесі де инциденттерді (теріс әрекеттерді) ақпараттың қорғалуына қауіп төндіруі мүмкін тосын оқиғалар ретінде қарастырады.

Бұл жерде басқару назарына – нәтижесі инциденттерге әкелуі мүмкін аномалиялардың алдын алудың бірден бір жолы – оны болжау қарастырылады. Аномалиялардың алдын алуды болжау

барысында оны бағдарламалық қамтамасыз ету жабдықтары мен математикалық қамтамасыз ету жабдықтарының мүмкіндіктері талданады.

Ақпараттық қауіпсіздікті қорғауды автоматтандыру жабдығы ретіндегі SIEM (Security information and event management) жүйесінің инциденттерді басқару және оларды нақты уақыт режимінде табу мүмкіндігі баяндалады. Инциденттерді анықтау шаралары, оларды тексеру және байқалған жағдайда алдын алу тәсілдері талданады.

Желілік трафикте байқалған аномалиялар шабуылдың немесе техникалық ақаудың болғанын байқатуы мүмкін. Оны анықтауда регрессия метрикаларын, үрдістерін қолдануға болатыны баяндалады. Уақыт қатарының желідегі мәліметтер ағынындағы аномалияларды табуда қолданылатын модельдер сипаты келтірілген. Алдын ала айқындалған ауытқулар нәтижесі басшылық барысындағы дұрыс шешім қабылдауға көмегін тигізеді.

Түйінді сөздер: желілік инцидент, шабуыл, аномалия, SIEM жүйесі, DLP жүйесі, Ирвин моделі, болжау модельдері.

Байшолан Н.[1]*, Турдалыулы М.[2], Байшоланова К.С.[1], Кубаев К.Е.[1], Тунгушбаев М.Т.[3]

[1]Казахский национальный университет имени аль-Фараби, Алматы, Казахстан;
[2]Казахский национальный исследовательский технический университет имени имени К.И. Сатпаева, Алматы, Казахстан;
[3]161 лицей имени Жамбула Жабаева, Алматы, Казахстан.
E-mail**:** baisholan@gmail.com

ПРОГРАММНОЕ И МАТЕМАТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПРОГНОЗИРОВАНИЯ АТАК В СОБЫТИЯХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. Сегодня отмечается актуальность защиты информации, что непосредственно влияет на бизнес-процессы любой компании, уязвимость базы данных на проникновение, обилие списков IP-адресов, а также атаки на веб-приложения с использованием SQL-запросов требуют принятия мер информационной безопасности.

Фишинговые атаки и социальная инженерия, которые чаще всего наблюдаются в финансовых организациях и страховых отраслях, в онлайн-платежных системах, также стали источниками методов атак на информационную безопасность.

В статье рассматривается необходимость выявления атак в управлении событиями информационной безопасности в режиме реального времени и выявления аномалий в их предотвращении. Авторыуделяют внимание процессу прогнозирования как одной из функций управления. Система менеджмента защиты информации также рассматривает инциденты как неожиданные события, которые могут поставить под угрозу защиту информации.

В работе процесс прогнозирования является частью функции управленияи рассматривается, как единственный способ своевременно обнаружить аномалии, с целью предотвращения инцидентов. В процессе прогнозирования предупреждения аномалий анализируются возможности средства программного обеспечения и средства математического обеспечения.

Излагается возможность управления инцидентами и обнаружения их в режиме реального времени с помощью SIEM (Security Information and Event Management) системы, как средства автоматизации защиты информационной безопасности. Анализируются меры выявления инцидентов, способы их расследования и предупреждения в случае обнаружения.

Аномалия, наблюдаемая в сетевом трафике, может свидетельствовать о наличии атаки или технического сбоя. При его определении можно использовать метрики регрессии, тенденции. Рассмотрены модели, используемые при обнаружении аномалий в потоке данных в сети временного ряда. Результаты предопределённых отклонений помогут руководству принять правильное решение.

Ключевые слова: сетевые аномалии, инциденты в сети, сетевые атаки, система SIEM, система DLP, модель Ирвина, модели прогнозирования.

Information about the authors:

Baisholan Nazerke – PhD student, specialty 8D06301 Information Security Systems, Department of Information Systems, Faculty of Information Technologies, Al-Farabi Kazakh National University, al-Farabi av., 71, mob: +7 7059818918; e-mail: baisholan@gmail.com, https://orcid.org/0000-0002-8134-0466;

Turdalyuly Mussa – PhD, Head of the Department of Software Engineering, Satbayev University.mob:+7 778 835 9999; e-mail: m.turdalyuly@gmail.com, https://orcid.org/0000-0002-1470-3706;

Baisholanova Karlygash – Doctor of Economic Sciences,Professor of the Department of Information Systems, Al-Farabi Kazakh National University, al-Farabi av.,71, mob:+7 7026159530; e-mail: baisholanova.k@gmail.com, https://orcid.org/0000-0001-7375-5998;

Kubayev Kazila – Doctor of Economic Sciences,Professor of the Department of Information Systems, Al-Farabi Kazakh National University, al-Farabi av., 71, mob:+7 7013257343; e-mail: kubaevk@mail.ru, https://orcid.org/0000-0002-9083-4257;

Tungushbayev Mukhit – Zhambyl Zhabayev Lyceum 161, computer science teacher, mob:+7 7023224262; e-mail: mtungushbayev@bk.ru.

