Usage of Decision Support Technologies in Information Security Domain: Opportunities and Prospects

Kadenko S.V.
Institute for information recording of
the National academy of sciences of Ukraine,
Kyiv, Ukraine
Email: seriga2009@gmail.com

***Abstract*—Information security is an important national security sphere, characterized by multiple tangible and intangible factors of both quantitative and qualitative nature. In order to be able to set priorities and plan actions in the area of information security one needs to have a clear analytical, formal description of this subject domain. However, not all the data about informational security in general and informational operations in particular is deterministic or even quantifiable. Many authors list certain features of information operations, which allow us to conclude that they represent a weakly structured domain. One of the most effective (and sometimes the only) way to get a formal description of a weakly structured domain is to turn to experts for information. Multi-criteria decision support technologies allow decision-makers to get recommendations concerning selection of best options when it comes to strategic planning, resource allocation, prioritization, project selection etc. This paper explains why expert data-based decision support technologies provide a powerful tool for analytical description and formalization of informational operations and information security strategies, and describes the main stages of implementation of decision support arsenal in information security domain.**

Keywords*—information security, informational operation, decision-making, expert estimate, decision support system, strategic planning, hierarchic problem decomposition.

I. Introduction

During the last few decades the relevance of information security as a sub-domain of national security was growing rapidly. We can recall that informational impact was a powerful propaganda tool even in ancient times. However, in the modern world information security is more relevant than ever. Success in the information war is a necessary condition of the war success in general. That is why information security, particularly prevention of informational operations, should be a necessary activity component and an important strategic priority of any large organization (including national and local governments).

In this report it is suggested to use the definition of informational operation, provided in [1]. According to the authors, an informational operation is, usually, meant to

- introduce certain ideas and notions into the minds of the public in general and of specific individuals in particular
- disorientate and mislead the recipients of information
- weaken the conventions of citizens and the society in general
- intimidate the masses (sometimes).

Planning of activities, meant to strengthen the information security, prevent negative/alien information impacts and informational operations (as well as successful planning of actions in the process of informational combat) calls for in-depth knowledge of the subject domain. However, information security domain is a weakly-structured one, which is problematic to describe, particularly, in formal quantitative terms. Expert data-based decision-making support technologies provide the means for problem-solving in weakly-structured domains [2]. That is why we feel that usage of expert data-based decision support technologies in the area of informational security and specific context of implementation of certain methods deserve to be considered in a separate paper.

II. Information Security as a Weakly Structured Domain

The author of [3] lists the following features of weakly structured domains (Fig. 1): lack of functioning goal, which could be formalized, lack of optimality criterion, uniqueness, dynamics, incompleteness of description, inability to build an analytical model, lack of benchmarks, large dimensionality.

In [1] it is stated that informational operations are influenced by numerous solely qualitative criteria, factors, and parameters (including socio-psychological ones). It is problematic to provide a formal mathematical (analytic) description of these factors.

Gorbulin et al also point out the impossibility of development and practical application of some universal methodology for modeling of informational operations, first and foremost, due to weak formalization of concepts and factors. These authors stress, that in each particular case one should consult the analysts (i. e. information operation experts) and rely on their competency. The analysts are sometimes able to build accurate forecasts of certain dependencies, which are later confirmed by practice. Analysts (experts) should be consulted to provide description of subjective factors. When it comes to objective factors, their description and analysis can be performed using well-known methods, which operate determined data, including mathematical statistics and analysis

