axioms

MDPI

Article

Mathematical Model of Cyber Risks Management Based on the Expansion of Piecewise Continuous Analytical Approximation Functions of Cyber Attacks in the Fourier Series

Valentyn Sobchuk [1,†], Oleg Barabash [2,†], Andrii Musienko [2,†], Iryna Tsyganivska [1,†] and Oleksandr Kurylko [1,*,†]

[1] Faculty of Mechanics and Mathematics, Taras Shevchenko National University of Kyiv, 4E Academician Glushkov Avenue, 03127 Kyiv, Ukraine; sobchuk@knu.ua (V.S.); itsy8009@knu.ua (I.T.)
[2] Educational and Scientific Institute of Atomic Thermal Energy, National Technical University of Ukraine "Ihor Sikorsky Kyiv Polytechnic Institute", 6 Polytechnichna St., Building No. 5, 03056 Kyiv, Ukraine; bar64@ukr.net (O.B.); mysienkoandrey@gmail.com (A.M.)
* Correspondence: alexandr.kurylko@knu.ua
† These authors contributed equally to this work.

Abstract: The comprehensive system of information security of an enterprise includes both tactical aspects of information and strategic priorities, reflecting the information policy and information strategy of the enterprise. Ensuring a given level of cybersecurity requires the identification of threat actors, their purpose, intentions of attacks on the IT infrastructure, and weak points of the enterprise's information security. To achieve these goals, enterprises need new information security solutions. In this work, a mathematical model of the process of cyber risk management in the enterprise, which is based on the distribution of piecewise continuous analytical approximating functions of cyber attacks in the Fourier series, is obtained. A constant continuous monitoring and conduction of cyber regulatory control of the enterprise on time makes it possible to effectively ensure the cybersecurity of the enterprise in real time—predicting the emergence of cyber threats to some extent—which, in turn, determines the management of cyber risks arising in the field of information security of the enterprise. Such a Fourier series expansion of the piecewise continuous analytical approximating function of the intensity of cyber attacks on damage to standard software, obtained by approximating empirical–statistical slices of the intensity of cyber attacks on damage to standard software for each time period by analytical functions, opens up new mathematical possibilities of transition to systems of regulatory control of cyber threats of the enterprise from discrete to continuous automated process for such types of control.

Keywords: Fourier series; cyber threat; piecewise continuous function; mathematical model; information security of an enterprise

MSC: 42A16

check for updates

Citation: Sobchuk, V.; Barabash, O.; Musienko, A.; Tsyganivska, I.; Kurylko, O. Mathematical Model of Cyber Risks Management Based on the Expansion of Piecewise Continuous Analytical Approximation Functions of Cyber Attacks in the Fourier Series. *Axioms* **2023**, *12*, 924. https://doi.org/10.3390/axioms12100924

Academic Editor: Giovanni Nastasi

Received: 30 August 2023
Revised: 25 September 2023
Accepted: 25 September 2023
Published: 28 September 2023

Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

With the appearance of new IT technologies, the intensity of new cyber attacks on enterprise IT systems is increasing. It is also worth noting that traditional cybersecurity activities cannot fully prevent or contain these attacks due to the increasing speed and frequency of cyber attacks. The enterprise's comprehensive information security system includes both tactical aspects of information protection (express audit of the enterprise's information threats) and strategic priorities reflected in the enterprise's information policy and information strategy. Ensuring a given level of cybersecurity requires the identification of threat actors, their purpose, intentions of attacks on the IT infrastructure, and weak points of the enterprise's information security. To achieve these goals, enterprises need new

information security solutions that not only meet the realities of today but also have significant development potential, taking into account current trends in the field of information security in general. At the same time, the issues of researching the intensity of cyber attacks, and their prediction and forecasting, are insufficiently researched in the scientific literature, which is related to the complexity of predicting cyber attacks as well as the availability of modern relevant methods for their forecasting.

The fight against the growing intensity of cyber threats requires the creation of a multifaceted information security strategy of the enterprise, which, in particular, includes the prediction of cyber attacks. In their scientific works, scientists Palash Goyal, Ashok Deb, and Nazgol Tavabi described computer programming methods based on neural networks and autoregressive time series models (AR, ARMA, ARIMA, ARIMAX) that use external signals from publicly available web sources to forecast cyber attacks. However, such models usually require a significant amount of data to implement computer programming in order to establish an accurate estimate of the model parameters. Most research efforts have focused on using network traffic to build predictive models. These studies are presented in the works of scientists such as E. Pontes, A. E. Guelfi, S. T. Kofuji, and A. A. Silva. Other researchers such as E. Gandotra, D. Bansal, and S. Sofat built cyber predictions using statistical modeling and algorithmic modeling. R. Douc, E. Moulines, and D. Stoffer were engaged in the use of ARCH and GARCH models, which are extensions of the classical autoregression model.

However, developing an accurate model of the dynamic behavior of time series is a difficult and important task. Therefore, there is a need for further research and development of a scientific and methodological apparatus for determining the relationship between the level of cyber risk and the frequency of audits, which makes it possible to ensure effective automation of enterprise cybersecurity processes. The general task of ensuring information security conditions the study of vulnerabilities of the IT infrastructure of the enterprise and relevant models of cyber attack prevention. In this regard, it is necessary to conduct a study of the relevant vulnerabilities and problems of all groups of cyber attacks on the enterprise.

As a result of the spread of freelance relations, as a modern type of business relation of an enterprise, there is a need to process and analyze statistical data of cyber attacks in the field of activity of an IT enterprise that involves a freelance resource. These studies should be designed to use temporal correlations between the number of cyber attacks over a period of time in order to predict the future intensity of cyber incidents, which will allow the creation of an effective forecasting system. Therefore, predicting the number of cyber attacks for a set rational time period is necessary to determine the effective frequency of the audit.

2. Literature Analysis

Fourier series are widely used in research in various fields of activity. Thus, particularly in [1–3], the speed of approximation of differentiable functions by generalized methods of summation of Fourier series was investigated. In [4,5], the conditions of convergence of Fourier transformations were investigated. Applied aspects of approximate properties of Fourier series were considered in [6–8], while the properties and application of isometric classes of functions based on their Fourier series were studied in [9,10].

