Example of Differential Transformations Application in Cybersecurity

Ruslan Hryshchuk [1]

[1] *Korolyov Zhytomyr Military Institute, 22 Mira Avenue, Zhytomyr, 10004, Ukraine*

Abstract

Cybersecurity as a relatively new science covers quite a large number of areas, most of which are still in their infancy. The basis of cybersecurity, like any exact science, is mathematics. But the non-stationary and at the same time nonlinear nature of phenomena and processes occurring in cyberspace places special requirements on the mathematical tools used in cybersecurity. On the one hand, it should be adapted as much as possible for solving specialized problems, on the other hand, such mathematical tools should describe the phenomena and processes that are being studied quite fully and adequately. Today, in the field of cybersecurity, mathematical tools based on set theories, graphs, logic, probabilities, etc. are widely used. A special place in this field today is given to data mining, simulation, situational and cognitive modeling, parametric and structural synthesis of information security systems. The article develops the idea of applying in the field of cybersecurity the well-known mathematical apparatus of differential transformations of Academician of the National Academy of Sciences of Ukraine G. Pukhov, which has already found wide application in other branches of science and technology-electronics, electrical engineering, mechanics, chemical technologies, space research, etc. For this purpose, examples of the use of differential transformations for constructing models of cyberattack patterns for attack detection systems, mathematical models for assessing the level of security of information and telecommunications systems from zero-day cyberattacks by security analysis systems, and for building new cryptographic systems are given. The prospects for applying differential transformations to study the processes of interaction in social networks, as an example of sociotechnical cybernetic systems, are shown.

Keywords

Cybersecurity, differential transformations, original, image, model, cyberattack pattern, security level, system of differential equations, graph model, differential game.

1. Introduction

Differential transformations of Academician of the National Academy of Sciences of Ukraine G. E. Pukhov [1] have now become an effective tool for studying nonlinear and non-stationary processes in many branches of Science and technology. One of the first applied applications of differential transformations was their use for solving electrical engineering problems [1]. Over time, differential transformations began to be used to solve problems in radio engineering [2], mechanics [3], heat engineering [4], optimal control [5], computer engineering [6], and Space Research [7]. Such a wide range of applications of differential transformations is due to their significant advantages over the known LaPlace, Fourier, Mellin, and Taylor-Cauchy integral transformations. The main advantage of differential transformations over the integral transformations mentioned above is the possibility of their application for the correct solution of nonlinear problems described by a

III International Scientific And Practical Conference "Information Security And Information Technologies", September 13–19, 2021, Odesa, Ukraine
EMAIL: Dr.Hry@i.ua
ORCID: 0000-0001-9985-8477

fairly wide class of systems of Integral and differential equations [1].

In the field of cybersecurity, as is known [8], most of the phenomena and processes that occur in information security systems are non-stationary. Many of them can be described and are already described by systems of linear and nonlinear inhomogeneous differential equations. For example, today models of various malicious software samples such as SIS, SIR, SAIR, PSIDR, described by systems of differential equations, are widely known [8]. Some processes, such as the encryption process for a new type of symmetric cryptosystems, are described by Integral Equations [9].

Therefore, given the prospects of differential transformations as a modern mathematical tool, it is considered appropriate to expand the scope of its application in the interests of Applied Solutions to cybersecurity problems.

2. The Latest Studies and Printed Works Analysis

For the first time, the use of differential transformations for solving cybersecurity problems was proposed in [10]. Their main purpose was to solve linear and nonlinear inhomogeneous systems of differential equations that describe the processes of attacking information in information security systems. During 2009-2010, the theoretical foundations of modeling the processes of attack on information and its protection based on differential transformations were developed. The result of the research was the publication of the corresponding monograph [11]. Over time, differential transformations found a place in the creation of symmetric cryptosystems [12] and began to be used to construct patterns of potentially dangerous cyber attacks [13]. There is still no unified vision of the role and place of differential transformation in the field of cybersecurity.

3. Purpose

The purpose of the article is to systematize the well-known areas of application of differential transformations of Academician of the National Academy of Sciences of Ukraine G. E. Pukhov in the field of cybersecurity and determine further promising ways of their implementation in this industry.

4. Concept presentation

The essence and content of differential transformations are described in the works of their author, for example in [1] and others. let's consider an example of their application for differential game modeling of cyberattack processes [10, 14].

Example. Let the change in cybersecurity States in a computer network be described by a graph model (fig. 1).

