Cybersecurity challanges for critical infrastructure protection

Sergii Kavun
Department of computer systems and technologies, Kharkiv National University of Economics, Kharkiv, Ukraine

Robert Brumnik
Metra engineering Ltd. Ljubljana, Slovenia &GEA College, Ljubljana, Slovenia

Abstract

In today's worldin the processthe variousenterprisesthere are caseswhen some-employees(lateronobtained an*insider*name) under the influence of variousfactors (externaland internal) are beginning to producedifferent informationto recipientsoutsidethe confidential nature(e.g., commercial, personal, corporate, etc.).To date,the existing approachesfor identifyinginsider activity (or insiders), such as psychological,technical, physical(searching) are not effectivebecausethey applyuponfulfillmentof the incident(leakage, distortion, substitution, etc.), besides these measures (actions, events)do not allowto predictor to preventthese similar incidents(leakages of information) in the early stagesofinsider activities.Therefore, the problem of insider detection for the modern enterprises and their activity and financial position may be considered of one the most important task that are required to be undertaken. Because, for the author’s opinion (on base of Geyets (2006) interpretation of the Pareto principle), a leakage of 20% of commercial secrets of enterprise in 80% of cases leads to collapse of this enterprise. The many enterprises learned how to be on the defensive from external threats (cyber-attacks, intrusions, viruses etc.) but before internal threats (the insiders); many enterprises maybe considered defenseless!

1. Methods of the detection insiders as a part of system of corporate security based on cartography analysis

Definition 1: An Insider is a fellow, whose work varies in time under the influence of external, internal, and individual causes (Kavun, Sorbat and Kalashnikov, 2009). This work reflects a readiness of this fellow for actions. In addition, the socio-cultural environment of this fellow can be regarded as a violation of existing standards (disclosure of information with restricted access) and traditions (not doing the job, it is the second distinction).

Definition 2: Insider Information is substantial undisclosed Public Service Information (PSI) for the enterprise (Kurkin, 2004; Kavun and Sorbat, 2009). This information if disclosed could lead to the loss of competitiveness of the company or into its collapse (it’s the first distinction from other definitions). Employees who have this information are typically the system's administrators or the owners. Employees who received this information have called insiders. All these processes refer to the sphere of economic and information security (Kavun, 2012).

In the course of its commercial activities, various organizations are subject to economic crime, negligence of employees, which leads them to financial, physical, temporal, economic and other kinds of losses. Such activities of the staff are called insider ones. The problem of insider's detection was been considered in the report of Computer Security Institute in 2007 (Kavun, 2008). From year 2011 (INFECO, 2012), this problem has stated as being in first place in world among all set of threats and vulnerabilities. Thus, the problem of insider's detection and defense preceded the problem of virus's defense. Especially susceptible to insider attacks are the enterprises of bank and those associated with the financial sector. Insider attacks have a very high level of latency (concealment) and the lowest level of detection. Nevertheless, these methods have provided as only preventing the consequences of insider attacks, and are not providing for the detection of insiders within the enterprise.These concepts are part of the categorical system fields of information and corporate security.The well-known experts and scholars in this area are Ponomarenko, Klebanova and Chernov (2004);Oleynikov (1997); Kurkin (2004);Messmer (2008); Campbell, Gordon, Loeb and Zhou,(2003); Yazar (2002), and Shkarlet (2007). Their works have demonstrated a systematic approach to address threats to information and economic security, but most of these studies relate to external threats. Since the unauthorized information access within an enterprise by insider activity brings financial losses, there is a need to address the urgent task of preventing or identifying an insider or a group of insiders (the insider trading activity).Also in their works have been investigated questions of a systematic approach to eliminate the threats information and economic security, but most of these researches are based on the technical and technological aspects, which eliminates the possibility of identifying at early stages of insiders and prevent the loss of assets. No completely unresolved question of internal threats, which is also a consequence of the issue of detection (detection) insiders.

