Estimation of the Effectiveness and Functioning of Enterprises in Boards of Corporate Security

Sergii Kavun
Department of Computer Systems and Technologies, Kharkiv National University of Economics, Kharkiv, Ukraine
E-mail: kavserg@gmail.com
Tel: +38-067-7095577

Denis Čaleta
ICS Institute, Ljubljana, Slovenia
E-mail: denis.caleta@ics-institut.si

Miran Vršec
ICS Institute, Ljubljana, Slovenia
E-mail: miran.vrsec@ics-institut.si

Robert Brumnik
ICS Institute, Ljubljana, Slovenia
E-mail: robert.brumnik@ics-institut.si

JEL Classifications C02, C13, C15, C53, C63, G32, G34, K22, L30

Abstract

The main purpose of this study is to show the possibility of estimating the effectiveness and functioning of a System of Economic Security (SES) for enterprises. This estimation will show examples of some of the activities of SES. The conceptual provisions and model basis are based on some of the real indicators of a functioning enterprise. This method can also be used for enterprises in any area of activity that have confirmed the results of modelling from real enterprises and which are functioning under some of the conditions of a high level of uncertainty from the external environment. The model basis is presented as a mathematical model, which is not frequently used in the area of corporate security. Moreover, some of the results received, based on real enterprises, have confirmed the reliability of using these mathematical models based on the results of modelling. Mathematical models were formed based on the data from real enterprises for estimating its effectiveness and functioning. These will allow improvements in the management system and aid forecasting. This possibility is based on received dependences, which can help to create positive recommendations for the future development of enterprises and to carry out optimisation of different kind of expenses.

Keywords: Estimation, Enterprise Functioning and Development, Security, Effectiveness, Mathematical Method

1. Introduction

In an age of global financial and economic crisis, the market is including some operations of enterprises, has acquired a different meaning, especially in some special economic zones. The global idea is that the use of previously known approaches and concepts today justify their merits. Examples are the various statistical and analytical studies of well-known companies such as CSI (their famous report about Computer Crime and Security Survey), Perimetrix, RSA, Finjan, IT Policy Compliance

Group, Ernst & Young, Ponemon Institute and others (Kavun, 2007). All the results presented have shown dynamically increasing losses (financial, economic, industrial, personnel, etc.). These losses affect the overall economic development of enterprises in special economic zones. The results of these events are often bankruptcy, a sharp decline in production efficiency, global job cuts, the absorption of small enterprises by larger ones and other negative processes.

2. Previous Research

Enterprises in special economic zones trying to 'survive' in the circumstances, may consider various mechanisms to overcome the crisis. One such mechanism is undoubtedly the synthesis and implementation of a System of Economic Security of Enterprise (SESE) that takes into account all of the processes that occur. However, most existing approaches (Dovbnya and Gichova, 2008; Geetc et al., 2006; Kallol and Godwin, 2003; Kavun, 2009; Khristianovski, Kavun, and Zyma, 2011; Ortynskii, Kernitckii and Givko, 2009; Stevenson, 2004; Lindsey, 2010) are either static or based on performance.

In order to prove the relevance of the present global research 'Think Tank InfoWatch' (Kavun, 2007) on some indicators, this study aims to analyse all types of leaks of classified information (including personal information). During the reporting period, there were 249 incidents where due to the total number of records of personal data, it has been argued that over 100 million people have been affected.

3. Statistical Basis of the Study

All the causes of leakage of classified information have been divided into intentional and non-intentional (random). For example, a common theft of computer technology, which occurs during theft from a vehicle, where there are reasonable grounds to believe the offence wasn't the primary reason for the theft; in this case the leak is accidental and not leakage of classified information. The study (Kavun, 2009) and the distribution of leakage of classified information is shown in Fig. 1.

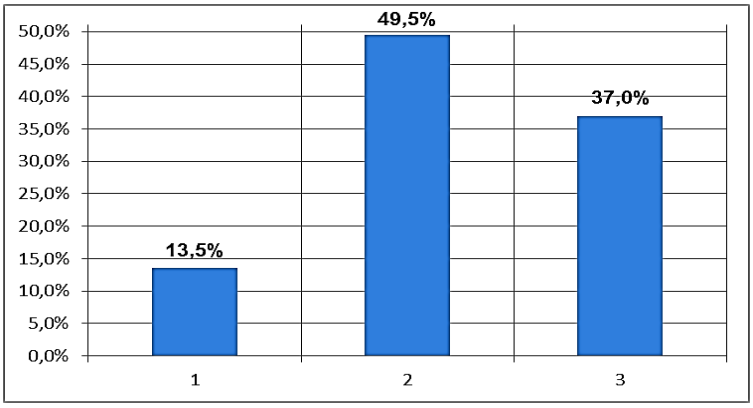

Fig. 1. Breakdown leaking classified information (in %)
1 – source is not established,
2 – source is random,
3 – source is intentional.

We can confidently assert that the priority is the fight against unintentional leaks of classified information in an enterprise. The prevention of such leaks is easier and cheaper than fighting against the difficult consequences of deliberate leaks of classified information. It is more difficult task, than other tasks in this area. The effectiveness of such a struggle is lower, than the similar struggle with some consequences from insiders (Kavun, Sorbat and Kalashnikov, 2012).

The source of the leaks of classified information has been divided into three categories (most currently): government, business and others. The study (Kavun, 2012) showing the source of leaks by types of organisation is presented in Fig. 2.

The distribution has changed little compared with 2008-2009 (Kavun and Mikhalchyk, 2010). Measures to prevent leakage of classified information are used in public and commercial SESE (Kavun and Zyma, 2009).

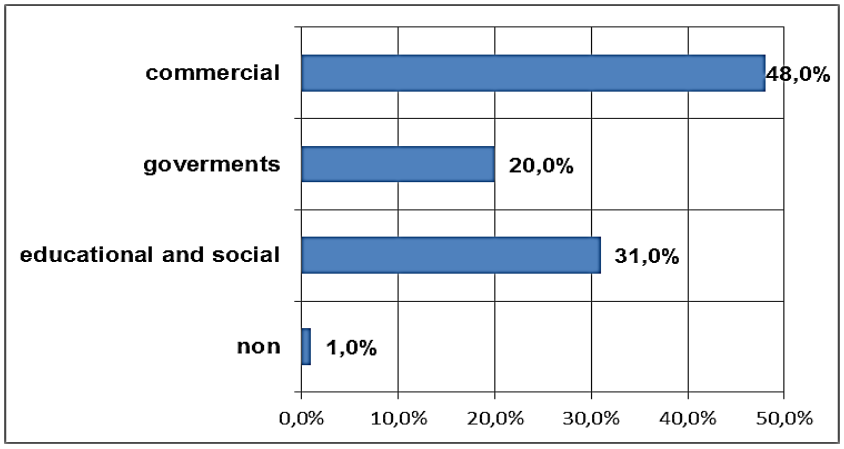

Fig. 2. Distribution of particle sources and intentional leakage by types of enterprise,%

For determine an objectiveness of received data to need define abeyance (Table 1) for leakages of the information with restricted access (on example personal data).

Table 1: Latency of leakages of personal data (Ponomarenko and Kavun, 2008)

Country	Number of leakages	Part	Number of leakages per million of population
AU, Austria	1	0.40%	0.050
CA, Canada	5	2.01%	0.154
CL, Chili	1	0.40%	0.064
CN, China	3	1.20%	0.002
DE, Germany	2	0.80%	0.024
FR, France	1	0.40%	0.017
GB, Great Britain	23	9.24%	0.382
IE, Ireland	3	1.20%	0.500
IN, India	1	0.40%	0.001
IT, Italy	2	0.80%	0.034
UA, Ukraine	3	1.20%	0.062
RU, Russia	4	1.61%	0.028
US, the USA	192	77.11%	0.655
Others	7	2.81%	-

The last figure shows the number of leakages of classified information per one million of the population – in countries where personal data registration is little changed. As before, it can be stated that there is approximately one leak of classified information per year per million of the population.

This analysis included only those sources of classified information that became public. According to experts (Stevenson, 2004; Wang, 2008; Lindsey, 2010), latent leaks of classified information amount to about the same. In addition, in those countries, where the registration process of leakages has not being increased, are possible make the comparison of performance based on the indicator of abeyance, which is much higher. There are many leaks of classified information which are not disclosed at all.

The distribution of the leakages of classified information was also studied according to their type (Fig. 3). However, on the basis of media reports, other statistics (Ortynskii, Kernitckii and Givko, 2009) for other types of classified information are not expected. Fact leaking state secrets is the state secret. Similarly, a leakage of commercial information secret is the commercial information secret. However, the leakages of personal data are not usually announce in the first place (Kozachenko and Lyashenko, 2003; Kavun and Sorbat, 2012).

This study has been performed to determine the types of media used for leakage; the results are shown in Fig. 3-6 (Kavun, 2009).

The majority of data flowed through the network, however some data was held on portable computers. Data is lost and stolen at an ever-increasing pace. To achieve more objectives, it was decided

to merge the PC with mobile media (CD, DVD, flash media) and call it "mobile media". This category almost equalled the leakage through the network (25% vs. 29%). For occasional sources (it's the sources, which are not constant), "mobile media" is not only catching up but is quite ahead of the leakage through the network (30% vs. 24%, Fig. 6).

