UDC 004.056
DOI: 10.15587/1729-4061.2017.90506

DESIGNING A DECISION SUPPORT SYSTEM FOR THE WEAKLY FORMALIZED PROBLEMS IN THE PROVISION OF CYBERSECURITY

B. Akhmetov
PhD, Associate Professor
Department of Computer Engineering
International Kazakh-Turkish University named after H. A. Yesevi
B. Sattarhanov str., 29, Turkistan, Kazakhstan, 161200
E-mail: Berik.Akhmetov@ayu.edu.kz

V. Lakhno
Doctor of Technical Science, Associate Professor
Department of Managing Information Security
European University
Academician Vernadskiy blvd., 16 V, Kyiv, Ukraine, 03115
E-mail: lva964@gmail.com

Y. Boiko
Associate Professor
Department of Information Technology Security*
E-mail: julia_boyko2010@ukr.net

A. Mishchenko
Associate Professor
Department of Information Security Protection*
E-mail: partpravo@i.ua
*National Aviation University
Kosmonavta Komarova ave., 1, Kyiv, Ukraine, 03058

Розроблено систему підтримки прийняття рішень (СППР) в слабко формалізуємих завданнях забезпечення кібербезпеки. Система базується на моделях опису завдань кіберзахисту в понятійному і функціональному аспектах. Описано процес формування бази знань СППР для обставин, пов'язаних з виявленням важко пояснюваних ознак аномалій та атак. Запропонована СППР дозволяє підвищити розуміння ситуації, яка підлягає аналізу в процесі кіберзахисту комп'ютерних систем

Ключові слова: система підтримки прийняття рішень, кібербезпека, слабо формалізовані завдання, інтерпретація ситуації

Разработана система поддержки принятия решений (СППР) в слабо формализуемых задачах обеспечения кибербезопасности. Система базируется на моделях описания задач киберзащиты в понятийном и функциональном аспектах. Описан процесс формирования базы знаний СППР для обстоятельств, связанных с выявлением труднообъяснимых признаков аномалий и атак. Предложенная СППР позволяет повысить понимание анализируемых ситуаций в процессе киберзащиты компьютерных систем

Ключевые слова: система поддержки принятия решений, кибербезопасность, слабо формализуемые задачи, интерпретация ситуации

1. Introduction

In connection with the growing number of complex targeted cyberattacks directed at the mission critical computer systems (MCCS), one of the vital problems of society is the information security (IS) and its component – cybersecurity (CS). When conducting targeted attacks, cybercriminals frequently are used unique harmful programs and methods of penetrating the MCCS (objects of cyberprotection – OBCP). Resisting a constant increase in the complexity of illegitimate actions on MCCS is possible, in particular, using the systems for the intelligent recognition of cyberattacks (SIRCA), equipped with the modules for decision support system (DSS). The architecture of the latter implies, as a rule, a system for intelligent data analysis (SIDA or Data Mining). SIRCA make it possible to reveal regularities in the dynamics of development of the OBCP states, combining the knowledge and experience of decision making by experts, as well as the SIDA computational potential.

When complex situations of the guaranteed provision of OBCP IS arise, the decision-making process should be performed under condition of active interaction with experts; in this case, such an operation proves to be rather labor consuming without computer technologies. Even the initial problem of designing the integrated systems for information protection (ISIP) can be attributed to the weakly formalized problems with incomplete information. Similar tasks include the situations, connected with the recognition of prolonged targeted cyberattacks, which are not distinguished by explicit attributes. Therefore, the subject of the study that addresses the development of models and software (SW) of DSS in the weakly structured and difficult-to-formalize tasks in the provision of OBCP IS appears relevant.

2. Literature review and problem statement

An increase in the number of cyberattacks on MCCS in recent years has generated interest towards the development of efficient SIRCA [1, 2]. A separate direction of studies in this area is the articles about the development of methods, models and SW for DSS [3, 4] and expert systems (ES) [5, 6] in the field of IS.

Papers [7, 8] examined Data Mining technologies in the problems of IS and CS that make it possible to reveal regularities in the evolution of situation, related to the protection of information (PI) at OBCP. The papers examined did not result in practical realization, in the form of applied SW.

Articles [9, 10] analyzed a methodology of intelligent simulation, intended for the analysis and decision making in the insufficiently structured situations of PI. The studies were not implemented in either hardware or software realization.