Purpose of work is show the possibility of formalizing task of identifying insiders (insider activity) in the company based on the authors developed a new modified criteria method and cartographic analysis. This type of analysis allows will visually estimate the current state of the activity of the employee, will determine the allowable ranges exceeding boundary values, will look the trends of activity for a given period, and will take appropriate counter-measures to prevent any loss(Kavun and Sorbat, 2012).

2. Research problem definitions and issues

The relevance of research confirms the results (Fig. 1) analyzing the weight fraction of terms (keywords), field of study, obtained on the basis the author's method of Internet analysis Kavun, Mykhalchuk, Kalashnykova and Zyma,2012). Studies were been performed for a period of 10 years in search systems Google, Bing, and others on the terms: “insider”, “insider activity”, “insider information”. Also on the graph shows the trend line for forecasting proportion by weight of further using terms, which in turn will confirm the relevance of this area of research for the subsequent period.

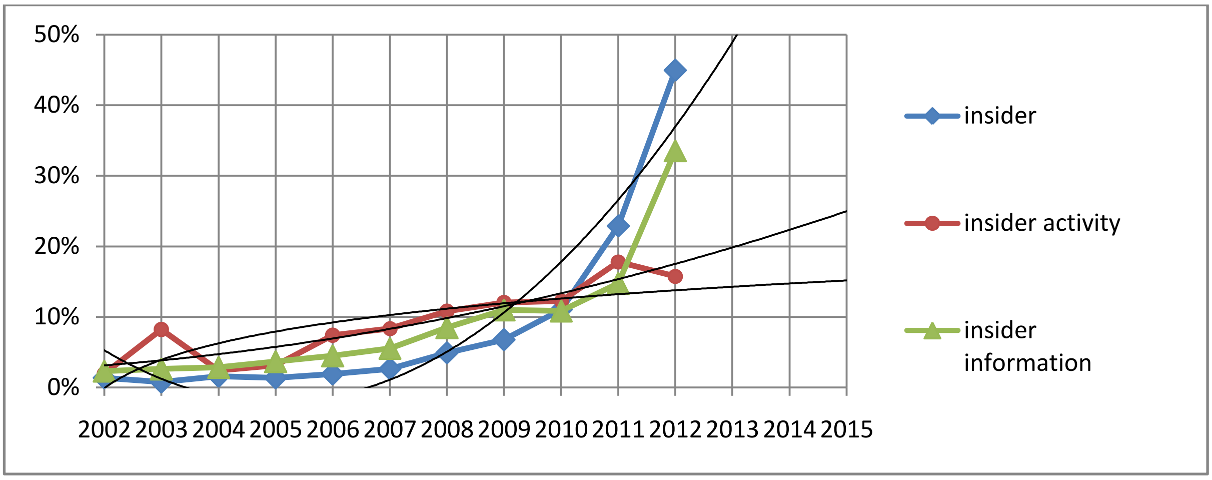


Fig. 1.Dynamics of changes in the weight fraction the use of the terms in research (Kavun, Mykhalchuk, Kalashnykova and Zyma,2012)

The analysis of the open sources of Murdoch (2011); Johnson (2008); Kavun (2012) and Geyets (2006) confirmed the lack of a common interpretation of the mathematical task of identifying the insiders (or their activity) in the study of different authors. Thus, the task of identifying the insiders (or their activity) can has reduced to a class of problems is not interpretable, the classification of which has shown in Fig. 2, based on original author research.

