Design with Preset Parameters and Reliability Assessment of Single Level Personal Data Protection System

Borys Zhurylenko [1[0000-0003-2980-5630]], Kirill Nikolaev [2[0000-0003-2980-9870]] and Marek Aleksander [3 [0000-0003-2619-1063]]

[1]National Aviation University, Kyiv, Ukraine
[2] Traffic safety expert, DIN Technical Committee 226 WG3 member
[3] State Higher Vocational School in Nowy Sącz, Nowy Sącz, Poland
zhurylenko@gmail.com, kyrylo.nikolaiev@gmail.com

Abstract. Current study shows the possibility of a different approach to design with specified parameters and reliability assessment of single level personal data protection system. The considered approach to single level personal data protection system design and reliability assessment provides a quantitative assessment of protection in the form of probability and differs from the approach adopted in the regulatory documents of Ukraine. The correlation between attempt and time of personal data theft time is defined considering projected theft attempts frequency. It is shown that the parameter that determines the reliability of a single level protection against personal data theft can be not only a constant value with the dimension of time, but also depend on the theft attempts and the time of these theft attempts or, in other words, hacking protection. Based on the attempts and time of protection break-ins, equations are obtained for assessing the reliability of protection with the parameters inherent in a particular designed protection system, which take into account the initial and required data for the design of protection. Expressions are obtained for determining such parameters as probability values, coordinates of attempts and time for the hacking line which is used for theft. The obtained parameters of the hacking line allow not only to design protection, but also to investigate, control and manage the process of hacking by coincidence or deviation from the line of the real hacking events.

Keywords: protection against personal data theft, reliability, hacking probability, preset hacking protection parameters, distribution of the maximum probability of hacking, hacking attempt, hacking time, designed protection system.

1 Introduction

Currently, Ukraine is theoretically developing methods for personal data protection, that is, in other words, information protection (IP), using a systematic approach, expert evaluation analysis of fuzzy sets, game theory and others [1-4]. The published

 CybHyg-2019: International Workshop on Cyber Hygiene, Kyiv, Ukraine, November 30, 2019.

studies do not provide or describe the methods of IP tools design with specific security requirements in terms of the number of possible attempts and the time of personal data theft. Before designing the construction of one or another technical protection of information (TPI) for the prevention of personal data theft, it would be desirable to know its designed reliability for hacking or protection. When designing, the main parameters that are understandable to the customer of the TPI are its cost, protection efficiency, attempt and time of the attempt, at which TPI can be hacked. Therefore, when designing and evaluating the reliability of a functional protection against personal data theft, these parameters should reflect the real physical nature and reliability of the protection.

Technical protection of information (TPI) from personal data theft in various countries is carried out in accordance with its regulatory documents and developed methods. In this case, the constructed TPI basically has a quality assessment of protection that meets the initial conditions for the use of protection and is not related to the real process of personal data theft. And only some methods of constructing TPI give a quantitative assessment.

Naturally, it is important for the customer and developer of protection against personal data theft to know the probability of penetration through protection at each stage of its operation, and preferably from real hacking attempts. In real conditions, when TPI is hacked and personal data is stolen, the only facts or parameters that can be recorded are the hacking attempt and its time, that is in these coordinates the actual direction of the TPI hacking. In this case if the probability of hacking of working TPI for each moment of time is known from initial data, it is possible to estimate the probability of a possible penetration through protection by the real parameters of hacking attempts, for example, by the number of attempts and time of these hacking attempts. These results will help the developer to decide on the replacement of the used TPI or its modernization, which will save financial and material resources invested in protecting information, as well as losses from personal data theft.

The relevance of the work lies in the development of a new methodology and approach to the development of design and evaluation of working protection based on real physical processes of hacking.

Scientific novelty lies in the development of a new approach to the design, analysis and assessment of the status of a working TPI in order to save financial costs invested in protection.

2 Analysis of existing research

There are no known defenses from open sources that would be developed according to regulatory documents and which would provide control of their condition against the number of hacking attempts in time. On the other hand, control of the number of attempts and the time of hacking would allow determining the intensity and direction of hacking. Since the direction of hacking depends on two parameters, the reliability should also depend on the attempts and time of hacking, and the parameters of attempts and time are interconnected by the direction of hacking. There are publications by B. Zhurylenko, in which an attempt was made to develop a methodology for build-

ing protection, monitoring its condition during operation, modernizing TPI depending on financial investments in protection, the effectiveness of the protection being created and the direction of the hack. However, in these works there is no rigorous proof of reliability depending on the direction of the hack.

