Insider Detection Method in a Company

Anatoly Adamovich Kornienko, Mark Aleksandrovich Polyanichko

Abstract: ***Managers often focus on external threats mainly due to the difficulties in evaluating the losses from the insider activities. The purpose of the study is to improve the efficient performance of an information security department and a company itself in counteracting insider threats by increasing the accuracy and rate of assessing the insider threat for each employee and ranking employees in accordance with the assessment of a summarized technical threat indicator. The authors morphologically analyze the features of insider activities in three sections and identify a promising area for combating the insiders – a prompt identification of unusual behavior signaling a breach of confidentiality. The paper describes an algorithm developed by the authors for assessing the insider threat for each employee of a company and ranking all employees by a summarized technical threat indicator. The steps to implement the algorithm are described in detail and a fuzzy derivation scheme of a summarized technical threat indicator is presented; an example is used to test the algorithm. The algorithm can be implemented as a part of a corporate information system. It is cheap to use and own, and it is rated as cost-efficient.***

Keywords: ***Internal threats, insider, insider detection, risk management, linguistic variables.***

I. INTRODUCTION

Threat management aimed to maintain information security presupposes the collection, processing, and application of knowledge about threats which a company faces in order to improve, identify security measures and to respond with the management tools until all threats are completely eliminated. The same is mainly true for the risk management in business. However, the focus on the external threats and exclusion or ignorance about insider threats are one of the key issues which scholars, consultants, crisis managers, etc. come across with. This is partly connected with the fact that the insider activity losses are difficult to measure, since their cause is deeply rooted, mainly with no explicit connection between the losses and the insiders. What is more, these losses are various in nature and their levels – from minor to huge and even fatal for the owners (bankruptcy or an illegal takeover). Material, financial, goodwill impairment, as well as problems with the corporate culture which has a double feedback with the insider activity make the situation even worse: a low level of the corporate culture provokes the insiders, which, in its turn, deteriorates a corporate culture.

The attempts to raise the problems of the insider threats are sometimes neglected by the assumptions that the insider threats are myths or unlikely events. At the same time, there are studies which disprove this assumption, which proves the need to turn the inside threat management into a business priority of the companies [11].

Revised Manuscript Received on December 15, 2019.

***** Correspondence Author

Anatoly Adamovich Kornienko, Emperor Alexander I St. Petersburg State Transport University, Saint Petersburg, Russia.

Mark Aleksandrovich Polyanichko*, Emperor Alexander I St. Petersburg State Transport University, Saint Petersburg, Russia. Email: polyanichko.spstu@bk.ru

Detection of the accidental and malicious insider threats is the task being solved by the information security analysts and administrators both in a business sector and in public organizations [11]. Up to 75% of insider threats are still found manually, and only 19% of the actions are revealed by combining computer-aided means and manual procedures [16]. However, the company reports prepared by the information security software developers illustrate that the number of the incidents associated with the insider activities is growing [5].

The issues connected with the insider threats are more difficult to be solved in comparison with the technical faults. People behave differently (polymorphous behavior), they often tend to hide their true emotions from the others, to change their behavior in the context of the situations. An insider will always analyze and evaluate the risk of being caught. Therefore, potential insider detection requires a method combining technical and organizational measures [21, 24].

Insider associated risk evaluation and risk management significantly improve the efficiency of company management and stability of a company on the whole. Therefore, the purpose of the paper is to describe an approach to the insider threat detection, one of the possible sets of data and their processing algorithm which can be applied nearly in any company.

II. MORPHOLOGICAL ANALYSIS OF THE INSIDER ACTIVITY FEATURES

A. Literature Review

The Russian scholars contributed a lot into the law focused studies of the insider activities, including the regulatory aspect of information security. Most works are associated with the most evident and properly regulated issues of the insider activities at the stock exchanges (The most important documents selected by a search query “Insider information”), also the psychological aspects of the insider activity, its motivation, insider classifications [13, 21, 23], as well as the non-technical ways to counteract the insiders [1, 32, 26] are thoroughly developed. The management issues of corporate information security are discussed in the works of the foreign researchers: [7]Dong et al. (2015), [10] Fu and Zhou (2011), [16] Keeney et al. (2005), [31] Xuepeng and Wei (2018).

Diagnostic behavior evaluation of an insider activity inclined personality has a special place in the studies, because “a person, being either a system operator, or a user, or the one performing other functions, is considered to be a weak link in the automated information system in terms of its security” [14]. The tools for diagnostic

Table 1. Morphological box (the result of a morphological analysis) of the insider features (the most dangerous insiders are shaded).