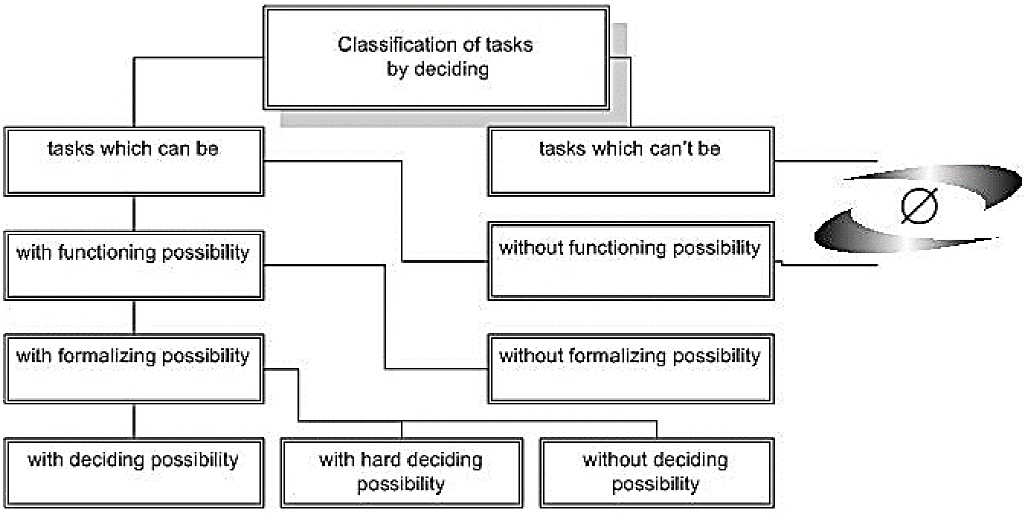

Classification of tasks by deciding
tasks which can be
tasks which can't be
with functioning possibility
without functioning possibility
with formalizing possibility
without formalizing possibility
with deciding possibility
with hard deciding possibility
without deciding possibility
∅

Fig. 2. Classification of the tasks by deciding

Thus, the authors can develop the criteria method (criteria method, CRIM) for identifying insiders or their activity. The CRIM based on using some set of indicators (or their reasons) – set$\{p_i\}i = 1 \div 42$(Kavun and Sorbat, 2009).

The insider activity is often (it is one from aims) leads to creatingof financial losses(Kavun, Sorbat and Kalashnikov, 2009), then to need to solving a task of prevention (or/and forecasting)or identifying insiders or insiders group (insider activity) on the earlier stage.Authors are proposing three methods of identifying insiders (Kavun and Sorbat, 2012):

1) Matrix method (MM).
2) Base criteria method (CRIM).
3) Modifycriteria method (MCRIM).

3. MCRIM method modeling

Matrix method, its essence, advantages and disadvantages was been described in following publications (Kavun, Sorbat and Kalashnikov, 2012; Kavun and Sorbat, 2009; Kavun and Sorbat, 2012). CRIM disadvantage is that at the analysis of the input data using the same number of considered criteria's for different job categories, at the same an advantage it is probable error of determining the values of the attribute, which does not allow us to allocate the risk zone *Z*(Kavun and Sorbat, 2009).Therefore, the modification has carried out based on the CRIM multistage filtration (Fig. 3), the result is the MCRIM.

At the first stage of filtration has needed some coefficients of animportance of the criterion– kvp_i (in this example for 10 criterions, Table 1). For this case has needed to build one-dimension matrix of these importance of the criterion$KVP = \{kvp_i\} = \overline{1,100}$. At the same, all volume of the indicators has detected with help of expert method (employer can hire some expert or he was the employee of the enterprise) however:

$$\sum_{i=1}^{n} kvp_i = 100, \tag{1}$$

where i – number of criteria estimates (reasons).

