Setting the Optimum Time for a Special Audit to Improve the Enterprise's Cyber Security

Barabash Oleg, Halakhov Yevhen

Abstract**: *The article presents a method for setting the optimal time for special audit to improve the level of cyber defense of an enterprise working in the field of market relations of IT services. Studying the issue of providing measures to reduce the risk of a cyber-incident, analyzed the time series of the intensity of cyber-attacks of the enterprise. An analytical function of the cyber-attack intensity at an enterprise that satisfies the nonlinear Bernoulli differential equation is considered. The elasticity interval of the analytic function of the cyber-attack intensity at the enterprise is found. Analysis of cyber-attack time series on the enterprise system for the same time periods falling within the time interval from the end of the planned audit to the beginning of the next one. An analytical alignment of the time series of the cyber-attack intensity function was performed using a logistic curve. A stepwise p-transformation of a small parameter into a cyber-attack intensity function for an enterprise was introduced and the dimensionlessness of the variables was performed, which made it possible to calculate the sensitivity of a dimensionless cyber-attack intensity function from a small parameter p over a set time period. The study is based on the application of the theory of elasticity of the intensity function of cyber-attacks, which determines the time interval at which to conduct a special audit at the enterprise. Due to the found elasticity interval of the cyber-attack intensity function, the optimal time for special audit was determined.***

Keywords: cyber security, time series, cyber-attack intensity, logistic curve, elasticity, Bernoulli equation, p-transformations, filtering, special audit.

I. INTRODUCTION

Enterprise cyber security as a component of information security is defined as the protection of local and cloud business infrastructure, as well as the verification of third-party vendors and the protection of the growing number of endpoints connecting to the enterprise information system via the Internet [1]. As the threat and cost of cybercrime grows, so does the need for tactical actions (express audits, etc.) and a comprehensive enterprise information security strategy [3]. The modern approach of enterprise risk management consists of the following successive stages: predicting the number of possible cyber-attacks, conducting their statistical and analytical evaluation of cyber-attacks, timely identification, developing a plan of action and preventive measures to eliminate identical cyber-attacks, implementing a control system and introducing modernized approaches to the appropriate approaches [4].

In modern conditions there is a need for mathematical modeling of time series of cyber-attack intensity per enterprise and presentation of effective solutions for enhancing information security of the enterprise [1]. The analysis of cyber-attacks between planned audits has received little attention in the technical literature [2]. The authors in [3] study different types of attacks. The identification of characteristics of cyber-attacks is devoted to work [4, 5, 6]. The denial of service (DoS) cyber-attacks [7], the study of worms and botnet activity [8], the analysis of data on the number of cyber-attacks collected in a black hole [9] and in one-way motion [10] are investigated in the scientific literature. Studies [11, 12] are devoted to classifying data into classes. In [13], the position of the enterprise cyber security is characterized on the basis of data collected in black holes.

It should be noted that today the problem of the study of the intensity of cyber-attacks and their prediction is poorly understood. This is due to the unpredictability of cyber-attacks and the lack of statistics in many cases, as well as the methods available for predicting them. It should be noted that auditing is a complex process that determines strategic priorities and guidelines of information security of the enterprise. Rapid detection and response and protection of critical infrastructure and functions along with powerful information sharing are key issues that need to be addressed [13]. One aspect of addressing this is to conduct timely audits, which are not only limited to routine screening, but also provide insight into and take appropriate steps to prevent cyber-attacks [13]. Upon completion of the audits, a comprehensive research report is provided that identifies areas that need to be addressed to improve security. An enterprise audit report is used to identify areas in the corporate environment that can be improved through cyber security controls [14]. The results of this report provide useful examples, recommendations, and links. In general, the report has a baseline that can be used to improve security by taking tangible steps and avoiding further risk.

II. METHODOLOGY

The simulation of the cyber-attack intensity function is based on a retrospective statistical analysis of cyber-attack time series and the application of time series filtering, which made it possible to eliminate peak points for smoothing it. The problem of defining audit timeframes and approximating statistical sections with analytical functions is achieved by statistical analysis methods and graphical visualization of cyber risk identification.

Revised Manuscript Received on February 15, 2020.