The conclusion of the analysis of the study is that the effectiveness of existing assets is 3.5% - not enough to close the most common channels of information leakage. It is therefore necessary to carry out encryption of data on the disks of mobile computers, for example, by works (Kavun (patent), 2006; Kavun (patent), 2009).

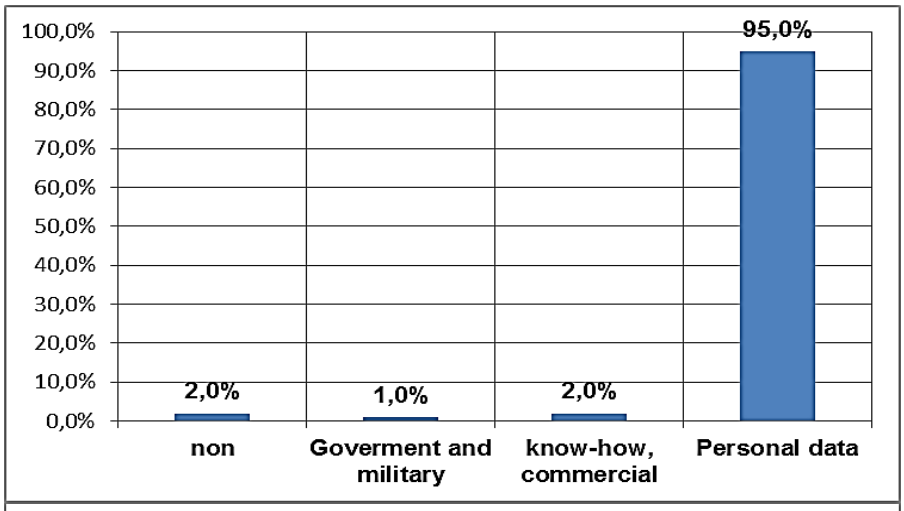

Fig. 3. Distribution of shares by type of leakage of classified information,%

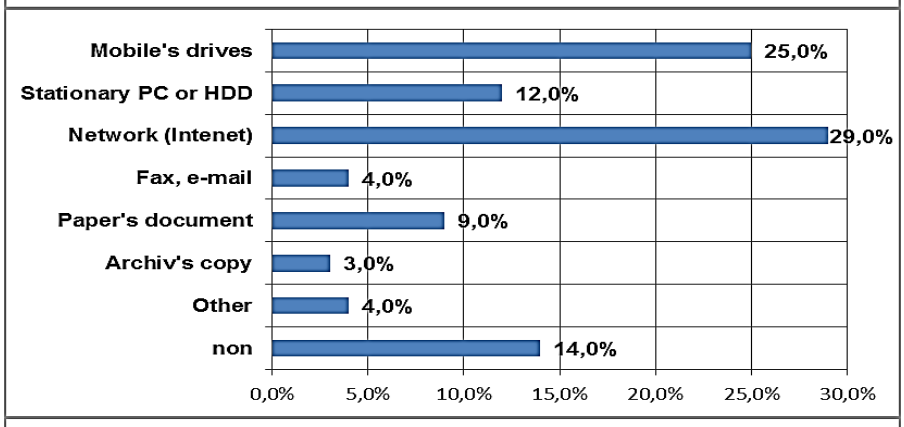

Fig. 4. Distribution by type of media sources,%

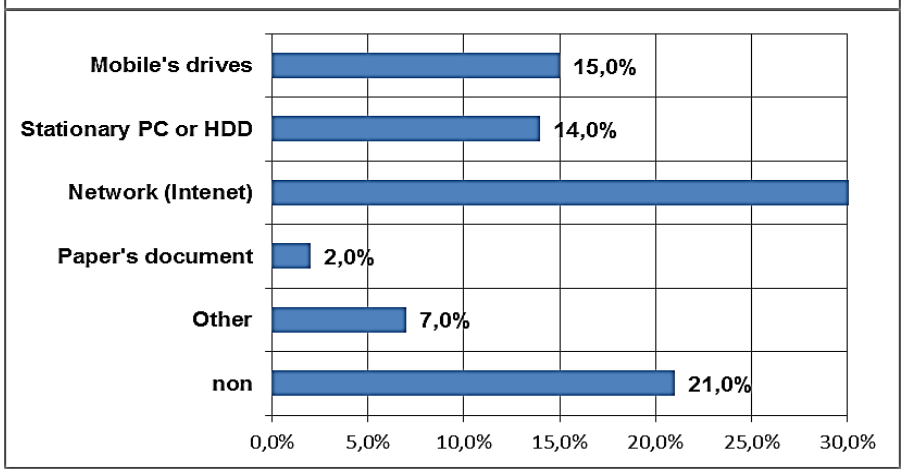

Fig. 5. Distribution of deliberate leaks by the media,%

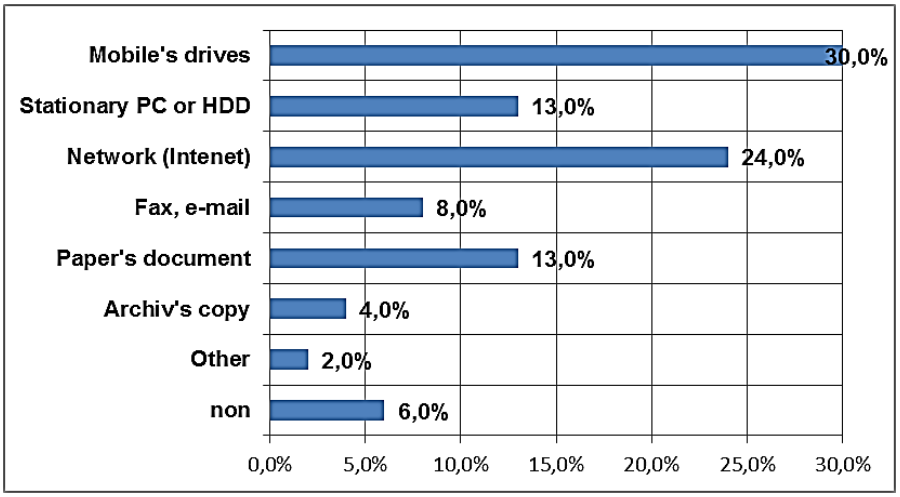

Fig. 6. The distribution of occasional sources for carriers,% (Kavun, 2009)

4. Hypotheses

In order to study the mathematical fundamentals of the possibility of estimating the effectiveness and functioning of SES for enterprises, the following hypotheses were tested:

- **H1:** Will be able to make a real estimation of effectiveness and functioning (as a level) of SES for enterprises in digital kind (type) or numerically (no empirically) based on real indicators of a functioning enterprise with visual interpretation.
- **H2:** Will be able to detect some kind of dependences between incoming data and some external factors or impacts. For example, some (positive) dependence can be detected between the level of effectiveness of economic security and the number of negative impacts; and an average time between incidents in an area of information (corporate) security and negative impacts. However, no (negative) dependence can be detected between the level of effectiveness of SES functioning and an average number of headcounts; and an average recovered time z^{th} node of SES and number of negative impacts.
- **H3:** Will be able to make some practical recommendations for enterprises about optimising internal resources (human, technical, technological, etc.) based on the results of this research.

5. Mathematical Model of Researching

A significant issue for the head of any link management is the effectiveness and implementation of management decisions. It is necessary to use such knowledge or the development of new mechanisms of evaluating the effectiveness (SESE) (Ponomarenko and Kavun, 2009; Lindsey, 2010; Wang, 2008; Kavun and Mikhalchyk, 2010; Kavun, 2009).

First it is necessary to deal with unintentional leaks of classified information. To improve the efficiency of removal of channels of information leakage (CIL), the concept of the level of economic efficiency SESE was introduced and denoted as LEES (Level of Efficiency of Economic Security). Since the concept of SESE (Kavun, 2007-2010) uses as a basis SESE within the life cycle (Kavun, 2008), then

$$\mathrm{LEES} = \max\{\mathrm{LEES_h}\}, \quad (1)$$

where $\mathrm{LEES_h}$ a significant level of efficiency of SESE at time *h*, if the duration of the study is one year and the frequency rate of one every month, for instance, it is possible to obtain the dynamics of changes in the level of efficiency of SESE (Fig. 7).