The tasks of the CS provision at the occurrence of new classes of attacks, which are difficult to formalize and structure, prove to be complicated for the analysis and decision making support related OBCP IS [11]. In this case, qualitative indicators [12] can represent parameters of the OBCP IS state, which is not always expedient.

In the opinion of authors [13, 14], the analysis of MCCS protection and development of the plan to counteract targeted cyberattacks must be preceded by the stage of detecting the basic threats and vulnerabilities. In this case, as indicated by researchers, a task of the formalization of connections between the threats and the OBCP vulnerabilities remains challenging.

An essential shortcoming of articles [15, 16] is the lack of architectural realization of DSS for the tasks of OBCP IS, which are difficult to formalize. As recognized by authors [16], the majority of similar DSS and ES have been at the stage of testing so far.

Papers [17, 18] examined deficiencies of existing DSS and ES in the area of IS. Such deficiencies include the need for the presence of highly qualified experts while compiling a knowledge base (KB) and the field of knowledge (FOK), difficulties in the algorithmization of separate methods and models, impossibility to estimate the effectiveness of specific DSS and others.

Thus, taking into account the discussion in the papers examined, it is obvious that it is necessary to continue research into the practically implemented solutions for DSS in the field of OBCP IS. Similar studies, in particular, should focus on solving complex formalized untypical problems of PI, for example, in the processes of realization of multistage targeted cyberattacks.

3. The aim and tasks of the study

The aim of present work is the development of models and SW for DSS to manage IS, taken in the course of complex formalized untypical situations of realization of multistage targeted cyberattacks on MCCS.

To achieve the set aim, the following tasks were to be solved:

– to devise a model for the description of metaknowledge for DSS about the weakly structured situations, related to the MCCS cyberprotection;

– to develop and test a software program, which realizes the structurization of a complicated situation for IS, and its representation in the form of a set of interfaces that allow the visualization and interpretation of results.

4. Model for describing the metaknowledge in DSS for the provision of cybersecurity

Contemporary MCCS are usually well protected [1, 3, 17]. In order to succeed, those attacking have to switch off or overcome protection in the process of realization of different classes of cyberattacks, Fig. 1. Thus, DSS as part of SIRCA should be designed for the continuous process of updating the knowledge base (KB).

Since the hardware-software complexes, which realize the mechanisms of adaptive cyberprotection (ACP) based on SIRCA and DSS, are still at the stage of creation, a formalized formulation of the problem for their development is formulated as follows. Initial data for such SIRCA are the data, which are contained in KB – REP (or the field of knowledge – FOK):

$$\mathrm{REP} = \langle \mathrm{SYS}, \mathrm{Events}, \mathrm{TAI}, \mathrm{NIS}, \mathrm{gov} \rangle, \qquad (1)$$

where SYS are the data on the OBCP infrastructure (for example, topology, users, tools and the methods of protection and others); Events are the events, registered by SIRCA; TAI are the templates (scripts) [2–4]; NIS are the scripts for countering the attacks; gov are the decision rules at the detection of attacks [6, 17].

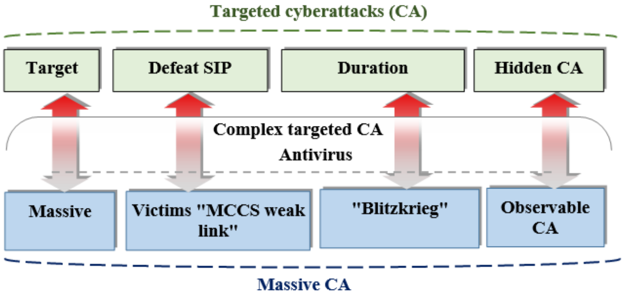


Fig. 1. Interrelation between the types of attacks, which are subject to analysis by the attributes of DSS

The problems, solved by SIRCA, are determined as follows.

Analysis of OBCP protection:

$$\mathrm{IOFP}_j = \mathrm{FS}\ (\mathrm{SYS},\ \mathrm{TAI},\ \mathrm{AT},\ \mathrm{gov}), \qquad (2)$$

where IOFP_j – j is the index of OBCP protection; AT are the events, connected to the violation of IS; FS is the function, determined by the security policy (SP).