***** Correspondence Author

Barabash Oleg, Department of Mathematics, State University of Telecommunications, Kyiv, Ukraine, E-mail bar64@ukr.net

Halakhov Yevhen*, Department of Mathematics, State University of Telecommunications, Kyiv, Ukraine. E-mail evgen.galakhov@gmail.com

Retrieval Number: C4677029320 /2020©BEIESP
DOI: 10.35940/ijeat.C4677.029320

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

The development of a forecasting and analytical model for conducting audits is based on the theory of elasticity, which determines the finding of the elasticity interval of the cyber-attack intensity function, which is subject to the logistic law, which made it possible to apply modernized approaches to the existing audit system of the enterprise. Thus, continuous on-going monitoring and auditing of enterprise cyber threats provides management with key, real-time information on enterprise cyber security effectiveness, enabling them to not only better understand their occurrence issues, but also to anticipate their occurrence, which improves their ability to manage risks and opportunities.

Note that a comprehensive enterprise information security system should include both tactical aspects of information security (express audit of information threats to the enterprise), as well as strategic priorities, which reflects the information policy and information strategy of the enterprise.

III. RESULTS

Let's present mathematical modeling of cyber-attack intensity times per enterprise to provide complex solutions and forecasts for enhancing enterprise resilience against current targeted cyber threats.

Consider the functional dependence of cyber-attack intensity $I_K(t)$, which is the solution of the nonlinear Bernoulli differential equation, which, according to the hypothesis that the integral cyber-attack intensity function is subject to the logistic law, describes the process of the time series of cyber-attack intensity:

$$\frac{\dot{I}_K(t)}{I_K(t)} = \zeta \cdot \frac{I_K(t)_{Max} - I_K(t)}{I_K(t)_{Max}}, \qquad (1)$$

$$I_K(0) = I_{K_0}, \quad \zeta = \frac{\alpha}{\beta}.$$

Where $I_K(t)_{Max}$ - the maximum possible level of function of intensity of cyber-attacks;

$I_K(0) = I_{K_0}$ - the initial level of cyber-attack intensity function after a scheduled audit;

$\frac{\dot{I}_K(t)}{I_K(t)}$ - relative change in the rate of intensity of cyber-attacks;

$\frac{I_K(t)_{Max} - I_K(t)}{I_K(t)_{Max}} = 1 - \frac{I_K(t)}{I_K(t)_{Max}}, \quad 0 < \frac{I_K(t)}{I_K(t)_{Max}} < 1$ - the relative deviation of the value of the function of the intensity of cyber-attacks from its maximum possible level, as a proportion of possible damage to the enterprise system of cyber-attacks, provided that timely and special audits are not conducted;

$\zeta = \frac{\alpha}{\beta}$ - The level of cyber-attack threat correction due to the regular audit;

α - The level of threats to the information security of the enterprise, which could be affected if approached $I_K(t)_{Max}$ subject to late audits;

β - Coefficient of influence of factors of information security system on the function of intensity of cyber-attacks.

Equation (1) is written in the form:

$$\frac{\dot{I}_K(t)}{I_K(t)} = \zeta \cdot \left(1 - \frac{I_K(t)}{I_K(t)_{Max}}\right),$$

$$0 < \frac{I_K(t)}{I_K(t)_{Max}} < 1, I_K(0) = I_{K_0}, \quad \zeta = \frac{\alpha}{\beta}. \qquad (2)$$

The solution of differential equation (2) is obtained in the form:

$$I_K(t) = \frac{I_K(t)_{Max}}{1 + \frac{I_K(t)_{Max} - I_{K_0}}{I_{K_0}} \cdot e^{-\zeta \cdot t}} \qquad (3)$$

Point $D\left(\frac{1}{\zeta} \cdot \ln \frac{I_K(t)_{Max} - I_{K_0}}{I_{K_0}}, \frac{I_K(t)_{Max}}{2}\right)$ - inflection point. Find the boundary:

$$\lim_{t \to \infty} I_K(t) = \lim_{t \to \infty} \frac{I_K(t)_{Max}}{1 + \frac{I_K(t)_{Max} - I_{K_0}}{I_{K_0}} \cdot e^{-\zeta \cdot t}} = I_K(t)_{Max} \qquad (4)$$

Thus, $I_K(t) = I_K(t)_{Max}$ - the horizontal asymptote of the s-curve.