The aim of the work is to obtain the distributions of the probability's maximums and probability of breaking TPI depending on the direction of hacking, determined by two parameters - the hacking attempt and time of this attempt.

3 Theoretical basis of a single level technical information protection system design method

To create a methodology of protection design against personal data theft let's first obtain the dependences of the probability's maximum distribution and the probability distribution on attempts and hacking time for a single level protection with predetermined parameters.

Let's define t_0 as parameter, defining the properties of technical protection of information over time and associated with the reliability of TPI. The specific properties of the parameter t_0 will be determined later. Then t – the current time during which protection is carried out, $p_0(t)$ is the probability of protection of the TPI in time.

Then the properties of TPI through security risks over time are:

$$(t_0 + t) \cdot p_0(t) = f(t), \tag{1}$$

where *f(t)* is positive function that depends on time and has the dimension of time. Function *f(t)* must be positive, since the left side of the expression (1) - time and probability - in the process of hacking the defense cannot be negative. Analyzing expression (1), we can say that to ensure protection against identity theft, the function *f(t)*, which we define as a function of the risks of protecting information over time, should be at least constant while time *t* increases. The constancy of *f(t)* over time provides a boundary selected acceptable level of protection. If *f(t)* will decrease over time, then the used TPI is not effective and it must be changed to another more effective protection system. If the function *f(t)* increases with time, then such a TPI is more efficient. Moreover, the stronger *f(t)* increases with time, the more effective the TPI becomes.

From (1) we write down the probability of system being protected from personal data theft

$$p_0(t) = \frac{f(t)}{t_0 + t}. \tag{2}$$

Let's define *f(t)* from initial conditions. When *t=0* (no theft) probability of protection $p_0(0)=1$. Hence

$$p_0(0) = \frac{f(t)}{t_0} = 1; \text{ or } f(t) = t_0. \tag{3}$$

Expression $f(t)$ and t_0 from (1) are the mathematical expectation of security for given TPI. And from (3) follows, that $f(t)$ first corresponds to some initial conditions for $t=0$, and then should increase or be constant with increasing time.

Consequently, the probability of TPI security over time will be

$$p_0(t)=\frac{f(t)}{f(t)+t}. \tag{4}$$

The probability of hacking in time

$$p(t)=\frac{t}{f(t)+t}. \tag{5}$$

Let's choose the independence of the hacking probability from the results of previous attempts. If the next hacking attempt was unsuccessful, then we believe that the probability of hacking the protection used remains the same. Such a distribution of hacking attempts will obey the geometric law of probability distribution, and in this case, according to [5], the probability of a hacking event on the m attempt can be written as

$$P_m(t)=[\,p_0(t)]^{m-1}\cdot p(t)=\left(\frac{f(t)}{f(t)+t}\right)^{m-1}\cdot\left(\frac{t}{f(t)+t}\right). \tag{6}$$

Let's find the distribution curve of the hacking probabilities' maximums $P_m(t)$. To do this, we determine the probability m of a hacking attempt in time, setting the first derivative of expression (6) equal to zero. We get

$$\begin{aligned}\frac{\partial P_m(t)}{\partial t}=&[\,f(t)+t\cdot(m-1)\cdot\frac{\partial f(t)}{\partial t}-t\cdot m\times\\ &\times\frac{f(t)}{f(t)+t}\cdot\left(\frac{\partial f(t)}{\partial t}+1\right)]\cdot\frac{f^{m-2}(t)}{(f(t)+t)^m}=0.\end{aligned} \tag{7}$$