In addition, the study has obtained functional dependence of the efficiency of various factors of SESE enterprise development (Kavun, 2009, 2011). When calculated the following dependences are found:

$$LEES_h = f(\overline{T}, \overline{T_Z^B}, V_{ST}, V_{VCO}, V_{VSSF}, V_{ND}, V_{AR}, V_{All}), \quad (2)$$

$$LEES_h = f(\overline{T}, \overline{T_Z^B}, V_{SES}). \quad (3)$$

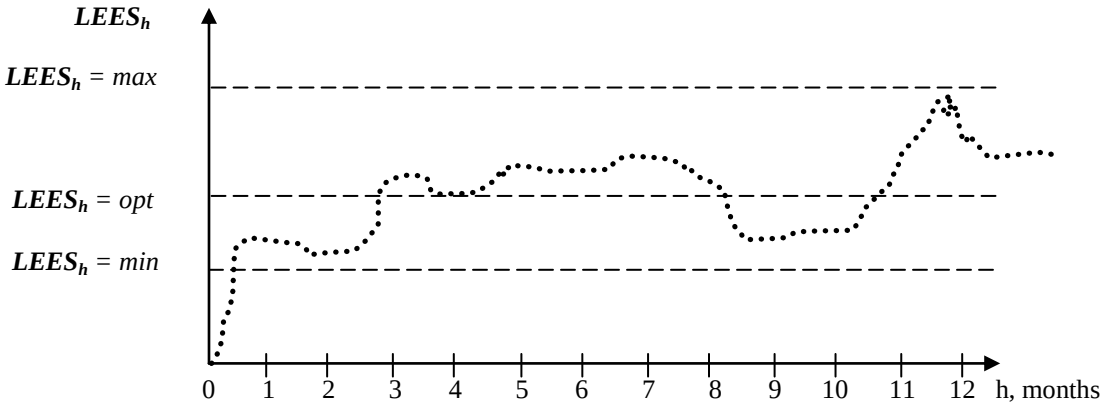

Fig. 7. Example of dynamics of effectiveness changes of SESE (Kavun, 2009)

At the same time, $\overline{T} \to max$, $\overline{T_Z^B} \to min$, $V_{SES} \to min$,

where

$$\overline{T} = \frac{1}{\frac{1}{N}\sum_{i=1}^{N}\sum_{j=1}^{K} IES_{ij}}, \quad (4)$$

$\overline{T}$ – the average time between incidents in SESE during the research period;

N – the number of time periods, at the same time, usually N = 12, so, it is the number of months and the duration of this study for one year;

K – the number of kinds or types of economic (or other) crimes used, based on the study by Ponomarenko and Kavun (2008);

IES_{ij} – the frequency of emergence for the incidents in SESE (for example, an incident of economic or informational security) for the i^{th} time period j^{th} kind or type of economic crime (Ponomarenko and Kavun, 2008);

$\overline{T_Z^B}$ - the average recovery time for z^{th} node of SESE;

$$\overline{T_Z^B} = \frac{1}{N}\sum_{j=1}^{N} t_{zj}^B, \quad (5)$$

where t_{zj}^B – the recovery time for z^{th} node of SESE for the j^{th} time period;

V_{ST} (standards) – the volume (number) of sub-systems or business-processes that comply with the standards of SESE determine the appropriate cost of implementing the standards EBSH, the costs should be not less than 30% (this is an expert estimation);

- V_{VCO} (vulnerabilities, channel of outflow) – the volume (number) of sub-systems or business processes, in which the analysis of vulnerabilities and channel leaks of classified information, determine the appropriate cost analysis, the costs should not be less than 28% (this is an expert estimation);
- V_{VSSF} (antivirus, anti-spam, anti-spyware, firewalls) – the volume (number) of sub-systems or business processes for which the anti-virus, anti-spam, anti-spyware tools and software firewalls determine the associated costs of purchase, installation and maintenance, the costs should not be less than 12% (this is an expert estimation);
- V_{ND} (normative documents) – the volume (number) of sub-systems or business processes, which are developed and implemented regulations (Kavun, 2009, 2011), to determine the appropriate cost of developing and implementation for a workflow system, the costs should be not less than 15% (this is an expert estimation);

- V_{AR} (audit and level of risks) – the volume (number) of sub-systems or business processes for which an audit was conducted and rated by risk level to determine the appropriate cost of implementing these measures, the costs should not be less than 10% (this is an expert estimation);
- V_{All} – the volume (number) of sub-systems or business processes that remain (business processes) to determine the appropriate cost of their implementation, the costs should be less than 5% (this is an expert estimation);
- V_{SES} (system of economic security (safety) – the volume (number) of all sub-systems or all business processes, which determine the costs. Then

$$\mathbf{V_{SES} = V_{ST} + V_{VCO} + V_{VSSF} + V_{ND} + V_{AR} + V_{All} = 100\%.}$$

This gives a graphical view of the distribution V_{SES} considering the share of certain components derived from an expert survey (Fig. 8). Thus, the generated description of the new method of evaluating the effectiveness of SESE is based on the volume (number) of sub-systems and their distribution according to the authors (based on an expert method) (Kavun, 2007, 2008, 2010).

Such distribution is not an effective method (Kavun, 2009) of determining the level of the economic efficiency of SESE. In addition, these type of expenses have to be performed following conditions, which ensure the feasibility and necessity of SESE.

If $\mathbf{V_{All} > V_{ST} + V_{VCO} + V_{VSSF} + V_{ND} + V_{AR}}$, we estimate that the cost effectiveness of SESE is not appropriate due to the cost of implementing and supporting sub-systems and the remaining excess costs that are surplus to SESE.

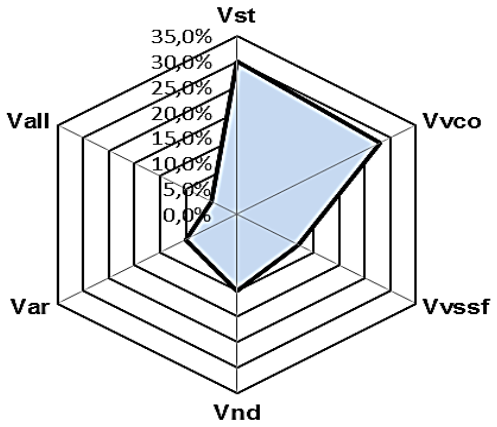

Fig. 8. Distribution of costs for the volume (number) of sub-systems of SESE in a radar diagram, which quite clearly shows the advantages of the variables V_{ST} and V_{VCO}, %

Using an optimisation approach to evaluating the economic efficiency of SESE expression (2) becomes:

$$LEES_h = f\left\{\begin{array}{c} \overline{T} \to \max \\ \overline{T_z^B} \to \min \\ V_{ST} \to \max \\ V_{VCO} \to \max \\ V_{VSSF} \to \max \\ V_{ND} \to \max \\ V_{AR} \to \max \\ V_{All} \to \min \end{array}\right. . \quad (6)$$

To enable the calculation of the level of economic efficiency, SESE must enter SESE physical parameters that would provide the opportunity to obtain a dynamic, automated method:

- K_{PC} – the number of workstations (workstations or personal computers), involved in ensuring the functioning of SESE, assuming that on average 85% (Kavun, 2009) of employees (M) in a

modern company with workplace computers, and also taking into account that $V_{ST} = \{V_{VCO}\} \cup \{V_{VSSF}\} \cup \{V_{AR}\}$, then

$$\mathbf{K_{PC} = \lceil 0{,}85 \times M \rceil.}$$

- K_S – the number of servers involved in ensuring the functioning of SESE, assuming an average of 20-25 workstations each with one server, then

$$\mathbf{K_S = \lfloor K_{PC} / 25 \rfloor.}$$

- K_{NE} – the number of pieces of network equipment involved in ensuring the functioning of workstations and servers, provided that the number of ports for connecting network equipment Z = 5, 8, 12, 16, 32, 64, 128 depending on the manufacturer's specifications and network equipment and if the company uses similar and typical equipment, then

$$\mathbf{K_{NE} = \lceil (K_{PC} + K_S)/Z \rceil.}$$

- K_{SE} – the amount of communication equipment provided to the company's employees (PDAs, cell phones, PDA phones, smartphones, netbooks, mini-PCs, etc.), because in the simplest case, K_{NE} is the number of employees (M). However, taking into account that on average every 3rd employee has several similar devices, then

$$\mathbf{K_{CE} = 0{,}33 \times M + M = \lceil 1{,}33 \times M \rceil.}$$

- K_{CTI} – the number of channels for data transmission (channel of transfer information, CTI), which form the channels of information leakage (CIL) and classification are presented in Table 2.

By using the entered classification of CIL the following formula was determined:

$$\mathbf{K_{CTI} = \lceil (20 + K_{NE}) \times (K_{PC} + K_S) + 17 \times K_{CE} + 2 \times (K_F + K_T) \rceil,} \quad (7)$$

where K_T – the number of fixed telephones,

K_F – the number of fixed faxes and for the fax features there are two CILs: acoustic and data.