In Fig. 1 depicts the intensity curve of cyber-attacks from time to time with the inflection point D at which the inflection tangent is made.

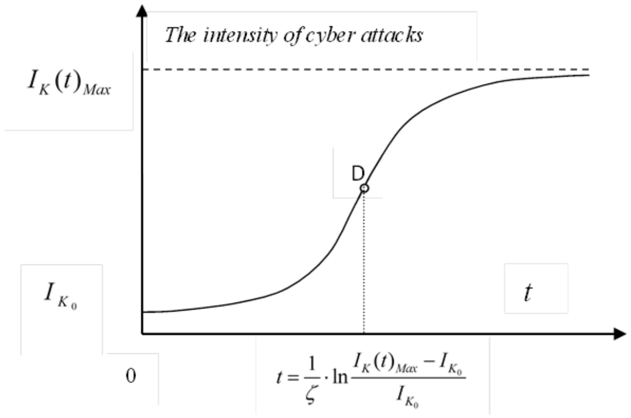


Fig.1. Logistic curve of function of intensity of cyber-attacks of the enterprise depending on the time

Source: authors development

Calculate the elasticity El_t of the intensity of cyber-attacks enterprise versus time using the following formula:

$$El_t = \frac{t \cdot I_K{}'(t)}{I_K(t)} > 1. \qquad (5)$$

By the formula (5) we find:

$$\zeta\cdot\frac{I_K(t)_{Max}-I_{K_0}}{I_{K_0}}\cdot t-\frac{I_K(t)_{Max}-I_{K_0}}{I_{K_0}}>e^{\zeta\cdot t}. \qquad (6)$$

Therefore, the inequality solution (6) is the elasticity interval. When determining the parameters $\frac{I_K(t)_{Max}-I_{K_0}}{I_{K_0}}$, $\frac{1}{\zeta}$, inequality (6) is solved numerically. Thus, it is possible to determine the elasticity interval $\left[t_1^{el},t_2^{el}\right]$ (Fig. 2).

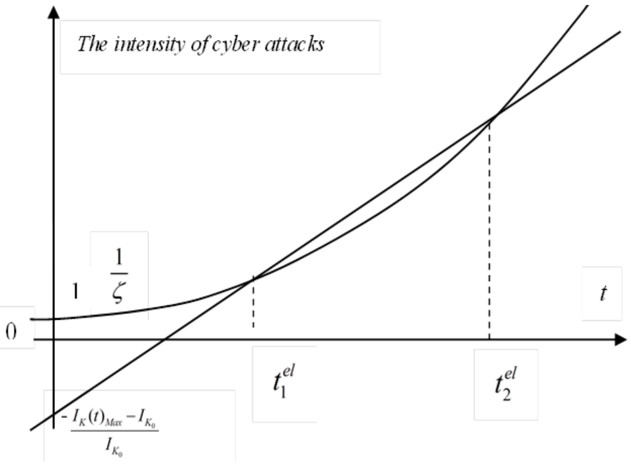


Fig. 2. Finding the elasticity interval
Source: authors development

For conveniences in the formula (3) introduce a replacement:

$$I_K(t)=y(t),\quad I_K(t)_{Max}=k,\quad -\zeta=a,\quad \frac{I_K(t)_{Max}-I_{K_0}}{I_{K_0}}=b.$$

Then we rewrite the function $y(t)=\frac{k}{1+b\cdot e^{at}}$ as:

$$\frac{k}{y(t)}-1=b\cdot e^{at}, \qquad (7)$$

logarithm (7), we have

$$\ln\left(\frac{k}{y(t)}-1\right)=\ln b+at.$$

Let's introduce a new designation:

$$B(t)=\ln\left(\frac{k}{y(t)}-1\right)$$

Then write the system of normal equations:

$$\begin{cases}\sum B(t)=n\ln b+a\sum t,\\ \sum B(t)\cdot t=\ln b\sum t+a\sum t^2.\end{cases} \qquad (8)$$

Let the statistical regression approximation, as the solution of system (8), be:

$$y(t)=\frac{k}{1+b\cdot e^{at}}. \qquad (9)$$

Find the difference of inverted neighboring values:

$$\frac{1}{y(t+1)}-\frac{1}{y(t)}=\frac{b\cdot e^{at}\cdot(e^a-1)}{k}=\frac{\left(\frac{k}{y(t)}-1\right)\cdot(e^a-1)}{k},$$