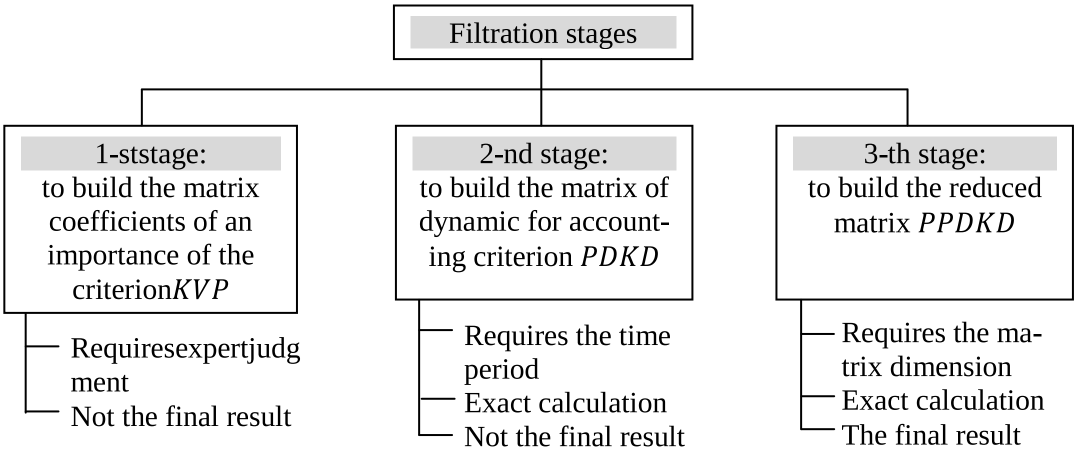

Filtration stages
1-ststage:
to build the matrix coefficients of an importance of the criterionKVP
Requiresexpertjudgment
Not the final result
2-nd stage:
to build the matrix of dynamic for accounting criterion $PDKD$
Requires the time period
Exact calculation
Not the final result
3-th stage:
to build the reduced matrix $PPDKD$
Requires the matrix dimension
Exact calculation
The final result

Fig. 3. Filtration stages for MCRIM-method

In the second stage introduces a dynamic accounting of criteria's. Introduce the matrix *PDKD* dynamic accounting criteria's, which will be different of increasing of the number of columns that eventually allows counting the days, months, years.

Rows of the matrix *PDKD* are job categories of employees, and columns are days, months, and years (any period). In latter cells has determined by the sum of all the criteria (features) identified in a single day of the month (Table 2). Itisalsoproposedparameter$d_r$fordynamicsaccounting.

Table 1. The coefficient matrix of the importance of the criterion (feature), KVP

№	the criterion (feature)	kvp_i	№	the criterion (feature)	kvp_i
1	$p1$	8	6	$p6$	14
2	$p2$	12	7	$p7$	11
3	$p3$	6	8	$p8$	8
4	$p4$	5	9	$p9$	16
5	$p5$	13	10	$p10$	7
				∑=(over all values)	100

Coefficient of importance of the criterion takes into account and gives the normal selection risk zone *Z*.For the matrix *PDKD* (Table 2) can be identified to track employees, according to the results of the first stage filtering, i.e. employees belonging to a risk zone (*Z* = 55% it's the threshold identified by the authors with help of expert approach), which is an additional rule for MCRIM-method.

Table 2. Matrix of dynamic accounting of criteria's, $PDKD$

№	Month (day), d_r	January				February				…				December				$\sum_{U_j}$
	Job categories, dk_j	1	2	…	31	1	2	…	28					1	2	…	31	
1	dk_1	2	1	…	4	1	3	…	0					0	5	…	1	17
2	dk_2	0	1	…	0	0	0	…	2					1	2	…	0	5
…	…….	….	..	…	..	..	..	…	..					..	..	…	..	..
n	dk_n	0	0	…	0	0	0	…	0					1	1	…	0	2

$$\mathrm{PDKD} = \{\mathrm{pdkd}_{\mathrm{ij}}^{\mathrm{d}}\}, \text{ where}$$

$$\mathrm{pdkd}_{\mathrm{ij}}^{\mathrm{d}} = \begin{cases} \sum_{\mathrm{i}=1}^{\mathrm{n}} \mathrm{pdk}_{\mathrm{ij}} \\ 0, \text{in opportunity case,} \end{cases} \qquad (2)$$

wherei $= \overline{1, \mathrm{n}}$ – numbers of criteria's (features); $\mathrm{j} = \overline{1, \mathrm{m}}$ – numbers of job categories; d_1 – some kind of accounting, d_2– time (or period) of accounting, at the same$\mathrm{d}_2 \subseteq \mathrm{d}_1$.