Simulation of the transformation of situation in the process of attack realization:

$$\mathrm{ESC}_{cr} = \mathrm{Model}\ (\mathrm{SYS},\ \mathrm{TAI},\ \mathrm{AT},\ \mathrm{gov},\ \mathrm{T}), \qquad (3)$$

where $\mathrm{ESC}_{cr} \subset \mathrm{SYS}$ is the critical element of OBCP; Model is the model of cyberattack in time – T.

Support of decisions to counter attacks, in particular, for the weakly formalized problems of the information protection:

$$\mathrm{CM} = \arg\ \min \left| \mathrm{IOFP} - \mathrm{IOFP}_{rt} \right|, \qquad (4)$$

where $\mathrm{CM} \subset \mathrm{gov}$ are the countermeasures; IOFP, IOFP_{rt} are the current and reference value of OBCP protection, respectively.

A procedure of structurization of the situation, related to the task of supporting a decision for the provision of OBCP IS, is examined in the functional and structural contexts of the concept – the field of knowledge (FOK) of cybersecurity.

A variant of structural approach makes it possible to perform decomposition of the situation. This allows us to analyze the structural-functional relations of its constituent components (se_i). The selection of components (se_i) is realized in the course of interaction between DSS and SIRCA [17]. The result of such an interaction is represented by hierarchical component "Part – Whole", $\langle PA, WH \rangle$, where $PA = \{pa_i\}$ is the whole (set or alphabet (se_i)), WH is the ratio "Part – Whole" on the alphabet $PA, i = 1,...,n$.

For the variant of functional approach, the definition of situation determines the basic estimations of illegitimate interference in the MCCS work. It is accepted for all the components of situation $SI_i = \{si_{ij}\}, j = 1,...,m$ is the set of apexes, AM_i is the adjacency matrix (AM) of the directed graph (DG), which determines for each component (se_i) of the situation (pa_i) its functional structure. Using the experts, we build cognitive maps (COGM) (SI_i, AM_i), which reflect the subjective treatment of regularities in the functioning of OCP element. Next, obtained COGM are grouped (SI, AM), where $SI = \cup SI_i$ is the totality of attributes ("A") that characterize a change in the situation.

In the developed DSS we used a model of representation of the knowledge in the form of sign DG, as well as the field of knowledge (FOK) [19, 20]. FOK is assigned: by input information (factors – X) of the tasks for DSS; by conclusions (output data – Y); by a model (MO) that is used for the transformation of initial data into the conclusion. The model is described by systems SC_{pa}, FS_{si}, which reflect, accordingly, the structure of the situation and the regularities of OBCP SP realization.

COGM (SI, AM) are described in the functional system (FS) of FOK. In the process of COGM description, we applied the scale of informativeness "A" [21, 22]. For the description of COGM we also used methods for the identification of preferences of an expert (or a person who makes decision – DM), who analyzes the scripts of transformation of the situations (pa_i).

Using method [17], we obtained the ordered set $ML_{ij} = \{ml_{ijz}\}$ of linguistic values (LV) of *j*th "A" ith judgment for *z*th number of LV, whose elements are represented in the range [0, 1]. For each "A" judgment, we determined scale X_{ij}. A scale point has linguistic interpretation $ml_{ijz} \in ML_{ij}$.

For the situation when it is necessary to obtain the script of transformation of the situation, the initial data are: a set of factors $SI = \{si_i\}$; scale(s) of factors X_{ij}; the initial state of OBCP prior to the occurrence of analyzed situation $X(t_0)=(x_{11},...,x_{nm})$; AM $AM = |am_{ijsl}|$, where i,s is the number of judgment, j,l is the number of "A" judgment, with numbers $i \vee s$, respectively.

In a general case, it is necessary to determine addition vector "A" (AVA)

$$V(t), V(t+1), ..., V(t+n)$$

and to track a change in the state of OBCP for the input factors of data X(t), (t+1),..., X(t+n) in moments t,...t+n.

For solving the problem, we employed a method of successive iterations, in the course of which AVA was determined from expression

$$V(t+1) = V(t) \circ AM.$$

The state of OBCP in moment t+1 is characterized by equality X(t+1)=X(t)+V(t+1).