Reasons for insider activities [Ravilov, 2009 with authors' updates]	Insider's incompetence	Insider's carelessness	Personal animus towards an employer	Revenge against an employer and/or colleagues	Self-interest	Blackmail
Insider categories	Citizens	Trespassers		Renegades	Betrayers	
Types by reasons for an insider activity (Insider threats in Russia 2009)	Careless	Manipulated	Offended	Disloyal	Doing part-time job	Undercover
Methods of social engineering (Kabanov, Los, Suroev, 2016)	Information collection and analysis from open sources	Misrepresentation		Reverse engineering	Direct impact	

behavior evaluation were mainly developed by [22] McCrae and John (1992), [4] Batarshev (2005), [17] Kilmann (2011), [28] Thomas and Kilmann (2010). We addressed their works in developing the approach to insider threat detection.

The findings of the above-mentioned studies have not been compared up till now. We decided to carry out a morphological analysis of these findings to put their diversity in order and to make the choice among the insider activity factors easier for the experts (the first stage in detecting the insider threats).

B. Morphological Analysis of the Insider Features

The purpose of a morphological analysis is to define the combinations of features for insiders and their activities which are of great interest in the context of insider risk management: the most frequent, the most loss-intensive, the least observable, etc.

The morphological box (Table 1) could be extensively used to develop typical profiles for the insiders in a particular company which is planning to apply the described approach to insider threat detection. For example, a successful law company could be vulnerable to the shaded insiders, while a wholesale and retail company with a great number of branches and many employees could suffer from insufficiently competent, negligent and easily manipulated workers.

C. Morphological Analysis of Insider Activity Risk Factors

However, it is not enough to be aware of the typical and/or risky insiders for a company, it also requires the understanding of the threat area and scale to select the counteracting methods and measures. Therefore, the second stage of a morphological analysis includes the methodology of risk management under ISO31000:2018, Table 2 shows the results.

Table 2. A morphological box of insider activity risk factors

Probability of losses from the insider activities	Not available or nearly not available	Low	Average	High	
Types of losses from the insider activities	Financial	Material	Goodwill	Others (specify)	
Scale of loss from the insider activities	Small	Non-extensive (no extra funding)	Visible (impact on funding, but covered by operating means)	Extensive (extra external funding is required)	Catastrophic (can lead to bankruptcy)
Expected expenses on insider activity counteracting	Small	Not high	Tangible	Significant	Huge

Table 3. A morphological box with the features for the insider activity counteracting measures

Stages of Human Resource management	Job application		While being employed		Upon employment termination	
Conditions for unenforceable crime	Organizational and technical measures	Physical protection	Human resource management	Power division, etc.	Sanctions	Protection from malfunctions
Steps to work with the symptoms of insider crimes	Monitoring the information about employees		Forecasting insider crimes			
Localization of observation for the symptoms of insider crimes	At a workplace (including tutorship)		Internal [audit]		External [audit]	
Non-technical counteracting methods for insider activities	Material		Non-material			
Technical counteracting methods for insider activities	Mobile devices	Devices for instant messaging	WEB-technologies	Theft of equipment		
Main counteracting measures for insider activities	Counteracting the thefts	Counteracting espionage activities	Preventing accidental, unintended actions			

Table 4. Features of insider activity counteracting measures.

Human Resource management	Job application	While being employed
Symptoms of the insider crimes	Monitoring the information about the employees	Forecasting the insider crimes
Observation focus on the symptoms of insider crimes	Work place (incl. tutorship)	Corporate [audit]

D. Morphological Analysis of the Insider Activity Counteracting Measures

A morphological analysis of the insider activity features logically leads to the analysis of the insider activity counteracting measures.

The morphological box (Table 3) derived from the analysis defines the insider activity counteracting tools and measures which a company lacks – for example (features are randomly described), forecasting the insider crimes when an employee is fired due to the external audit at the expense of non-material non-technical measures (cooperation?) aimed to prevent the accidental actions.

E. Description of the Developed Tools Aimed to Detect the Insider Threats Under the Morphological Analysis

We mainly concentrated on the following features of insider activities:

1) Insiders' features – any (
2));
3) Insider activity risk factors – any (**Error! Reference source not found.**);
4) Features of insider activity counteracting measures (Table 4).

Insider activity counteracting measures could not be limited to the ones stated in Table **3**.

III. TOOLS (METHODS) FOR INSIDER THREAT DETECTION

Our working hypothesis is an assumption that monitoring the employees' activity factors could detect irregular behavior illustrating or signaling a risk of confidentiality breach.