Parameter of dynamics $\mathrm{d}_1$has determined some kind of accounting (by weeks, by months, by quarter etc.) with possibility of detailing d_2 (every days, every weeks, every month'setc.), then $\mathrm{d}_\mathrm{r} = \{1, 7, 14, 31, 52, 93, 186, 356\}$.
At the same an account of the parameter of dynamics will be have the following type;

$$d_r = \begin{cases} d = \overline{1,365}\,, \text{if have an account every years,} \\ d = \overline{1,31}\,,\ \text{if have an account every month's,} \\ d = \overline{1,124}\,,\ \text{if have an account every days, during quarter.} \end{cases} \qquad (3)$$

It should also be noted that the job categories DK is recognizing on the basis of simultaneity, then based on formula (3) can build (or create) the matrix distribution of the parameter dynamics d_r. Choice of the decision maker (DM) from the table of the parameter$d_r$it is a very important decision that will allow to use a parameter in a decision support system (DSS).For example, as DSS can be following systems: Emperor, ConceptDraw MINDMAP to identify insiders in the company. If parameter d_r = (1÷365), then DM will get the most accurate solutions that will allow at this time to identify insiders in the enterprise.However, it also will lead to increase of used resources. Therefore,needtochoosea“middlegoldground”.

In the third stage of filtration (method MCRIM) taking into account dynamics, can obtain estimates that are more accurate. Therefore, the authors suggest using a cartographic analysis, for which as the result of modeling has received some surface diagrams, called the distribution maps of the employees (DME).

4. Cartographic analysis of MCRIM results

Authors have identified the following types of DME:

1) Surfacemap(Fig. 4), M_{SM};

2) Three-dimensional map, based on dataM_{SM} (Fig. 5-6), M_{3DSM}.

3) Individually map (Fig. 7) for each selected employee,M_{ID}.

In addition, in Fig. 4-7 also shows the dynamics of some changes types of DME. Using cartographic analysis (see Fig. 4) and based on the results of modeling method MCRIM, can conclude (and for the company's management can get some recommendation), which in June (for example, on the map highlighted in light color, probably during the holiday season) all employees increase their negative activity (to the company).

