Modeling the Process of Counteracting Fraud in E-banking

Olga Syniavska[0000-0002-7507-3541], Nadiya Dekhtyar[0000-0001-7932-8620], Olga Deyneka[0000-0001-5852-4163], Tetiana Zhukova

Sumy State University, 2, Rymskoho-Korsakova Str., Sumy, 40000, Ukraine
{o.syniavska, n.dekhtiar, o.deineka}@uabs.sumdu.edu.ua, gtanya@buh.sumdu.edu.ua

Olena Syniavska

Kharkiv National University of Internal Affairs, 27, Lev Landau Ave., Kharkiv, 61000, Ukraine
sinyavskaya.elen@gmail.com

Abstract. The paper is devoted to the current issue of the counteracting cyberattacks in the banking sector, in particular in the field of e-banking. The main types of banking fraud, which are carried out in the online sphere, are considered. The authors propose a mathematical model that describes the process of counteracting e-banking fraud. Proposed model is based on the classic Lotka-Volterra model with logistic growth and the Holling-Tanner dynamic models. The fixed points of a dynamic system were calculated and analyzed. It was determined that there are 4 possible types of fixed points: saddle and the line of stable fixed points, which are unlikely may be in real life, stable node and a stable degenerate node, which are, in practice, the most likely cases. The constructed model could be used for theoretical study, different simulation experiments with changing input parameters could be done. Unfortunately, it is difficult to investigate this question on real data, since the statistics on cyberattacks are closed.

Keywords: e-commerce, e-banking, fraud, e-banking fraud, fraudulent attack, cyberattack.

1 Introduction

The lack of proper attention to the security of online operations can make them vulnerable to criminals.

Today, most financial transactions are carried out via the Internet. The development of e-commerce has led to the fact that these trends have spread to the banking sector. Since the beginning of the 80's, the term "e-banking" has entered the economic terminology.

Due to the flow of funds through the Internet communication channels, fraudsters, who are coming up with more and more new cyberattacks schemes, have become more active. With the advent of new cyberattacks, new countering instruments are emerging.

The study of this issue, although it is relevant, but, unfortunately, is at a basic level. This is due to the fact that, in the first place, all information about cyberattacks that are carried out in the banking sector is confidential.

At the same time, it is theoretically and practically justified that the emergence of new fraudulent schemes leads to the development of new instruments to combat them. Thus, there is a kind of race that can go on forever.

Thus, scientists are faced with the task of studying the dynamics of the emergence of cyberattacks in the banking sector and the development of instruments of counteracting e-banking fraud. This article proposes to develop a mathematical model that would describe the process.

2 The Concept of E-banking

Innovative development of the economy of any country depends on the direction of society to the information space. Nowadays the main direction of innovation in the business is the transfer of commercial activity in the Internet space. Every year, from 30% to 70% of business in any country (regardless of its level of development) goes into on-line sphere. That is, companies are increasingly using e-commerce systems to conduct business.

The beginning of the Internet economy can be associated with the breakthrough of the World Wide Web system in the mid-1990s. Today, to describe economic relations on the Internet, the concept of "electronic commerce" is used, which is a part of the Internet economy. Thus, the Organization for Economic Cooperation and Development provides such definition of this term (in a broad sense): any form of business relationship where interaction between actors occurs using Internet technologies [1].

Finally, e-commerce could be defined as a relationship aimed at making a profit, carried out remotely using information and telecommunication systems, as a result of which participants have rights and obligations of a property nature [2].

In general, e-commerce is subdivided into: Electronic Data Interchange (EDI); Electronic Funds Transfer (EFT); e-trade; e-cash; e-marketing; e-insurance; and, finally, e-banking.

E-banking is a remote banking technology that gives the ability to receive banking services via the Internet [3]. To connect the client to the Internet banking system it is enough to have access to the global network, installed on the computer browser program, enter into a contract with the bank, get a set of passwords or special devices for logging in and operations, go to the secure page of the e-banking, sign up and connect to the system.

Traditionally, e-banking includes such operations: carry out banking operations on any computer connected to the Internet; pay for cable and satellite television, mobile communication operators, telephony; online games; to make utility payments; receive extracts about the movement of funds by card or account in the last few days, calendar

month, another arbitrary time period; open deposit; repay the loan; carry out transfer of funds between own accounts; various credit card transactions; view currency rates, bank announcements; submit applications for purchase / sale / currency conversion; blocking a card by a customer, for example, in case of theft or loss etc.