Each AM

$$AM = |am_{ijsl}|_{n \times n}$$

for the positive and negative components was transformed under the following conditions:

$$\text{if } am_{ijsl} > 0 \text{ then } am'_{i(2j-1)s(2l-1)} = am_{ijsl}, am'_{i(2j)s(2l)} = am_{ijsl};$$

$$\text{if } am_{ijsl} < 0 \text{ then } am'_{i(2j-1)s(2l-1)} = \\ = -am_{ijsl}, am'_{i(2j)s(2l)} = -am_{ijsl} \qquad (5)$$

to positively determined dual AM

$$AM' = |am'_{ijsl}|_{2n \times 2n}.$$

Consequently, AVA of V(t) and predicted values of attribute(s) V(t+1) have dimensionality 2n, too. In this case, the rules of synthesis of initial AVA V'(t) with dimensionality 2n are satisfied:

$$\text{if } v_{ij}(t) > 0 \text{ then } v'_{i(2j-1)}(t) = v_{ij}(t), v'_{i(2j)}(t) = 0;$$

$$\text{if } v_{ij}(t) < 0 \text{ then } v'_{i(2j)}(t) = v_{ij}(t), v'_{i(2j-1)}(t) = 0. \qquad (6)$$

In vector

$$V'(t) = (v^-_{11}, v^+_{11}, ..., v^-_{nm}, v^+_{nm})$$

the significance "A" si_{ij} is determined by two components with index 2j that characterizes v^+_{ij}, as well as with index $2j-1$, which determines v^-_{ij} addition si_{ij}.

AVA $V'(t+1)$ for positively determined AM AM' is represented as

$$V'(t+1) = V'(t) \circ AM'.$$

As a result of transposition of the AVA component for moments of time

$$V'(t+1), ..., V'(t+n),$$

we obtained block matrix (BM). In the BM, the lines are the addition "A" in moments t, the columns are the addition "A" in the moment of time, which corresponds to column:

$$V^t = \left| V'(t+1)^T, ..., P'(t+n)^T \right|.$$

The obtained matrix V^t is applied in the subsystem for the prediction of transformation of the situation with OBCP IS.

The degree of mismatch of elements FOK – $dis_{ij}(t)$, taking into account papers [17, 21, 22], is determined by expression:

$$dis_{ij}(t) = \frac{|v^+_{ij}(t) - v^-_{ij}(t)|}{v^+_{ij}(t) + v^-_{ij}(t)}, 0 \le v_{ij}(t) \le 1, \qquad (7)$$

where $v^+_{ij}(t)$, $v^-_{ij}(t)$ is the addition of positive and negative "A" in moments t, respectively.

Parameter $dis_{ij}(t)$ characterizes trust of DM in the process of adding $v_{ij}(t)$ for si_{ij}. For $dis_{ij}(t)\approx 1$ (a case when $v_{ij}^{+}(t)>>v_{ij}^{-}(t)$ or $v_{ij}^{-}(t)>>v_{ij}^{+}(t)$), the trust of DM is in the value of attribute $v_{ij}(t)\to\max$. For $dis_{ij}(t)\approx 0$ (a case when $v_{ij}^{+}(t)\approx v_{ij}^{-}(t)$), the value is $v_{ij}(t)\to\min$.

Tracking dynamics in the transformation of situation, while realization of illegitimate actions by the criminal in moments $X(t),...,X(t+n)$, is expressed in DSS in the process of transformation by term:

$$\left\langle v_{ijk}(t+1), dis_{ij}(t+1)\right\rangle,$$

$$v_{ij}(t+1)=$$

$$=\operatorname{sgn}\left(v_{ij}^{+}(t+1)-v_{ij}^{-}(t+1)\right)\max\left(v_{ij}^{+}(t+1),v_{ij}^{-}(t+1)\right). \qquad (8)$$

It is accepted that if inequality

$$v_{ij}^{+}(t+1)>v_{ij}^{-}(t+1)$$

is valid, then the sign $v_{ij}(t+1)$ is positive. If inequality

$$v_{ij}^{+}(t+1)<v_{ij}^{-}(t+1)$$

is valid, the sign is negative. Consequently, the transformation of situation in the course of prediction will be determined by tuple:

$$\left\langle X(t+1), DIS(t+1)\right\rangle, \qquad (9)$$

where

$$x_{ij}(t+1)=x_{ij}(t)+v_{ij}(t+1);\ \ dis_{ij}(t+1)\in DIS(t+1).$$

In the developed DSS, the transformation of situation is represented by matrix

$$X^{t}=\left|X(t+1)^{T},...,X(t+n)^{T}\right|.$$

Matrix X^{t} is used for the visual representation of the results, generated in the course of searching for solutions.