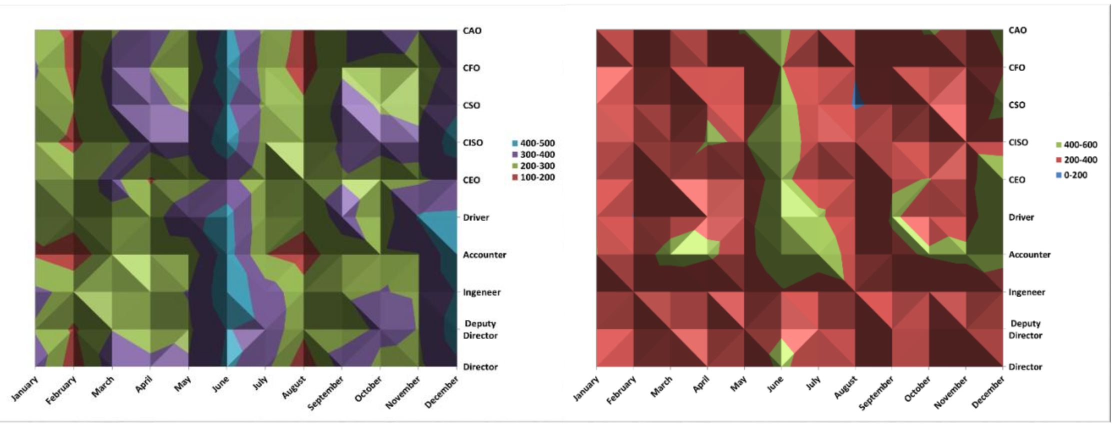


Fig. 4. Dynamic of changes the surface map, M_{SM}

Therefore, it is necessary to strengthen control over the staff and / or apply some set (complex) of countermeasures. If will making a comparative analysis with the same period by other year (simulation was conducted at intervals of a year), can select a subset of employees (there are three: CEO, Driver, and CFO), which exhibit similar activity repeatedly. Thus, can select some dynamics based on the activity of a particular category of staff.Also based on the results by low-level obtained indicators of method MCRIM – can encourage employees to avoid the symptoms of further negative activity (insider activity), which is leading to threats of leaks in the enterprise.Based on three-dimensional maps (as shown in the example of Fig. 5) we can assess the results in two ways.

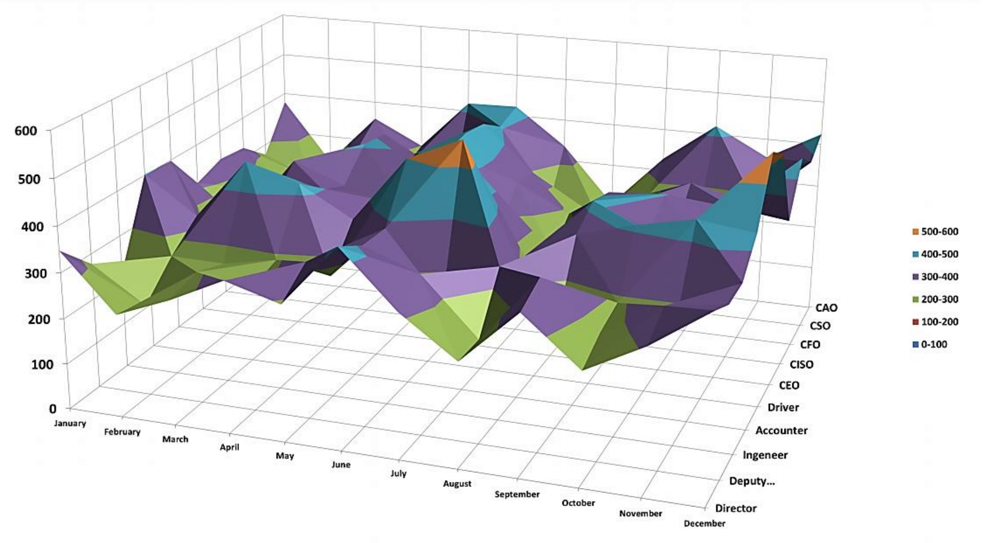
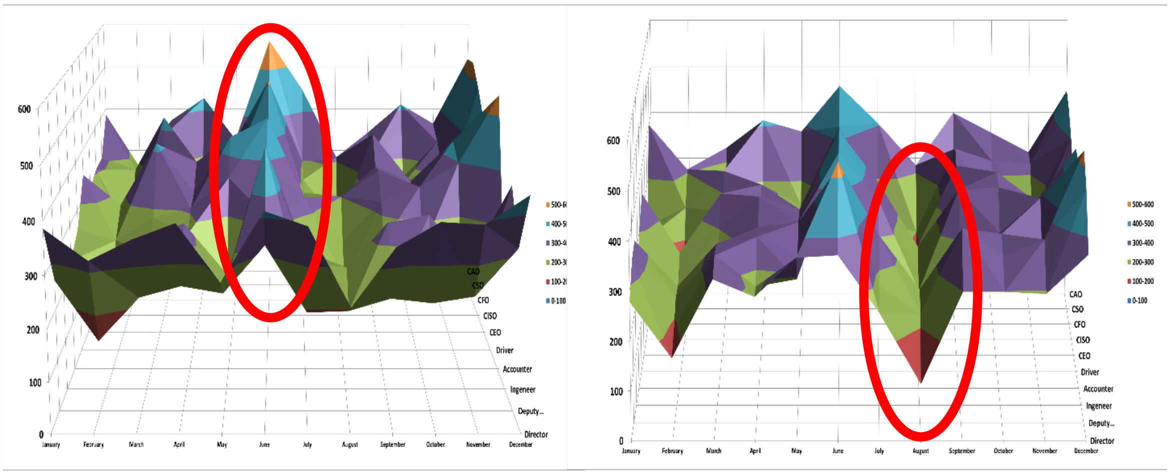