According to statistics, more than 80% of all banking operations can be done by a person sitting at a computer at home or at the office. Benefit from this kind of activity is received by all involved persons: clients of banks, banks, software developers and owners of companies representing their products and services on the Internet.

At the same time, the intensification of financial activities through the Internet leads to the fact that a large amount of personal information, including financial, passes through communication channels. This, in turn, leads to increasing e-banking fraud.

3 Types of E-banking Fraud

Nowadays, the development of various fraud schemes has reached a global level. In connection with the development of information technology, fraudsters are moving to a new level, organizing cyberattacks on automated systems of various companies and enterprises.

Cyberattacks penetrated absolutely all areas of business. The Fig. 1 shows 5 areas of business that have suffered the greatest costs due to cyber fraud in August 2018.

Fig. 1 shows that the most unprofitable cyberattacks were for the financial sector. At the same time, about 90% of the attacks fall on the banking sector. Especially active frauds are held in the field of electronic banking.

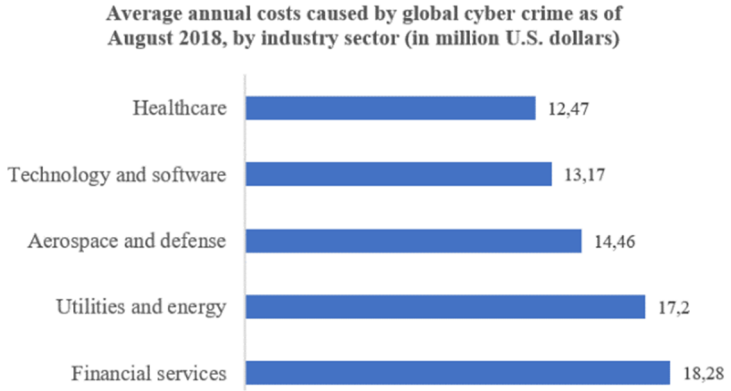

Fig. 1. Average annual costs caused by global cybercrime as of August 2018, by industry sector (in million U.S. dollars). [5]

The most common type of fraud in the e-banking sector today is phishing and its subspecies (Fig. 2).

Generally, phishing could be defined as a scalable act of deception whereby impersonation is used to obtain information from a target [4].

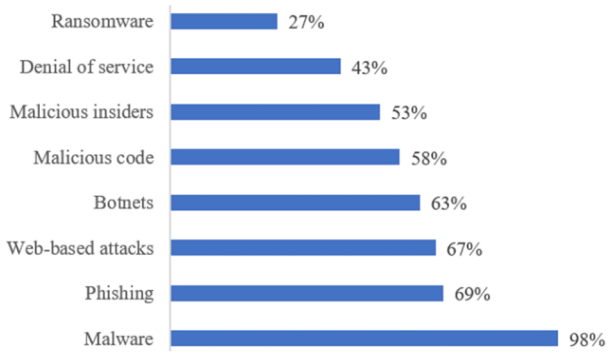

Fig. 2. Types of cyberattacks experienced by companies worldwide as of August 2018. [5]

More precisely, phishing is a form of social engineering in which an attacker, also known as a phisher, attempts to fraudulently retrieve legitimate users' confidential or sensitive credentials by mimicking electronic communications or phone calls from a trustworthy or public organization in an automated fashion [6].

In general, there are 2 basic phishing principles:

- on a mobile phone, sometimes not even tied to an account, the bell of a bank employee or even his security service rings. The client is told about the dubious movements on the card and is asked to call the CVV - the verification code of the card's payment system. You should never report anything, if the call was not made by the client himself by the support number, any information can be used for theft. It is better to interrupt the call and call your bank manager yourself;
- a letter comes to the client's mail, signed by its servicing bank. The link proposed in the letter leads to an analogue of a personal account in which you need to enter your login and password. Banks never use this way of working with clients, any letters to personal mail with a proposal to provide personal data, card number or enter the username and password, signed by an employee of the bank, is always sent to a fraudster.

A complete phishing attack involves three roles of phishers. Firstly, mailers send out a large number of fraudulent emails (usually through botnets), which direct users to fraudulent websites. Secondly, collectors set up fraudulent websites (usually hosted on compromised machines), which actively prompt users to provide confidential information. Finally, cashers use the confidential information to achieve a pay-out. Monetary exchanges often occur between those phishers [7]. The information flow is shown in Fig. 3.