The proposed method for insider threat detection combines the organizational and technical approaches and aggregates various data. The application of the proposed method together with the analysis of the risk indicator values could contribute into the detection of an insider threat.

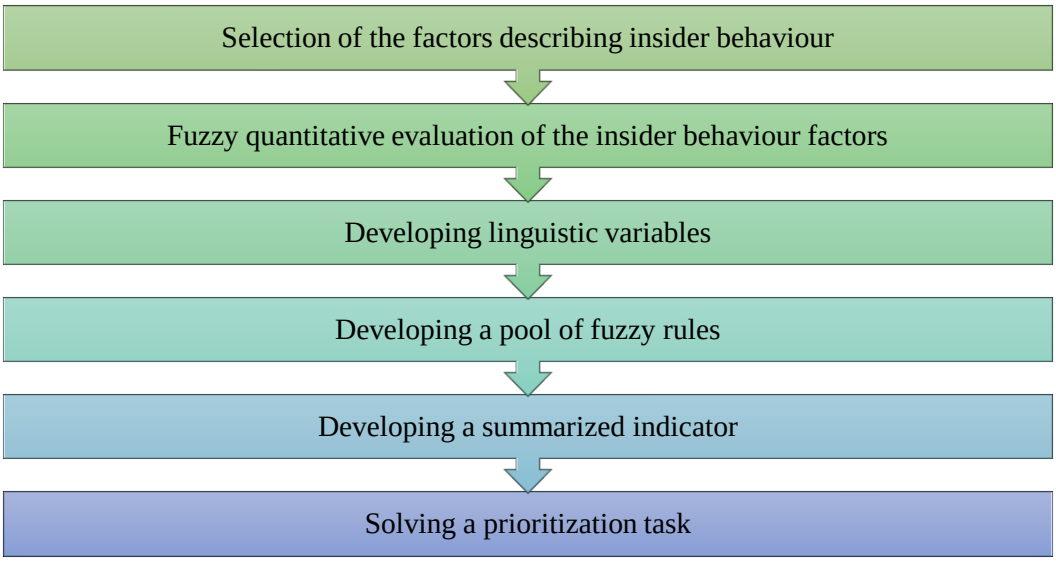

Figure 1. An approach to detection of a potential insider threat

A. Procedure for Detecting a Potential Insider Threat

The following actions are proposed to detect a potential insider threat in a company (Figure 1).

B. Factors in Question

The method works with the factors which could be divided into groups by their update frequency and methods:

- dynamic (they are updated automatically or semi-automatically in real time or at the time of information entry into the corporate information system, they are in cursive in Figure 2);
- updated from time to time;
- stationary (do not change, in bold).

Figure 2 gives a recommended and practice tested standard list of factors divided into groups by content. We emphasize that a particular company may refer to some factors as stationary ones – for example, a breach of a rule and procedure could be recorded both instantly (a dynamic factor) or from time to time.

A technical factor (DLP, IDS or SIEM combined) refers to the dynamic factors. This factor could be automatically evaluated by the data from the company's computer network and its information systems [1]. The technical factor is determined by the work of the users dealing with printing the documents, with search queries, providing the access to the information resources, downloading the information and browser usage.

Psychological and communicative personality dependent factors refer to the stationary factors. Psychological factors (extraversion, agreeableness, conscientiousness, neuroticism, openness to experience) are determined by a five-factor questionnaire "Big Five" developed by the American psychologists [22] McCrae and John (1992).

Communicative factors (communicativeness, cooperativeness, finding a compromise, problem avoidance behavior or adaptability) are determined by a sociability test by [15] Karelin (2007) and methodology for evaluating a personality behavior in a conflict situation (Thomas Kennet's instrument "TKI assessment" [30]).

The values of occasionally manifested factors are calculated by an analytic hierarchy process. They could refer to any group of factors (Figure 2) and generally comprise a major part of the factors in question. It is evident that the values of the most factors are linguistic, that is they convey the meaning from the natural or artificial language (Entry Disposition (predisposition)).

Linguistic variables and the appropriate fuzzy sets are characterized by a number of advantages:

- they continuously deal with the time changing dynamic input data;
- they help to switch to the unified qualitative measurement scale;
- they provide a qualitative evaluation of both input data and output results.

C. An Assessment of an Insider Threat for Each Employee

To define a potential threat which an employee poses, it is necessary to become aware of his/her predisposition to violation (readiness, inclination for a behavioral act, action, deed, their particular sequence (Entry Disposition (predisposition))). This task refers to the assessment based on a set of objects by a multi-dimensional set of qualitative and quantitative factors with regard to the linguistic statements of the experts. These tasks require a fuzzy generalization of the analytic hierarchy process [1, 2, 3, 7, 10, 31].

