-sociological surveys among Internet users, professional data research agencies;

-receiving additional data about visitors (registration data, filled-in questionnaires, identification using cookies linked to geographic databases, etc.);

- receiving data within the advertiser's company.

Most often, they use programs for collecting statistics (visit counters), which can beset on a separate page or located on all pages of the site.

It is believed that there are two directions for evaluating the effectiveness of advertising: communicative or informational efficiencyadvertising that allows to establish how effective a specific advertising appeal is in conveying the necessary information to the target audience andeconomic efficiency,what is determined by the ratio between the result from advertising and the amount of material and financial costs for it for a fixed period.

The main criterion for the communicative effectiveness of advertising is index awareness of AW, which is equal to the ratio of the number of users who know about the content of advertising to the total volume of the target audience. Indicators characterizing economic efficiency include: amount orders for goods or services, depth of interest, percentage of returns, feedback.

Information sources:

1. Baranov O.A. Internet rechei i blokchein. *Informatsiia i pravo*. № 1(24). 2018. S. 59-71.
2. Pleskach V. Tekhnolohii elektronnoho biznesu: [monohrafiia]. K.: KNTEU. 2004. 223 s.
3. Lytvyn I. Informatsiini tekhnolohii v ekonomitsi: navch. posibnyk. Ternopil, 2001. 296 s.
4. Makarova M.V. Elektronna komertsiia. K.: Vyd. tsentr „Akademiia. 2002. 272 s.

PRACTICAL APPLICATION OF MATHEMATICAL METHODS IN THE FORMATION OF A CYBERSECURITY SYSTEM AT THE ENTERPRISE

Levkin D., Candidate of Engineering Science, Associate Prof.
Kotko Ya., Candidate of Economic Sciences
Levkin A., Candidate of Technical Sciences, Associate Prof.
State Biotechnological University

In recent years, the information space of Ukraine has been developing and implementing the latest services, technologies, channels, platforms, online products and online services that reduce transaction costs and improve the standard of living of society. At the same time, the risk of security of one's own information system is growing due to constant attempts of cyberattacks and cybercrime related to access to personal information and data on confidential transactions. The number of such cyberattacks has been steadily increasing in recent years and poses a real threat to the stable functioning of your own information system. While more than 1,100 cybercrimes were recorded in Ukraine in the last four months of 2021, more than 2,194 cyberattacks were registered in Ukraine in 2022, 1/4 of which targeted government institutions. In modern scientific research, much attention has been paid

to the development and application of mathematical methods and approaches for analyzing and classifying intrusion detection in the information space [1, 2], issues related to the use of mathematical methods to improve the cybersecurity of information systems [3, 4].

There is a need to introduce effective measures to combat cyberattacks, counteract cyberfraud, cybercrime, and unauthorized interference with the system. These measures will be based on mathematical methods that can be used in the process of solving the tasks related to online risk research, identifying cyber threats, detecting cyber attacks, neutralizing trojans (viruses that take over system control), phishing emails (the threat of maliciously gaining access to personal accounts), stalking (online harassment, financial crimes), skimming and pharming (fraud to steal money), exploit prevention (software code errors to gain control over the system), detection of payment system duplicates, etc.

In accordance with the types of cyberattacks, cybercrime and cyberfraud considered, we will analyze the latest mathematical areas used to counter them. These include binary mathematics (understanding and creating unique programs that ensure network security and facilitate understanding of weaknesses in bytes or byte combinations); Boolean algebra (used to express solutions and adequate responses); cryptography tools (applying algorithms based on the theory of computational complexity to ensure data confidentiality); hexadecimal mathematics (ensuring the expression of binary values); linear algebra (creating computer systems, visualizing graphs).

The most well-known mathematical methods in cybersecurity today are:

- graph technologies – construction of information systems in the form of an oriented graph containing system components displayed as nodes. Accordingly, the adjacency of information system components is defined as an adjacency matrix. The model of this program appears in the form of an arithmetic expression and is the most effective means of automating programming used to audit network security, identify weaknesses in security systems and predict the actions of cybercriminals;

- mathematical method of determining reliability based on the mean square deviation provides an idea of the level of deviation of the system from the expected results. This method is used to control the level of cybersecurity of the information environment in an enterprise, and is important for economic and mathematical modeling of production processes, as it can be used to assess the effectiveness of applied mathematical models. It should be noted that the lower the level of the indicator, the closer the system function is to its intended purpose;

- mathematical method based on the Doppler effect, which is used to process complex systems in the information space. When choosing a different mode, it is necessary to take into account the relevant data for filtering mathematical models and building ROC curves;

- applied optimization mathematical methods are used to calculate and optimize the parameters of complex systems. Their adequacy is substantiated by the use of algorithms based on the theory of pseudo-differential operators in the space of generalized slow power functions [5];

- mathematical method for solving the Lotka-Voltaire equation is based on first-order nonlinear differential equations that describe the dynamics of relationships in the information space (phishing fraud, online predators, or malware distribution). After all, differentials represent the instantaneous growth rates of two species competing for a common resource, sometimes describing an interaction between two or more species in which each species receives a certain benefit;