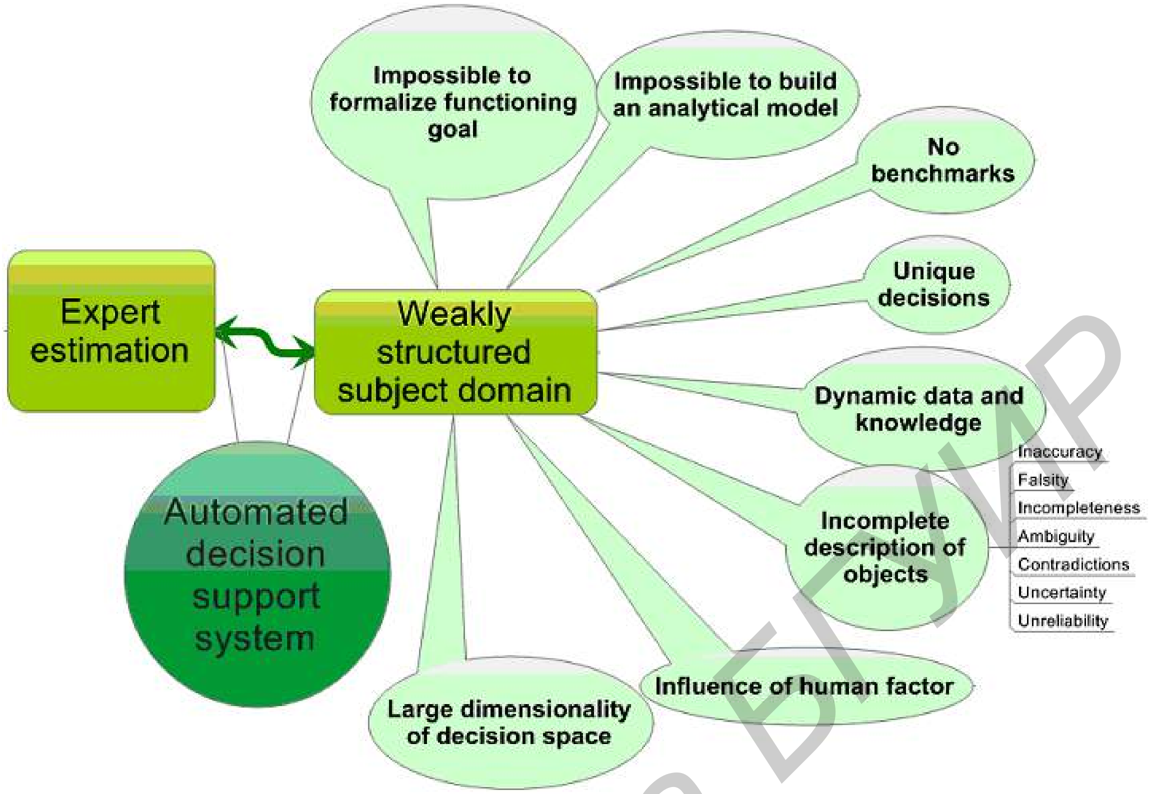

Figure 1. Features of weakly structured domains

of time series. However, these methods are targeted only at description of formal aspects, and do not touch upon content-related aspects. As a result, Gorbulin et al stress the necessity of extension of technological arsenal, which can be used for analysis and modeling of informational operations.

As we can see, informational operations (like all other operations, requiring human participation) represent a vivid example of a weakly-structured subject domain. We feel that expert data-based decision support technologies should become one of the technical tools for analysis and modeling of informational operations. The relevance of expert data usage in weakly structured subject domains is also corroborated by the research, conducted by Delphi Group, listing the sources of knowledge, possessed by organizations [4] (Fig. 2).

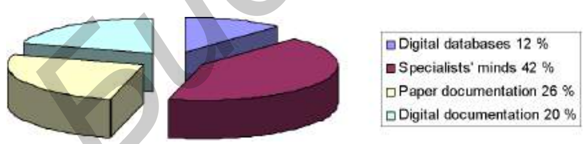

Figure 2. Sources of knowledge about an organization, according to Delphi Group research

The research indicated that a considerable share of knowledge is stored not in the databases, or on paper and digital mediums, but rather in the minds of experts (analysts, specialists). Consequently, in the context of description and analysis of informational operations, expert knowledge should, definitely, be involved, especially when it comes to subjective qualitative factors.

III. Hierarchic decomposition and complex target-oriented dynamic evaluation of alternatives

As it is stated in [1], an informational operation is an inter-disciplinary set of methods and technologies that encompasses multiple spheres, from military science to sociology. At the same time, there is no universal standard information operation technology (which could serve both the military and the management of large governmental or business agencies). So, according to Gorbulin et al, development of a scientific basis of informational operations remains an extremely relevant issue.

With the inter-disciplinary nature of informational operations in mind, we feel that expert knowledge-based hierarchic decomposition should become a handy informational operation description tool. Particularly, a hierarchic approach provides the basis for the method of complex target-oriented dynamic evaluation of alternatives (MCTDEA), suggested by V.Totsenko [2] and further improved by V.Tsyganok [5]. The method allows to aggregate a large quantity of criteria of different nature (i.e. belonging to different spheres) (Fig. 3), that influence a specified main goal, into a unified hierarchy.