Solution of inverse problem (INPR) forms recommendations for DM that make it possible to transform current situation into the targeted state of OBCP. In this case, in the subsystem for the search for conclusions (SSC), we used transitive closure AM^{*} of the doubled adjacency matrix $AM'=\left|am'_{ijsl}\right|$.

In SSC, in particular when AM^{*} and target vector $P=(p_{1},...,p_{n})$, are assigned, the sets of input actions vectors are determined – $\Psi=\{D\}$. It is accepted that for all $D\in\Psi$, expression $D\circ AM^{*}=P$ is realized.

Variants of the INPR solution for D_{max} and D_{min} are presented in papers [21, 22]. Controlling influences D_{i}, a "A" s_{ij} are set by parameters v_{ij} and d_{isij}, that is,

$$D=\left(v_{11},dis_{11},...,v_{nm},dis_{nm}\right).$$

Parameters dis_{ij} and v_{ij} in DSS are determined using ratios (7) and (8), respectively.

The current state of FOK FS is determined by tuple: $\langle SI, X, X(0), AM\rangle$.

A conceptual system (CS) of FOK as a part of DSS makes it possible to conduct structural-functional decomposition of situation $\langle PA, WH\rangle$. Furthermore, it is used in the processes of interpretation of conclusions related to the scripts of transformation of the OBCP state, for example, in the course of realization of targeted cyberattacks.

Components of the situation are determined by the following parameters:

$$\left\langle pa_{i}, SI(pa_{i}), CV(pa_{i})\right\rangle,$$

where pa_{i} is the identifier of concept (judgment); $SI(pa_{i})$ is the intension of concept

$$\left(SI_{i}=\left\{si_{ij}\right\}, SI(pa_{i})=(x_{11},...,x_{nm})\right);$$

$CV(pa_{i})$ is the scope of the concept (component of the situation, described in the model).

Concept pa_{i} in DSS is mapped in space by a point with coordinates of "A" values. A feature space of attributes of the concepts is formed by the Cartesian product of scales of all "A" – $U(pa_{i})$.

In the CS model, CS the identifiers of concepts $pa_{i}\in PA$ are represented in the notional (semantic [23]) space $U(pa_{i})$. CS makes it possible to determine a set of semantic spaces $U(PA)=\left\{U(pa_{1}),...,U(pa_{n})\right\}$, and hierarchical component WH. Thus, the pair of concepts $U(pa_{i})$ and $U(pa_{q})$ is bound by relation WH.

For DSS, we performed structurization of the semantic space of concepts pa_{i} in the format of representative clusters CL^{i} of cybersecurity [24]. Clusters and concepts are conjugated by relations "Classes – Sub-classes".

It is accepted in DSS that pa_{i}^{1} represents class pa_{i}^{2}, if conditions

$$\left(SI\left(pa_{i}^{1}\right)\subset SI\left(pa_{i}^{2}\right)\right)\ \text{and}\ \left(CV\left(pa_{i}^{1}\right)\supset CV\left(pa_{i}^{2}\right)\right)$$

are satisfied.

Conceptual clusters (CCL) in the semantic space of IS are defined in the interpretation of basic (or supporting) concepts pa_{i}^{B} (BC). BC determine the class of objects, analyzed with the aid of SIRCA and DSS, (for example, the class of attack), and the category of situation to which element *pa* is related.

The interval of values

$$X_{ij}^{B}=\left[x_{ijb},x_{ijc}\right],\ x_{ij}\in X_{ij}^{B},\ \forall j$$

is established by expert evaluation, which assigns the boundaries of classes of the objects, examined by SIRCA and DSS.

Within the framework of notional (semantic) concepts of IS, which belong in the space of SP terms, that is, $U(pa^{o})\subseteq U(cv^{0})$, there are domains of permissible semantic values $U(pa^{o})$ for "A" si_{ij}, for example, vulnerabilities are detected, partially detected, not detected, etc.

BC is determined by parameters:

$$\left(pa_{i}^{B}, SI\left(pa_{i}^{B}\right), CV\left(pa_{i}^{B}\right)\right),$$

where pa_{i}^{B} is the identifier of BC; $SI\left(pa_{i}^{B}\right)$ is the intension of BC; $CV\left(pa_{i}^{B}\right)$ is the scope of BC. The scope of BC can be represented as a set of SP objects, for which values of "A" relate to the permissible. The permissible values, from the point of view of the analyst of information security (AIS), belong in the domain of permissible parameters of BC $AC(pa_{i}^{B})$.