Table 2: Classification of Channels of Information Leakage (Kavun, 2009; Ponomarenko and Kavun, 2008)

№	Type of CIL	№	Type of CIL
For PC and servers		**For cellphones and similar devices**	
1	e-mail	1	Wi-Fi- channel
2	FTP-service	2	IrDA- channel
3	HTTP- service	3	ICQ- service
4	P2 P- service	4	CHAT- service
5	CHAT- service	5	Skype- service
6	ICQ- service	6	EMS- service
7	IRC- service	7	WWW- service
8	Wi-Fi-channel	8	FTP- service
9	IrDA- channel	9	P2P- service
10	Bluetooth- channel	10	WAP- service
11	WWW- service	11	MMS- service
12	USB- interface	12	SMS- service
13	COM- interface	13	IRC- service
14	Card reader- channel	14	USB- channel
15	Skype- service	15	HTTP- service
16	SCSI- interface	16	Bluetooth- channel
17	LPT- interface	17	e-mail
18	FDD- interface		
19	HDD- interface		
20	simple copying (with using a set $\{K_{NE}\}$)		

Then based on input system of indicators (6) is transformed into the following model:

$$LEES_h = f\left(\begin{cases} \overline{T} \to \max \\ \overline{T_z^B} \to \min \\ K_{PC} \to opt(\min) \\ K_S \to \min \\ K_{NE} \to \min \\ K_{CE} \to \min \\ K_{CTI} \to \min \end{cases}\right). \tag{8}$$

Based on the properties of absorption and transformation for the expression (6) and the direction for the optimisation can obtain the minimizing (it's a unified direction of the optimisation) of this system (8)

$$LEES_h = f\left(\begin{cases} \overline{T} \to \max \\ \overline{T_z^B} \to \min \\ K_{CTI} \to \min \end{cases}\right), \tag{9}$$

or in linear type

$$LEES_h^{LIN} = f\left(\max\left(\overline{T}\right) \times \min\left(T_z^B, K_{CTI}\right)\right). \tag{10}$$

In order to make this formula system (9-10) accord with the same pattern of optimisation, then

$$LEES_h = f\left(\begin{cases} \left(1 - \overline{T}\right) \to \min \\ \overline{T_z^B} \to \min \\ K_{CTI} \to \min \end{cases}\right), \tag{11}$$

$$LEES_h^{LIN} = f\left(\min\left(\left(1 - \overline{T}\right), T_z^B, K_{CTI}\right)\right). \tag{12}$$

Thus, the problem of economic efficiency of SESE is formulated as a multi-criteria (three factors) optimisation problem. Thus, the hypothesis H1 is confirmed.

If a dynamic account of time is entered, it takes into account the dynamics of the economic efficiency of SESE and it is also necessary to introduce rationing of intermediate factors. Then the system of relations takes the following form

$$\begin{cases} V_{SES} = \frac{1}{N}\sum_{i=1}^{N} V_{SES}^i, \\ \sum_{i=1}^{N} V_{ST}^i + \sum_{i=1}^{N} V_{VCO}^i + \sum_{i=1}^{N} V_{VSSF}^i + \sum_{i=1}^{N} V_{ND}^i + \sum_{i=1}^{N} V_{AR}^i + \sum_{i=1}^{N} V_{All}^i = N \times V_{SES}, \\ \sum_{i=1}^{N} V_{SES}^i = \sum_{i=1}^{N} V_{SES}^{i+1}, \\ \sum_{i=1}^{N} {}^H V_{ND}^i = 1, \sum_{i=1}^{N} {}^H V_{AR}^i = 1, \sum_{i=1}^{N} {}^H V_{All}^i = 1, \\ \left(V_{ST}^i + V_{VCO}^i + V_{VSSF}^i + V_{ND}^i + V_{AR}^i + V_{All}^i\right) = V_{SES} \text{ for } \forall \text{ i}, \\ V_{All}^i = V_{SES}^{i+1} - \sum_{i=1}^{N}\left(V_{ST}^i + V_{VCO}^i + V_{VSSF}^i + V_{ND}^i + V_{AR}^i\right), \\ \sum_{i=1}^{N} {}^H V_{ST}^i = 1, \sum_{i=1}^{N} {}^H V_{VCO}^i = 1, \sum_{i=1}^{N} {}^H V_{VSSFl}^i = 1, \end{cases} \tag{13}$$

$$\left|\begin{cases} \sum_{i=1}^{N} T_{CP}^i = 365, \\ \sum_{i=1}^{N} {}^H T_{CP}^i = 1, \end{cases} \begin{cases} \sum_{i=1}^{365/N} IES_{ij} < 365, \\ \sum_{i=1}^{365/N} {}^H IES_{ij} = 1, \end{cases} \begin{cases} \overline{T_Z^B} \times \frac{1}{N}\sum_{i=1}^{N} IES_{ij} < 365, \\ \sum_{i=1}^{N} \overline{{}^H T_Z^B} = 1, \end{cases}\right|, \tag{14}$$

$$\begin{cases} K_{PC} + K_S < M \ , \\ K_{PC} + K_S << V_{SES}, \\ \{V_{All}\} \neq K_S. \end{cases} \quad (15)$$

Thus, the ratio of (13-15) form a system of constraints, which exist, with the possibility of using the proposed estimation method based on "sub-volumes". Therefore, we have a ready model of a mathematical nature, where the functional is the formula (11) or (12) at the restrictions (13-15).

In addition, the synthesis of SESE must comply with the following conditions:

1. If $\overline{T_Z^B} \geq T_{ave}$ then SESE is considered with the lost capacity for work and cannot be restored, i.e. the recovery of i-node if there is another incident.

2. If $IES_{ij} \geq i$, then SESE is considered with the lost capacity for work and has not restored, i.e. the period of time during which there are a number of incidents that correspond with the duration of this period of the SESE, resulting in the company not functioning.

3. If $\overline{T_Z^B} \geq 1 / IES_{ij}$, then SESE is considered with the lost capacity for work and cannot be restored because the average time of recovery after one incident exceeds the time until the next incident.

6. The Results of Hypotheses Testing Based on Data of Real Enterprises

Depersonalized names of enterprises have been used with the aim of complying with the rules of anonymity and some legal acts from a legislative base, although these are based on real data.

As a result of research by the author (Kavun, 2009-2011) (for Enterprise 1, Enterprise 2, Enterprise 3, and Enterprise 4) with the economic efficiency of SESE, the findings (Table 3) made them averaging for further use during the simulation. In this table, some variables are shown with the index 'H' which means that they are normalised, thus, its weight fraction is in common volume which enables better comparison.

Based on the tabular data of real indicators for enterprises (Table 6) for the expression (12) can calculate the possible level of economic efficiency of SESE in dynamics during the year (Fig. 9).

In a further analysis based on (Fig. 9) predictions may be made for subsequent periods using known methods of forecasting. For example, the method based on polynomial trends depends to the 3rd degree on determining the value of the reliability approximation:

$$y = -1E\text{-}05x^6 + 0{,}0006x^5 - 0{,}0109x^4 + 0{,}0886x^3 - 0{,}328x^2 + 0{,}4946x - 0{,}033; \ R^2 = 0{,}4992.$$

Table 3: Data functioning of SESE (based on copyright statistical observations (Kavun, 2007-2008))

Time period / **Indicators**		***i = 1..12***												
		January	February	March	April	May	June	July	August	September	October	November	December	**Total**
$\overline{T^i}$, twenty four hours		48	25	28	19	40	23	24	23	45	29	23	38	**365**
$\overline{{}^H T^i}$		0,13	0,07	0,08	0,05	0,11	0,06	0,07	0,06	0,13	0,08	0,06	0,10	**1**
IES_{ij} per month		0	1	0	2	1	3	6	13	0	2	3	4	**35**
${}^H IES_{ij}$		0,00	0,03	0,00	0,06	0,03	0,09	0,16	0,37	0,00	0,06	0,09	0,11	**1**
$\overline{{}_i T_z^B}$, hours		0	1	0	3	2	5	9	27	0	2	8	7	**64**
$\overline{{}^H {}_i T_z^B}$		0,00	0,02	0,00	0,05	0,03	0,08	0,14	0,41	0,00	0,03	0,13	0,11	**1**
$V_{SES} = 66$	V_{ST}	5	5	5	6	6	6	6	7	7	7	8	8	**76**
	${}^H V_{ST}$	0,07	0,07	0,07	0,08	0,08	0,08	0,08	0,08	0,08	0,09	0,11	0,11	**1**
	V_{VCO}	2	3	5	6	7	7	7	8	8	8	10	12	**83**
	${}^H V_{VCO}$	0,02	0,04	0,06	0,07	0,09	0,08	0,08	0,10	0,10	0,10	0,12	0,14	**1**

	V_{VSSF}	10	13	13	17	18	18	18	18	18	18	19	23	**203**
	$^{n}V_{VSSF}$	0,05	0,06	0,07	0,08	0,09	0,09	0,09	0,09	0,09	0,09	0,09	0,11	**1**
	V_{ND}	1	1	1	2	2	3	6	7	8	11	11	11	**64**
	$^{n}V_{ND}$	0,02	0,02	0,02	0,03	0,03	0,05	0,09	0,11	0,13	0,17	0,16	0,17	**1**
	V_{AR}	6	6	6	6	6	6	6	6	7	7	7	7	**76**
	$^{n}V_{AR}$	0,08	0,08	0,08	0,08	0,08	0,08	0,08	0,08	0,09	0,09	0,09	0,09	**1**
	V_{All}	42	38	36	29	27	26	23	20	18	15	11	5	**290**
	$^{n}V_{All}$	0,14	0,13	0,12	0,10	0,09	0,09	0,08	0,07	0,06	0,05	0,04	0,02	**1**
K_{PC}		23	23	23	23	23	23	23	23	23	23	23	23	**276**
$^{n}K_{PC}$		0,09	0,08	0,08	0,08	0,08	0,09	0,09	0,08	0,08	0,08	0,08	0,09	**1**
K_{S}		1	1	1	1	1	1	1	1	1	1	1	1	**12**
$^{n}K_{S}$		0,08	0,08	0,08	0,09	0,08	0,09	0,08	0,09	0,08	0,08	0,09	0,08	**1**
K_{NE} $(Z = 16)$		2	2	2	2	2	2	2	2	2	2	2	2	**24**
$^{n}K_{NE}$		0,09	0,08	0,08	0,08	0,08	0,09	0,09	0,08	0,08	0,08	0,08	0,09	**1**
K_{CE} $(M = 27)$		32	32	32	32	32	32	32	32	32	32	32	32	**384**
$^{n}K_{CE}$		0,09	0,08	0,08	0,08	0,08	0,09	0,09	0,08	0,08	0,08	0,08	0,09	**1**
K_{CTI}		707	707	707	707	707	707	707	707	707	707	707	707	**8484**
$^{n}K_{CTI}$		0,09	0,08	0,08	0,08	0,08	0,09	0,09	0,08	0,08	0,08	0,08	0,09	**1**
K_{T+F}		7	7	7	7	7	7	7	7	7	7	7	7	**84**
$^{n}K_{T+F}$		0,09	0,08	0,08	0,08	0,08	0,09	0,09	0,08	0,08	0,08	0,08	0,09	**1**