Phishing can also be divided into such types depending on the mechanisms used:

- "Man-in-the-Middle" attack – hackers place themselves between banks and customers while customers are using their online banking accounts [8];
- deceptive phishing attack – sending false notifications through email [9]. In this type of phishing attack, an attacker sends email messages to users, masquerading as one of the bank's representatives [10].

- pharming – this method is more complicated and works only with small banks. Pharming is a type of attack intended to redirect traffic to a fake Internet host. There are different methods for pharming attacks, among which DNS cache poisoning is the most common [7]. Thus, the fraudster "replaces" the real Internet bank of the bank with the same visually, but fake, where the client enters his data, and the fraudster, respectively, receives all the necessary personal data.
- malware-based phishing – malware is a piece of software developed either for the purpose of harming a computing device or for deriving benefits from it to the detriment of its user [11]. Malware can be used to collect confidential information directly, or aid other phishing techniques.
- phishing through PDF Documents – some key functions of a PDF programming language could be misused by an attacker or a hacker to design a new PDF document to his/her own advantage and extract the desired personal information from the victim [7].

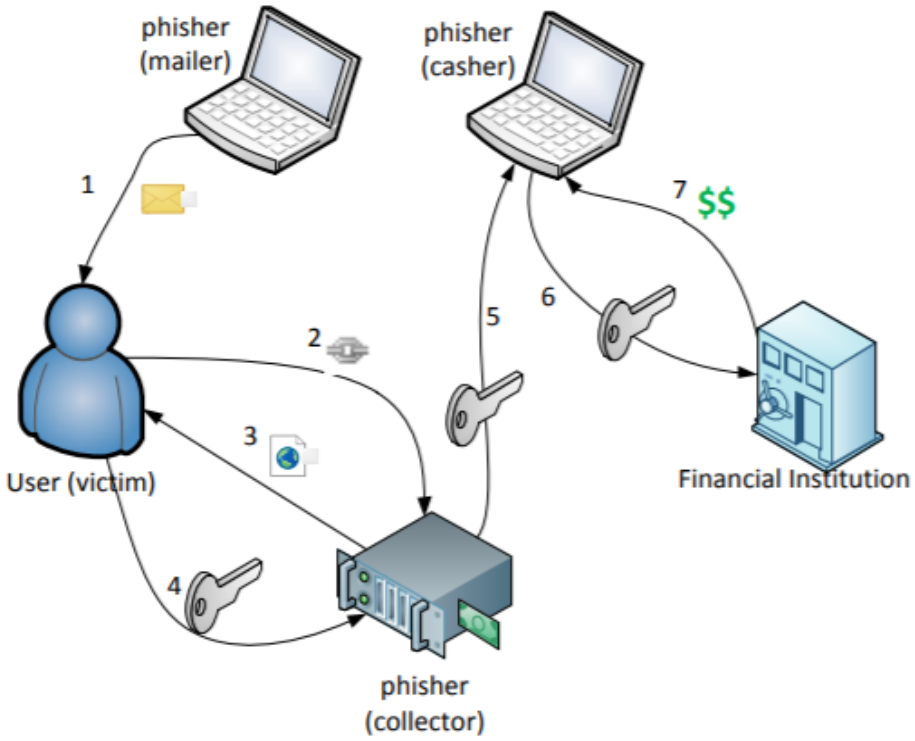

Fig. 3. Phishing information flow. [7]

Analysis of statistics on the total number of phishing attacks around the world shows that their number is gradually increasing (Fig. 4).

It may me noticed that the time series has a certain frequency. This is due to the fact that certain instruments of counteracting existing fraudulent attacks are created.

However, bypassing the emerging instruments, new types of attacks are created. Thus, the decrease in the number of phishing attacks due to the use of counteracting instruments is replaced by a sharp increase in their number.

Fig. 4. Number of global phishing attacks from 2012 to 2016 worldwide. [5]

Talking about payment systems that are most often subjected to phishing attacks, the statistics are shown in the Fig. 5.