REFERENCES

[1] Sevostyanov A. (2021) Enterprises, banks and factories all need integrated security. Conference proceedings . IT security day.of 7 April 2021. *https: //www.tadviser.ru/images /9/95/4._%D0%A1%D0%B5%D0%B2%D0%BE%D1% 81%D1%82%D1%8C%D1%8F%D0%BD%D0%BE%D0%B2.pdf* [in Russ.].

[2] Information technology. Protection methods. Information protection management systems. Requirements. INTERNATIONAL STANDARD. (2006) ISO/IEC 27001. CJSC "Technormativ" Translation into Russian. - 56 p. [in Russ.].

[3] Standards ISO/IEC 17799:2002 (BS 7799:2000) *https://helpiks.org/2-38949.html*[in Russ.].

[4] ST RK 34.005-2002 Information technology. Basic terms and definitions. *https://www.enbek.gov.kz/ru/node/595* [in Russ.].

[5] ST RK 34.007-2002 Information technology. Telecommunication networks. Non-communication terminator and extension cord. https://www.egfntd.kz/rus/tv/ 80253. Html [in Khaz.].

[6] State Standard of the Republic of Kazakhstan ST RK ISO / IEC17799-2006. *https://www.egfntd.kz/kaz/tv/339075.html* [in Khaz.].

[7] Pisarenko I. Identifying information security incidents. (2020). *https: //lib.itsec.ru/articles2/control/vyyavlenie-incidentov-informacionnoy-bezopasnosti*. [in Russ.].

[8] Kandybovich D. Implementing the requirements of 187-FZ at the interface of SIEM and DLP (2020). 13/10/20 *https://www.itsec.ru/articles/realizaciya-trebovanij-187-fz-na-styke-siem-i-dlp*. [in Russ.].

[9] Identifying I.S. incidents using the SIEM system. (2020) Incidents_SIEM_A4.RUS.0005.01. OKT.02.2020. – 14 с. *https: //www.ptsecurity.com/upload/corporate/ru-ru/analytics/incidents-siem-2020-rus.pdf.* [in Russ.].

[10] SearchInform SIEM - SearchInform. *(2021) https: //searchinform.ru/products/siem/.* [in Russ.].

[11] Girik A.V. (2013) Data transmission security information threat detection method based on network statistics analysis. Abstract.St. Petersburg: NRU ITMO. *http://diss.seluk.ru/av-informatika/737854-1-metod-obnaruzheniya-informacionnih-ugroz-bezopasnosti-peredachi-dannih-osnove-analiza-setevoy-statistiki.php*.

[12] Trofimenko S.V., Marshalov Ya.I., Grib N.N., Kolodeznikov I.I. (2014) Modification of the Irwin method for detecting anomalous levels of time series: methodology and numerical experiments // Modern problems of science and education. № 5. 204-208 p.[in Russ.].

[13] Lukashin Yu.P. (2003) Adaptive methods of short-term forecasting of time series. -M.: Finance and Statistics. - 416 p. ISBN 5-279-02740-5. [in Russ.].

[14]. Vallis O., Hochenbaum L., Kejariwal A. (2008) A novel technique for long-term anomaly detection in the cloud // Proceedings of the ITS Specialist Seminar on Network Usage and Traffic. P.1-15. *https://www.usenix.org/system/files/conference/hotcloud14/hotcloud14-vallis.pdf*.(In Eng.).

[15] *Münz G.*, Garle G. (2014) Application of forecasting techniques and control charts for traffic anomaly detection // Proceedings of the USENIX Conference on Hot Topics in Cloud Computin. *https: //www.net.in.tum.de /fileadmin /TUM/members /muenz /documents /muenz08control-charts.pdf*. (In Eng.).

МАХМҰНЫ

ФИЗИКА

ИНФОРМАТИКА

МАТЕМАТИКА

СОДЕРЖАНИЕ

ФИЗИКА

ИНФОРМАТИКА

МАТЕМАТИКА

CONTENTS

PHYSICS

COMPUTER SCIENCE

MATHEMATICS

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 10.12.2021.
Формат 60x881/8. Бумага офсетная. Печать –ризограф.
9,5 п.л. Тираж 300. Заказ 6.

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