The analytic hierarchy process consists of two steps:

- establishing private factors influencing the predisposition assessment and
- fuzzy assessment on the basis of quantitative assessment of private indicators.

The experts prepare a set of indicators $\{ind_1(Pr_i), \dots, ind_{n_i}(Pr_i)\}$

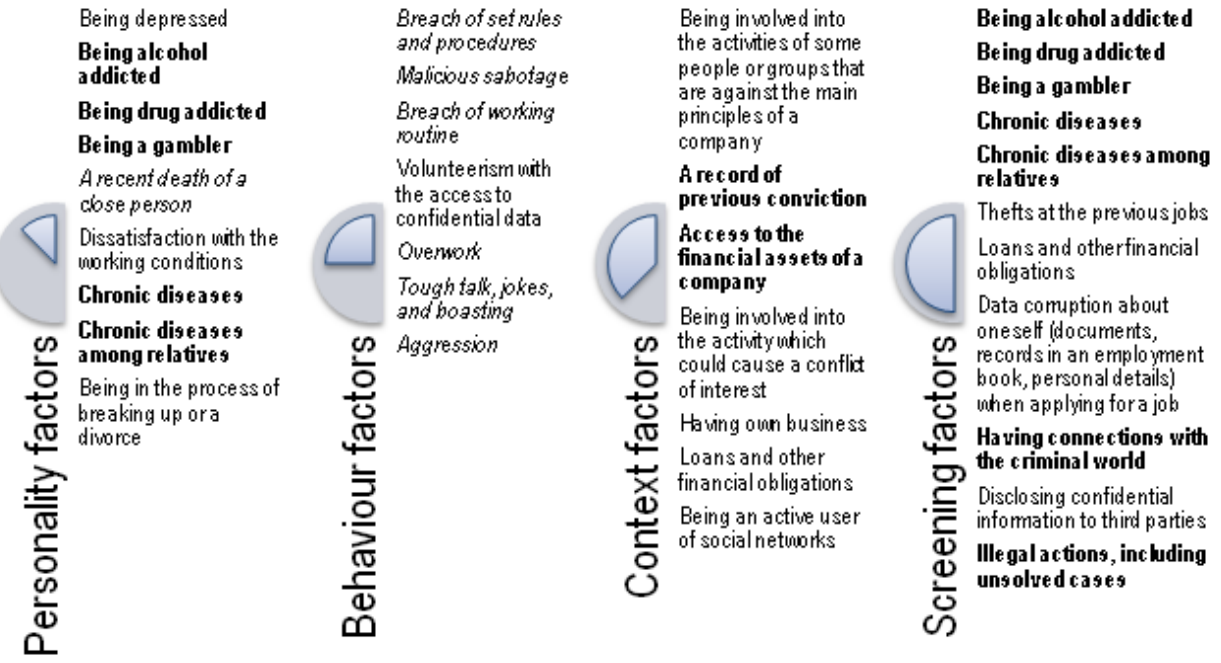

Figure 2. Diagram of evaluation factors for employee predisposition for insider activities

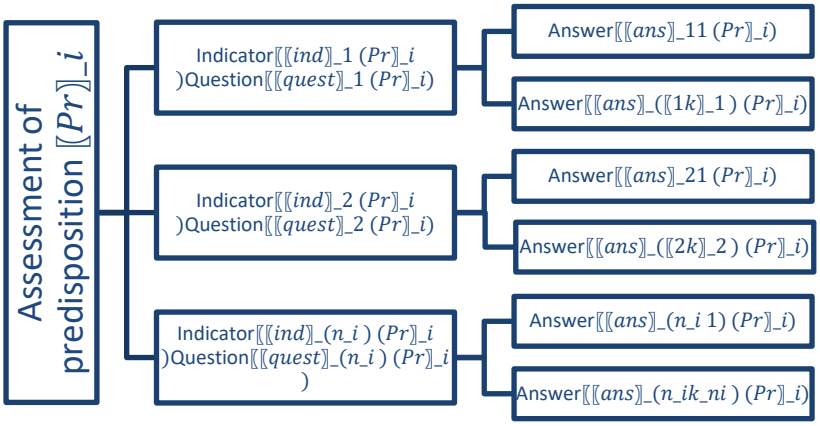

Figure 3. Decomposition tree for i-th predisposition

.

influencing the predisposition Pr_i. To assess each indicator, the appropriate questionnaire $quest_j(Pr_i)$ with a set of answers $ans_{jk}(Pr_i)$ is prepared.