In modern technical literature, the scientific problems of enterprise information security related, in particular, to the improvement of attack graphs for monitoring cybersecurity, handling of inaccuracies, cycle processing, display of incidents, and automatic selection of protective measures were investigated in the works of O.A. Lapteva [11–14], E.M. Galakhova [15], O.V. Kapustyan [16], S.P. Yevseiev, [17], and A.P. Musienko [18], respectively. The stability of the information system, in terms of functioning with the conditions of external and internal destabilizing factors, was studied in [19]. External and internal destabilizing factors include mean failures, failures of system modules, mechanical damage, thermal effects, and errors of service personnel. Ref. [20] investigated how, on the basis of the functional dependence of the probability of missing failures on a certain

probability value, at different values of the probability of second-order control error, it is possible to determine the recommended interval of issuing the result, which will ensure, at a given intensity of readiness control, an acceptable probability of missing a failure. It was illustrated how, with a given intensity of issuing the result, it is possible to determine such an intensity of readiness control at which the probability of failure will not exceed the maximum permissible value. It was shown that it is possible to talk about a weak dependence of the probability of omission on the control error of the second kind, which means that the achievement of the specified reliability of the control is ensured on the basis of the intensity of the readiness control and depends less on the reliability of individual elementary checks. For the case when, in the intervals between the moments when the result is issued, the system checks the readiness of the modules randomly, the methodology for calculating the probability of failure was described. In [21], based on the use of a hierarchical concept of the organization of means of ensuring the functional stability of the company's information system, two algorithms were developed that form a two-level system for diagnosing hidden failures. Diagnosis begins with the execution of the first algorithm, the advantages of which compared with known algorithms are that it requires less system redundancy, only two rounds of message exchange between nodes of the information system, and provides diagnosis of the information system of the subtribe when almost half of its nodes fail. In the case of an ambiguous solution to the diagnosis problem, the algorithm generates a signal about its failure and the diagnosis of the information system continues according to the second algorithm, which uses the duration of the phases as a criterion.

In [22–24], for evolutionary nonlinear problems with control parameters, the problems of approximate minimax estimation and making optimal decisions were considered. The authors investigated the problems of the behavior of evolutionary systems, when the system is under the influence of impulse forces of an instantaneous nature. This is important, because even in the case of linear systems, the presence of impulse action makes the behavior of the system significantly nonlinear, and the control of solutions of such systems is extremely difficult. At the same time, cyber attacks have a similar nature when they try to destabilize the system through the influence of external forces. Prediction of the number of possible cyber attacks, statistical and analytical assessments of cyber attacks, timely identification, development of an action plan and preventive measures to eliminate identical cyber attacks, implementation of a control system, and the introduction of modernized approaches to regulatory control of cyber attacks in the enterprise were carried out in [25,26].

The purpose of this work is to develop a mathematical model of cyber risks management of the enterprise, which makes it possible to move the system of regulatory control of cyber threats of the enterprise from a discrete to a continuous automated process of regulatory control.

3. Main Part

Let us consider a mathematical model of the process of managing cyber risks of the enterprise, which makes it possible to move the system of regulatory control of cyber threats of the enterprise from a discrete to a continuous automated process of regulatory control. This model differs from the existing ones, based mainly on the statistical analysis of time series, in that piecewise continuous analytical approximating functions of cyber attacks are decomposed into a Fourier series.

The research interest of this model is to determine the recommended frequency for the cyber risk management process in the enterprise. The model focuses on the following key stages of research:

1. Retrospective statistical analysis of cyber risk identification time series.
    1.1. Determination of time intervals of regulatory control and approximation of statistical sections by analytical functions (Figures 1 and 2).

1.2. Graphical visualization of the implemented statistical analysis of time series of cyber risk identification (Figure 1).

2. Analysis of the enterprise's existing cyber risks strategy based on the retrospective statistical analysis of cyber risk identification time series, conducted above, highlighting weaknesses of the existing strategy, possible cyber threats, identification of potential strengths, and opportunities for further modernization.
3. Development of a predictive and analytical model of regulatory control.
4. Introduction of modernized approaches into the existing system of regulatory control of the enterprise.

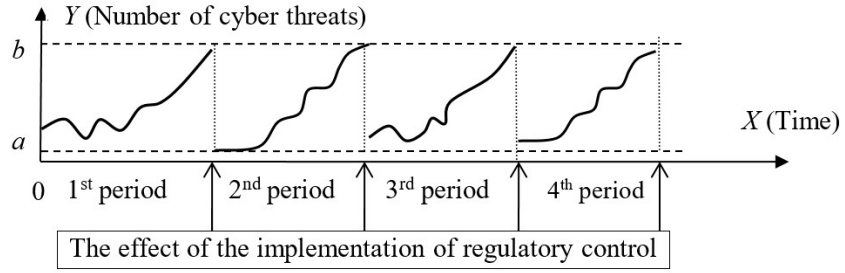


Figure 1. Dependence of the number of cyber threats on the frequency of regulatory control over 4 time intervals.

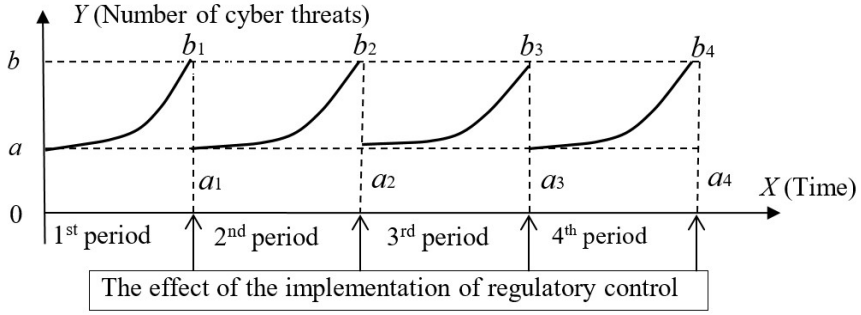


Figure 2. Approximation of statistical slices of cyber attacks on damage to network infrastructure by analytical functions.

Figure 1 shows 4 time periods of regulatory control within the framework of the proposed model. The implementation of consistent activities of regulatory control ensures the minimization of cyber threats in each time period, which is illustrated in Figure 1. Figure 1 illustrates similar effects from the implementation of regulatory control and almost the same behavior in the number of cyber threats between the conducted audits.

According to part 1.1 of the abovementioned key bases of model research, an approximation of the statistical slices of cyber attacks on damage to the network infrastructure was carried out by analytical functions in the period between 4 time periods of regulatory control within the framework of the proposed model (Table 1).

Table 1. Approximation of time series of cyber attacks on damage to network infrastructure by analytical functions.

Time Period	Nonlinear Equation of the Approximating Function on the Interval (0; 1)	Coefficient of Determination
1st period	$y = 1.0643 \times e^{0.064x}$	0.9032
2nd period	$y = 1.0534 \times e^{0.053x}$	0.9040
3rd period	$y = 1.0626 \times e^{0.065x}$	0.9012
4th period	$y = 1.0596 \times e^{0.059x}$	0.8933

Figure 2 presents a graphical interpretation of the approximation of the time series of cyber attacks on damage to the network infrastructure by analytical functions with averaged values for each time period in view of the almost identical equations of the approximating functions for different periods, which are presented in Table 1.