Depending on the type of a specific informational operation (offensive or defensive [1]), the analyst (expert) or the decision-maker (DM) himself can formulate the main goal. Any informational operation is decomposed into certain stages (or steps), which are listed in [1]. The contents of these steps can vary, depending, again, on the type and context of the operation. For example, during modeling and decomposition of an informational attack against the Academy of sciences (using MCTDEA), a goal formulated as “Discredit an aca-

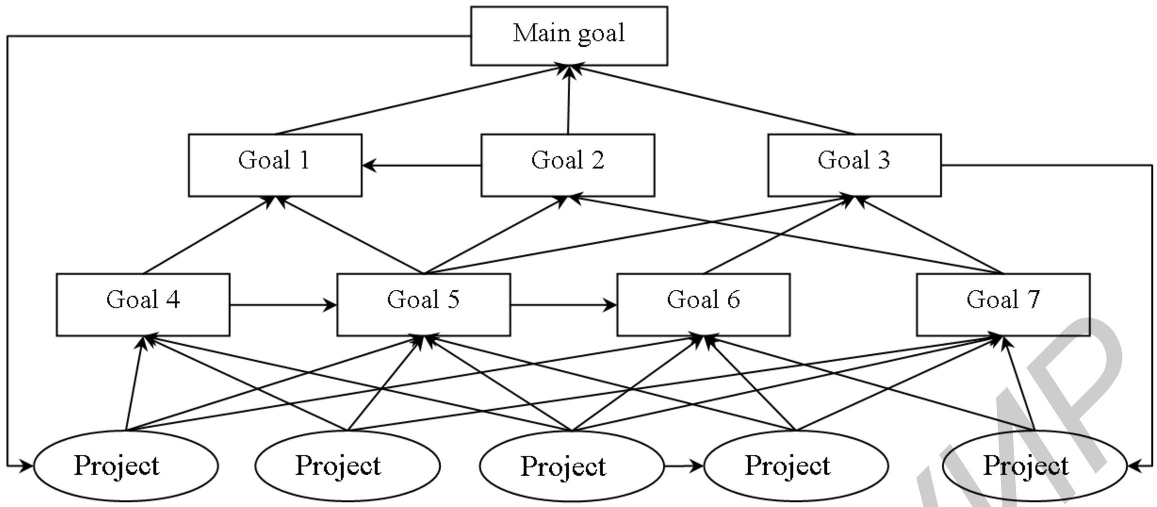

Figure 3. An example of goal hierarchy

demic institution in the media" can be decomposed into the following lower-level sub-goals: "Discredit academic papers and achievements" and "Discredit academic researchers".

In MCTDEA decomposition is performed down to the level of "atomic", elementary sub-goals (factors, criteria) that can be directly influenced by the DM. These goals are called projects (see Fig. 3), and, generally, can be characterized by a certain value (absolute/relative numeric, Boolean, or threshold-type).

The general conceptual task of decision support methods, involving hierarchic decomposition of a problem, particularly, MCTDEA and analytic hierarchy/network process (AHP/ANP) [6], is to build a rating or ranking of objects (alternatives, projects). Based on such rating, a DM can make an informed choice of the best alternative (decision variant) from a given set, or set priorities in his/her activity (i.e., determine, which factors or actions are most important for achievement of a given main goal). In order to build such a rating, one should define the relative importance of all goals in the hierarchy graph, built by experts (or by knowledge engineers through dialogues with experts). In order to define the relative importance of sub-goals of a given goal (its "descendants" in the hierarchy graph), experts should compare them pair-wise (unless they are able to provide direct estimates). Evaluation of impacts (weights) can be conducted by experts in different pair-wise comparison scales. Recent research of V.Tsyganok [7],[8] has shown that the expert should be given an opportunity to input every single pair-wise comparison value in the scale, which is most convenient for him or her (i.e. which reflects his/her knowledge of the subject domain most accurately). When the experts have evaluated all relative weights (priorities) in the hierarchy graph, relative impacts of all the projects upon the main goal (their relative efficiencies) can be calculated as shown in [2].