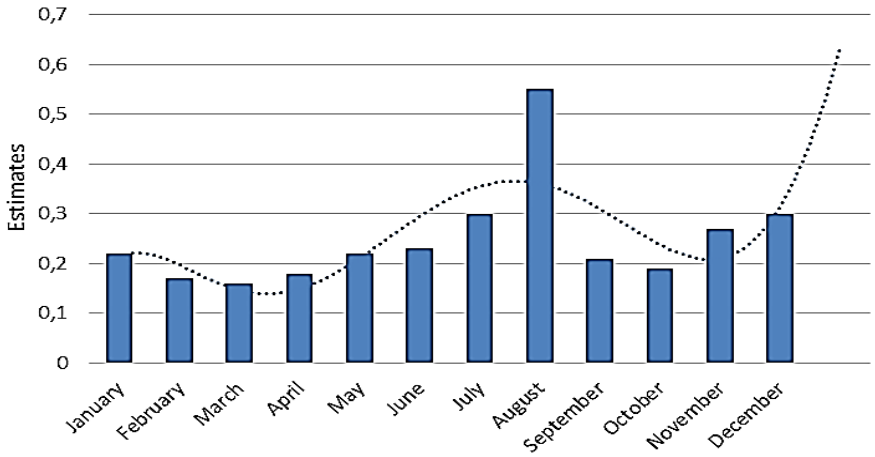

Fig. 9. Dynamics of changes in economic efficiency for SESE (example)

Due to the value of the reliability approximation (R^2) not being large enough, it proves there is insufficient data and points to the need to increase the period of the study. However, these calculations have shown, only for visual display, opportunities for further research. In addition, the results of the obtained distribution (Fig. 9) can be used as a basis for recommendations for improving strategic planning management using SESE.

During this study, the practicality of calculating the economic efficiency evaluation of SESE, based on actual performance considering the dynamics of change, was proved. A confirmation for hypothesis of H1 still remains.

7. Interpreting the results of the estimation method

To continue the analysis of the research data, the calculation of the importance of channels of information leakage to determine recommendations for the allocation of funds and the appropriate means to address the channels of information leakage or reduce losses from leaks of classified information has been presented.

Interpretation of organisational structure and management subjects of entities are presented in a graph model (Fig. 10), for the following notations have been introduced (Kavun, Sorbat and Kalashnikov, 2012) vertices of G: D – Director (if any Board of Directors, we have $\{D_w\}$, where w – number of directors (e.g., general, commercial, financial and others), ZD – Deputy Director (if any board of directors, we have $\{ZD_w\}$), C – Secretary (if any board of directors, we have $\{C_w\}$), S – lawyer (if there is a legal department, we have $\{S_q\}$, where q – number of employees in the department), M – manager (if there are several departments, we have $\{M_k\}$, where k – number of managers in departments), I – engineer (if there are several sections of an engineer, we have $\{I_z\}$,

where z – number of engineers in the department), T – Technologist (in several departments there may be several technologies, i.e. get $\{T_S\}$, where s – total number of technologists).

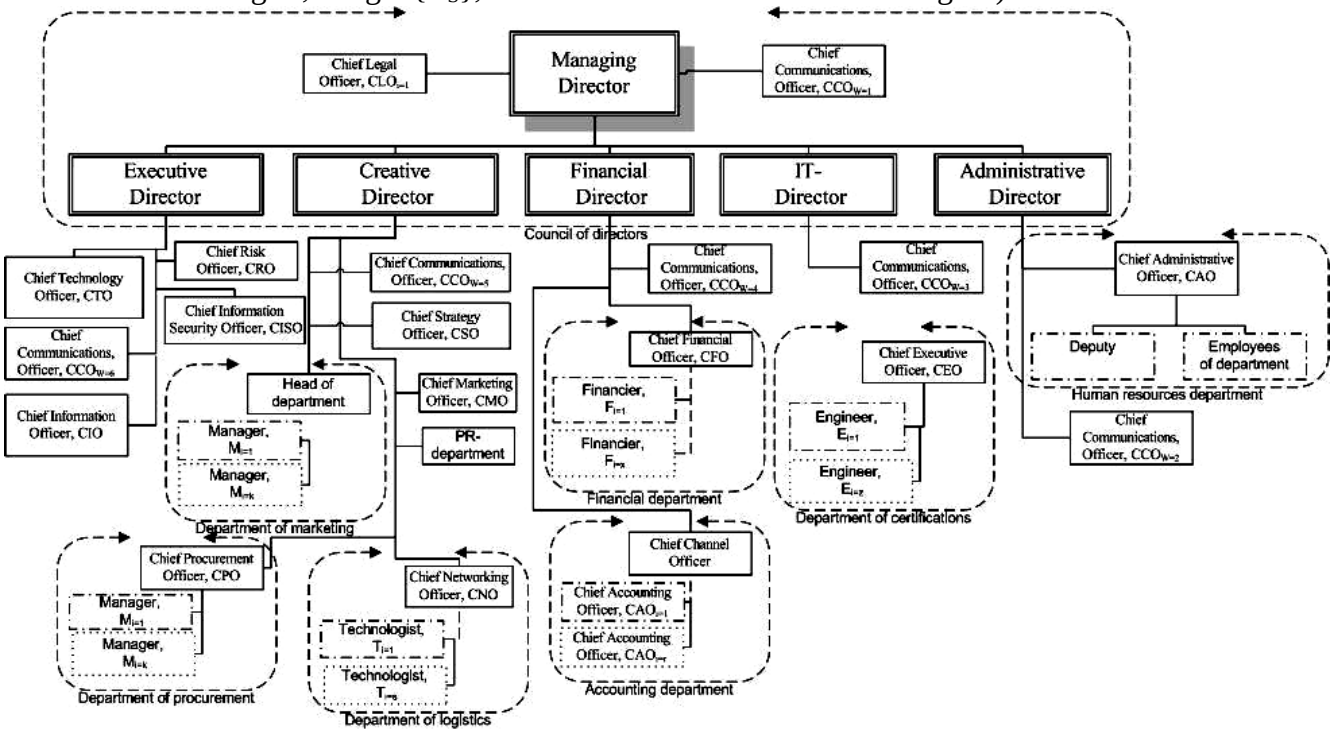

Fig. 10. Example graph model of organisational and administrative structure of subjects of enterprise

The proposed graph model is common and typical, so does not reflect the full structure of the real subjects of management.

Let us allocate, for example, two departments of enterprise conditionally in Fig. 10. Then after finding types (species) of classified information and documents, the necessary data for a certain period can be obtained (Table 5).

We can use similar data by way of the frequency of occurrence of a particular type (species) of classified information, and to calculate as the ratio of specific types of information (a file) for the total amount of information (in the form of files), i.e.

$$n_i = \frac{N_i}{\sum_{i=1}^{k} N_i}, \tag{17}$$

where n_i – a frequency of the i^{th} type of classified information (for example, personal data, court secret, state secrets, commercial secrets, etc.),

Table 5: Statistical data leaks of classified information in the enterprise (frequency)

Indicators / Department	$n_i = 1$ (for service using)	$n_i = 2$ (state secret)	$n_i = 3$ (commercial secret)	$n_i = 4$ (personal data)	$n_i = 5$ (court secret)
Financial	0,2	0	0,41	0,2	0,01
…	…	…	…	…	…
Certification	0,04	0	0,36	0,33	0

N_i – the total number of i-type (kinds) of classified information found in the form of files;

k – the total number of files in the system.

In addition, the enterprises (under the proposed methodic of the SESE) will be able to introduce or determine appropriate recommendations (after consultation with management) based on the following criteria:

1. If 0 <n_i <0,25, oral instructions are introduced for the use and work rules regarding i-type (species) of information with restricted access.

2. If 0,26 <n_i <0,45, amendments are then introduced in separate paragraphs for use and work rules regarding i-type (species) of information with restricted access.

3. If 0,46 <n_i <0,75, separate instructions are introduced on the use and rules of operation relative to the i^{th} type (species) of information with restricted access.

4. If 0,76 <n_i <0,99, a change in the charter of the organisation was introduced to the handling and rules of operation relative to the i^{th} type (species) of information with restricted access.