From Figure 2, we establish that the function is periodic with a period $T = 1$ ($2l = 1$, $l = 1/2$); then, we expand the given function into a Fourier series on the closed interval $[0, 2l] = [0, 1]$. Let us write down the equation of the given function presented in Figure 2 with unknown coefficients: $y = A \times e^{Bx}$. Let us determine the estimated coordinates of the points from the bundle of nonlinear curves approximating the statistical series, which are in the confidence interval with the smallest variances in the form $y = 1.0595 \times e^{0.060205x}$. Note that 0.52975 is the statistical average value of the cyber threat function at its points of jump discontinuity. Thus, we have

$$y = \begin{cases} 1.0595 \times e^{0.060205x} & k < x < k+1 \\ 0.52975 & x = k, k \in Z \end{cases} \tag{1}$$

For function (1), we find the coefficients of the Fourier series:

$$a_0 = \int_0^1 1.0595 \times e^{0.060205x} dx = \frac{1.0595}{0.060205} \times (e^{0.060205x})|_0^1 = 17.5982(e^{0.060205} - 1) = 1.09351. \tag{2}$$

Denoting the desired integral by I and applying the method of integration by parts twice, we obtain

$$\begin{aligned} a_n &= \frac{1}{1/2} \int_0^1 1.0595 e^{0.060205x} \times \cos\left(\frac{\pi n x}{1/2}\right) dx = 2 \times 1.0595 \times I = 2.119 \times I \\ &= \begin{vmatrix} e^{0.060205x} = U & 0.060205 e^{0.060205x} dx = dU \\ \cos(2\pi n x) dx = dV & V = \frac{1}{2\pi n} \sin(2\pi n x) \end{vmatrix} \\ &= 2.119 \left[\left(e^{0.060205x} \times \frac{1}{2\pi n} \sin(2\pi n x) \right) |_0^1 - \frac{0.060205}{2\pi n} \int_0^1 e^{0.060205x} \sin(2\pi n x) dx \right] \\ &= \begin{vmatrix} e^{0.060205x} = U & 0.060205 e^{0.060205x} dx = dU \\ \sin(2\pi n x) dx = dV & V = -\frac{1}{2\pi n} \cos(2\pi n x) \end{vmatrix} \\ &= -2.119 \times \frac{0.060205}{2\pi n} \left[-\frac{e^{0.060205x}}{2\pi n} \cos(2\pi n x) \right] |_0^1 + \frac{0.060205}{2\pi n} \int_0^1 e^{0.060205x} \cos(2\pi n x) dx \\ &= \frac{0.127574}{2\pi n} \left(-\frac{e^{0.060205} - 1}{2\pi n} + \frac{0.060205}{2\pi n} \right) \times I \end{aligned} \tag{3}$$

To find the integral I, we solve the following equation:

$$\begin{aligned} 2.119 \times I &= \frac{0.127574}{2\pi n} \left(-\frac{e^{0.060205} - 1}{2\pi n} + \frac{0.060205}{2\pi n} \right) \times I \Rightarrow \\ \Rightarrow I \left(2.119 - \frac{0.127574}{2\pi n} \times \frac{0.060205}{2\pi n} \right) &= -\frac{0.127574}{2\pi n} \times \frac{e^{0.060205} - 1}{2\pi n} \end{aligned} \tag{4}$$

Thus, we have

$$I = \frac{0.127574(e^{0.060205} - 1)}{0.00678 - 2.119(2\pi n)^2}. \tag{5}$$

Then, the coefficients a_n are obtained in the form

$$\begin{aligned} a_n &= \frac{1}{1/2} \int_0^1 1.06^{1-x} \times \cos\left(\frac{\pi n x}{1/2}\right) dx = 2.119 \times I \\ &= \frac{2.119 \times 0.127574(e^{0.060205} - 1)}{0.00678 - 2.119(2\pi n)^2} = \frac{0.27033(e^{0.060205} - 1)}{0.00678 - 2.119(2\pi n)^2}. \end{aligned} \tag{6}$$

Similarly, we find the coefficients b_n:

$$\begin{aligned} b_n &= \frac{1}{1/2}\int_0^1 1.0595e^{0.060205x}\sin\left(\frac{\pi nx}{1/2}\right)dx = 2\times 1.0595\times I = 2.119\times I \\ &= \left|\begin{matrix} e^{0.060205x} = U & 0.060205e^{0.060205x}dx = dU \\ \sin(2\pi nx)dx = dV & V = -\frac{1}{2\pi n}\cos(2\pi nx)\end{matrix}\right| \\ &= 2.119\left[\left(-e^{0.060205x}\times\frac{1}{2\pi n}\sin(2\pi nx)\right)|_0^1 + \frac{0.060205}{2\pi n}\int_0^1 e^{0.060205x}\cos(2\pi nx)dx\right] \\ &= \left|\begin{matrix} e^{0.060205x} = U & 0.060205e^{0.060205x}dx = dU \\ \cos(2\pi nx)dx = dV & V = \frac{1}{2\pi n}\sin(2\pi nx)\end{matrix}\right| \\ &= 2.119\left[-\left(e^{0.060205}-1\right)\times\frac{1}{2\pi n} + \frac{0.060205}{2\pi n}\left[\frac{e^{0.060205x}}{2\pi n}\sin(2\pi nx)|_0^1 - \frac{0.060205}{2\pi n}\int_0^1 e^{0.060205x}\sin(2\pi nx)dx\right]\right] \\ &= \frac{2.119\left(1-e^{0.060205}\right)}{2\pi n} - \frac{0.0076806}{(2\pi n)^2}\times I \end{aligned} \tag{7}$$

To find the integral I, we solve the following equation:

$$\begin{aligned} 2.119\times I &= \frac{2.119\left(1-e^{0.060205}\right)}{2\pi n} - \frac{0.0076806}{(2\pi n)^2}\times I \Rightarrow \\ \Rightarrow I\left[2.119 + \frac{0.0076806}{(2\pi n)^2}\right] &= \frac{2.119\left(1-e^{0.060205}\right)}{2\pi n}. \end{aligned} \tag{8}$$

Thus, we obtain

$$I = \frac{2.119\left(1-e^{0.060205}\right)}{2\pi n\left(2.119 + \frac{0.0076806}{(2\pi n)^2}\right)}. \tag{9}$$

Then, the coefficients b_n will have the following form:

$$b_n = \frac{4.49020\left(1-e^{0.060205}\right)}{2\pi n\left(2.119 + \frac{0.0076806}{(2\pi n)^2}\right)}. \tag{10}$$

Hence, let us write down the expansion of Function (1) in the Fourier series:

$$f(x) = 1.09351 + \sum_{n=1}^{\infty}\left[\frac{0.27033\left(e^{0.060205}-1\right)}{0.00678 - 2.119(2\pi n)^2}\times\cos(2\pi nx) + \frac{4.49020\left(1-e^{0.060205}\right)}{2\pi n\left(2.119 + \frac{0.0076806}{(2\pi n)^2}\right)}\times\sin(2\pi nx)\right] \tag{11}$$

Thus, Function (11) is a continuous function that models a piecewise continuous function with points of jump irremovable discontinuities. Such a mathematical model is based on the expansion of a piecewise continuous analytical approximating function into the Fourier series, which makes it possible to move the system of regulatory control of cyber threats of the enterprise from a discrete to a continuous automated process of regulatory control.