We consider that the expression $\frac{f^{m-2}(t)}{(f(t)+t)^m}\neq 0$, $f(t)>0$ и $t\geq 0$. If $f(t)$=0 for any time $t\geq 0$, then according to expression (1) there are no security risks for personal data and, therefore, it is necessary to change the protection system. On the other hand it is possible that $f(t=0)$=0, since the process of protecting personal data has not yet begun. Dividing by this expression and equating in (7) the value in square brackets to zero, after certain transformations, we obtain

$$\begin{aligned}&f(t)-t\cdot m\cdot\frac{f(t)}{f(t)+t}=\\ &=[t\cdot m\cdot\frac{f(t)}{f(t)+t}-t\cdot(m-1)]\cdot\frac{\partial f(t)}{\partial t}\end{aligned} \tag{8}$$

or, considering stated above, we consider $f(t)+t>0$, then we get

$$f(t)\cdot[f(t)-(m-1)\cdot t]=t\cdot[f(t)-(m-1)\cdot t]\cdot\frac{\partial f(t)}{\partial t}. \quad (9)$$

From equality (9) we find one of its solutions, equating the expression in square brackets to zero. We will get

$$f(t)=(m-1)\cdot t. \quad (10)$$

The second solution of equality (9) can be found if we divide both its parts by expression in square brackets, which is not equal to zero. As a result of simple transformations, we have

$$\frac{\partial t}{t}=\frac{\partial f(t)}{f(t)}. \quad (11)$$

By integrating expression (11)

$$lg[f(t)]=lg\,t+const, \quad (12)$$

and then, potentiating equality (12), we obtain the second solution of equation (9)

$$f(t)=t\cdot const. \quad (13)$$

Comparing expressions (13) and (10), we see that they will be equal if *const = (m-1)*. Since the constant can be any value, we can conclude that equality (9) has one solution defined by expression (10). At the same time, expression (10) determines the relationship between hacking attempts *m* and the time of this attempt *t*, that is, determines the direction of the hacking process. The second time derivative of the hacking probability distribution (6) gives a maximum at the point defined by expression (10).

Thus, in the process of the above calculations, it was shown that the parameter *t0 = f (t)* is the mathematical expectation of the security of this TPI and can be a variable depending on the product of the number of hacking attempts and the time of hacking. This is an important result, since in real conditions, if the hacking attempts or the time of protection increase, then a high level of security risks exists.

Thus, the surface of the probability distribution of hacking $P(m,t)$ on *m* –attempt will be described by the expression

$$P(m,t)=\left[\frac{f(m,t)}{f(m,t)+t}\right]^{m-1}\cdot\left[\frac{t}{f(m,t)+t}\right]=\left[\frac{(m-1)\cdot t}{(m-1)\cdot t+t}\right]^{m-1}\cdot\left[\frac{t}{(m-1)\cdot t+t}\right], \quad (14)$$

or the surface of hacking probabilities' maximums distribution $P(m,t)$ from any attempts and hacking time

$$P(m,t)=\left[\frac{f(m,t)}{f(m,t)+t}\right]^{\frac{f(m,t)}{t}}\cdot\left[\frac{t}{f(m,t)+t}\right]. \quad (15)$$

Expression (14) corresponds to the physical requirement that the reliability $P(m,t)$ depends on hacking attempts and independence on the time of hacking when there are no hacking attempts. To prove this, we write expression (14) in the form

$$\lim_{t\to\infty} P(m,t) = \lim_{t\to\infty}\left\{\left[\frac{(m-1)\cdot t}{(m-1)\cdot t + t}\right]^{m-1} \cdot \left[\frac{t}{(m-1)\cdot t + t}\right]\right\} =$$

$$= \lim_{t\to\infty}\left[\frac{(m-1)^{(m-1)}}{(m)^{(m)}}\right] = const. \quad (16)$$

In this case, if there is no subsequent hacking attempt, then regardless of the current time (up to an infinite time), the probability of hacking remains constant in accordance with the previous attempt, since in expression (16) the time in the numerator and denominator is cut. On the other hand, if a possible hacking attempt tends to infinity, then the probability of hacking will be determined by the expression

$$\lim_{m\to\infty} P(m,t) = \lim_{m\to\infty}\left[\frac{(m-1)^{(m-1)}}{(m)^{(m)}}\right] =$$
$$= \lim_{m\to\infty}\left[\left(\frac{m-1}{m}\right)^{m-1}\cdot\frac{1}{m}\right] = \lim_{m\to\infty}\left[\frac{1}{e\cdot m}\right] = 0. \quad (17)$$

Thus, if a hacking attempt occurs at infinity, then the probability of hacking will be zero.