$\{ind_1(Pr_i), \dots, ind_{n_i}(Pr_i)\}$,

where Pr_i is the predisposition;

$ind_j(Pr_i), j = 1, \dots, n_i$ are the predisposition indicators.

This hierarchy can be presented as a decomposition tree (Figure 3).

Predisposition is assessed under the following algorithm [1], (Table 5).

Potential insider behavior is identified by a consistent application of the fuzzy inference rule base for different factors (Figure 4).

Every base of fuzzy rules which could be called a linguistic model consists of a set of fuzzy rules $R^{(k)}, k = 1, \dots, N$, of type

Table 5. Predisposition is assessed under the following algorithm [1].

Algorithm steps	Content
1. Finding the experts	Each expert should be assigned with a weight δ. The number of experts equals N. A type of presupposition could affect the decision whether the experts should include employees from IT-departments, information security or HR departments.

Algorithm steps	Content
2. Prioritizing the questions	The experts compare the questions in pairs by their impact on the assessment of a particular predisposition Pr_i. Each expert is assigned with a vector of priority $(w\ quest^i)_z = (w\ quest^i_1, \dots, w\ quest^i_{n_i})_z$, questions $Quest_j(Pr_i)$, where the number of an expert is $z = \overline{1,N}$.
3. Developing fuzzy priorities for the questions	A fuzzy priority for a question $Quest_j(Pr_i)$ is given as a fuzzy number $\widetilde{w}\widehat{quest}^i_j$.
4. Defining fuzzy values	$\overline{SCORE}_j(Pr_i)$ is a fuzzy value for the scores allocated for each separate question $Quest_j(Pr_i)$.
5. Prioritizing for the answers inside the questions	Similar to Step 2 of the algorithm. Each expert compares the answers $Ans_{jk}(Pr_i)$, $k = \overline{1, k_j(Pr_i)}$ in pairs and calculates the priority vectors $(w\ ans^i)_z = (w\ ans^i_{j1}, \dots, w\ ans^i_{jk_i(Pr_i)})_z$, where the number of an expert is $z = \overline{1,N}$
6. Identifying fuzzy priorities for the answers inside the questions	A fuzzy priority of the question $F = Ans_{jk}(Pr_i)$ is given as a fuzzy number $\widetilde{w}\widehat{ans}^i_{jk}$.
7. Defining absolute values	$\lvert\overline{score}_{jk}(Pr_i)\rvert$ is as fuzzy numbers depending on the answer chosen by an expert. The number of the score is $\lvert\overline{score}_{jk}(Pr_i)\rvert = \overline{SCORE}_j(Pr_i) \cdot \widetilde{w}\widehat{ans}^i_{jk}$.
8. Defining the values influencing the predisposition assessment	Negative values of the scores are opposite to their absolute values.
9. Getting possible answers from an expert	The experts give an answer s_j to each question $Quest_j(Pr_i)$.
10. Rating the total scores	Scores for the answers on the test questions $\tilde{P}_i = \sum_{j=1}^{p_i} \overline{score}_{jk_j}$ are rated by the following formula: $$\psi(\tilde{P}_i) = \frac{(\tilde{P}_i - P_i^{min})}{(P_i^{max} - P_i^{min})}$$ where $P_{min} = \min_S(\sum_{j=\overline{1,p_i}} \tilde{P}_j^{min})$; $P_{max} = \max_S(\sum_{j=\overline{1,p_i}} \tilde{P}_j^{max})$; $\tilde{P}_j^{min} = \min_{k=\overline{1,k_j(Pr_i)}} \overline{score}^i_{jk}$ is the minimum value of the scores for an answer to a question; $\tilde{P}_j^{max} = \max_{k=\overline{1,k_j(Pr_i)}} \overline{score}^i_{jk}$ is the maximum value of the scores for an answer to a question;
11. Predisposition assessment	Predisposition assessment equals $\psi(\tilde{P}_i) = Pred(Pr_i)$.

$R^{(k)}$: ***IF*** (var_1 is A_1^k ***AND*** var_2 is A_2^k ... ***AND*** var_n is A_n^k) ***THEN*** (res_1 is y_1^k ***AND*** res_2 is y_2^k ... ***AND*** res_m is B_m^k),

where N is the number of fuzzy rules;

A_i^k is the fuzzy sets $A_i^k \subseteq VAR_i \subset R, i = 1, \dots, n$;

B_i^k is the fuzzy sets $B_i^k \subseteq RES_i \subset R, j = 1, \dots, m$;

$var_1, var_2, \dots, var_n$ are the input linguistic variables, where $(var_1, var_2, \dots, var_n)^T = var \in VAR_1 \times VAR_2 \times \dots \times VAR_n$;

$res_1, res_2, \dots, res_n$ are the output linguistic variables, where $(res_1, res_2, \dots, res_m)^T = res \in RES_1 \times RES_2 \times \dots \times RES_m$.