If evaluation is done by several experts, then a few important aspects should be taken into consideration. The first aspect is expert competence. If it is known that the experts, who evaluate criteria, projects, or alternatives, have different competencies, their relative competence levels should be calculated based on three components: self-assessment, mutual assessment, and objective data (as shown in [2]). Differences in relative competence levels of the experts can be neglected only when the size of the expert group is large enough [9]. The second important aspect is consistency of estimates, provided by different expert group members. Expert estimates' consistency should be checked (as recommendations to the DM, based on inconsistent or incompatible expert data will provoke distrust). In order to evaluate consistency level of expert estimates, in our view, it is appropriate to use so-called spectral methods, described, for instance, in [10] and [11]. The advantage of spectral methods over other approaches to consistency evaluation (for example, those suggested by Saaty and colleagues [12]) is as follows. If necessary (i.e., if consistency level of expert estimates in the group is low), spectral methods allow the knowledge engineer to organize step-by-step feedback with experts. Experts are requested to change the respective outlying estimates so as to make overall consistency level reach the required threshold (as shown on Fig. 4).

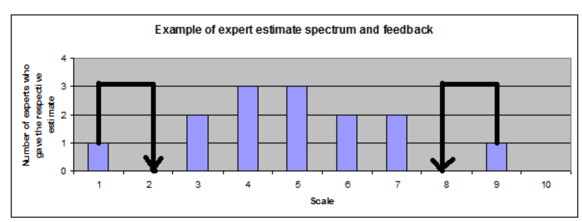

Figure 4. Example of consistency improvement during group expert estimation

When estimates, provided by different members of the expert group, achieve the level of consistency, that is high enough, they can be aggregated (used for calculation of generalized group estimates). For aggregation of expert estimates, we suggest using the combinatory aggregation method [13]. The most important of the method's advantages over other aggregation methods are as follows. First, it can be used for aggregation of incomplete pair-wise comparison matrices. Second, it utilizes the redundancy of information most thoroughly.

In the context of MCTDEA the "weighted" hierarchy of criteria (goals) is called the knowledge base (KB) of the subject domain. This paper is focused on subject domains, related to information security, particularly, information operations. In terms of content, such KB represents one of the types of subject domain models. The KB is built by experts (or by knowledge engineers through dialogues with experts) using special software tools – automated decision support systems (DSS) (see Fig. 1).

We should note that MCTDEA does not require all the data, input into DSS KB, to be represented by expert estimates only. For instance, when it comes to comparison of several alternatives according to some criterion, estimate values should not necessarily be expressed by grades of pair-wise comparison scales. Sometimes, the values can be absolute ones, available from open information sources. For example, in order to analyze the information policy or campaign of some organization absolute values are often used, such as "number of publications with negative flavor per month". An indicator like this "has all the rights" to be included into a hierarchy of criteria, describing the information policy of an organization.

IV. Issues concerning dialogues with experts

An expert (analyst), usually, comes from a narrow-focused subject domain and, in the general case, is not familiar with decision support methods and technologies. Consequently, it is extremely important to make the process of expert data input into the DSS as comfortable for experts as possible. Formal side of the process (expert data formalization) should be delegated to the knowledge engineer, and mathematical calculations – to the automated DSS. In order to achieve this objective during expert examination it is appropriate to keep several important issues in mind.

First, if an expert is completely new to decision support technologies, it makes sense to familiarize him/her at least with the general agenda of the examination. In the ideal case examination participants should be given a thorough explanation of the whole technology, used to process their estimates and to form recommendations for the DM as to decision variant selection. Such an explanation will increase the level of trust the experts have towards the process and allow them to input data into the DSS in the most convenient format. So, before starting to collect information from the experts, it is reasonable to hold coaching sessions with them.

Second, criteria (goal) hierarchy (See Fig. 3) should be well-balanced. It is preferable to locate all the projects on one level (because, as it is shown in [6], their weights should belong to one order of magnitude). With human psycho-physiological constraints taken into consideration, any goal in the hierarchy graph should not have more than 72 descendants [14]. In the process of hierarchy building, it is preferable not to "bother" the expert with multiple similar questions (particularly, concerning positive or negative character of impact of goals upon their common "ancestor" in the graph, or pair-wise compatibility of "descendant" goals).