Function $f(m,t)$, inherent in this technical protection, determines its protective properties and the direction of hacking. This function is responsible for the distribution of probabilities' maximums surfaces and hacking probabilities $P(m,t)$ and depends on the coordinates *m* and *t* of the hacking point. The relationship between the coordinates *m* and *t* of the hacking point at constant values of the function is shown in Fig. 1 by lines 1, 2, 3, 4. With increasing line number from 1 to 4, the value of the function will change, respectively, 1, 10, 20, 40. Lines 5, 6 give the hacking direction, which is determined by two hacking points. Moreover, one of the points can be determined by the origin, that is, *m-1 = 0* and *t = 0*. Thus, the intersection of the lines of constancy of the function and the directions of hacking will give the values of the probability of hacking at each point of intersection with a given hacking attempt.

In real conditions, each specific hacking attempt corresponds to the values m_1, t_1 and m_2, t_2. Moreover, each subsequent hacking attempt will have values $m_2 > m_1$, $t_2 > t_1$ and, therefore, according to expression (10), the value $f(m,t)$ should increase. In Fig. 1, this fact is represented by a straight line of the hacking direction (line 5) between the two values $f(m_1,t_1)$ and $f(m_2,t_2)$ and coordinates m_1, t_1 and m_2, t_2.

Function $f(m,t)$ in the direction of hacking, depending on a change in one of the coordinates, can be represented as:

time

$$f(t) = \left[(m_1 - 1) + \frac{m_2 - m_1}{t_2 - t_1}\cdot(t - t_1)\right]\cdot t\,, \quad (18)$$

And hacking attempt

$$f(m) = \left[t_1 + \frac{t_2 - t_1}{m_2 - m_1}\cdot(m - m_1)\right]\cdot(m-1)\,. \quad (19)$$

The values of expressions (10), (18) and (19) are equal to each other and determine the probability value at the hacking point. Expression (10) in expression (15)

defines the hacking probability's maximums distribution surface, which is described by two coordinates *m* and *t* of hacking point. Expression (18) describes the probability of breaking from one time coordinate *t* of the hacking point. Expression (19) describes the probability of breaking from the coordinate *m* of the hacking point. Thus, we can write

$$f(m,t) = f(t) = f(m)\,. \tag{20}$$

We introduce the concept of the intensity or frequency of hacking attempts

$$\omega = \frac{m_2 - m_1}{t_2 - t_1}\,. \tag{21}$$

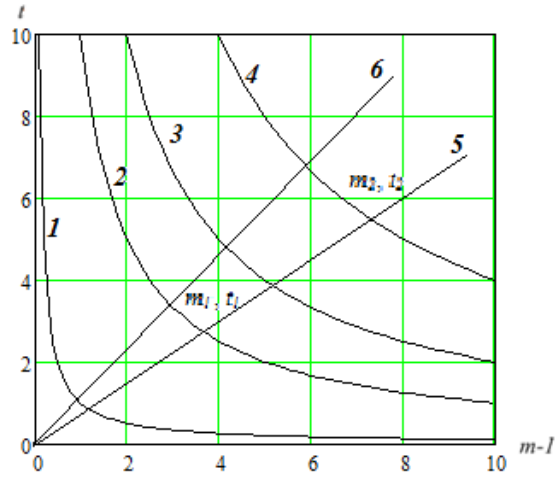

Fig. 1. Correlation between the coordinates *m* and *t* of the hacking point for constant values of function $f(m,t)$ and hacking direction. Line 1 corresponds to $(m,t) = 1$, line 2 - $f(m,t) = 10$, line 3 - $f(m,t) = 20$, line 4 - $f(m,t) = 40$, lines – 5, 6 give hacking directions.