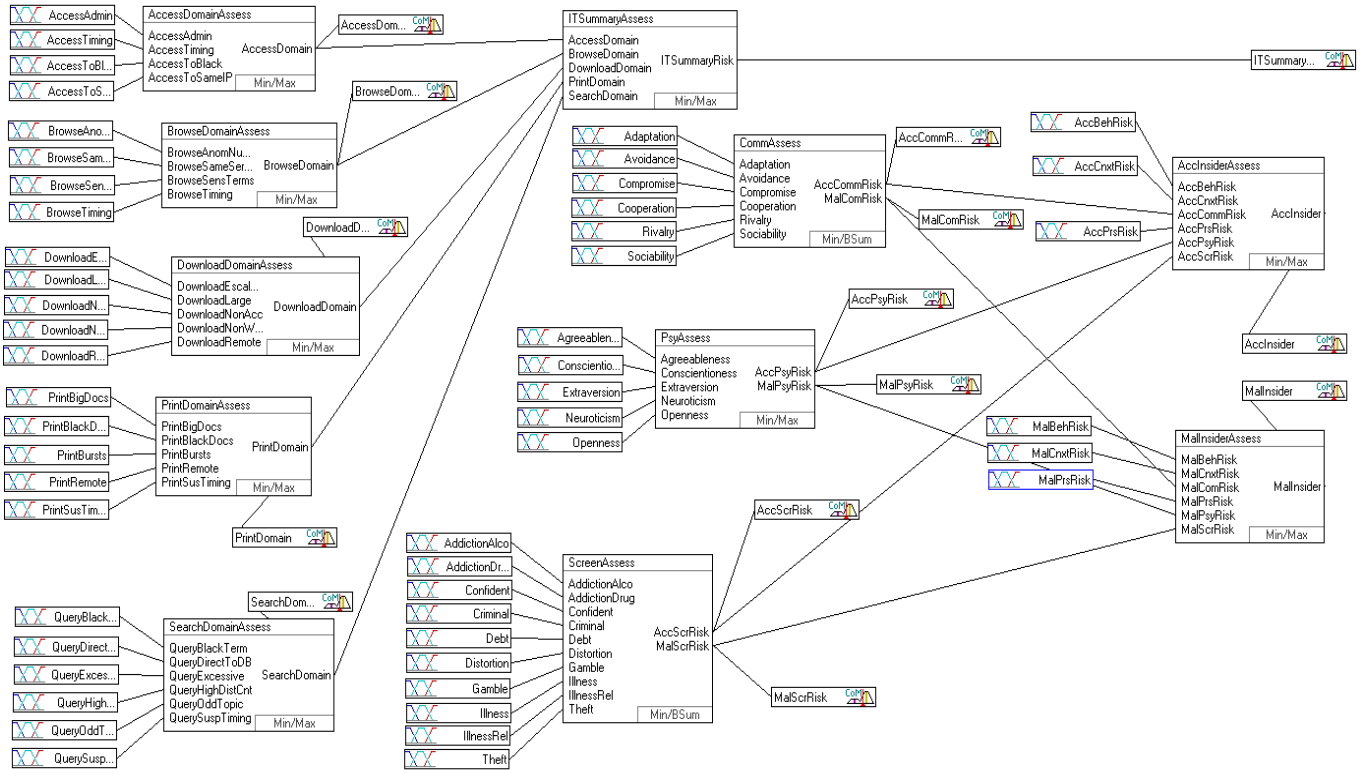

Figure 4. A diagram of fuzzy inference for a summarized factor

The proposed derivation scheme shows that an assessed employee is given several scores characterizing his/her inclination to an accidental or intended insider activity. The scheme also assesses the summarized technical indicator vulnerable to suspicious actions.

At the final stage of the method, the above-mentioned scores rate all employees by their possible threat. Each employee is given three assessment scores:

1) inclination to an accidental insider behavior AccInsider;
2) inclination to a malicious insider behavior MalInsider;
3) summarized technical indicator ITSummary.