Then

$$\frac{1}{y(t+1)}=\frac{(e^a-1)}{k}+e^a\cdot\frac{1}{y(t)}, \qquad (10)$$

Let's estimate the parameters $\frac{(e^a-1)}{k}$ and. e^a. We find the minimum of the function:

$$\min\left\{\sum\left(\frac{1}{y(t)}-\frac{1}{y(t)}\right)^2\right\}, \qquad (11)$$

Write the system of normal equations in the following form:

$$\begin{cases}\sum_{t=1}^{n-1}\frac{1}{y(t+1)}=(n-1)\cdot\frac{(1-e^a)}{k}+e^a\cdot\sum_{t=1}^{n-1}\frac{1}{y(t)},\\ \sum_{t=1}^{n-1}\frac{1}{y(t+1)}\cdot\frac{1}{y(t)}=\frac{(1-e^a)}{k}\cdot\sum_{t=1}^{n-1}\frac{1}{y(t+1)}+e^a\cdot\sum_{t=1}^{n-1}\frac{1}{y(t)^2},\end{cases} \qquad (12)$$

The solution to this system is:

$$e^a=\frac{(n-2)}{(n-1)\cdot\sum_{t=1}^{n-1}\frac{1}{y(t)^2}-\left(\sum_{t=1}^{n-1}\frac{1}{y(t)}\right)^2},$$

$$\frac{(1-e^a)}{k}=\frac{\sum_{t=1}^{n-1}\frac{1}{y(t+1)}\cdot\sum_{t=1}^{n-1}\frac{1}{y(t)}-\sum_{t=1}^{n-1}\frac{1}{y(t)}\cdot\sum_{t=1}^{n-1}\frac{1}{y(t+1)}\cdot\frac{1}{y(t)}}{(n-1)\cdot\sum_{t=1}^{n-1}\frac{1}{y(t)^2}-\left(\sum_{t=1}^{n-1}\frac{1}{y(t)}\right)^2}=A.$$

Where

$$k=\frac{1-e^a}{A}. \qquad (13)$$

Thus, after estimating the parameters *k* and *a* of equation (6), we proceed to the estimation of parameter *b*. To do this, we transform equation (10):

$$\frac{k}{y(t)}-1=b\cdot e^{at},$$

after logarithm, we get:

$$\frac{\sum_{t=1}^{n}\ln b}{n}=\frac{-a\cdot\sum_{t=1}^{n}\frac{n(n+1)}{2}}{n}+\frac{\sum_{t=1}^{n}\ln\left(\frac{k}{y(t)}-1\right)}{n}.$$

Let's assume that

$$\sum_{t=1}^{n}\ln\left(\frac{k}{y(t)}-1\right)=\sum_{t=1}^{n}\ln\left(\frac{k}{y(t)}-1\right) \qquad (14)$$

Then we have:

$$\ln b=\frac{-a\cdot(n+1)}{2}+\frac{1}{n}\cdot\sum_{t=1}^{n}\ln\left(\frac{k}{y(t)}-1\right).$$

Retrieval Number: C4677029320 /2020©BEIESP
DOI: 10.35940/ijeat.C4677.029320

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Apply to the intensity function of cyberattacks *p*-transformation of the following form:

$$I_K(t) \to i_K(t)^{p-1}, p \in (0,1) \cup (1,\infty). \quad (15)$$

Taking into account the p-transformation, equation (2) is transformed as follows:

$$-(p-1) \cdot i_K(t)^{-p} + \zeta \cdot i_K(t)^{1-p} = \zeta \cdot \frac{1}{i_K(t)^{p-1}{}_{Max}}.$$

Given the replacement $i_K(t)^{1-p} = \Psi$, we have:

$$\dot{\Psi} + \zeta \cdot \Psi = \zeta \cdot \frac{1}{i_K(t)^{p-1}{}_{Max}}, \Psi(0) = i_K{}^{1-p}(0). \quad (16)$$