Third, when evaluating the impacts, verbal values should be used rather than their numeric equivalents (for instance "1" – equality, "2" – weak preference, … , "5" – extremely strong preference). See Fig. 5, illustrating one of pair-wise comparison scale examples, suggested by Saaty [6].

Numerical values	Verbal term	Explanation
1	Equally important	Two elements have equal importance
3	Moderately more important	Experience or judgment slightly favors one element
5	Strongly more important	Experience or judgment strongly favors one element
7	Very strongly more important	Dominance of one element proved in practice
9	Extremely more important	The highest order dominance of one element over another
2,4,6,8	Important intermediate values	Compromise is needed

Figure 5. Fundamental pair-wise comparison scale with 9 grades

Another scale type, which is used for interviewing of respondents from most diverse subject domains is Likert's agreement/disagreement scale. Interviewees are offered to agree or disagree with some positively formulated statements (like, for instance, "Posts in social networks with positive flavor substantially improve the image of the business"). Afterwards their answers are assigned numerical values (one of the correspondence rules is shown on Fig. 6 and aggregated.

Strongly Disagree	Disagree	Undecided	Agree	Strongly Agree
1	2	3	4	5

Figure 6. Likert's agreement scale example

On the whole, interface of an automated DSS should be user-friendly, intuitively understandable, and easy to master.

More detailed analysis of peculiar features of working with experts is provided in [15].

V. Elicitation of patterns and parameters of informational impact dissemination based on available data and experience

In the context of information operations research authors of [1] stress, that it is important to be able to evaluate parameters of the model based on real behavior patterns and dependencies. Detected patterns and dependencies will provide the basis for forecasts of information operation impacts even if clear picture is still missing. Moreover, such a forecast may be more accurate than the results of regular expert examinations (where experts make forecasts in the form of estimates).

In this regard (returning to decision support perspective) we should mention the relevance of factor analysis and neural network algorithms, which allow to determine model parameters based on given sets of "input" and "output" values.

This opportunity was noted by V.Totsenko in [2], who listed specific factor analysis methods in his book: group method of data handling (GMDH), least squares method (LSM), multi-dimensional linear extrapolation, and minimum discrepancy method.

We should stress, that input data for factor analysis can be represented by both determined data of actual system behavior (particularly, input and output parameters, characterizing an informational operation) and expert data. Above-listed factor analysis methods (as well as neural networks) are relevant if input data is cardinal (numeric). If only ordinal-type data (that contains information about the order of alternatives in the ranking, but not about quantitative relation between them) is available, then ordinal factor analysis methods, set forth in [16], [17], [18], should be used. For example, if after parliamentary election ratings and final ranks of parties are already known, relative weights of certain strategic points in their election programs can be calculated based on available ratings.

Cardinal and ordinal factor analysis methods also allow us to define, which parameters influence the centrality of an element in some network-type structure (Gorbulin et al dedicate a separate section of their book to network methods and structures in the context of information operations). Such a calculation was attempted, for example, in [20].

Beside that, when it comes to information network structure, we should remember, that its elements often reflect certain social relationships among network agents (or nodes) [1]. For instance, members of a community in a social (or terrorist) network can be associated through common ideas, slogans, references, links, etc. Elicitation of such relationships can be performed based on semantic similarity of content, attributed to members of this or that network structure. Even if there are no explicit connections, semantic analysis of respective online content can allow to detect latent, hidden connections. Content similarity methods are set forth (from decision support perspective) in the recent works of O.Andriichuk, such as [21].

VI. Strategic planning

A separate informational operation can have powerful impact. However, it represents, so to say, tactic level. Moving to strategic level, we should note that information security strategy is a necessary component of the general national security strategy [1].

In [22] Tsyganok et al show, that the strategy can be represented as an optimum (for a given moment in time) distribution of limited resources among top-priority projects in a specific domain. In [23] the subject domain, where the strategy is built, is represented by space activity and production of space equipment. In [22] the subject domain is the defense industry. A similar strategy can be built in the area of informational security as well.