In addition, if the observed frequencies in different departments are big enough, you will be able to make some grouping or clustering, the results of which could be a recommendations to reduce the number of staff in a particular category. For example, one engineer can work with similar information in different departments, thus there is no need to have two engineers. It is also possible (Fig. 11) for the reverse transition from channels of information leakage to information channels, resulting from termination to the handling of information channels in malicious cases, i.e. CTI → CIL → CTI.

In addition, all of these transients occur at a time when a certain "critical" value is reached. For example:

t_i – the start time using CTI for their appointments during its activation;

$\{t_i; t_{i+1}\}$ – the time period of the normal functioning of channels of information for the specified purposes;

t_{i+1} – the time at which the probability of an incident (threats, vulnerabilities) in SESE becomes $p_i > 0$;

$\{t_{i+1}; t_{i+2}\}$ – the time period during which the incident seen (not visually) in full force and its flow begins to affect the functioning of the enterprise;

t_{i+2} – the time at which a turning point occurs in the process of (or commitment of) the incident, it is found, localised and a complex set of measures are formed to eliminate it;

$\{t_{i+2}; t_{i+3}\}$ – the time period during which the action of the incident weakens due to the use of counter measures. Enterprise functioning is restored to normal levels, management defines a set of measures and tools for future use, an analysis of damage;

t_{i+3} – the time during which the report of the damage is formed, the cash equivalent is counted, planned measures are put in place to prevent further possibilities of the incident;

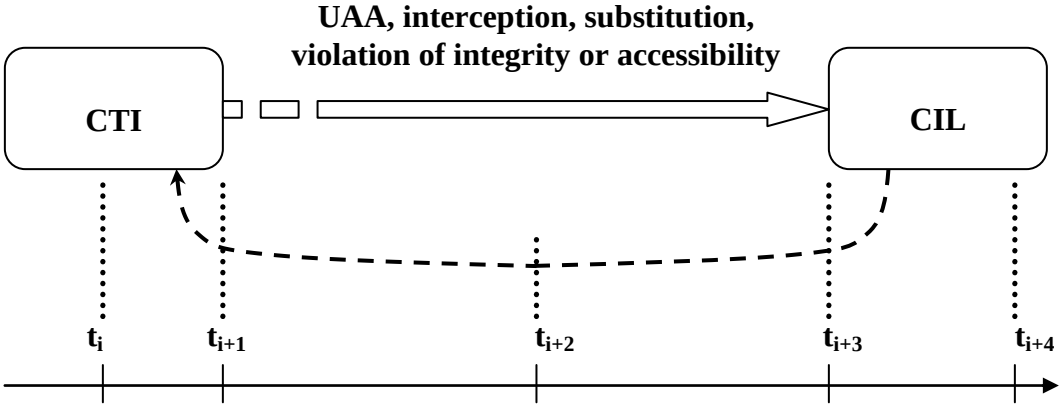

Fig. 11. Dynamics of transition processes CTI → CIL → CTI

$\{t_{i+3}; t_{i+4}\}$ – the time period during which the planned measures are implemented to prevent further cases. Sources of the incident are detected; if it is the subject (i.e. it is some person), then need to form some mechanism of refund of loss of return (with help of claim in court, for example); however, if it is the object, then are estimating a need of existence of this object;

t_{i+4} – the time at which the company returns to the mainstream of normal functioning, recovering lost connections and understandings. Perhaps the company may move to a new level of development.

Different periods of time and reports can have different durations (length). Moreover, it will have a direct dependence on emerging and accompanying circumstances (as they are known to be different), so talk about uniformity dynamic processes does not make sense (Kavun, 2008).

Based on input classifications of knowledge and ways of obtaining unauthorised access to classified information, a table (matrix) model can be built showing the dependences for any enterprise (Kavun, 2007).

Due to these actions, frequency (or normalised frequency) analysis can be obtained showing unauthorised access to facilities and sources of classified information with reference to the types of channels of information leakage over time. Thus, the dynamism of unauthorised access to and use of channels of information leakage in the company is obtained. The result of this should been used when developing and implementing policies of SESE (Kavun, 2007).

8. Simulation Evaluation of the Effectiveness of the System of Economic Security

A simulation model was developed based on the SESE method of economic efficiency by taking into account the volume of sub-systems conducted based on mathematical calculations performed by the expressions (1-16). The main goal of the proposed method is to obtain objective and proven advice on optimising the level of the economic efficiency of SESE.

Identification, by evaluating the economic efficiency of SESE based sub-systems, can been used in practice due to the constructed hierarchy of sub-systems and their volumes. As with a company in its current state of functioning, receiving input data for the calculation of the proposed method is not possible. This is due to the lack of generally accepted conceptions of SESE and the single methodological and methods of synthesis and subsequent implementation of SESE within the full path of the life cycle. This simulation has been conducted with the processing and synthesis based on the generated input of 650 polls (experiments). The number of negative impacts (attacks) is calculated with a maximum value (15 per month) and the average time between incidents in SESE was 170 days, which is a valid and sufficient factor in a typical organisational structure of an enterprise.

The main indicators of the company (see Table 6) are obtained from open sources. The calculated interim targets and the level of economic efficiency SEBSH are based on the proposed method by taking into account the volume of sub-systems.

The proposed method of estimation of economic efficiency is taking into account the enterprise subsystems requires for minimise the objective function (13) some data, which will need to obtain based on calculating the possible formation of recommendations for individual companies for increasing the economic efficiency of SESE. . For example, the calculation was performed on 650 experiments, which provided a generalised metric value in the initial data (Table 7).

Table 6: Main indicators of enterprise activity

Name of enterprise / **Indicators**	**Enterprise 1**	**Enterprise 2**	**Enterprise 3**	**Enterprise 4**	**Enterprise 5**	**Enterprise 6**	**Enterprise 7**	**Enterprise 8**	**Enterprise 9**	**Enterprise 10**	**Enterprise 11**	**Enterprise 12**	**Enterprise 13**
Cost of capital assets, thousands of equivalent units	3 520 560	549 318	87 368	70 900	312 888	698 362	1 327 454	279 076	245 982	265 395	2 465 758	579 115	307 757
Average number of counts, people	5748	120 2	140 6	254 9	227 1	308 1	3507	190 2	1602	153 8	1909	245 3	762
Fund payment labour all employees, thousands of equivalent units	1825 74,6	316 32	375 11, 9	956 27, 5	108 747	110 102 ,5	9941 8	559 24, 4	45839 ,3	440 20, 1	74464, 7	751 84, 1	184 90, 8
Profitability of products, %	12,9	-9,5	12, 8	1,4	12, 9	14, 9	5	1,4	4,3	3,5	49,4	2,5	0,8

Average hourly salary of employees, equivalent units	31,76	26,32	26,68	37,52	47,89	35,74	28,35	29,40	28,61	28,62	39,01	30,65	24,27
Current assets, million dollars	1476	215	61,4	73,5	1837	202		177	12 800		363	?	
Net profit, million dollars	199	25,6	0,85	4,24	190	12,3		3,8	2 140	1200	35,3	?	
The share of mining mouth in a country, %	19,1	5,2	2,4	4	12,1	7,3		13,9	12,7	12,1	10	1,2	
Number of CTI	1830931	116120	149573	413068	338020	580953		732673	1432250	250250	386805	57430	
Number of workstations	4885	1021	1195	2166	1930	2618		2980	4285	1622	2085	647	
Number of servers	195	40	47	86	77	104		119	171	64	83	25	
Number of network devices	317	66	77	140	125	170		193	278	105	135	42	
Number of communication devices	6897	1442	1687	3058	2725	3697		4208	6050	2290	2943	914	
Level of Efficiency of Economic Security, $LEES_h$	0,7615200 7	0,4910344 6	0,2841167 8	0,3281986 6	0,2939359 6	0,51851758		0,7668095 6	0,80921023	0,4411977 4	0,70431129	0,4022557	

Table 7: Comparing the data with enterprise

Name of enterprise	Enterprise 1		Enterprise 2		Enterprise 3	
	X	XX	X	XX	X	XX
Average number of counts, people	852	762	1176	1202	1334	1406
Number of CTI	94	57430	110	116120	122	149573
Number of workstations	724	647	999	1021	1133	1195
Number of servers	28	25	39	40	45	47
Number of network devices	47	42	64	66	73	77
Number of communication devices	1022	914	1411	1442	1600	1687
Level of Efficiency of Economic Security, $LEES_h$	0,7	0,4	0,7	0,49	0,7	0,28

X – data by own calculations, XX – data of enterprises.

Having observed Enterprise 1, the following is recommended: a slight increase in the number of staff (up to 90 people – resulting in more jobs, reducing unemployment). This would provide a significant increase in the level of the economic efficiency of SESE (30%) while significantly reducing the number of channels of information leakage (greater than 600 times). The number of of workstations (77) servers (3) pieces of network equipment (+5) and communication equipment (108) remains almost unchanged, which leads to the preservation of the existing technical infrastructure of the enterprise. This makes a significant economic efficiency in the synthesis and implementation of SESE.