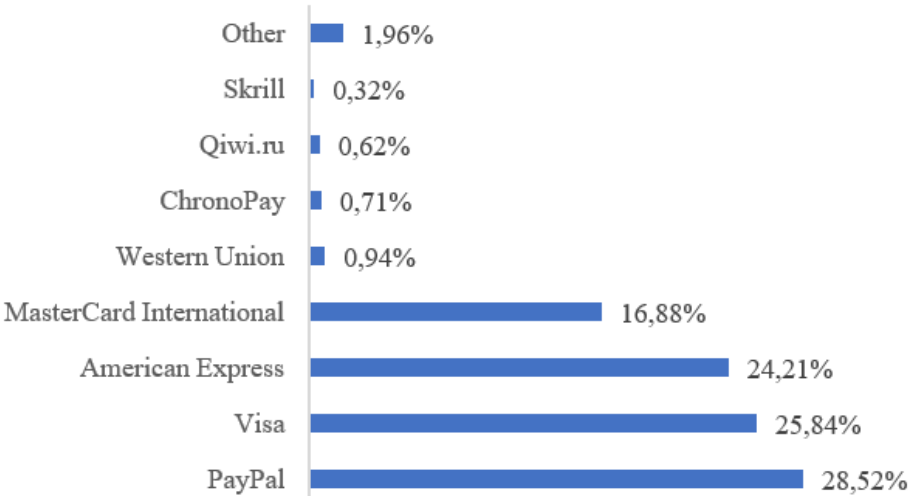

Fig. 5. Distribution of global phishing attacks aimed at online payment systems as of 4st quarter 2016. [5]

Thus, phishing is distinguished as the most common type of cyberattack in e-banking. Thus, further the mathematical model of counteracting similar bank fraudulent attacks will be proposed.

4 Mathematical Model of the Process of Counteracting Bank Fraud

Modeling a process of counteracting bank fraud is a complex issue in terms of collecting real data. The relevant statistics are closed. In addition, a huge number of fraudulent schemes does not reach the level of law enforcement agencies. Therefore, this question can be investigated in theoretical form.

This study proposes to simulate the process of counteracting bank fraud using a model of economic dynamics. So, the use of instruments to combat fraud and the emergence of new attacks can be compared to the classic "predator-prey" model [8].

$$\begin{cases} x` = (a - c \cdot y)x \\ y` = -(b + d \cdot x)y \end{cases} \quad (1)$$

where x – the number of prey;

y – the number of predators;

a, b, c, d – coefficients reflecting the interactions between species.

Suppose that for our subject area, x is the number of fraudulent attacks, and y is the number of instruments to combat bank fraudulent attacks.

The use of the Lotka-Volterra model with logistic growth [13] and the Holling-Tanner model [14] allows us to propose a model of counteracting bank frauds:

$$\begin{cases} x` = (a - d \cdot x - b \cdot y)x \\ y` = -c \cdot y + \frac{1}{b} - y \end{cases} \quad (2)$$

where x – number of fraudulent attacks at the time t;

y – number of available tools to combat fraudulent attacks at the time t;

a – the coefficient of natural increase in the number of fraudulent attacks;

b – the coefficient of effectiveness of one instrument of counteracting fraudulent attacks;

c – coefficient of natural decrease in the number of instruments of counteracting fraudulent attacks per time unit;

d – coefficient of interspecific competition for attackers. d=1/D, where D – the maximum possible number of attacks.

The next step is to find the fixed points of the system.

On the basis of symbolic calculations, we obtain two fixed points.

$$(x_1; y_1) = \left(0; \frac{1}{(1+c)b}\right) \quad (3)$$

$$(x_2; y_2) = \left(\frac{(1+c)a-1}{(1+c)d}; \frac{1}{(1+c)b}\right) \quad (4)$$

The study of the first fixed point is inappropriate from a practical point of view, since it is assumed that the number of fraudulent attacks equal 0. Therefore, we will investigate the second special point. We will linearize the model with Jacobian matrix.

$$J(x,y) = \begin{pmatrix} a - b \cdot y - 2 \cdot d \cdot x & -b \cdot x \\ 0 & -c - 1 \end{pmatrix} \quad (5)$$

We replace *x* and *y* in Jacobian with the values of the second fixed point and calculate the trace and determinant for the received matrix.

$$tr = a - c - \frac{2a+2ac-2}{c+1} - \frac{b}{b+bc} - 1 \quad (6)$$

$$\Delta = a + a \cdot c - 1 \quad (7)$$

Based on the analysis of characteristic regression, the following expression was obtained for the discriminant:

$$D = \left(c - a + \frac{b}{b+bc} + \frac{2d(a+ac-1)}{(1+c)d} + 1\right)^2 - 4 \cdot a - 4 \cdot a \cdot c + 4 \quad (8)$$

Given the economic content of the input parameters of the proposed model, the discriminant can not be negative. Consequently, the roots of the characteristic equation can not be complex values. Moreover, given that the second root of the characteristic equation will always be a negative number, we can conclude that the roots of the characteristic equation can take the following values:

1. real, negative, different – fixed point type is stable node;
2. real, repeating, negative – fixed point type is stable degenerate node;
3. real, different, with different signs – fixed point type is saddle;
4. the first root is 0, the second is negative – fixed point type is a line of stable fixed points.