The process of strategic planning, based on multi-criteria decision support technologies using both expert and objective data, incorporates all the procedures, listed in the previous sections of this paper. It includes the following phases:

- Formulation of the main goal, which characterizes the subject domain, by the DM.
- Selection of a group of experts (specialists, analysts) to participate in the examination.
- Building of a hierarchy of criteria (factors), influencing the achievement of the main goal (through dialogues with experts).
- Expert evaluation of relative impacts of criteria (projects) in the hierarchy.
- Calculation of relative efficiencies of the projects, i.e. their contributions to the achievement of the main goal.
- Determination of the optimal development strategy.

In this case we are talking about information security development. As noted above, a strategy is a distribution of limited resources among separate projects, which guarantees the most effective achievement of the main goal. According to Tsyganok et al., as of now, the best way to find such a distribution is to select it from the set of all possible resource distributions using genetic algorithm. Particular algorithm of resource distribution selection is the subject of separate studies.

VII. Conclusion

Due to inter-disciplinary nature, impossibility of formalization, presence of human factor, and other reasons, strict analytical and mathematical description of informational operations represents a serious problem. However, such description is absolutely necessary in the context of active informational combat. Alongside other approaches, such as multi-agent modeling (using cellular automation and other means), expert data-based decision support technologies allow us to get a clearer and more formal understanding of informational operations and their effects. While multi-agent approaches provide a reliable tool for modeling of the process of dissemination of informational impact or effect of informational operations, multi-criteria decision aids using expert and objective data should provide means of formal description and analysis of planning and implementation of informational operations.

Particular areas of decision support technology implementation in the information security domain include:

- formalization and analytical description of informational operations;
- decomposition of offensive and defensive informational operations into elementary steps/phases;
- setting of priorities in informational combat;
- informational policy making;
- elicitation and analysis of informational impact dissemination parameters;
- detection of relations between agents in information networks through content analysis;
- development of information security strategies.

This paper is prepared as part of project F73/23558 “Development of Decision-making Support Methods and Means for Detection of Informational Operations”. The project won the contest F73 for grant support of scientific research projects held by The State Fund For Fundamental Research of Ukraine and Belarusian Republican Foundation for Fundamental Research.

REFERENCES

[1] Горбулін В.П., Додонов О.Г., Ланде Д.В. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія – К., Інтертехнологія, 2009 – 164 с.

[2] Тоценко В. Г. Методы и системы поддержки принятия решений. Алгоритмический аспект [Текст]/ В. Г. Тоценко; ИПРИ НАНУ. – К.: Наукова думка, 2002. – 382 с.

[3] Таран Т.А. Искусственный интеллект. Теория и приложения / Т.А. Таран, Д.А. Зубов; Восточноукр. нац. ун-т им. Владимира Даля. — Луганск: ВНУ им. В.Даля, 2006. — 239 с.

[4] Тузовский А.Ф. Системы управления знаниями (методы и технологии) / А.Ф. Тузовский, С.В. Чириков, В.З. Ямпольский – Томск: Изд-во НТЛ, 2005. – 260 с.

[5] Циганок В.В. Удосконалення методу goalового динамічного оцінювання альтернатив та особливості його застосування / В. В. Циганок // Реєстрація, зберігання і обробка даних. - 2013. - Т. 15, № 1. - С. 90-99.

[6] Saaty T.L. Relative measurement and its generalization in decision making. Why pairwise comparisons are central in mathematics for the measurement of intangible factors. The Analytic Hierarchy/Network Process / T.L.Saaty // Statistics and Operations Research, Vol. 102(2), 2008 – pp.251-318.

[7] Циганок В.В. Агрегація групових експертних оцінок, що отримані у різних шкалах / В.В.Циганок // Реєстрація, зберігання і обробка даних. – 2011. – т.13. – №4.– С.74-83.

[8] Циганок В.В. Експериментальний аналіз технології експертного оцінювання / В.В.Циганок, П.Т.Качанов, С.В.Каденко, О.В.Андрійчук, Г.А.Гоменюк // Реєстрація, зберігання і обробка даних. – 2012. – Т. 14, № 1. – С. 91-100.

[9] Tsyganok, V. Significance of expert competence consideration in group decision making using AHP. / V. Tsyganok, S. Kadenko, O.Andriichuk//International Journal of Production Research. Vol. 50, Issue 17, 2012 – pp. 4785-4792

[10] Zgurovsky, M.Z. Group incomplete paired comparisons with account of expert competence / Zgurovsky, M.Z., Totsenko, V.G., Tsyganok,V.V.// Mathematical and Computer Modelling, 39(4), 2004 – pp.349–361.