The general solution to this equation is:

$$\Psi = \frac{1}{i_K(t)^{p-1}{}_{Max}} + ce^{-\zeta t}. \quad (17)$$

Now we obtain the solution of differential equation (16) in the form:

$$i_K(t) = \frac{i_K(t)_{Max}}{\left(1 + \frac{i_K(t)^{p-1}{}_{Max} - i_K{}^{p-1}(0)}{i_K{}^{p-1}(0)} \cdot e^{-\zeta t}\right)^{\frac{1}{p-1}}} \quad (18)$$

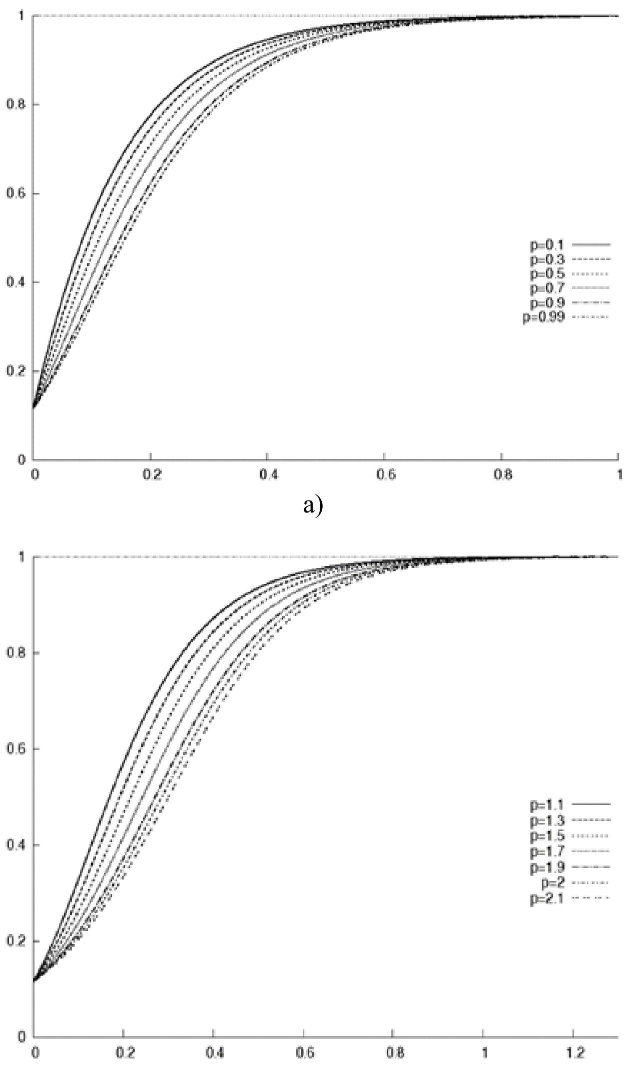
Finally, we obtain the intensity function of cyber-attacks, taking into account the degree of *p*-transformation in the form:

$$i_K{}^*(t) = \frac{1}{\left(1 + \frac{1 - i_K{}^*(0)}{i_K{}^*(0)} \cdot e^{-\zeta t^*}\right)^{\frac{1}{p-1}}}, i_K{}^*(t) = \frac{i_K(t)}{i_K(t)_{Max}}, t^* = \frac{t}{T}. \quad (19)$$

Consider the statistics of the number of cyber attacks on the enterprise, provided that the scheduled audit is carried out once a quarter.

In Fig. 3 presents a geometric visualization of the change in the slope of the logistic curve of the intensity of cyber-attacks at a parameter and in steps of 0.2 over a period of time T.

Therefore, it is necessary to approximate the total number of statistics for 4 periods for 2017 - 2019 with the selection of the appropriate parameters p with p-transformation and to find a predictable confidence interval of the intensity function of cyberattacks, which will allow to apply the theory of elasticity of the function of cyberattacks, which, in turn, will lead to the definition of a time interval in which to conduct a special audit at the enterprise. Thus, based on formulas (8) - (12), it is possible to perform an analytical alignment of the time series for the cyberattack intensity function using a logistic curve. Considering that the scheduled audits were conducted at the beginning of the quarters, let us consider the cyber attack time series on the enterprise system for the same time periods from July to November (1.07-30.09) 2017-2019, which falls in the time period from the end of the third audit to the beginning of the fourth.



a)