In order to achieve these types of fixed points we will form the constraints that must be imposed on the ratio of input parameters (Table 1).

Table 1. Type of fixed point depending on the ratio of the input parameters of the model.

Type of fixed point	The ratio of the input parameters
Stable node	$a + a \cdot c - 1 > 0$ $\frac{\sqrt{D}}{2} \neq 0$
Stable degenerate node	$a + a \cdot c - 1 > 0$ $\frac{\sqrt{D}}{2} = 0$
Saddle	$a + a \cdot c - 1 < 0$
Line of stable fixed points	$a + a \cdot c - 1 = 0$

To carry out numerical experiments and study the behavior of the proposed model, we will construct an imitative model of the process of counteracting bank fraud in terms of system dynamics (Fig. 6).

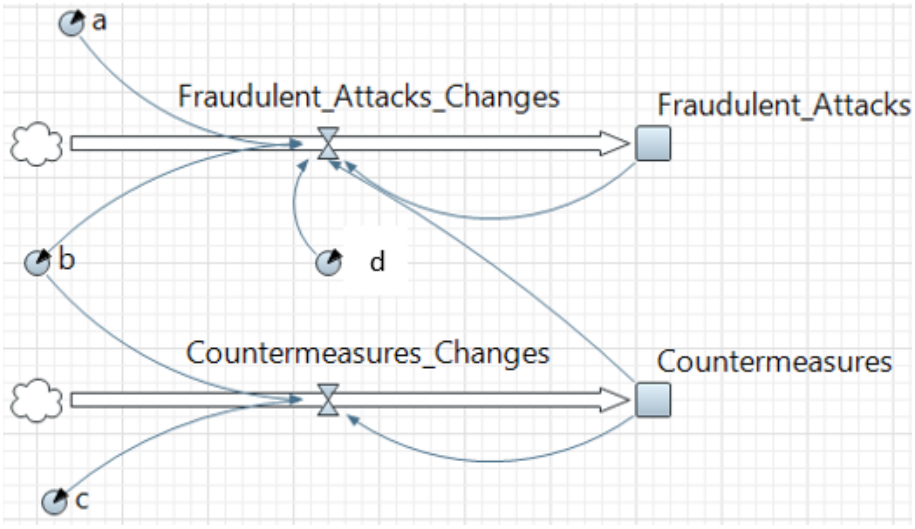

Fig. 6. Stock and flow diagram for the model of the process of counteracting bank fraud.

The structure of constructed model is presented in Table 2.

Table 2. Description of diagram elements.

Name of the diagram	Element of stock and flow diagram
Fraudulent_Attacks	Stock
Countermeasures	Stock
Fraudulent_Attacks_Changes	Flow
Countermeasures_Changes	Flow
a	Parameter
b	Parameter
c	Parameter
d	Parameter

The constructed diagram allowed to carry out simulation experiments, which take into account the various ratios of the input parameters of the proposed model of the process of counteracting bank fraud for obtaining fixed points of the specified types.

The conducted simulation experiments for the saddle case have shown that the number of fraudulent attacks goes to zero over time, and the number of instruments to combat them is approaching some stationary value.

Model experiments for the line of stable fixed points showed a case similar to a saddle.

The construction of timelines and phase portraits of the proposed model for the case of a stable degenerate node caused the necessity of selecting the parameters in such a way that the discriminant of the characteristic equation assumed zero. Such a situation is possible only in the case when the parameter c=0. This means that the instruments to counteract fraudulent attacks are successful and there is no their “dead out”. But this

situation is not very attractive from a practical point of view. *X* and *y*, as in the case of a stable node, go to some stationary state. But the value of *x* is quite high. And it will be larger, the more the value of parameter *a*, the more new fraudulent attacks generate attacks that ended successfully.

Summing up the results of computer simulation, we can conclude that from a practical point of view saddle case and the line of stable fixed points are more acceptable, since in these cases the value of *x* (the number of fraudulent attacks) goes to zero, regardless of the initial coordinates *x* and *y* (coordinates of the initial state of the system). So the value of *a* parameter must be $a \leq \frac{1}{1+c}$. In terms of its economic content, the parameter *c* can take values from 0 to 1. Thus, the parameter *a* should vary from 0.5 to 1. It means that in response to every successful fraud attack, in addition at least one new attack must arise, which is unlikely may be in real life. As a rule, they arise much more.