During TPI design, control or modernization it may be necessary to determine one of parameters either *m* or *t* using second known parameter *t* or *m* respectively using a function $f(t)$ or $f(m)$ and hacking direction. This will allow, when assessing the quality of the T3I, to determine a possible attempt or its hacking time at a constant frequency or intensity of hacking. Given equality (20), from expressions (18) and (19) we find the dependence of time on a hacking attempt

$$t(m) = \frac{\sqrt{A^2 + \frac{4}{\omega} f(m)}}{2} - \frac{A}{2}\,, \text{ где } A = t_1 + \frac{m_1 - 1}{\omega}\,, \tag{22}$$

and the dependence of the hacking attempt on time

$$m(t) = \frac{\sqrt{B^2 + 4 \cdot \omega \cdot f(t)}}{2} - \frac{B}{2} + 1\,, \text{ где } B = \omega \cdot t_1 - (m_1 - 1)\,. \tag{23}$$

It should be considered that in (23) during the first hacking attempt $(t) = 1$, that is, corresponds to the upcoming real hacking attempt, when the real initial time is still zero.

In studies [6,7] it is shown how the financial costs of the designed protection and the coefficient of protection efficiency are taken into account in the expression for the probability of hacking γ.

Function $f(m,t)$ determines the direction of hacking, but does not take into account the effectiveness of protection, that is, gives the value of the probability of hacking with a protection efficiency ratio (PER) equal to $\gamma = 1$, which corresponds to hacking on infinitive attempt. In real conditions, hacking occurs on the final attempt at when PER is less than 1.

Considering PER with respect to [7], expression (15) will look like

$$P(m,t) = \left\{ \left[\frac{f(m,t)}{f(m,t)+t} \right]^{\frac{f(m,t)}{t}} \cdot \left[\frac{t}{f(m,t)+t} \right] \right\}^{\gamma}. \quad (24)$$

When designing the TPI, hacking parameters are set by the developer and must correspond to the initial data. In this case, it is necessary to know the reliability of the TPI in the designed hacking direction and in the direction of the real hacking process. In order to construct the designed surface for a specific hacking attempt and the hacking time chosen by the system developer, in expressions (14) or (15), it is necessary to express the degree in terms of the parameters of a specific hacking attempt, for example, $m = m_c$, $t = t_c$. Then (14) will look like

$$P(m,t) = \left\{ \left[\frac{f(m,t)}{f(m,t)+t} \right]^{m_c-1} \cdot \left[\frac{t}{f(m,t)+t} \right] \right\}^{\gamma}, \quad (25)$$

and (15)

$$P(m,t) = \left\{ \left[\frac{f(m,t)}{f(m,t)+t} \right]^{\frac{f(m_c,t_c)}{t_c}} \cdot \left[\frac{t}{f(m,t)+t} \right] \right\}^{\gamma} = \left\{ \left[\frac{f(m,t)}{f(m,t)+t} \right]^{\frac{f(m_c)}{t_c}} \cdot \left[\frac{t}{f(m,t)+t} \right] \right\}^{\gamma}. \quad (26)$$

In Fig. 2, the surface of hacking probabilities' maximums distribution according to formula (24) is plotted. According to this formula, each point is built according to the maximum probability of hacking against personal data theft, for example, with the selected protection efficiency γ=0,7. A surface with a selected projected hacking direction along line 5 is shown, and line 6 corresponds to another, for example, real hacking direction. On lines 5 and 6, the probabilities of hacking are plotted depending on the direction of the hacking. The points of intersection of the surface with the lines give the coordinates of the maximum probabilities of hacking in this direction. For line 5, these coordinates will be $m_м$ = 9, $t_м$ = 6 with a maximum probability of hacking at a given point, and for the line 6 – $m_м$ = 12, $t_м$ = 11.

Fig. 3 shows a surface with a hacking probability maximum at a point with a chosen breaking direction along line 5, for example, with a maximum at a point m_c = 9, t_c = 6. Line 5 corresponds to the chosen direction, and line 6 corresponds to another real hacking direction, but along the surface projected along line 5. The surface of the

probability distribution of hacking in Fig. 3 is constructed according to the formula (26).

It can be seen from Fig. 3 that with a change in the direction of hacking (line 6), the reliability of the TPI will change and it must be taken into account during design process.