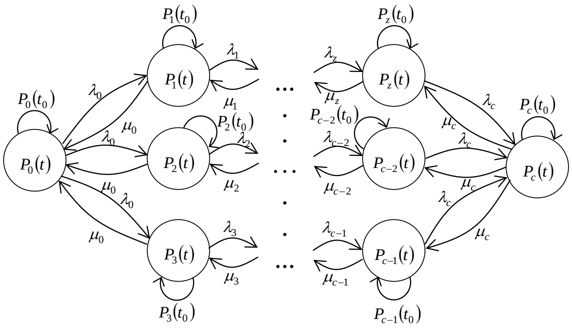

Figure 1: Cybersecurity state change graph model

In fig. 1 the following designations are accepted:

$\{P_z(t)\}$ – probabilities of a computer network being in one of the cybersecurity states $z=\overline{0,c}$ at some point in time t;

$\{P_z(t_0)\}$ – zero initial conditions when a computer network is in one of the cybersecurity states $z=\overline{0,c}$ at a time t_0;

$\{\lambda_z\}$ – intensity of recovery streams of infected hosts on the computer network, $z=\overline{0,c}$;

$\{\mu_z\}$ – intensity of streams infection of hosts in the computer network with malware, $z=\overline{0,c}$.

Circles on fig. 1 indicates the cybersecurity States in which the computer network may be located. Above the transition Arrows are the corresponding flow intensities that put the network in the corresponding states.

According to the above example (see fig. 1) it is necessary to build a differential game model of the cyberattack process on a computer network and assess its level of security under the accepted conditions.

Solving the example. Let's make a system of Kolmogorov-Chapman differential equations. The number of equations in a given system is determined by the number of states in which a computer network can be located (see fig. 1). The following general rule should be followed when compiling the system:

on the left side of each equation of the system is the derivative of the probability of a certain (z -th) state;

on the right - the sum of the products of the probabilities of all states from which the arrows enter this state, on the intensity of the corresponding information flows, minus the total intensity of all flows that bring the system out of this state, multiplied by the probability of this (z -th) state.

Based on the above rule we have

$$\begin{cases} \dfrac{dP_0(t)}{dt} = -3\lambda_0 P_0(t) + \mu_0\Big(P_1(t) \ + \\ \qquad\qquad + P_2(t) + P_3(t)\Big); \\ \dfrac{dP_2(t)}{dt} = -(\mu_0 + \lambda_1)P_1(t) + \\ \qquad\qquad \ldots + \lambda_0 P_0(t); \\ \qquad\qquad \vdots \\ \dfrac{dP_c(t)}{dt} = -3\mu_c P_0(t) + \lambda_c\Big(P_z(t) \ + \\ \qquad\qquad + P_{c-2}(t) + P_{c-1}(t)\Big). \end{cases} \tag{1}$$

Let us impose additional (initial) conditions on System (1) that will provide it with a single solution

$$P_0(t_0) = 1, \ P_2(t_0) = \ldots = P_c(t_0) = 0, \tag{2}$$

we will also define the rationing conditions

$$P_0(t_0) + P_2(t_0) + \ \ldots \ + P_c(t_0) = 1. \tag{3}$$

In the differential game setting [11], the intensity of flows $\{\lambda_z\}$ and $\{\mu_z\}$ are called strategies of players of cyber attack and cyber defense, respectively, and are limited in their boundaries

$$0 \le \lambda_z \le \lambda_{z\max}, \tag{4}$$

$$0 \le \mu_z \le \mu_{z\max}, \tag{5}$$

where $\lambda_{z\max}$ and $\mu_{z\max}$ – are the maximum flow intensities in the z -th state, respectively.

Using the method of differential transformations [1], we obtain a spectral model of cybersecurity states

$$\begin{cases} P_0(k+1) = \dfrac{T}{k+1}\Big[-3\lambda_0 P_0(k) + \\ + \mu_0\Big(P_1(k) + P_2(k) + P_3(k) \ \Big)\Big]; \\ P_1(k+1) = \dfrac{T}{k+1}\Big[-(\mu_0 + \lambda_1)P_1(k) + \\ + \ldots + \lambda_0 P_0(k)\Big]; \\ \qquad\qquad \vdots \\ P_c(k+1) = \dfrac{T}{k+1}\Big[-3\mu_c P_0(k) + \\ + \lambda_c\Big(P_z(k) + P_{c-2}(k) + P_{c-1}(k) \ \Big)\Big]. \end{cases} \tag{6}$$

When receiving the system (6), the condition is assumed that the constant H duration T of infection of the computer network with malware.