Therefore, the approximation of statistical slices of cyber attacks on damage to the network infrastructure by analytical functions in the period between 4 time periods of regulatory control within the framework of the proposed model provides an automated approach to minimizing cyber threats in each time period.

Let us consider the mathematical possibilities of transition from a discrete to continuous automated process of cyber regulatory control of the enterprise. The modern approach to the information security of an enterprise in the sphere of action of cyber attacks is determined by the following stages: forecasting the number of possible cyber attacks; carrying

out empirical–statistical and analytical evaluation of cyber attacks; identification of cyber attacks on time; development of an action plan and preventive activities to eliminate similar cyber attacks; and, most importantly, the implementation of the control system and the introduction of innovative approaches to the timely regulatory control of cyber attacks in the enterprise.

Therefore, with the growth of cyber threats, the need for express audits and their implementation on time increases the effectiveness of the enterprise's comprehensive information security strategy.

Figure 3 schematically reflects the behavior of the intensity of cyber attacks on damage to standard software for 4 time periods between conducting the scheduled regulatory control. After the scheduled regulatory control before the first time period, activities were taken that ensured the minimization of cyber threats in the first 2 time periods after the scheduled regulatory control.

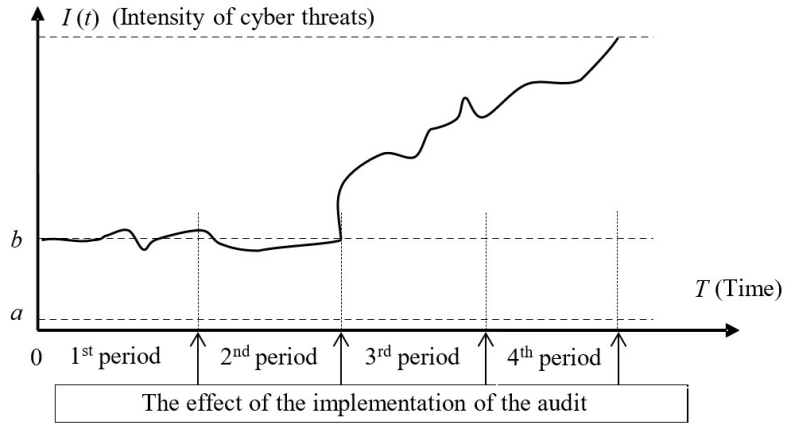


Figure 3. Dependence of the number of cyber attacks on the damage standard software from frequency of carrying out regulatory control for 4 time intervals.

Approximation of the statistical slices of cyber attacks on damage to standard software for each period by analytical functions was carried out (Table 2).

Table 2. Approximation of time series of cyber attacks on damage to standard software by analytical functions.

Time Period	An Equation of the Approximating Function on the Interval (0; 1)	Coefficient of Determination
1st period	$I(t) = 1.0364$	0.8731
2nd period	$I(t) = 1.0453$	0.8540
3rd period	$I(t) = 1.00076t$	0.8912
4th period	$I(t) = 1.0237t$	0.8721

Based on Table 2, given the almost identical equations of approximating functions for the 1st, 2nd and 3rd, and 4th periods, respectively, it is possible to represent analytically the function of the intensity of cyber attacks on damage to standard software, combining the 1st, 2nd and 3rd, and 4th periods. Then, analytically, the function of the intensity of cyber attacks can be represented as

$$I(t) = \begin{cases} 1, & 0 \le t < 2 \\ t, & 2 \le t \le 4. \end{cases} \tag{12}$$

Let us expand Function (12) into a Fourier series, which will make it possible to move the regulatory control system of cyber attacks on damage of the enterprise's standard software from a discrete to a continuous automated process of regulatory control.

Let us find the following coefficients:

$$\begin{aligned} a_n = \frac{1}{2}\int_0^4 f(t)\cos\frac{\pi nt}{2}dt &= \frac{1}{2}\left(\int_0^2 \cos\frac{\pi nt}{2}dt + \int_2^4 t\cos\frac{\pi nt}{2}dt\right) \\ &= \left|\begin{matrix} t = U & dt = dU \\ \cos\frac{\pi nt}{2} = dV & V = \frac{2}{\pi n}\sin\frac{\pi nt}{2}\end{matrix}\right| \\ &= \frac{1}{2}\left(\frac{2}{\pi n}\sin\frac{\pi nt}{2}|_0^2 + \left(\frac{2t}{\pi n}\sin\frac{\pi nt}{2} + \frac{4}{\pi^2 n^2}\cos\frac{\pi nt}{2}\right)|_2^4\right) \\ = \frac{1}{2}\times\frac{4}{\pi^2 n^2}(\cos 2\pi n - \cos\pi n) &= \frac{2}{\pi^2 n^2}(1-\cos\pi n) = \frac{2}{\pi^2 n^2}(1-(-1)^n); \end{aligned} \tag{13}$$

$$a_0 = \frac{1}{2}\int_0^4 f(t)dt = \frac{1}{2}\left(\int_0^2 dt + \int_2^4 tdt\right) = \frac{1}{2}\left(2 + \frac{t^2}{2}\,|_2^4\right) = \frac{1}{2}(2+6) = 4; \tag{14}$$

$$\begin{aligned} b_n = \frac{1}{2}\int_0^4 f(t)\sin\frac{\pi nt}{2}dt &= \frac{1}{2}\left(\int_0^2 \sin\frac{\pi nt}{2}dt + \int_2^4 t\sin\frac{\pi nt}{2}dt\right) \\ &= \left|\begin{matrix} t = U & dt = dU \\ \sin\frac{\pi nt}{2} = dV & V = -\frac{2}{\pi n}\cos\frac{\pi nt}{2}\end{matrix}\right| \\ &= \frac{1}{2}\left(-\frac{2}{\pi n}\cos\frac{\pi nt}{2}|_0^2 + \left(-\frac{2t}{\pi n}\cos\frac{\pi nt}{2} + \frac{4}{\pi^2 n^2}\sin\frac{\pi nt}{2}\right)|_2^4\right) \\ = -\frac{1}{2}\times\frac{2}{\pi n}\left(\cos\frac{\pi nt}{2}|_0^2 + t\cos\frac{\pi nt}{2}|_2^4\right) &= -\frac{1}{\pi n}(\cos\pi n - 1 + 4\cos 2\pi n - 2\cos\pi n) \\ &= -\frac{1}{\pi n}(3-\cos\pi n) = \frac{1}{\pi n}((-1)^n - 3). \end{aligned} \tag{15}$$

The desired expansion looks like

$$I(t) = 2 + \sum_{n=1}^{\infty}\left[\frac{2}{\pi^2 n^2}(1-(-1)^n)\cos\frac{\pi nt}{2} + \frac{1}{\pi n}((-1)^n - 3)\sin\frac{\pi nt}{2}\right]. \tag{16}$$