[11] Olenko, A. Double Entropy Inter-Rater Agreement Indices / Olenko Andriy Tsyganok Vitaliy // Applied Psychological Measurement 40(1), 2016 – pp. 37–55.

[12] Forman, E.Aggregating individual judgments and priorities with the analytic hierarchy process/ Forman, E. Peniwati, K // European Jouranl of Operational Research, Vol. 108, 1998 – pp.131-145.

[13] Циганок В.В. Комбінаторний алгоритм парних порівнянь зі зворотним зв'язком з експертом / В.В.Циганок // Реєстрація, зберігання і обробка даних. – 2000. – Т.2, №2. – С.92-102.

[14] Miller G. A. The Magical Number Seven, Plus or Minus Two / G. A. Miller // The Psychological Review, - 1956, - vol. 63 – pp. 81—97.

[15] Каденко С.В. Проблеми представлення експертних даних у системах підтримки прийняття рішень/ С.В. Каденко // Реєстрація, зберігання і обробка даних, Т. 18 № 3, 2016 – с. 67-74.

[16] Kadenko S.V. Personnel-related decision making using ordinal expert estimates / S.V.Kadenko// OR52 Keynotes and Extended Abstracts - 52nd Conference of the Operational Research Society – 2010 – pp. 178-184.

[17] Kadenko S.V. Determination of Parameters of Criteria of "Tree"Type Hierarchy on the Basis of Ordinal Estimates / S.V.Kadenko // Journal of Information and Automation Sciences – 2008 – vol. 40, i.8 – pp. 7-15.

[18] Kadenko S.V Defining the Relative Weights of the Alternatives Estimation Criteria Based on Clear and Fuzzy Rankings / S.V. Kadenko // Journal of Information and Automation Sciences – 2013 – vol. 45, i. 2 – pp. 41-49.

[19] Горбов І.В. Визначення потенційних експертних груп науковців у мережі співавторства з використанням методів підтримки прийняття рішень / І. В. Горбов, С. В. Каденко, І. В. Балагура, Д. Ю. Манько, О. В. Андрійчук // Реєстрація, зберігання і обробка даних. - 2013. - 15, № 4. - С. 86-96.

[20] Андрійчук О.В. Метод змістової ідентифікації об'єктів баз знань систем підтримки прийняття рішень / О.В. Андрійчук // Реєстрація, зберігання і обробка даних. — 2014. — Т. 16, № 1. — С. 65-78.

[21] Андрійчук О.В. Метод змістової ідентифікації об'єктів баз знань систем підтримки прийняття рішень / О.В. Андрійчук // Реєстрація, зберігання і обробка даних. — 2014. — Т. 16, № 1. — С. 65-78.

[22] Циганок В.В. Інструментарій підтримки прийняття рішень як засіб стратегічного планування / В.В.Циганок, С.В.Каденко, О.В.Андрійчук, П.Т.Качанов, П.Д.Роїк // Озброєння та військова техніка – 2015, № 3(7). – С. 59-66.

[23] Tsyganok, V.V. Using Different Pair-wise Comparison Scales for Developing Industrial Strategies / Tsyganok, V.V, Kadenko, S.V., Andriichuk, O.V. // . Int. J. Management and Decision Making, 14(3), 2015 – pp.224-250.

ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ВОЗМОЖНОСТИ И ПЕРСПЕКТИВЫ

Каденко С.В.

В докладе проанализированы особенности сферы информационной безопасности как слабо структурированной предметной области. Показано, что информационная безопасность в целом и информационные операции в частности представляют собой яркий пример слабо структурированной предметной области, которая плохо поддается формальному описанию. Тем не менее, необходимость в формальном описании и анализе информационных операций остается актуальной. Вследствие слабой структурированности предметной области, для решения задач ранжирования, построения рейтинга мероприятий, расстановки приоритетов и стратегического планирования в сфере информационных операций целесообразно применять методы экспертной поддержки принятия решений. В тексте доклада описаны принципы использования экспертных технологий поддержки принятия решений на различных этапах анализа и планирования информационных операций, а также – противодействия вражеским информационным операциям.