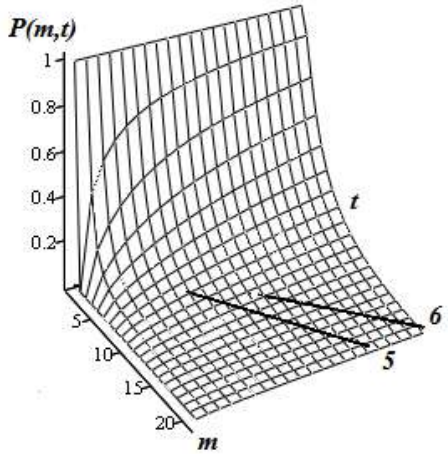

Fig. 2. The surface of the hacking probability maximums plotted according to formula (24) with the protection efficiency $\gamma = 0.7$; 5, 6 - hacking lines, the direction of which corresponds to the lines of Fig. 1. The points of intersection of the surface with the lines give the coordinates of the maximum probability of hacking in this direction.

On the surface along the coordinates *m*, *t*, the values of hacking probabilities' maximums are visible. The intersection point of both maximums and lines gives the point of maximum hacking probability in this direction. There can be only one such point and in Fig. 2 it is represented by the intersection of the surface with the direction line of the hacking process for line 5, these coordinates will be $m_м = 9$, $t_м = 6$, and for line 6 – $m_м = 12$, $t_м = 11$.

Figure 4a shows a surface with hacking probability maximum at a point with projected hacking direction along line 1, with maximum at a point $m_c = 10$, $t_c = 5$. Line 2 corresponds to the probability distribution of another real hacking direction, but on a surface designed with the hacking direction along line 1. Line 3 gives the direction of a real hack if the attacker changes the real process of attack. It can be seen from Fig.4b that the real process of hacking with the hacking probability surface [8-11] described by the expression ***P(m)=1/m*** (white surface) and the surface of the designed protection (gray surface) will flow with probability determined by the line of intersection of the white and gray surfaces. In this case, according to Fig.4b, the hacking process with the calculated maximum probability value will only be for the direction of the designed TPI (line 1), and for other directions the value of the hacking probability will be lower (lines 2 and 3). If the direction of the real hacking process is close to the projected direction of protection, then TPI hacking can occur at values close to the

projected hacking attempt m_{hack}, especially with small increases in time between hacking attempts.

With significant increases in time between hacking attempts, hacking case may not occur at all. A similar situation where hacking does not happen is possible if hacking attempts will follow each other very often.

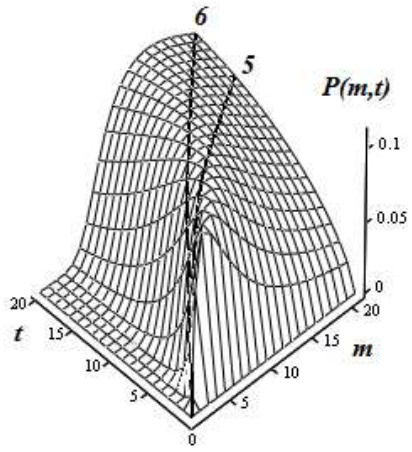

Fig. 3. A surface with hacking probability maximum at a point with a chosen hacking direction along line 5 with a maximum at a point $m_c = 9$, $t_c = 6$. Line 5 corresponds to the chosen direction, and line 6 corresponds to the actual hacking direction.

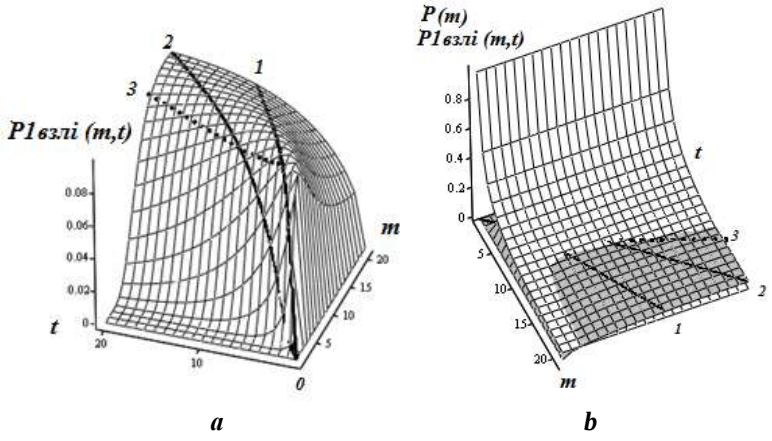

Fig. 4. Hacking probability distribution: **a** - with the projected hacking direction along line 1 (gray surface); **b** - surface fig.a and the real hacking surface (white surface), calculated by the formula ***P(m)=1/m***

3 Conclusions

Based on protection risks of TPI there was acquired function $f(m,t)$, depending on hacking process direction, which is inherent in this protection, that is mathematical expectation of TPI protection and defines the reliability of technical protection in designed hacking direction.