For all $t \in (0;2)$, we have in the open interval $(0;2)$ the sum of the series $s(t) = 1$, while in the open interval $(2;4)$, we have the sum of the series $s(t) = t$. At the point of jump discontinuity $t = 2$,

$$s(t) = \frac{f(2-) + f(2+)}{2} = \frac{1+2}{2} = \frac{3}{2}. \tag{17}$$

At points $t = 0$ and $t = 4$, the sum $s(t)$ is equal to

$$s(t) = \frac{f(0) + f(4)}{2} = \frac{1+4}{2} = \frac{5}{2}. \tag{18}$$

Consider the first nine terms of the series (16)

$$\begin{aligned} I(t) &= 2+\sum_{n=1}^{8}\left[\frac{2}{\pi^2 n^2}(1-(-1)^n)\cos\frac{\pi n t}{2}+\frac{1}{\pi n}((-1)^n-3)\sin\frac{\pi n t}{2}\right] \\ &= 2+\left(\frac{2}{\pi^2}(2)\cos\frac{\pi t}{2}+\frac{1}{\pi}(-4)\sin\frac{\pi t}{2}\right)+\left(\frac{1}{2\pi}(-2)\sin\pi t\right) \\ &+\left(\frac{2}{9\pi^2}(2)\cos\frac{3\pi t}{2}+\frac{1}{3\pi}(-4)\sin\frac{3\pi t}{2}\right)+\left(\frac{1}{4\pi}(-2)\sin 2\pi t\right) \\ &+\left(\frac{2}{25\pi^2}(2)\cos\frac{5\pi t}{2}+\frac{1}{5\pi}(-4)\sin\frac{5\pi t}{2}\right)+\left(\frac{1}{6\pi}(-2)\sin 3\pi t\right) \\ &+\left(\frac{2}{49\pi^2}(2)\cos\frac{7\pi t}{2}+\frac{1}{7\pi}(-4)\sin\frac{7\pi t}{2}\right)+\left(\frac{1}{8\pi}(-2)\sin 4\pi t\right). \end{aligned} \tag{19}$$

Figure 4 presents the graphs of the expansion of $I(t)$ into the Fourier series, taking into account from 3 to 8 terms in (16), respectively.

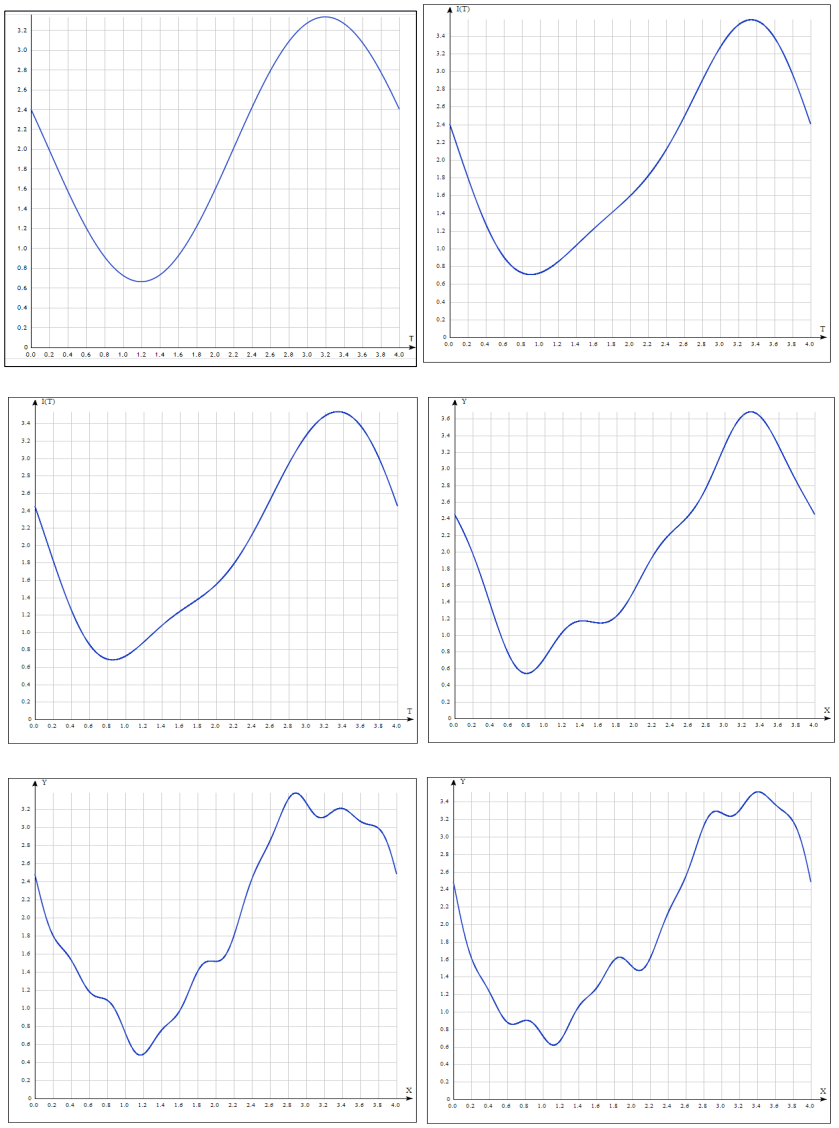


Figure 4. Visualization when increasing the terms of the Fourier series (from three members of the series to eight) as a function of the intensity of cyber attacks on damage to standard software.

Therefore, constant continuous monitoring and timely conduction of cyber regulatory control of the enterprise makes it possible to effectively ensure the cybersecurity of the enterprise in real time—predicting the emergence of cyber threats, to some extent—which, in turn, determines the management of cyber risks arising in the field of information security of the enterprise.

Such a Fourier series expansion of the piecewise continuous analytical approximating function of the intensity of cyber attacks on damage to standard software, obtained by approximating empirical–statistical slices of the intensity of cyber attacks on damage to standard software for each time period by analytical functions, opens up new mathematical possibilities of transition to systems of regulatory control of cyber threats of the enterprise from a discrete to a continuous automated process of regulatory control.

Figure 5 presents a graphical interpretation of the approximation of the time series of the intensity of cyber attacks on e-mail damage by analytical functions with averaged values for each time period.

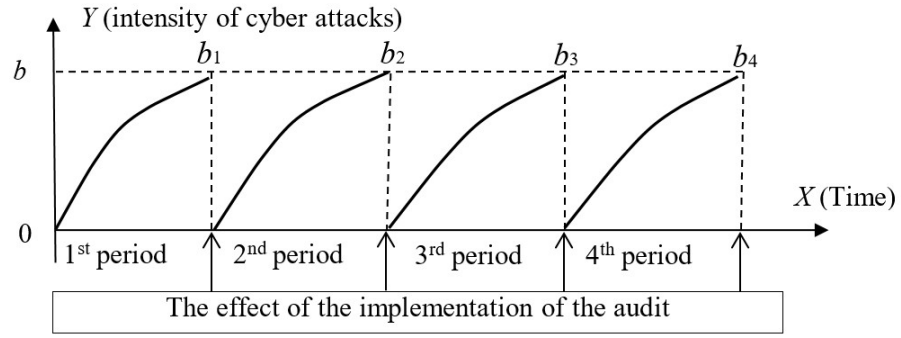


Figure 5. Dependence of the intensity of cyber attacks on e-mail damage on the frequency of regulatory control over 4 time intervals.