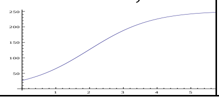
b)

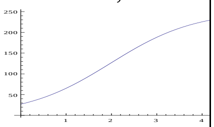
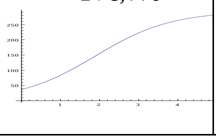
Fig. 3. Changing the slope of the logistic curve of the intensity of cyber-attacksin increments of 0.2 for the time period T at the parameter: a) $p \in (0,1)$; b) $p \in (1, \ \ 2.1)$

Source: author's calculations

In the table. 1 presents the analytical alignment of the time series of cyberattacks on the enterprise system in the period 1.07-30.09 2017-2019 with the provisional three-point filtering.

Table- I: Analytical alignment of cyberattack time periods on the enterprise system in the period 1.07-30.09 2017-2019

Time perio d	**Logistic model** **Graph of analytical alignment of the intensity of cyber-attacks**	**Inequality of elasticity** **Elasticity interval** $t^* \in \left[t_1^{el}, t_2^{el}\right]$
1.07-30.09 2017 p.	$I_K(t) = \frac{253,47}{1 + 9,41 \cdot e^{-1.}}$ 	$9,317t^* - 9,41 > e^{0,23t^*}$ $t^* \in (0,42; \ 0,51)$

1.07-30.09 2018 p.	$I_K(t)=\frac{241,35}{1+8,07\cdot e^{-1.31t}}$ 	$8,31t^*-8,07>e^{0,39t^*}$ $t^*\in(0,64;\ 0,93)$
1.07-30.09 2019 p.	$I_K(t)=\frac{261,23}{1+8,77e^{-1,19t}}$ 	$8,664t^*-8,77>e^{0,19t^*}$ $t^*\in(0,65;\ 0,91)$

Source: author's calculations based on enterprise data

Using p-conversion function intensity of cyber-attacks on the company, for the solution of equation (18) as:

$$I_K(t)\to i_K(t)^{p-1},\ p\in(0,1)\cup(1,\infty)$$

the solution of equation (1) is transformed to a dimensionless appearance of the form:

$$i_K{}^*(t)=\frac{1}{\left(1+\frac{1-i_K{}^*(0)}{i_K{}^*(0)}\cdot e^{-\zeta t^*}\right)^{\frac{1}{p-1}}},$$

$$i_K{}^*(t)=\frac{i_K(t)}{i_K(t)_{Max}}, \qquad t^*=\frac{t}{T} \qquad (20)$$

where T is the period between scheduled audits.

This makes it possible to find the sensitivity of the dimensionless cyberattack intensity function from the parameter *p*.

Figure 4 presents the sensitivity of the cyberattack intensity function from the parameter $p\in[1,9;2,15]$ for the period 1.07-30.09 2019 provided that the time series filtering is performed on three points. Curve labels (dotted lines) indicate inflection points.

The graph with vertical lines shows the time interval of the elasticity of the cyberattack intensity function, which determines the effective time of the special audit (0.64; 0.93) or, from the 57th day after the scheduled audit to the 83rd day, a special audit is required.

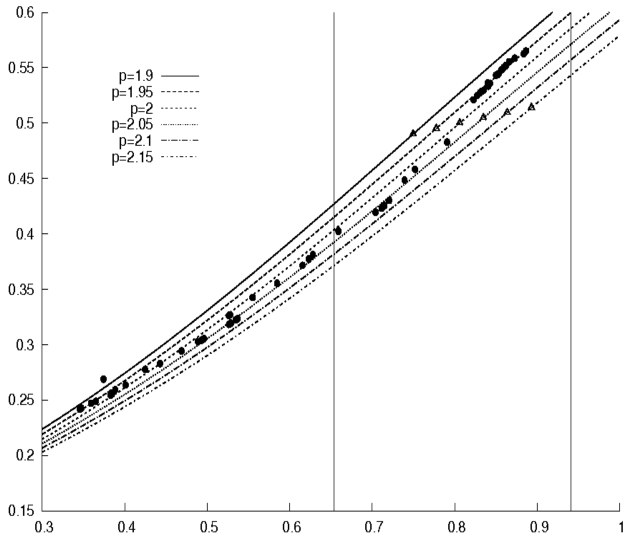


Fig. 3. Sensitivity of dimensionless cyberattack intensity function from the parameter *p* for the period 1.07-30.09 2019 provided time series filtering on three points.