A procedure of BC generalization is realized by removing repetitive “A” or their combinations.

It is accepted that BC for IS possess for m a number of abstractions – $A=2^m-1$. Universalized BC are categorized by parameters

$$\left(pa_i^{Ba}, SI\left(pa_i^{Ba}\right), CV\left(pa_i^{Ba}\right)\right),$$

where a=1,...,A.

It is accepted that the values of BC are implemented into permissible values of the generalized concepts of IS alphabet. Thus, $AC\left(pa_i^B\right)\subset AC\left(pa_i^{Ba}\right)$ and $CV\left(pa_i^B\right)\subset CV\left(pa_i^{Ba}\right)$.

An intention of BC and its abstractions forms a partially ordered set

$$\left\{SI\left(pa_i^B\right),SI\left(pa_i^{B1}\right),...,SI\left(pa_i^{BA}\right)\right\}.$$

The formed set is a conceptual cluster of BC – PA^i. The formed CCL make it possible to structure semantic space of CS. In the clusters, we determine transitions from BC pa_i^B to those generalized pa_i^{Ba}. In CS, the transitions are assigned by the tuple of vectors:

$$\left\langle CN(t),CC(t),SV(t)\right\rangle, \qquad (10)$$

where

$$CN(t)=\left(pa_1^{Ba},...,pa_n^{Ba}\right)$$

are the identifiers of concepts within the framework of description of the situations;

$$CC(t)=\left(SI\left(pa_1^{Ba}\right),...,SI\left(pa_n^{Ba}\right)\right)$$

are the intentions of CS

$$pa_i^{Ba}\in CN(t);\ SV(t)=\left(CV\left(pa_1^{Ba}\right),...,CV\left(pa_n^{Ba}\right)\right)$$

are the scopes of concepts $pa_i^{Ba}\in CN(t), \forall i$.

In the process of DSS operation, we determined rules for the CS transformation:

1) if, when predicting results of the course of a cyberattack, value of “A” concept exceeded the limits, permitted by BC, a new concept is formed;

2) new concepts generalize initial BC according to the attributes whose values deviate from those permitted.

The rules are formally represented as the reflection of FS state X(T) into the state of CS, that is,

$$\left\langle CN(t),CC(t),SV(t)\right\rangle,$$
$$UM: X(t)\rightarrow\left(CN(t),CC(t),SV(t)\right), \qquad (11)$$

where $UM=\left(UM_i\right)$ is the vector of rules of BC transformation pa_i^B into generalized $pa_i^{Ba}, \forall i$.

Expression (11) provides DM with the possibility to interpret and generalize IS concepts, characterized by the set “A”.

Thus, taking into account (11), a model for the representation of FOK is determined by tuple:

$$\left\langle SC_{pa}, FS_{si}, UM\right\rangle, \qquad (12)$$

where SC_{pa} – FOK CS, FS_{si} – FOK FS,

$$\left\langle U(PA), WH, PA^i, \left(CN(t), CC(t), SV(t)\right)\right\rangle.$$

A problem on searching for conclusion and obtaining the solution is reduced to the development of strategy for the transformation of situation from the current state of IS to the targeted one. Thus, the INPR is solved. In the course of solving,

$$X(0)=\left(x_{11}^0,...,x_{nm}^0\right) \text{ and } X^P=\left(x_{11}^p,...,x_{nm}^p\right)$$

of FOK are determined. Next, target addition vector

$$P=\left(v_{1j},...,v_{nm}\right)$$

is determined, where

$$v_{11}=x_{11}^p-x_{11}^0,\ v_{12}=x_{12}^p-x_{12}^0$$

and so on. The target vector indicates the direction and magnitude of changes in “A” attack from initial X(0) of OBCP into the targeted X^P state. Controlling resources of SPI for MCCS are determined as:

$$V^R=\left(v_{11}^r,...,v_{nm}^r\right).$$

A set of conclusions $D=\left\{D_1,...D_{cv}\right\}$ is formed while solving INPR, that is, when changing the situation, which arose when a cyberattack was realized, from the current state into the targeted one.

In a number of situations, there are the precedents possible when there is no any solution. However, by changing the structure of cognitive model of the situation, it is possible to find a solution by using heuristic approach, in particular, by engaging experts on IS.