D. Algorithm Validation, Employee Rating by Their Potential Insider Threat and Recommendations

The Laplace criterion is applied to rate the employees by their potential insider activity threat:

$$L_i = \frac{\sum_{j=1}^{M} x_{ij}}{M}$$

where x_{ij} is the value of the indicator.

Here is a particular presentation of the Laplace criterion for an accidental insider behavior:

$$L_i = \frac{AccInsider + ITSummary}{2}$$

Here is a particular presentation of the Laplace criterion for a malicious insider behavior:

$$L_i = \frac{MalInsider + ITSummary}{2}$$

Let us assume that the method of insider threat identification found the scores for the accidental insider threat and a summarized technical indicator (Table 6).

Table 6. Scores for the accidental insider threat and a summarized technical indicator

Employee (conventional #)	**AccInsider** inclination to an accidental insider behavior	**ITSummary** summarized technical indicator
1	0.8	0.1
2	0.2	0.3
3	0.6	0.8
4	0.9	0.4

Thus, once the Laplace criterion is calculated, the following priorities are obtained (Table 7).

Thus, the algorithm validation shows that an employee inclined to a malicious insider behavior with the above average and maximum score for the summarized technical indicator is considered to be the biggest threat for a company.

Table 7. An accidental insider threat, a summarized technical indicator, the Laplace criterion, the Laplace criterion, and priorities

Employee (conventional #)	**AccInsider**	**ITSummary**	**L_i**	**Priority**	**Recommendation**
1	0.8	0.1	0.45	3	Average risk, recommended to control
2	0.2	0.3	0.25	4	Low risk
3	0.6	0.8	0.7	1	High risk, recommended to redouble attention

IV. CONCLUSION

Thus, our morphological indicator-based analysis of the insider activity features showed a successful application of the efforts aimed to counteract the insiders – a quick detection of an unusual behavior illustrating or signaling a risk of confidentiality violation – and helped to develop an algorithm for insider threat assessment for each employee in a company and for employee rating under the summarized technical indicator of a threat. This algorithm can be implemented as a part of a corporate information system (CIS), it is cheap to apply and to own and is considered to be cost effective even with no additional special calculations.