Accordingly, in practice, the most likely cases are a stable node and a stable degenerate node and should seek to reduce the value. Thus, we should seek to reduce the value of $x = \frac{(1+c)a-1}{(1+c)d}$. From this expression we can see that the most influential are the parameters *a* and *d*. Moreover, for *a*, the connection is straight, and for *d* is converse.

To summarize, it can be argued that in order to obtain a more favorable situation from a practical point of view, it is necessary to reduce the values of the parameters *a* and *c* and increase the parameter *d*.

5 Conclusions

1. E-banking is an innovative part of e-commerce sphere and could be defined as a remote banking technology that gives the ability to receive banking services via the Internet.
2. The most common type of e-banking fraudulent attack is phishing, which, in general, is a method of acquiring personal financial data of a bank customer with the help of fictitious phone calls, emails and substitution of real websites of banking institutions.
3. In the paper a model of counteracting bank frauds based on of the Lotka-Volterra model with logistic growth and the Holling-Tanner model proposed. It allows to investigate the question of counteracting bank frauds in theoretical form.
4. Simulation experiments, made with the usage of built model, showed that saddle case and the line of stable fixed points are unlikely may be in real life, because it means that in response to every successful fraud attack, in addition at least one new attack must arise. As a rule, they arise much more. In practice, the most likely cases are a stable node and a stable degenerate node.

6 Acknowledgements

The article was executed in the framework of state budget scientific research work No. 0118U003574 “Cyber security in the fight against bank fraud: protection of

financial services consumers and growth of financial and economic security of Ukraine".

References

1. OECD science, technology, and industry scoreboard: Towards a knowledge-based economy. Organisation for Economic Cooperation and Development. http://www.oecd.org/ (2019). Accessed 13 Mar 2019
2. Babenko, V., Syniavska, O.: Analysis of the current state of development of electronic commerce market in Ukraine. Tech. Aud. and Prod. Res. **5**(4(43)), 40–45 (2018). doi:10.15587/2312-8372.2018.146341
3. Mia, A., Rahman, M., Uddin, M.: E-Banking: Evolution, Status and Prospects. Cost & Manag. **1**(35), 36–48 (2007)
4. Lastdrager, E.: Achieving a consensual definition of phishing based on a systematic review of the literature. Crime Science. 3:9 (2014). doi:10.1186/s40163-014-0009-y
5. The Statistical Portal. https://www.statista.com/ (2019). Accessed 13 Mar 2019
6. Jakobsson, M., Myers, S. (ed.) Phishing and countermeasures: understanding the increasing problem of electronic identity theft. John Wiley & Sons, Inc. (2007)
7. J. Shi, S. Saleem.: Phishing: Final Report. https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2014/Resources/presentations/2012/topic5-final/report.pdf (2012). Accessed 9 Mar 2019
8. Swanink, R.: Persistent effects of manin-the-middle attacks. Bachelor Thesis, Radboud University (2016)
9. Damodaram, R.: Study on phishing attacks and antiphishing tools. IRJET. **3**(1), 700–705 (2016)
10. Alsayed, A., Bilgrami, A.: E-banking security: Internet hacking, phishing attacks, analysis and prevention of fraudulent activities. Int. J. Of Emerg. Techn. and Adv. Activ. 7(1), 109–115 (2017)
11. Delgado, O., Fuster-Sabater, A., Sierra, J.: Analysis of new threats to online banking authentication schemes. In: Proceedings of the X Spanish Meeting on Cryptology and Information Security (RECSI 2008), pp. 337–344 (2008)
12. Hussein, S.: Predator-Prey Modeling. Undergraduate Journal of Mathematical Modeling: One + Two. **3**(1), 20 (2010). doi:10.5038/2326-3652.3.1.32
13. Oliinyk, V., Wiebe, I., Syniavska O., Yatsenko, V.: Optimization model of Bass. JAES, **8**(62), 2168–2183 (2018)
14. Gupta, R.: Dynamics of a Holling-Tanner Model. AJER. **6**(4), 132–140 (2017)
15. Syniavska, O., Dekhtyar, N., Deyneka, O., Zhukova, T., Syniavska, O.: Security of e-banking systems: modelling the process of counteracting e-banking fraud. SHS Web of Conferences. **65**, 03004 (2019). doi:10.1051/shsconf/20196503004