Assigning sequentially integer values to the argument $k =: 0, 1, \ldots$ according to the spectral Model (6), we find the discrete of differential spectra for the desired model $P_0(k+1)$, i.e.

$$P_0(0) = \big[P_0(t_0)\big] = 1 \ , \ P_0(1) = \ldots . \tag{7}$$

Let's find the best strategies for allocating players resources λ_z^{opt} i μ_z^{opt}, game price I^* (level of protection of the computer network from the malware) and, in fact, the model $P_0(t)$ itself, which is the trajectory of the game.

To do this, we will present the board I with a general integral model

$$I = \frac{1}{T}\int_{t_0}^{T} P_0(t)\, dt. \tag{8}$$

When players choose a minimax strategy

$$\min_{\lambda(t) \in E_\lambda} \ \max_{\mu(t) \in E_\mu} = I\big(t, P_0(t), \lambda(t), \mu(t)\big)$$

using a direct differential transformation [1], the fee (8) is defined in terms of differential spectrum discretion $P_0(k)$ (7) as

$$I = \sum_{k=0}^{k=\infty} \frac{P_0(k)}{k+1}. \qquad (9)$$

To find optimal strategies λ_0^{opt} and μ_0^{opt} allocate available resources (4) and (5), we examine functionality I (9) for an extremum (expression (9) takes the form of a functional when the values of the corresponding discretes (7) are substituted for it).

The necessary conditions for the existence of the extremum of the functional $I(\lambda_0, \mu_0)$ (9) allow us to determine the optimal strategies of players:

$$\begin{cases} \dfrac{\partial I(\lambda_0, \mu_0)}{\partial \lambda_0} = 0; \\ \dfrac{\partial I(\lambda_0, \mu_0)}{\partial \mu_0} = 0. \end{cases} \rightarrow \begin{cases} \lambda_0^{opt}; \\ \mu_0^{opt}. \end{cases} \qquad (10)$$

Sufficient conditions for the existence of the extremum of functional $I(\lambda_0, \mu_0)$ (9) allow us to determine the sign of the found extremums, i.e.

$$\begin{cases} \dfrac{\partial^2 I(\lambda_0, \mu_0)}{\partial \lambda_0^2} > 0; \\ \dfrac{\partial^2 I(\lambda_0, \mu_0)}{\partial \mu_0^2} < 0. \end{cases} \rightarrow \begin{cases} \lambda_{0\min}^{opt}; \\ \mu_{0\max}^{opt}. \end{cases} \qquad (11)$$

Fulfilling the condition of existence saddle point Δ:

$$\Delta > 0, \qquad (12)$$

where

$$\Delta = \left(\frac{\partial^2 I_1(\lambda_0, \mu_0)}{\partial \lambda_0 \, \partial \mu_0} \right)^2 - \\ -\left(\frac{\partial^2 I_1(\lambda_0, \mu_0)}{\partial {\lambda_0}^2} \right)\left(\frac{\partial^2 I_1(\lambda_0, \mu_0)}{\partial {\mu_0}^2} \right)$$

indicates that it is inappropriate for players to deviate from their optimal strategies (10), since any deviation from the optimal strategy by one of the players will inevitably lead to losses in the fee, provided that the optimal strategy is chosen by the other player, that is

$$I\left(t, P_0^{opt}(t), \lambda_0, \mu_{0\max}^{opt}\right) \geq \\ \geq \min_{\lambda \in E_\lambda} I\left(t, P_0(t), \lambda_0, \mu_{0\max}^{opt}\right), \\ I\left(t, P_0^{opt}(t), \lambda_{0\min}^{opt}, \mu_0\right) \leq \\ \leq \max_{\mu \in E_\mu} I\left(t, P_0(t), \lambda_{0\min}^{opt}, \mu_0\right).$$

So, if there is a saddle point Δ (12), then when players choose the optimal strategies (10), the price of the game – the level of protection of the computer network from the malware I^* is determined from the board (9).

When moving to the time domain using the inverse transformation [1], the trajectory of a differential game-a differential game model of the cyberattack process on a computer network $P_0^{opt}(t)$, provided that players choose optimal strategies (10), will have the form

$$P_0^{opt}(t) = \sum_{k=0}^{k=\infty} \left(\frac{t}{H} \right)^k P_0^{opt}(k). \qquad (13)$$

In all other cases –

$$P_0(t) = \sum_{k=0}^{k=\infty} \left(\frac{t}{H} \right)^k P_0(k). \qquad (14)$$

Thus, the given example shows the potential possibilities of using differential transformations in modeling cyberattack processes on computer systems and networks in the case of describing malicious software samples by systems of differential equations.