Having observed Enterprise 2, the following is recommended: a slight decrease in the number of staff (to 26 people, planned downsizing), provides a significant increase in the level of the economic efficiency of SESE (30%) while significantly reducing the number of channels of information leakage (greater than 1000 times). However, the number of workstations (-22), servers (-1) units of network equipment (-2) and communication equipment (-31) remains unchanged, which leads to savings in the current technical infrastructure. This makes a significant economic efficiency in the synthesis and implementation of SESE through cost savings while reducing the existing technical infrastructure.

Having observed Enterprise 3, the following is recommended: a slight decrease in the number of staff (to 72 people, planned downsizing or restructuring of the company), provides a significant increase in the level of the economic efficiency of SESE (30%) while significantly reducing the number of channels of information leakage (greater than 1200 times). The number of workstations (-62), servers (-2), pieces of network equipment (-4) and communications equipment (-87), remains almost unchanged which leads to the preservation of the existing technical infrastructure. This makes a

significant economic efficiency in the synthesis and implementation of SESE through cost savings while reducing the existing technical infrastructure.

Thus, can be getting some recommendations at the increasing of the staff of employees, and also at the decreasing of this staff of employees. In addition, will be able to make the potential calculation of these recommendations for improving economic efficiency of SESE for any enterprises. Thus, the hypothesis H3 is confirmed.

Based on the data calculations for the enterprise, the dependence of the level of economic efficiency of SESE (Fig. 12) was investigated using an average headcount number.

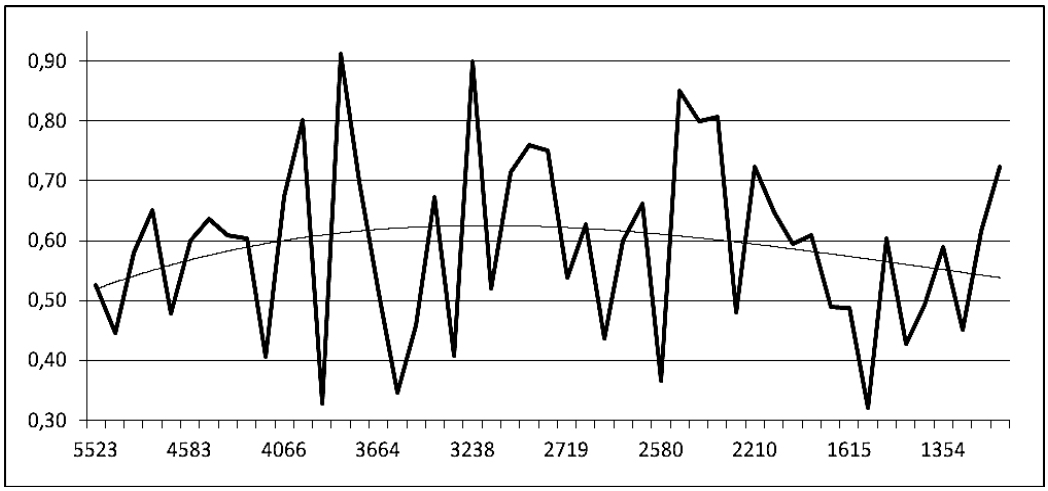

Fig. 12. Dependence of the level of efficiency of economic security from the average number of headcounts (this dependence hasn't any mathematical depends)

For the received image data, a trend model was calculated based on polynomial dependence of the 3rd stage (actually depending on the 1st degree, i.e. linear) determining the value of reliability approximation (R^2):

$$\mathbf{y = 3E\text{-}06x^3 - 0{,}0004x^2 + 0{,}0122x + 0{,}5074;\ R^2 = 0{,}0423.}$$

The resulting value of reliability approximation does not allow to a sufficient degree, the attainment of reliable and adaptive significance using forecasting techniques. It was proved that no dependence on the level of the economic efficiency of SESE for the average headcount number.

The dependence (Fig. 13) of the level of economic efficiency of SESE was also studied with a number of negative impacts (attacks on the existing infrastructure of the enterprise).

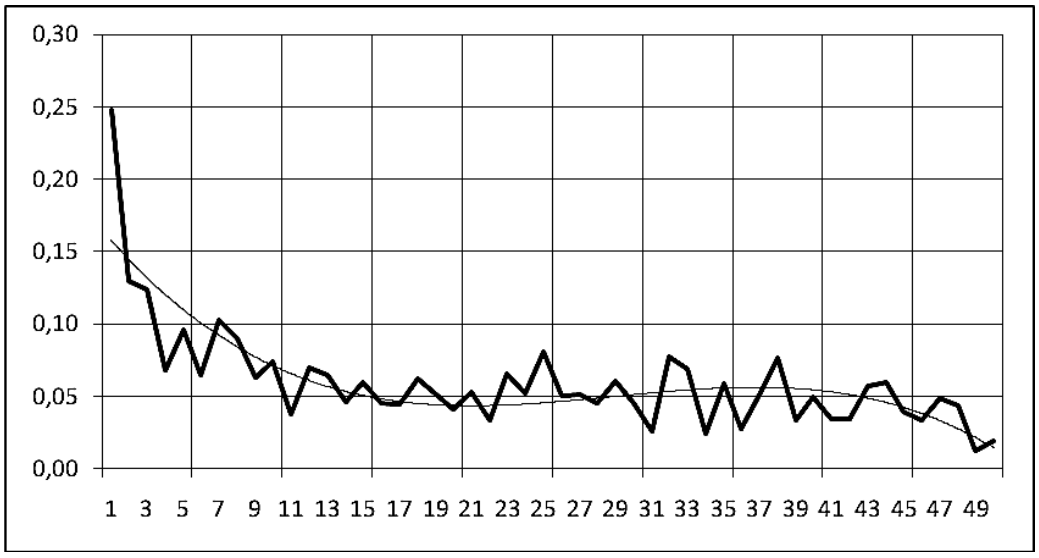

Fig. 13. Dependence of the level of efficiency of economic security from a number of negative impacts

For the received image data, a trend model was calculated based on polynomial dependence of the 3rd stage (actually depending on the 1st degree, i.e. quadratic) determining the value of the reliability approximation (R^2):

$$y = -7E\text{-}06x^3 + 0{,}0006x^2 - 0{,}0151x + 0{,}1726;\ R^2 = 0{,}6535.$$

The resulting value of the reliability approximations allows, to a sufficient degree, the attainment of reliable and adaptive significance using forecasting techniques. It was proved that the dependence of the economic efficiency of SESE and the number of negative impacts (for example, it can be the attacks on the existing infrastructure of the enterprise).

The mean time between incidents in SESE (in a twenty-four hour period) in the number of negative impacts (attacks on existing infrastructure company, Fig. 14) and the average recovery time for z^{th} node of SESE for the number of negative impacts (attacks on the existing infrastructure of the enterprise, Fig. 15) was also investigated.

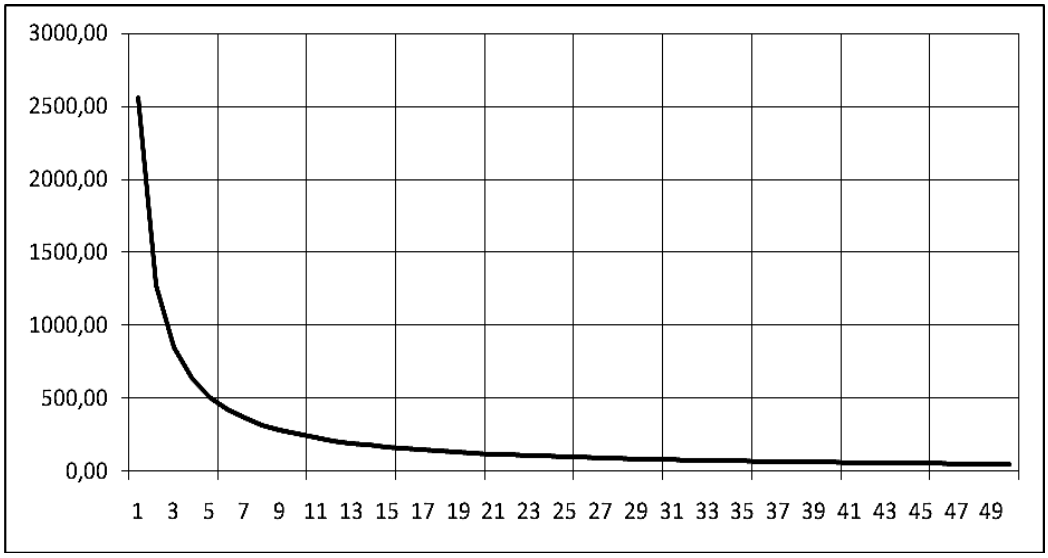

Fig. 14. Dependence of average time between incidents in areas of information (corporate) security from negative impacts