Source: author's calculations

Figure 4 shows the sensitivity of the cyberattack intensity function within the confidence interval at the parameter $p\in[1,9;2,1]$.

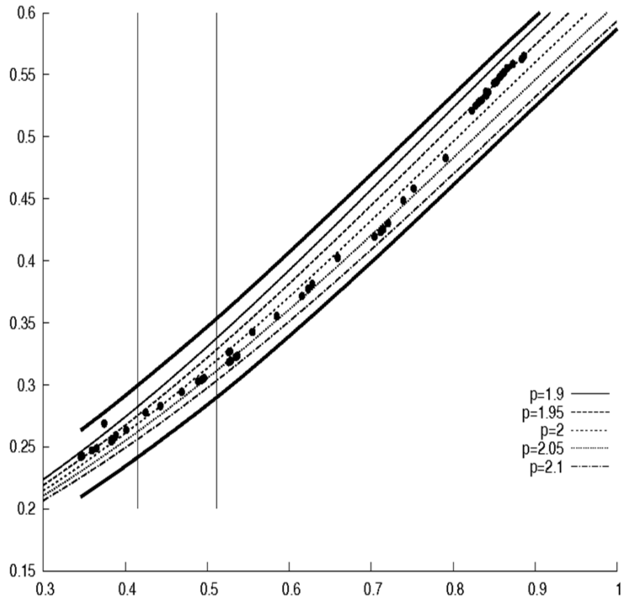


Fig. 4. Sensitivity of dimensionless cyberattack intensity function from the parameter for the period 1.10-30.11 2019 provided time series filtering on three points.

Source: author's calculations

The graph with vertical lines shows the time interval of the elasticity of the cyberattack intensity function, which determines the effective time of the special audit $t^*\in(0,42;\ 0,51)$ or starting from the 37th day after the scheduled audit to the 43rd day, a special audit is required.

IV. DISCUSSION

As new IT technologies emerge, the intensity of new cyber-attacks on enterprise IT systems increases. Traditional cyber security measures do not prevent or prevent these attacks because of their speed and frequency. In today's context, there is a need for mathematical modeling of time series of cyber-attack intensity for an enterprise to provide complex solutions and forecasts for enhancing the firm's resilience against current cyber-targeted targets.

V. CONCLUSION

The elasticity interval of the analytic function of the cyber-attack intensity per enterprise, which satisfies the nonlinear Bernoulli differential equation, and the analytical alignment of the time series of the cyber-attack intensity function by means of a logistic curve (with the provisional filtering of time series, enterprises for the same 2017-2019 time periods that fall within the time period from the end of the planned audit to the beginning of the next one.

Mathematical modeling of time series of cyber-attack intensity per enterprise is considered from the point of view of analytical interpretation by means of the nonlinear 1st order Bernoulli differential equation describing the process of time series of cyber-attack intensity. This made it possible to introduce a small parameter into the cyber-attack intensity function, which expresses the sensitivity of the logistic curve to the change in statistics and analytically characterizes the change in the slope of the logistic curve of the cyber-attack intensity. For the analysis of the cyber-attack intensity function, a power p-transform was applied by an analytical function. Applying the p-transform to the cyber-attack intensity function of an enterprise, given the dimensionlessness of the variables, the sensitivity of the dimensionless cyber-attack intensity function from the parameter p for the set time period of the year is presented, provided that three time points are pre-filtered. The optimum time for the special audit after the scheduled audit is determined.

The study is based on the application of the theory of elasticity of the function of intensity of cyber-attacks, which determines the time interval at which it is effective to conduct special audit at the enterprise.