The search for solutions includes the following stages:

– generation of conclusions;

– structurization of conclusions for the functional mapping;

– structurization of conclusions in the conceptual format.

The generation of conclusions is carried out when solving the INPR for the appropriate control circuits of IS. As a result, we obtain a set of solutions $\left\{D_1,...,D_{cv}\right\}$, which form a vector of controlling influences (VCI). VCI corresponds to AVA, taking into account cognitive consonance (c) [25], that is, $\left(v_{11},c_{11},...,v_{nm},c_{nm}\right)$. Thus, each conclusion $D_{cv}\in D$, is assigned with the corresponding state of OCP after a change in the situation in the functional mapping of FOK

$$X_{cc}=\left(x_{11}^0+v_{11},...,x_{nj}^0+v_{nj}\right).$$

For the structurization of conclusions of functional mapping, the following criteria were applied: realizability of the solution within the framework of existing SPI; conflictness of the solution.

In a DSS, decision that was made

$$D_{cc}=\left(v_{11},c_{11},...,v_{nm},c_{nm}\right)$$

can be realized, if

$$\forall v_{ij}\in D_{cc}\ \ \&\ \ v_{ij}\le v_{ij}^r,\ v_{ijk}^r\in V^R=\left(v_{1j}^r,...,v_{nj}^r\right).$$

A criterion of realizability, when applied to {D}, allowed us to divide conclusions into the subsets of realizable D^R and non-realizable D^N decisions.

Component of decision D_{cv} is assigned by parameters v_{ij} and c_{ij}. In papers [22, 25], the level of consonance in the problems of decision making about IS is assigned in the range c_{ij}=0.5–0.65. Values below c_{ij}<0,5 for making decisions D_{cv} are considered to be conflicting [25].

The model of knowledge representation (expression (12) realizes the structurization of conclusions in the conceptual format. We shall assume that the dynamics of transformation of the situation X_{cv} corresponds to each conclusion $D_{cv} \in D$. This is represented by the structure of CS, that is,

$$UM: X_{cv} \to \left(CN_{cv}, CC_{cv}, SV_{cv}\right).$$

Therefore, the set of conclusions of CS corresponds to the set of decisions D in FS, that is,

$$\Delta = \left\{D_{pa1}, \ldots, D_{pacv}\right\},$$

where $D_{pacv} = \left(CN_{cv}, CC_{cv}, SV_{cv}\right)$ is the state of DSS CS.

It is accepted that in the semantic space of CS, the coordinates of points, which determine acceptable characteristics of BC, are assigned by the state of situation X_{cv} and by decisions D_{cv}. It is possible that several values of BC and the solutions that correspond to them enter the domain, permitted by DM, at the same time. In this case, the combination of different decisions $D_{cv} \in D.$ is possible. Consequently, in the DSS CS, classes D_{pa}^{q} are formed. The class of the decision is characterized by tuple

$$D_{pa}^{e} = \left\langle CN^{q}, CC^{q}, SV^{q} \right\rangle,$$

where Q is the number of classes in CS. The content of classes $\left\{CC^{1}, \ldots, CC^{Q}\right\}$ is formed by the conceptual graph of decisions (GD), Fig. 2, Table 1.

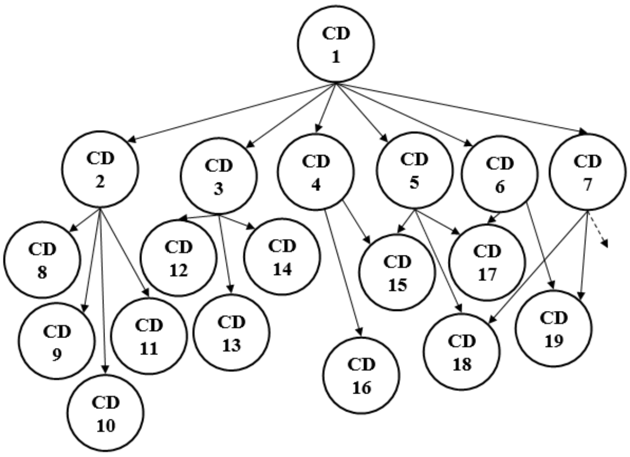


Fig. 2. Conceptual graph of decisions

Root apex of GD (level 0, L0) contains conclusions $D_v \in D$, in which none of the attributes ("A") exceeds the limits, set by BC for OBCP IS. At L1 are decisions D_v, in which not more than one "A" exceeded the limits of SP domain. At L2 are decisions D_v, in which not more than two "A" exceeded the limits of SP domain. The conclusions of L2 generalize conclusions of L1 by "A", and so on. For the situation when values of "A" exceed the limits, established by SP, a new class of objects is determined, with the structure and variants of actions different from basic SP [4, 6, 17].