In view of the homogeneity of the behavior of the intensity of cyber attacks in each time period, the approximation of the statistical slices of the intensity of cyber attacks on e-mail damage for each period was carried out using analytical functions (Table 3).

Table 3. Approximation of time series of the intensity of cyber attacks on e-mail damage by analytical functions.

Time Period	An Equation of the Approximating Function on the Interval (0; 1)	Coefficient of Determination
1st period	$I(t) = -1.0754t^2 + 4.9954t$	0.7942
2nd period	$I(t) = -0.99164t^2 + 5.0127t$	0.8184
3rd period	$I(t) = -1.0032t^2 + 5.0073t$	0.8532
4th period	$I(t) = -1.0116t^2 + 5.0096t$	0.8258

Based on the data given in Table 3, it is possible to present analytically the function of the intensity of cyber attacks on e-mail damage, combining all periods in view of the standard cyclicality in each period. Then, analytically, the function of the intensity of cyber attacks can be represented as

$$I(t) = \begin{cases} -t^2 + 5t, & 0 \le t < 1, \\ -(t-1)^2 + 5(t-1), & 1 \le t < 2, \\ -(t-2)^2 + 5(t-2), & 2 \le t < 3, \\ -(t-3)^2 + 5(t-3), & 3 \le t \le 4. \end{cases} \tag{20}$$

Let us write the Fourier series for Function (20) only on the first interval, the graph of which is shown in Figure 6, since periodicity is performed on the other intervals. This

will make it possible to move the system of regulatory control of cyber attacks on damage to standard enterprise software from a discrete to a continuous automated process of regulatory control.

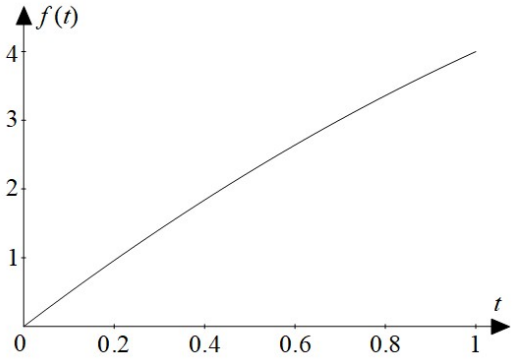


Figure 6. Analytical function of the intensity of cyber attacks on e-mail damage in the first time period.

Let us find the coefficients of the Fourier series for the function $f(t) = -t^2 + 5t$, $t \in [0;1]$.

The Fourier series expansion on the interval $(-T;T)$ has the form

$$f(t) = \frac{a_0}{2} + \sum_{n=1}^{\infty}\left(a_n \cos\frac{\pi nt}{T} + b_n \sin\frac{\pi nt}{T}\right), \tag{21}$$

$$a_0 = \frac{1}{T}\int_{-T}^{T} f(t)dt, \tag{22}$$

$$a_n = \frac{1}{T}\int_{-T}^{T} f(t) \times \cos\frac{\pi nt}{T}dt, \tag{23}$$

$$b_n = \frac{1}{T}\int_{-T}^{T} f(t) \times \sin\frac{\pi nt}{T}dt. \tag{24}$$

In our case, $T = 1$; so,

$$a_0 = \int_0^1 (-t^2 + 5t)dt = \left(-\frac{t^3}{3} + \frac{5t^2}{2}\right)|_0^1 = \frac{13}{6} - 0 = \frac{13}{6}, \tag{25}$$

$$\begin{aligned} a_n &= \int_0^1 (-t^2 + 5t) \times (\cos \pi nt)dt \\ &= \left[-t^2\frac{\sin(\pi nt)}{\pi n} + 5t\frac{\sin(\pi nt)}{\pi n} - 2t\frac{\cos(\pi nt)}{\pi^2 n^2} + 5\frac{\cos(\pi nt)}{\pi^2 n^2} + 2\frac{\sin(\pi nt)}{\pi^3 n^3}\right]|_0^1 \\ &= \left[4\frac{\sin(\pi n)}{\pi n} + 3\frac{\cos(\pi n)}{\pi^2 n^2} + 2\frac{\sin(\pi n)}{\pi n} - \frac{5}{\pi^2 n^2}\right] = \frac{3(-1)^n - 5}{\pi^2 n^2}, \end{aligned} \tag{26}$$

$$\begin{aligned} b_n &= \int_0^1 (-t^2 + 5t) \times \sin(\pi n t) dt \\ &= \left[-t^2 \frac{\cos(\pi n t)}{\pi n} - 5t \frac{\cos(\pi n t)}{\pi n} - 2t \frac{\sin(\pi n t)}{\pi^2 n^2} + 5 \frac{\sin(\pi n t)}{\pi^2 n^2} - 2 \frac{\cos(\pi n t)}{\pi^3 n^3} \right] |_0^1 \\ &= \left[-4 \frac{\cos(\pi n)}{\pi n} + 3 \frac{\sin(\pi n)}{\pi^2 n^2} - 2 \frac{\cos(\pi n)}{\pi^3 n^3} - \left(-\frac{2}{\pi^3 n^3} \right) \right] \\ &= 2 \frac{-2(-1)^n \pi^2 n^2 - (-1)^n + 1}{\pi^3 n^3}. \end{aligned} \tag{27}$$

Hence, for even numbers n ($n = 2k$), we have $b_n = 0$, and for odd n ($n = 2k - 1$),

$$b_k = \frac{4\pi^2 (2k-1)^2 + 4}{\pi^3 (2k-1)^3}. \tag{28}$$

Thus, we have

$$f(t) = \frac{13}{12} + \sum_{k=1}^{\infty} \left[\frac{3(-1)^k - 5}{\pi^2 k^2} \times \cos(\pi k t) + \frac{4\pi^2 (2k-1)^2 + 4}{\pi^3 (2k-1)^3} \times \sin(\pi (2k-1) t) \right]. \tag{29}$$

Figures 7–9 present graphs of the expansion of Function (20) on the interval (0;1) into the Fourier series, taking into account 3, 5, or 7 terms of the series, respectively.

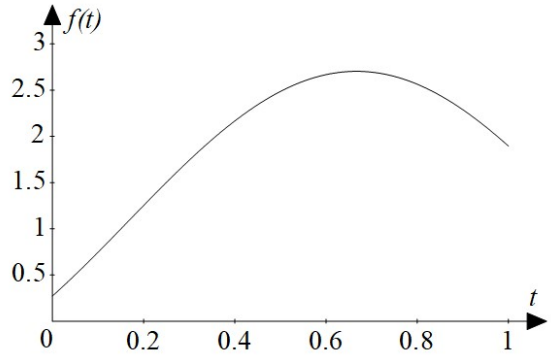


Figure 7. Expansion of the function of the intensity of e-mail cyber attacks in the Fourier series (29) for $k = 1$.