From the function of the direction of the hacking process, an expression that allows to determine one of the parameters using second parameter *m* or *t* is promising. This is important when designing, analyzing the state and modernizing the TPI, because it will allow one to find another using one of the known parameters in the direction of hacking. For example, using a known hacking attempt, you can evaluate the possible time when a protection hack occurs.

In this work, we obtain the TPI hacking probability distribution for the direction of the projected process of hacking, depending on the parameters of the attempt, the time of this hacking attempt. When designing protection, the hacking direction is selected in the form of a straight line, which is built according to the required initial data.

Using the expressions obtained in this work, we constructed the distribution surface of the hacking probabilities' maximums (Fig. 2), from which the most probable value of hacking and the coordinates of the hacking point are determined at the points of intersection of the surface and the line. The surfaces of the hacking probability distribution are constructed (Fig. 3, Fig. 4a) along the lines of the designed hacking directions (lines 5, line 1). The results of the work make it possible to assess the state of the residual probability of reliability of the working TPI of the real hacking process in directions of personal data theft chosen by the attacker.

In the future, the studies will allow us to create a new methodology for the design, modernization and analysis of the state of the working complex of technical protection of information, taking into account the financing invested in protection, the effectiveness of the developed protection and the hacking direction chosen by the developer.

References

1. Domarev V.V. Informational technologies' safety. Systematic approach. K.: TID «DS» Ltd., 2004. 992 p.
2. Korchenko A.G. Protection systems development based on fuzzy sets. Theory and practical solutions. K.: «MK-Press», 2006. – 320 p.
3. Arkhipov O.E., Arkhipova S.A. Experts work quality evaluation on the basis of multi-objective examination. Information protection: Scientific and technical journal. - K.: NAU, 2011. №4 (53). – p. 45-54.
4. Gryshchuk R.V. Theoretical bases of modeling the processes of attack on information by the methods of differential game theory and differential transformations: Monograph. Zhytomyr : Ruta, 2010. – 280 p.
5. Rumshinskiy L.Z. Elements of Probability Theory. M.: Pub. Nauka, Glavn. Red. Fiz.-mat. Lit., 1970. 256 p.

6. Zhurylenko B.E. Estimation of financial costs for building an information security system. Information protection: Scientific and technical journal - 2018. - №4(20). – p.231-239. DOI: 10.18372/2410-7840.20.13424
7. Zhurylenko B.E. A methodology for constructing and analyzing the state of a complex of technical information protection with probabilistic reliability and taking into account temporal hacking attempts. Information protection: Scientific and technical journal, 2015. №3(17). p.196-204.
8. S. Gnatyuk, Critical Aviation Information Systems Cybersecurity, Meeting Security Challenges Through Data Analytics and Decision Support, NATO Science for Peace and Security Series, D: Information and Communication Security. IOS Press Ebooks, Vol.47, №3, pp. 308-316, 2016.
9. Z. Hassan, R. Odarchenko, S. Gnatyuk, A. Zaman, M. Shah, Detection of Distributed Denial of Service Attacks Using Snort Rules in Cloud Computing & Remote Control Systems, Proceedings of the 2018 IEEE 5th International Conference on Methods and Systems of Navigation and Motion Control, October 16-18, 2018. Kyiv, Ukraine, pp. 283-288.
10. Shakhovska N., Fedushko S., Greguš ml. M., Melnykova N., Shvorob I., Syerov Yu. Big Data analysis in development of personalized medical system. The 10th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN 2019) November 4-7, 2019, Coimbra, Portugal. Procedia Computer Science, Volume 160, 2019, Pages 229-234. https://doi.org/10.1016/j.procs.2019.09.461
11. M. Zaliskyi, R. Odarchenko, S. Gnatyuk, Yu. Petrova. A. Chaplits, Method of traffic monitoring for DDoS attacks detection in e-health systems and networks, CEUR Workshop Proceedings, Vol. 2255, pp. 193-204, 2018.