Fig. 5. Common view of three-dimensionalmap M_{3DSM}

First way is when are expanding the map by direction “mount” can get “a monthly profile” (when visible intensity during the selected month) for selected employees.In this period, can see the growth of risk for the company or the increased of insider activity in the example for June (Fig. 6a – the selected area).



6. a

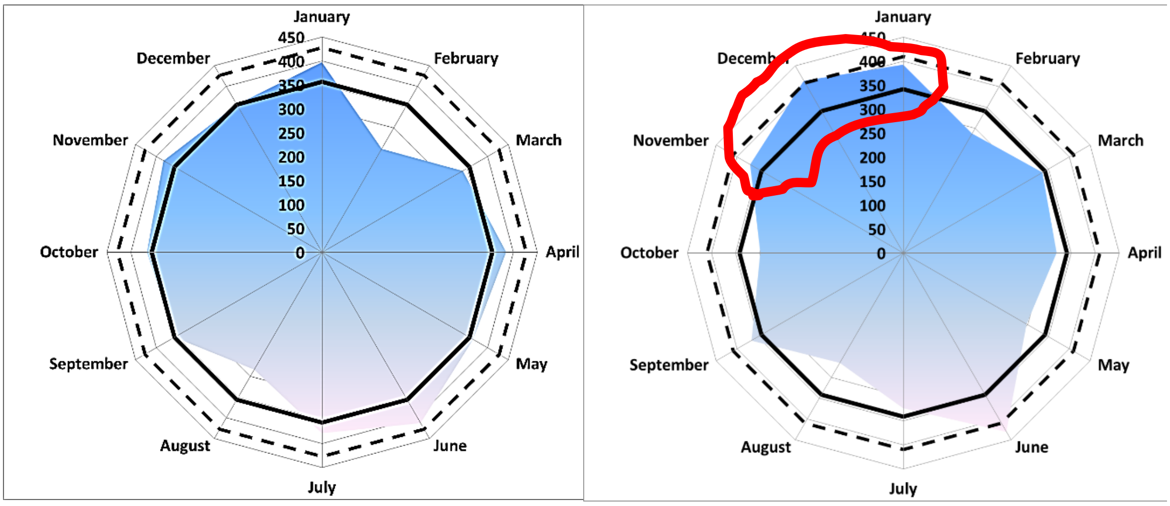
6. b

Fig. 6a, b. Dynamic variants changes of accounting based on three-dimensionalmap M_{3DSM}

The second way in the "job profile" is measured intensity for each job position during the period studied. In this direction, we can determine the employee (Driver on the example of Fig. 6b), whose activity increases the risk of losses of the business. There can be a consequence of the increased activity of employee insider activity.

ID maps of the dynamics estimates based on entered criteria's (author's proposed 42 criteria's) for a set of job categories are using for individual analysis of the negative activity of the employee (Fig. 7).We also analyzed the results of modeling can be some estimation in the specified period for the selected employee, if himself changes are within the acceptable range (Fig. 7a). If because of himself activities the employee allowed an increasing in activity (insider activity from November to January), then can see the time periods when it was doing (selected areas in Fig. 7b).

The dotted line denotes the recommended corridor feasible estimates of the average value, which has based on previous accounting periods.



a) b)

Fig. 7a, b. Individual map "ID maps"

Based on the received graphical representations can predict the list of countermeasures used to this official (employee) in a given period of time.Thus, for some security specialists this analysis presented will provide a description of recommendations with possible conclusions for building or creating some comprehensive and proactive measures to identify insider activities in the enterprise.