- mathematical methods of parallel computing of complex cyber systems for modeling and identification of high-performance technologies, in the presence of a significant number of feedbacks and interaction of a network of computing elements. These methods are based on multi-parameter regularization algorithms for identifying the parameters of a complex system (using hybrid methods of integral transforms to build high-speed feedback models);

- the Nicholson-Bailey mathematical method is used to monitor the population of cybercrime, determine the speed of their spread and the effectiveness of finding places in the information environment that are most vulnerable to cyberattacks;

- mathematical method based on the theory of disasters in network traffic is used to detect anomalies in the network of information data, provides a high probability of detecting anomalies and a low level of false intrusions in relation to cybercrime and cyberattacks in the cloud environment. In addition, it is an effective tool for characterizing network change processes due to the dynamic nature of the cloud environment;

- mathematical and statistical methods are used to design asynchronous algorithms with stable communication between network resources, modeling the stable properties of uncertainty caused by time-dependent input data.

Traditional and modern mathematical methods are important components of the process of developing an enterprise's information space and protecting it from cyberattacks. Their application formalizes the relationships between various information systems, allows solving problems of personal data protection, minimizing existing shortcomings of modern systems, and preventing intrusions. The considered mathematical methods are characterized by low complexity, stability, high adaptability to solving applied information security problems in enterprises, correctness and verifiability, and are able to effectively implement cybersecurity measures to counter cyberattacks, which are especially relevant today. After all, every company seeking to develop must adequately assess the consequences of any type of cyberattack and counteract them using all available means, methods, tools, etc., because their implementation is nothing more than an investment in the company's future and prospects.

Thus, cybersecurity plays a rather significant role in the activities of an enterprise in the current environment. After all, the real manifestations of cyberattacks are hardly predictable, and their result is significant financial and economic losses or unforeseen consequences of disruptions in the functioning of enterprise systems that affect the state of security and life processes. The application of mathematical methods in enterprise cybersecurity can be used to identify the likelihood of real cyberattacks, and new methods and research can be introduced to better understand them, especially with the emergence of modern and new malware

and the extraordinary growth of online fraud. Such mathematical methods play a useful role when it comes to secure planning or forecasting activities and system assessment, providing a better understanding of the threat itself and its impact throughout the duration of a cyberattack. Thus, the above mathematical methods play an important role in cybersecurity, creating important prerequisites for enterprise systems to quickly protect systems to combat cyberattacks, fraud, or malware.

Information sources:

1. Stepanenko S.V., Diachenko O.P. Informatsiini tekhnolohii yak instrument rozvytku inkliuzyvnoho ahrarnoho biznesu. *Tavriiskyi naukovyi visnyk. Seriia: «Ekonomika»*. 2023. No. 15. S. 116–122. https://doi.org/10.32782/2708-0366/2023.15.14

2. Kameneva I.P., Artemchuk V.O. Problema informatyvnosti ta vyznachennia informatyvnykh struktur dlia pidtrymky pryiniattia rishen v haluzi ekolohichnoi bezpeky. *Elektronne modeliuvannia*. 2022. Vol. 44. No. 3. S. 50–64. https://doi.org/44.03.050

3. Kuzmenko O.V., Yarovenko H.M., Skrynka L.O. Analiz matematychnykh modelei protydii bankivskym kibershakhraistvam. *Visnyk Sumskoho derzhavnoho universytetu. Seriia: «Ekonomika»*. 2022. No. 2. S. 111–120. DOI:10.21272/1817-9215.2022.2-13.

4. Shevchenko S., Zhdanova Y., Spasiteleva S. Matematychni metody v kiberbezpetsi: teoriia katastrof. *Kiberbezpeka: osvita, nauka, tekhnika.* 2023. No. 3. Issue. 19. S. 165–175. https://doi.org/10.28925/2663-4023.2023.19.165175.

5. Levkin D. Application of calculation methods for solving applied problems of heat and mass exchange in complex systems. *Measuring and computing devices in technological processes*. Khmelnytskyi, 2023. No. 2. S. 179–182. https://doi.org/10.31891/2219-9365-2023-74-24

ZARZĄDZANIA FINANSAMI Z ZASTOSOWANIEM MODELI CYBERNETYCZNYCH

Chabaniuk O., PhD
Lwowski Uniwersytet Handlowo-Ekonomiczny
Ohirko O., PhD
The Department of computerized control systems of the State University of Internal Affairs

Racjonalne planowanie finansów jest jednym z kluczowych aspektów nie tylko zarządzania finansami, ale zarządzania organizacją w ogóle. Warto więc, choćby krótko, odpowiedzieć na pytanie, czemu służy planowanie finansów w organizacjach pozarządowych. Mówiąc najkrócej proces ten służy planowaniu dochodów, które pozwolą na pokrycie kosztów zakładanych do realizacji działań. Warto przy okazji, pomyśleć o środkach finansowych z działalności gospodarczej, które pozwalają nam generować zysk. Z kolei wypracowany zysk daje organizacjom możliwość inwestowania środków, a tym samym budowania stabilności finansowej.

Planowanie, czy też monitoring finansów prowadzony na bieżąco daje możliwość minimalizowania kosztów aktualnych oraz planowanych działań. Planowanie uświadamia ile kosztuje nasza aktywność, ale też pomaga w poszukiwaniach potencjalnych oszczędności. Dotychczasowe doświadczenia