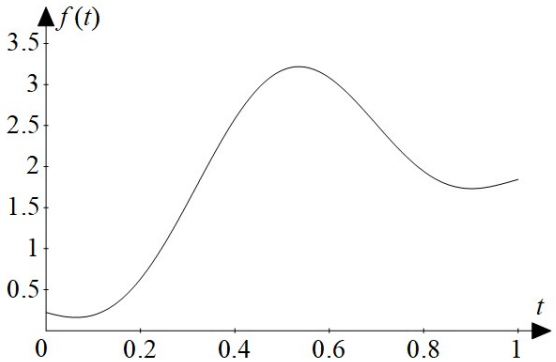


Figure 8. Expansion of the function of the intensity of e-mail cyber attacks in the Fourier series (29) for $k = 2$.

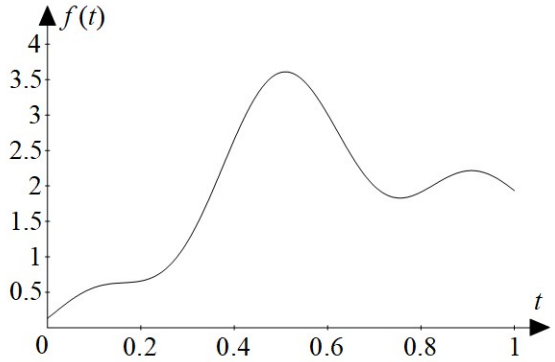


Figure 9. Expansion of the function of the intensity of e-mail cyber attacks in the Fourier series (29) for $k = 3$.

Figure 7 shows the graph of the function

$$f(t) = \frac{13}{12} - \frac{8\cos(\pi t)}{\pi^2} + \left(4 + 4\pi^2\right) \times \frac{\sin(\pi t)}{\pi^3}, \tag{30}$$

which is obtained from (29) for $k = 1$ on the interval $(0, 1)$.

Figure 8 shows the graph of the function

$$f(t) = \frac{13}{12} - \frac{8\cos(\pi t)}{\pi^2} + \left(4 + 4\pi^2\right) \times \frac{\sin(\pi t)}{\pi^3} - \frac{\cos(2\pi t)}{2\pi^2} + \left(4 + 36\pi^2\right) \times \frac{\sin(3\pi t)}{27\pi^3}, \tag{31}$$

which is obtained from (29) for $k = 2$ on the interval $(0, 1)$.

Figure 9 shows the graph of the function

$$\begin{aligned} f(t) = \frac{13}{12} - \frac{8\cos(\pi t)}{\pi^2} + \left(4 + 4\pi^2\right) \times \frac{\sin(\pi t)}{\pi^3} - \frac{\cos(2\pi t)}{2\pi^2} \\ + \left(4 + 36\pi^2\right) \times \frac{\sin(3\pi t)}{27\pi^3} - \frac{8\cos(3\pi t)}{9\pi^2} + \left(4 + 100\pi^2\right) \times \frac{\sin(5\pi t)}{125\pi^3}, \end{aligned} \tag{32}$$

which is obtained from (29) for $k = 3$ on the interval $(0, 1)$.

Therefore, with an increase in the number of terms of the Fourier series, the function will be continuous periodic in approximation to the piecewise continuous function, which enables constant continuous automated monitoring and timely conduction of cyber regulatory control of the enterprise in relation to e-mail attacks, which effectively ensures real-time cybersecurity of the enterprise.

This is due to the fact that information systems are widely implemented and used for processing, storing, and transmitting information, which, in turn, has led to the need to protect information systems, since information attacks can cause large financial and material losses. Auditing and monitoring serve to develop effective measures to ensure information security in enterprises, organizations, and institutions. With the help of an information security audit, the collection and analysis of information is carried out with regard to the information system being checked. It is conducted for the purpose of quantitative as well as qualitative assessment of the level of protection of the information system against possible attacks by intruders. The audit itself can provide an objective assessment of the security of any type of enterprise or institution, as well as prevent the realization of potential threats. The release of the company's products at the international level is not possible without the implementation of international and industry standards, such as ISO/IEC 27001:2013 "Information security management systems. Requirements", ITU-T X-1051 "Information security management systems. Requirements for telecommunications", as well as ISO/IEC 27035:2011 "Information technology. Security techniques. Information security incident management".

One of the most common types of audit is an active audit. It consists in studying the state of security of the information system from the point of view of an attacker (or an attacker with high IT skills). Active audits can be conditionally divided into two types—external and internal. Also, during an active audit, a study of system performance and stability, or stress test, is carried out. It is aimed at determining the critical load points at which the system, due to a denial-of-service attack or increased load, ceases to respond adequately to legitimate (defined by the security policy) user requests. The stress test will allow to identify "bottlenecks" in the process of formation and transmission of information and to determine the conditions under which normal operation of the system is impossible. Such testing involves simulating denial-of-service attacks as user requests to the system and conducting a general analysis of its performance. The result of an active audit is information about all vulnerabilities, degrees of their criticality and elimination methods, and information about publicly available information (information available to any potential violator) of the customer's network. Based on the results of an active audit, recommendations are provided for the modernization of the network protection system, which make it possible to eliminate dangerous vulnerabilities and, thus, increase the level of protection of the company's information system against the actions of an intruder with minimal costs for information security. It should be noted that the information security management system (ISMS) is a part of the overall management system, which is based on the assessment of business risks in order to create, implement, operate, constantly monitor, analyze, maintain, and improve the protection of information.

4. Conclusions

Constant continuous monitoring and regulatory control of enterprise's cyber threats provides management with key real-time information about the enterprise's cybersecurity efficiency, allowing not only to better understand problems when they occur but also to predict their occurrence, which improves the ability to manage risks and opportunities.

Note that the enterprise's comprehensive information security system should include both tactical aspects of information protection and strategic priorities, which are reflected in the information policy and information strategy of the enterprise.

Author Contributions: Conceptualization, V.S., O.B., A.M., I.T. and O.K.; methodology, V.S., O.B., A.M., I.T. and O.K.; formal analysis, V.S., O.B., A.M., I.T. and O.K.; investigation, V.S., O.B., A.M., I.T. and O.K.; writing—original draft preparation, V.S., O.B., A.M., I.T. and O.K.; writing—review and editing, V.S., O.B., A.M., I.T. and O.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not available.