References

1. Messmer, E. (2008). "Software watchdog working on enterprise security metrics; Center for Internet Security to release security benchmark by year-end," Network World.
2. Campbell, K., Gordon,L. A., Loeb,M. P., Zhou,L. (2003). "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market," Journal of Computer Security, vol. 11, issue 3, pp. 431-448.
3. Murdoch, C. (2001). "Economic factors as objects of security: Economics security & vulnerability". In: Knorr, K. Trager, F,Economics interests & national security, Lawrence, p. 867.

4. Gordon, L. A. (2006). “Economic aspects of information security: An emerging field of research”. In:Gordon, L. A, Loeb P. M., Information Systems Frontiers, Volume 8, Issue 5, pp. 335–337.
5. INFECO (2012). http://infeco.net/infeco-overview/article/158-statistical2.html
6. Johnson,M. E. (2008). “Managing Information Risk and the Economics of Security”, 1st edition, Interperiodical distributed exclusively by Springer Science + Business Media LLC, p. 347.
7. Oleynikov,E. (1997). “Principles of Economic Security (State, region, company, person)”.In: Oleynikov,E., Moscow: JSC "Business School" Intelligence-Synthesis, p. 288.
8. Ponomarenko,V., Klebanova,T., Chernov,N. (2004). “Economic security in the region: analysis, evaluation, and prediction: monograph”, Kharkiv: INZHEK, p. 143.
9. Kurkin,N. (2004). “Managing the economic security of the enterprise: monograph”. Dnepropetrovsk: Art-Press, p. 452.
10. Kavun,S. V. (2012). “Statistical analysis in area of economic and information security,” ES INFECO: International research portal of information and economic security.
11. Geyets,V. (2006). “The modeling of economic security: power, region, enterprise: monograph”. In:Kizim,M., Klebanova,T., Chernyak,O., Kharkiv: Pub. INZHEK, p. 240.
12. Shkarlet,S. (2007). “The economic security of enterprise: innovation aspect: monograph”, Kiev: Books view of the NAU, p. 436.
13. Kavun,S. V., Mykhalchuk, I. V., Kalashnykova,N. I.,Zyma,O. G. (2012). A Method of Internet-Analysis by the Tools of Graph Theory. Intelligent Decision Technologies. Smart Innovation, Systems and Technologies, Volume 15, Part 1, pp. 35-44.
14. Kavun,S. V., Sorbat,I. V.,Kalashnikov,V. V. (2012). Enterprise Insider Detection as an Integer Programming Problem. Intelligent Decision Technologies. Smart Innovation, Systems and Technologies, Volume 16, Part 2, pp. 281-289.
15. Yazar, Z.(2002). “A qualitative risk analysis and management tool – CRAMM”, SANS Institute.
16. Kavun,S. V. (2008).The life cycle of the system enterprise economic security, Development management, Kharkiv national university of economics, № 6, pp. 17-21.
17. Kavun,S. V., Sorbat,I. (2009).Mathematical interpretation of the task of identifying insider in the organization (enterprise), Economic: problems of theory and practice, Publishing “Russcience”, Vol. 4, № 246, pp. 862-869.
18. Kavun,S. V., Sorbat,I. (2012). Mathematical Formalization of the Criterion Method to Identify Insiders, "Scientific Visnik L'viv State University of Internal Affairs. Seria: Economical", L'viv State University of Internal Affairs, Vol. 1, pp. 138-151.
19. Kavun,S. V., Sorbat,I., Kalashnikov,V. (2012). Enterprise Insider Detection as an Integer Programming Problem. In: 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”, Vol. 12, Heidelber, Germany, pp. 820-829.
20. Kavun,S. V., Sorbat,I. (2012). Enterprise information portal is a tool against with the insider’s trading activities in the system of an economic security of the enterprise (in Russian, with I. Sorbat), Financial and credit activity: problems of theory and practice, Kharkiv Institute of Banking of the Ukrainian Academy of Banking of National Bank of Ukraine, Vol. 1, № 1(12), pp. 162-168.