REFERENCES

1. I.V. Anikin, "Technology of intellectual data analysis for identification in internal violators in computer systems," Scientific and Technical Bulletin of SPSPU. Computer Science. Telecommunication. Management, vol. 6, no. 113, 2010.
2. I.V. Anikin, Information Security Risks Assessment Method Based on AHP and Fuzzy Sets, 2nd Intl' Conference on Advances in Engineering Sciences and Applied Mathematics (ICAESAM'2014), May 4-5, 2014.
3. I.V. Anikin, Methods and algorithms of quantitative assessment and security risk management in fuzzy logics based corporate information networks. D.Sc. (in Engineering) Dissertation, Kazan, 2017.
4. A.V. Batarshev, Psychodiagnostics in management: Tutorial. Moscow: Delo, 2005.
5. CA Technologies. Insider Threat Report, 2018. https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf. Accessed on 18 July 2018.
6. D. Din, Personality types in stress. [Online]. Available: http://ru.laser.ru/socion/references/dean/index.html.
7. M. Dong, S. Li and H. Zhang, "Approaches to group decision making with incomplete information based on power geometric operators and triangular fuzzy AHP," Expert Systems and Applications, vol. 42, no. 21, pp. 7846-7857, 2015.
8. A.V. Drozd, "Psychology in the service of information security. Psychotypes," Information protection. INSIDE, vol. 6, no. 60, pp. 50-55, 2014.
9. Entry Disposition (predisposition). [Online]. Available: https://psychology_pedagogy.academic.ru/5872/диспозиция_%28предиспозиция%29
10. S. Fu and H. Zhou, "The information security risk assessment based on AHP and fuzzy comprehensive evaluation," IEEE 3rd International Conference on Communication Software and Networks, Xi'an, 2011, pp. 124-128.
11. Insider threats in Russia 2009 (results of a study among 1,046 Russian companies from different economy industries by Perimetrix specialists). [Online]. Available:
12. https://www.securitylab.ru/analytics/368176.php#_Toc221433879.
13. International standard ISO31000. Risk management – Tutorial – Translated by ISAR ANO DPO. (2nd edition), 2018. [Online]. Available: https://risk-academy.ru/download/iso31000/
14. A.S. Kabanov and A.B. Los, Reasons, preventive measures, and insider activity counteracting measures, 2016. [Online]. Available: http://xn----7sbbaj7auwnffhk.xn--p1ai/article/20730
15. A.S. Kabanov, A.B. Los and A.V. Suroev,. Social engineering methods in information security and their counteraction, 2016. [Online]. Available: http://xn----7sbbaj7auwnffhk.xn--p1ai/article/18216
16. A.A. Karelin, Big encyclopedia of psychological tests. Moscow: Eksmo, 2007.
17. M. Keeney, E. Kowalski, D. Cappelli, A. Moore, T. Shimeall and S. Rogers, Insider threat study: Computer system sabotage in critical infrastructure sectors. CMU/SEI and U.S. Secret Service, 2005.
18. R.H. Kilmann, Celebrating 40 Years with the TKI Assessment. A Summary of My Favorite Insights, 2011. [Online]. Available: https://www.kilmanndiagnostics.com/system/files/celebratingfortyyears.pdf
19. A. Kofman, Introduction into fuzzy set theory. Moscow: Radio and communication, 1982.
20. F. Kokhen, Non-technical counteracting measures against insider threats, 2015. [Online]. Available: https://www.securitylab.ru/analytics/473402.php
21. M. Sh. Levin, Solution support technology for modular systems, 2013. [Online]. Available: http://www.mtas.ru/search/search_results_ubs_new.php?publication_id=19154&IBLOCK_ID=10
22. E. A. Mamochka, "Personality types of a criminal-insider," Territory of New Possibilities. Bulletin of Vladivostok State University of Economics and Service, vol. 3, pp. 70–78, 2016.
23. R. R. McCrae and O. P. John, "An introduction to the five-factor model and its applications," Journal of Personality, vol. 60, no. 2, pp. 175–215, 1992.
24. M. A. Polianichko and A.I. Korolev, "Criteria for insider classification," Natural and Technical Sciences, vol. 9, no. 123, pp. 149-151, 2018.
25. M.A. Polianichko and K.V. Punanova, Key issues of practical implementation of personality-oriented approach to information security. "Fundamental and applied developments in technical and physics and mathematics" Collection of scientific papers of the third international round table, Moscow: KONVERT Limited liability company, 2018, pp. 57–60.
26. D. Ravilov, Methods of internal violator classifications, 2009. [Online]. Available: http://infocom.uz/2009/12/16/metodyi-klassifikatsii-vnutrennih-narushiteley/.
27. V. Iu. Skiba and V.A. Kurbatov, Tutorial on protection from internal threats to information security. Saint Petersburg: Piter, 2008.
28. The most important documents selected by a search query "Insider information" (regulatory legal acts, forms, articles, experts' consultations, and others). [Online]. Available: http://www.consultant.ru/law/podborki/insajderskaya_informaciya/
29. K. W. Thomas and R. H. Kilmann, An Overview of the Thomas-Kilmann Conflict Mode Instrument (TKI), 2010. [Online]. Available: https://www.kilmanndiagnostics.com/overview-thomas-kilmann-conflict-mode-instrument-tki
30. V. S. Vedeneev and I. V. Bychkov, "Means for finding the insiders in corporate information systems," Information Technology Security, vol. 21, no. 1, pp. 9-13, 2014.
31. "Verizon 2015 Data Breach Investigations Report," Information Security, pp. 1–70, 2015.
32. H. Xuepeng and X. Wei, "Method of Information Security Risk Assessment Based on Improved Fuzzy Theory of Evidence Establishing index system of information security risk assessment," International Journal of Online Engineering, vol. 14, pp. 188–196, 2018.
33. S. I. Zhurin, "An insider: main features and counteraction integrity," Information Technology Security, vol. 18, no. 4, pp. 176-183, 2011.

AUTHOR PROFILE

Anatoly Adamovich Kornienko works as the head of the Department of Informatics and information security in Emperor Alexander I St. Petersburg State Transport University, has a doctor of science degree and is an honored worker of science of the Russian Federation. Repeatedly acted as the head of the projects supported by Russian Foundation for basic research. Has as vast field of scientifical research, including information and telecommunication technologies, information security and information protection, modeling of information and telecommunication systems, analysis of information risks and security of information and information infrastructure, cryptographic methods and tools, intrusion detection systems, methods and automated means of verification, testing and recognition of undeclared software capabilities

Mark Aleksandrovich Polyanichko, works as an associate professor of the Department of Informatics and information security and Head of IT department in Emperor Alexander I St. Petersburg State Transport University, has a candidate of engineering science degree. Acted as the participant of the projects supported by Russian Foundation for basic research. Has as vast field of scientifical interests, including analysis of information risks and security of information and information infrastructure, developed a methodology of conflict detection and resolution in cyber attacks protection software on railway transport. Currently working on a research, addressing insider threat problem and malicious insider activity prevention.