Acknowledgments: The authors express their sincere gratitude for the opportunity to publish the work in this journal on a free basis.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Kal'chuk, I.V.; Kharkevych, Y.I. Approximation Properties of the Generalized Abel-Poisson Integrals on the Weyl-Nagy Classes. *Axioms* **2022**, *11*, 161. [CrossRef]
2. Kal'chuk, I.V.; Kharkevych, Y.I. Approximation of the classes $W^r_{\beta,\infty}$ by generalized Abel-Poisson integrals. *Ukr. Math. J.* **2022**, *74*, 575–585. [CrossRef]
3. Zhyhallo, T.V.; Kharkevych, Y.I. On approximation of functions from the class $L^{\psi}_{\beta,1}$ by the Abel-Poisson integrals in the integral metric. *Carpathian Math. Publ.* **2022**, *14*, 223–229. [CrossRef]
4. Zhyhallo, T.V.; Kharkevych, Y.I. Fourier transform of the summatory Abel–Poisson function. *Cybern. Syst. Anal.* **2022**, *58*, 957–965. [CrossRef]
5. Kharkevych, Y.; Stepaniuk, T. Approximate Properties of Abel-Poisson Integrals on Classes of Differentiable Functions Defined by Moduli of Continuity. *Carpathian Math. Publ.* **2023**, *15*, 286–294. [CrossRef]

6. Kharkevych, Y.I. On some asymptotic properties of solutions to biharmonic equations. *Cybern. Syst. Anal.* **2022**, *58*, 251–258. [CrossRef]
7. Kharkevych, Y.I. Approximation Theory and Related Applications. *Axioms* **2022**, *12*, 736. [CrossRef]
8. Kharkevych, Y.I. Approximative properties of the generalized Poisson integrals on the classes of functions determined by a modulus of continuity. *J. Autom. Inf. Sci.* **2019**, *51*, 43–54. [CrossRef]
9. Bushev, D.; Abdullayev, F.; Kal'chuk, I.; Imashkyzy, M. The use of the isometry of function spaces with different numbers of variables in the theory of approximation of functions. *Carpathian Math. Publ.* **2021**, *13*, 805–817. [CrossRef]
10. Bushev, D.N.; Kharkevych, Y.I. Finding Solution Subspaces of the Laplace and Heat Equations Isometric to Spaces of Real Functions, and Some of Their Applications. *Math. Notes* **2018**, *103*, 869–880. [CrossRef]
11. Laptiev, O.; Shuklin, G.; Hohonianc, S.; Zidan, A.; Salanda, I. Dynamic model of ceber defence diagnostics of information systems with the use of Fozzy technologies. In Proceedings of the IEEE ATIT Conference, Kyiv, Ukraine, 18–20 December 2019; pp. 116–120. [CrossRef]
12. Laptiev, O.; Savchenko, V.; Kotenko, A.; Akhramovych, V.; Samosyuk, V.; Shuklin, G.; Biehun, A. Method of determining trust and protection of personal dat a in social networks. *Int. J. Commun. Netw. Inf. Secur.* **2021**, *13*, 15–21.
13. Laptiev, O.; Savchenko, V.; Pravdyvyi, A.; Ablazov, I.; Lisnevskyi, O.; Kolos, V.; Hudyma, V. Method of detecting radio signals using means of covert by obtaining information on the basis of random signals model. *Int. J. Commun. Netw. Inf. Secur.* **2021**, *13*, 48–54. [CrossRef]
14. Laptiev, O.; Tkachev, O.; Pravdyvyi, A.; Maystrov, O.; Krasikov, P.; Open'ko, P.; Khoroshko, V.; Parkhuts, L. The method of spectral analysis of the determination of random digital signals. *Int. J. Commun. Netw. Inf. Secur.* **2021**, *13*, 271–277. [CrossRef]
15. Halakhov, Y.M.; Barabash, O.V. Strategic priorities of the information security system of an enterprise that engages a freelance resource. Modern information protection. *DUT* **2019**, *3*, 30–35. (In Ukrainian)
16. Kapustian, O.A.; Kapustyan, O.V.; Ryzhov, A.; Sobchuk, V. Approximate Optimal Control for a Parabolic System with Perturbations in the Coefficients on the Half-Axis. *Axioms* **2022**, *11*, 175. [CrossRef]
17. Yevseiev, S.; Khokhlachova, Y.; Ostapov, S.; Laptiev, O.; Korol, O.; Milevskyi, S. *Models of Socio-Cyber-Physical Systems Security*; Monograph; PC Technology Center: Kharkiv, Ukraine, 2023; p. 184. [CrossRef]
18. Laptiev, V.; Musienko, A.; Nakonechnyi, A.; Sobchuk, V.; Gakhov, S.; Kopytko, S. Algorithm for Recognition of Network Traffic Anomalies Based on Artificial Intelligence. In Proceedings of the 5th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Istanbul, Turkiye, 8–10 June 2023; pp. 1–5. [CrossRef]
19. Sobchuk, V.; Olimpiyeva, Y.; Musienko, A.; Sobchuk, A. Ensuring the properties of functional stability of manufacturing processes based on the application of neural networks. *CEUR Workshop Proc.* **2021**, *2845*, 106–116.
20. Barabash, O.; Tverdenko, V.; Sobchuk, V.; Musienko, A.; Lukova-Chuiko, N. The Assessment of the Quality of Functional Stability of the Automated Control System with Hierarchic Structure. In Proceedings of the 2020 IEEE Second International Conference on System Analysis and Intelligent Computing (SAIC), Kyiv, Ukraine, 5–9 October 2020; Igor Sikorsky Kyiv Polytechnic Institute: Kyiv, Ukraine, 2020; pp. 1–4. [CrossRef]
21. Sobchuk, V.; Barabash, O.; Musienko, A.; Laptiev, V.; Kozlovskyi, V.; Shcheblanin, Y. Evaluation of Efficiency of Application of Functionally Sustainable Generalized Information System of the Enterprise. In Proceedings of the 2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Ankara, Turkey, 9–11 June 2022; pp. 1–7. [CrossRef]
22. Kapustyan, O.V.; Kapustyan, O.A.; Sukretna, A.V. Approximate stabilization for a nonlinear parabolic boundary-value problem. *Ukr. Math. J.* **2011**, *63*, 759–767. [CrossRef]
23. Nakonechny, A.G.; Kapustian, O.A.; Chikrii, A.A. Control of impulse systems in a conflict situation. *J. Autom. Inf. Sci.* **2019**, *51*, 1–11. [CrossRef]
24. Nosenko, T.V.; Stanzhyts'kyi, O.M. Averaging method in some problems of optimal control. *J. Nonlinear Oscil.* **2008**, *11*, 539–547. [CrossRef]
25. Zamrii, I.; Haidur, H.; Sobchuk, A.; Hryshanovych, T.; Zinchenko, K.; Polovinkin, I. The Method of Increasing the Efficiency of Signal Processing Due to the Use of Harmonic Operators. In Proceedings of the IEEE 4th International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, 15–17 December 2022; pp. 138–141. [CrossRef]
26. Cheung, C.M.; Goyal, P.; Prasanna, V.K.; Tehrani, A.S. Oreonet: Deep convolutional network for oil reservoir optimization. In Proceedings of the IEEE International Conference on Big Data, Boston, MA, USA, 11–14 December 2017; pp. 1277–1282. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.