5. Conclusions

The article provides an overview of one of the examples of using differential transformations to solve cybersecurity problems. After analyzing other well-known examples of the use of differential transformations [15] in conclusion, we note that they can also be used to solve problems in cryptology.

6. Acknowledgements

Thanks to professors Vladimir Baranov, Vladimir Khoroshko and Alexander Korchenko introduction to differential transformations and cybersecurity.

7. References

[1] G. E. Pukhov. Taylor Transforms and Their Application in Electrical Engineering and Electronics [in Russian], Nauk. Dumka, Kyiv (1978).

[2] I. N. Efimov, E. D. Golovin and O. V. Stoukatch, "Exactitude of the electronic devices analysis by the differential transformations method," 2003 Siberian Russian Workshop on Electron Devices and Materials. Proceedings. 4th Annual (IEEE Cat. No.03EX664), 2003, pp. 150-151, doi: 10.1109/SREDM.2003.1224211.

[3] R. Hołubowski. Application of differential transformation finite element method in aperiodic vibration of non-prismatic beam. Procedia engineering 199 (2017): 360-365.

[4] M. Sharma, K. Singh, A. Kumar. MHD flow and heat transfer through non-Darcy porous medium bounded between two parallel plates with viscous and joule dissipation Spec. Top Rev. Porous Media Int. J., 5 (2014), pp. 1-11

[5] I. Hwang, J. Jinhua, D. Du. Differential transformation and its application to nonlinear optimal control. 2009.

[6] A. I. Stasiuk, R. V. Hryshchuk, L .L. Goncharova. A mathematical cybersecurity model of a computer network for the control of power supply of traction substations. Cybern. Syst. 53(3), 476–484 (2017).

[7] M.Yu. Rakushev, "Method for Prediction Of Space Vehicle Motion Based on the Multidimensional Differential-Teylor Transformations" in Journal of Automation and Information Sciences, Begell House Inc, vol. 51, no. 4, pp. 1-11, 2019.

[8] R. V. Hryshchuk. Osnovy kibernetychnoi bezpeky [Text]: monohrafiya / R. V. Hryshchuk, Yu. H. Danyk; Yu. H. Dannyk (Ed.). – Zhytomyr: ZhNAEU, 2016. – 636 p.

[9] G. Bronshpak, I. Gromiko, S. Docenko and E. Perchik, "Kriptografiya novogo pokoleniya Integralnie uravneniya kak alternativa algebraicheskoi metodologiyi", [New generation cryptography: Integral equations as an alternative to algebraic methodology], Prikladnaya elektronika, № 3, pp. 337-349, 2014. DOI: 10.13140/RG.2.1.1973.2645. (In Ukrainian).

[10] R.V. Hryshchuk Differential-game the spectral model of the process of attacking information has been rounded up / R.V. Grishchuk // Bulletin of ZhDTU. - Zhitomir: ZhDTU, 2009. - No. 48 (I). - S. 152–159.

[11] R. V. Hryshchuk. Teoretychni osnovy modeliuvannia protsesiv napadu na informatsyiu metodamy teoryi dyferentsialnykh ihor ta dyferentsialnykh peretvoren [Text]: monohrafiya / R. V. Hryshchuk. – Zhytomyr: Ruta, 2010. – 280 p.

[12] R. V. Hryshchuk, O. M. Hryshchuk. A Generalized Model of Fredholm's Cryptosystem. Cybersecurity: education, science, technique, 2019, Vol. 4 (4), pp. 14–23. DOI: 10.28925/2663-4023.2019.4.1423. (In Ukrainian).

[13] V.V. Okhrimchuk. The differential-game model is used to the template of a potentially unsafe cyber attack // Cyberbezpeka: education science and technology. Kiev: Kiev. University of B. Grinchenka, 2020. № 4 (8). S. 113-123.

[14] R. V. Hryshchuk. Method of differential-game P-model of processes in attack on information / R. V. Grishchuk // Information security. - Lugansk: SNU im. V. Dahl, 2009. - No. 2 (2). - S. 128-132.

[15] O. M. Hryshchuk. Features of the encryption key selection for the Fredholm cryptosystem. Computer Engineering and Cybersecurity: Achievement and Innovation: Materials II All-Ukrainian. nauk.-practical. conf. zdobuvachiv vishoï educate th young pupils, metro Kropyvnytskyi, 25-27 leaf. 2020 p. / Ministry of Education and Science of Ukraine, Derzh. sciences. established "Institute of Modernization for the Minister of Education", Tsentralnoukr. nat. tech. un-t; - Kropyvnytskyi: TsNTU, 2020. P. 109-110 p.