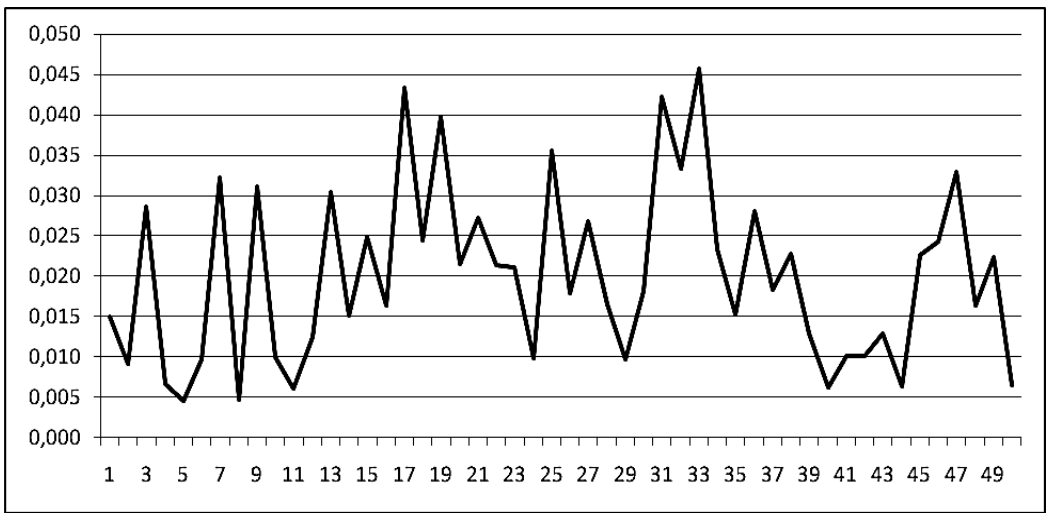

Fig. 15. Dependence of average recovered time z^{th} node of SESE from number of negative impacts

For the received image data, a trend model was calculated based on the polynomial dependence of the 3rd stage of determining the value of reliability approximation (R^2):

$$y = -0{,}0684x^3 + 6{,}2844x^2 - 177{,}35x + 1580{,}7;\ R^2 = 0{,}7336.$$

The resulting value of reliability approximations which allows, to a sufficient degree, attainment of reliable and adaptive significance using forecasting techniques. It was proved that the dependence of the average time between incidents in SESE and the number of negative impacts (attacks on existing company infrastructure), could result in failure of the entire enterprise (and perhaps bankruptcy), if such negative impacts of time between incidents in SESE were reduced to a value at which the restoration of the existing infrastructure is fundamentally impossible.

For the received image data a trend model was calculated based on polynomial dependence of the 3rd stage (actually depending on the 1st degree, i.e. linear) determining the value of reliability approximation (R^2):

$$\mathbf{y = 3E\text{-}07x^3 - 4E\text{-}05x^2 + 0{,}0015x + 0{,}0082;\ R^2 = 0{,}1241.}$$

Thus, with the help of Fig. 12 and Fig. 15 we confirmed the hypothesis H2 about negative dependence was confirmed and with the help of Fig. 13 and Fig. 14, the hypothesis H2 about positive dependences was also confirmed.

9. Conclusion

The resulting value of reliability approximation does not allow to a sufficient degree to obtain reliable and adaptive significance using forecasting techniques. It was proved that the average recovery time of the i^{th} node of SESE (in normalised values), had no dependence of the number of negative impacts. This means normal functioning of the existing infrastructure and rapid response (recovery) occurs if the impact has focused on individual nodes.

References

[1] Dovbnya, S., Gichova. N., 2008. "Diagnostic of the level of economic security of enterprise", *Finance of Ukraine, 4,* pp. 88-97.

[2] Geetc, V., Kizim, N., Klebanova, T., Chernyak, A., 2006. "Modelling of economic security: government, region, enterprise", Kharkiv, Pub. House "Ingek".

[3] Kallol, B., Godwin, U., 2003. "An analysis of the growth of computer and Internet security breaches", *Communications of the Association for Information Systems, 12,* pp. 684-700. www.slis.indiana.edu/faculty/hrosenba/www/l574/pdf/bagchi_security.pdf.

[4] Kavun, S., 2007. "Information security in business: monograph", Kharkiv, Pub. Kharkiv national university of economics.

[5] Kavun, S., 2007. "The matrix model of the system economic security", *Business Inform, 10(2),* pp. 45-49. www.msu.kharkov.ua/ru/downloads/ekonomika-07-2.pdf.

[6] Kavun, S., 2008. "Methods of estimation of effectiveness of the system economic security business activity", *Visnik L'vivs'koho Universitetu. Seria: Economical,* 40, pp. 287-290. http://www.lnu.edu.ua/faculty/ekonom/Visnyk_Econom/2008_40/59_S_Kavun.pdf.

[7] Kavun, S., 2008. "The life cycle of the system enterprise economic security", *Development management,* 6, pp. 17-21.

[8] Kavun, S., 2009. "Analysis of economic security of enterprises (Kharkiv and Kharkiv Region)", *Economy of Development,* 1(49), pp. 72-75.

[9] Kavun, S., 2009. "Classification of information and documents forms", *Scientific Bulletin of the Poltava University of Economics and Trade. Economic sciences,* 5(36), pp. 69-75.

[10] Kavun, S., Sorbat, I., Kalashnikov, V., 2012. "Enterprise Insider Detection as an Integer Programming Problem", Watada, J., Phillips-Wren, G., Jain, L.C., and Howlett, R.J. (Eds.). *Advances in Intelligent Decision Technologies, SpringerVerlag Series "Smart Innovation, Systems and Technologies,* 12, pp. 820-829.

[11] Kavun, S., 2009. "Mechanism for estimating the economic efficiency of the system of economic security", *Business Inform,* 8, pp. 58-64. www.nbuv.gov.ua/portal/Soc_Gum/Bi/2009_8/58-64.pdf.

[12] Kavun, S., 2009. “System of Economic Security: methodological and conceptual positions”, Kharkiv, Pub. Kharkiv national university of economics.
[13] Kavun, S., 2011. “Structuring the normative and legal providing in the system of economic security of enterprise”, *Foreign Trade. Economic Security*, 7, pp. 22-28.
[14] Kavun, S., 2012. “Estimating Enterprise’s Financial Losses Caused by Information System Incidents”, Tecnológico de Monterrey, Centro Estudiantil del Campus Monterrey, Monterrey, Mexico. http://www.mty.itesm.mx/dtie/doctorados/gt6005-11/Slides/SID-Kavun-Apr2012.zip.
[15] Kavun, S., Mikhalchyk, I., 2010. “Analysis of macro-level indicators of economic security (for example Western countries)”, Information and control systems for rail transport, *Ukrainian State Academy of Railway Transport*, 29, pp. 61-65.
[16] Kavun, S., Sorbat, I., 2012. “Aspects of the economic security of enterprise”, International Scientific Conference “Securitatea informaţională 2012”. http://security.ase.md/materials/publications/pdf/Conferinta_SI2012.pdf.
[17] Kavun, S., Zyma, O., 2009. “Scientific and technical collection is the "Communal economy of cities”, 89, pp. 440-449. www.eprints.kname.edu.ua/15050/1/440-449_Кавун_СВ.pdf.
[18] Khristianovski, V., Kavun, S., Zyma, O., 2011. “Assessments of the Level of Economic Security of Enterprises of By-Product-Coking and Petrochemical Industries and its Practical Use: Libermanivskie reading – 2011: economic heritage and modern problems”, V. Ponomarenko, M. Kizim (Eds.), (pp. 67-82), Kharkiv, Pub. “Ingek”
[19] Kozachenko, A., Lyashenko, O., Lyashenko, A., 2003. “Economic security of enterprise: essence and mechanism for ensuring”, Kiev, Libra.
[20] Ortynskii, V., Kernitckii, I., Givko, Z., 2009. “Economic security of the enterprises, organizations and institutions”, L’viv: All-Ukrainian Association of Publishers' “Legal unity“.
[21] Patent. Ukraine 34852, IPC (2006) G09C 1 / 00. Method Encryption of information / Stasyev J., Kuznetsov A., Grabchak V., Evseev S., Kavun S., Kuzhel I., Korolev R. Owner Kharkov University Air Force. - № u2008 03 481, declared. 03.18.2008, publ. 08.26.2008, Bul. № 16.
[22] Patent. Ukraine 39 676, IPC (2009) G09C 1 / 00. Method Encryption of information / Kuznetsov O., Evseev S., Sergienko R., Kavun S., Korol O., owner Evseyev S. - № u2008 10 865, declared. 09.03.2008, publ. 10.03.2009, Bul. № 5.
[23] Ponomarenko, V., Kavun, S., 2008. “Conceptual Foundations of Economic Security”, Kharkiv, Pub. Kharkiv national university of economics.
[24] Stevenson, G. Smith, 2004. “Recognizing and Preparing Loss Estimates from Cyber-Attacks”, *Information Systems Security*, 12(6), pp. 46-57. www.tandfonline.com/doi/pdf/10.1201/1086/44022.12.6.20040101/79786.8.
[25] Lindsey, Michael B., 2010. “A Method for Estimating the Financial Impact of Cyber Information Security Breaches Utilizing the Common Vulnerability Scoring System and Annual Loss Expectancy”, *Spring Semester*, https://kuscholarworks.ku.edu/dspace/bitstream/1808/6649/1/Lindsey/Michael B. EMGT Field Project.pdf.
[26] Wang, Ta-Wei, 2008. “Essays on information security from an economic perspective: information security disclosures, investors’ perceptions on security incidents, and two-factor authentication systems”, *Krannert Graduate School of Management*. https://www.krannert.purdue.edu/academics/mis/workshop/2008/davidProposal.pdf.