REFERENCES

1. Xu, Tingyang, Jiangwen Sun and Jinbo Bi (2015) ”Longitudinal lasso: Jointly learning features and temporal contingency for outcome prediction”. ACM, KDD 2015.
2. Zhenxin Zhan, Maochao Xu and Shouhuai Xu. (2016) “Predicting Cyber Attack Rates with Extreme Values”. arXiv:1603.07432v1 [cs.CR] 24 Mar 2016.
3. IBM i2 Enterprise Insight Analysis for Cyber Threat Hunting. ZZS03196-USEN-06. URL: https://www.ibm.com/downloads/cas/WZKLWGPB
4. A. Joulin, E. Grave, P. Bojanowski and T. Mikolov (2017) “Bag of tricks for efficient text classification”. In Proceedings of the 15th Conference of the European Chapter of the Association for Computational Linguistics: Volume 2, Short Papers. Association for Computational Linguistics, April 2017, pp. 427–431.
5. R. A. Bridges, C. L. Jones, M. D. Iannacone, K. M. Testa and J. R. Goodall (2014) “Automatic labeling for entity extraction in cyber security”. In ASE Third International Conference on Cyber Security, Academy of Science and Engineering (ASE), 2014.
6. S. K. Lim, A. O. Muis, W. Lu and C. H. Ong (2017) “Malwaretextdb: A database for annotated malware articles”. Proceedings of the 55th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers). Vancouver, Canada: Association for Computational Linguistics, July 2017, pp. 1557–1567. [Online]. Available: http://aclweb.org/anthology/P17-1143.
7. B. J. Dorr, M. Petrovic, J. F. Allen, C. M. Teng and A. Dalton (2014) “Discovering and characterizing emerging events in big data”. AAAI Fall Symposium Series, 2014.
8. Sauerwein, C. Sillaber, M. M. Huber, A. Mussmann and R. Breu (2018) “The tweet advantage: An empirical analysis of 0-day vulnerability information shared on twitter”. IFIP International Conference on ICT Systems Security and Privacy Protection. Springer, 2018, pp. 201–215.
9. Babko-Malaya O., Cathey R., Hinton S., Maimon D. and Gladkova T. (2017) “Detection of hacking behaviors and communication patterns on social media”. In: Proceedings of the 2017 IEEE International Conference on Big Data, pp. 4636 – 4641.
10. Accenture Security (2017). Cost of cybercrime study. https://www.accenture. com/us-en/insight-cost-of-cybercrime-2017. Accessed 5 Jan 2018.
11. Shuklin GV, Barabash OV A method of constructing a stabilization function for cybersecurity control based on a mathematical model of oscillations under the influence of delayed forces. Telecommunication and information technologies. Kiev. 2018. No. 2 (59). Pp. 110–116.
12. Tetiana Bludova, Nataliya Danylyuk, Oleksandr Dima, Olean Kashan, Olean Horokhova. Implementation of manufacturer and reseller interaction models, taking into account advertising costs. International Journal of Recent Technology and Engineering (IJRTE), published by “Blue Eyes Intelligence Engineering & Sciences Publication”. 2019. Vo. 8, Issue 4, pp. 4727-4736.
13. Bilge L., Han Y. and Dell’Amico M (2017). “Riskteller: Predicting the risk of cyber incidents”. In: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS). ACM, New York. pp 1299 – 1311. https://doi.org/10.1145/3133956.3134022.
14. Okutan A., Yang S.J. and McConky K. (2018). “Forecasting cyber-attacks with imbalanced data sets and different time granularities”. CoRR abs/1803.09560. http://arxiv.org/abs/1803.09560. 1803.09560

AUTHORS PROFILE

Barabash Oleg, doctor of technical sciences, professor, Head of the Department of Mathematics, State University of Telecommunications,Kyiv, Ukraine.

Barabash Oleg defended his dissertation for a doctor of technical sciences degree on the topic "Methodology of building functionally stable distributed special purpose information systems". Barabash Oleg teaches the following disciplines: Higher Mathematics, Probability Theory and Mathematical Statistics, Information Security of the State, Information Security Systems.

Scientific interests: Signal processing with frequency and phase shift keying modulation in telecommunications, Optimization of Parameters at SDN Technologie Networks, Models for Analysis and Prognostication of the Indicators of the Distributed Computer Systems’ Characteristics.

Halakhov Yevhen, Senior Lecturer of the Department of Mathematics, State University of Telecommunications, Kyiv, Ukraine.

Professional Education: National Aviation University. Halakhov Yevhen teaches the following disciplines: Higher Mathematics, Information Security of the State. Scientific interests: Strategic business priorities of the enterprise information security system, Development of models of cyberatakes in a plane enterprise information security, Mathematical modeling of enterprise cyberates of enterprise.