The search for structural solutions includes the following stages:

– evaluation of alternative decisions;
– assessment of prospects;
– formation of decision.

A conclusion on prospects of the variant of actions starts from the root apex of DG. DM should be aware of the situation, abstracting from "A", by which the generalization is conducted.

The formation of conclusion is performed based on the estimation of alternatives of separate decisions. The estimation is carried out during the introduction of structural transformations to the situation model $\left\langle SI, X\, X(0)\, AM \right\rangle$ and subsequent solution of INPR for structure $\left\langle SI^{*}, X^{*}\, X(0)\, AM^{*} \right\rangle$.

Table 1

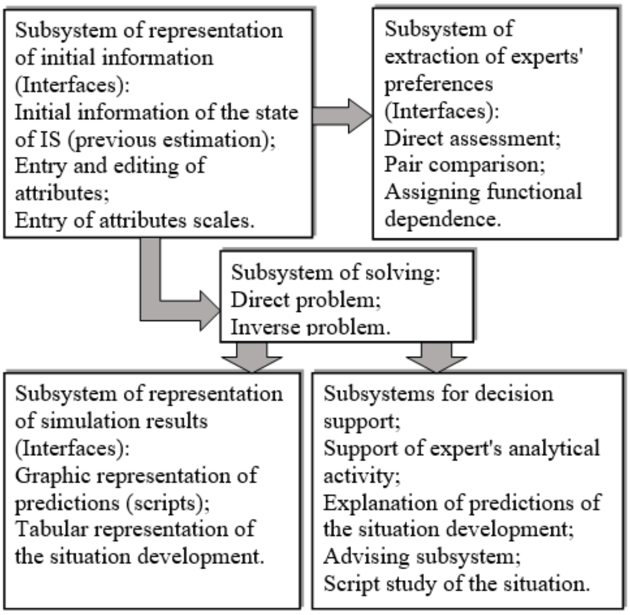
Designation of the class of decision (CD)

Transition in the graph of decisions	Number of «A»	Content of classes in «A» codes (attribute)
CD 1 – CD 2	si_{11}	111–11111–11–1111→011–11111–11–1111
CD 1 – CD 3	si_{12}	111–11111–11–1111→101–11111–11–1111
CD 1 – CD 4	si_{14}	111–11111–11–1111→110–11111–11–1111
CD 1 – CD 5	si_{23}	111–11111–11–1111→111–11011–11–1111
CD 1 – CD 6	si_{24}	111–11111–11–1111→111–11101–11–1111
CD 1 – CD 7	si_{25}	111–11111–11–1111→111–11110–11–1111
CD 2 – CD 8	si_{12}	011–11111–11–1111→001–11111–11–1111
CD 2 – CD 9	si_{23}	011–11111–11–1111→011–11011–11–1111
CD 2 – CD 10	si_{24}	011–11111–11–1111→011–11101–11–1111
CD 2 – CD 11	si_{25}	011–11111–11–1111→011–11110–11–1111
CD 3 – CD 12	si_{23}	101–11111–11–1111→101–11011–11–1111
CD 3 – CD 13	si_{24}	101–11111–11–1111→101–11101–11–1111
CD 3 – CD 14	si_{25}	101–11111–11–1111→101–11110–11–1111
CD 4 – CD 15	si_{24}	110–11111–11–1111→110–11011–11–1111
CD 4 – CD 16	si_{24}	110–11111–11–1111→110–11101–11–1111
CD 5 – CD 15	si_{13}	111–11011–11–1111→110–11011–11–1111
CD 5 – CD 17	si_{23}	111–11011–11–1111→111–11001–11–1111
CD 5 – CD 18	si_{13}	111–11011–11–1111→111–11010–11–1111
CD 6 – CD 17	si_{23}	111–11101–11–1111→111–11001–11–1111
CD 6 – CD 19	si_{24}	111–11101–11–1111→111–11100–11–1111
CD 7 – CD 18	si_{25}	111–11110–11–1111→111–11011–11–1111
CD 7 – CD 19	si_{24}	111–11110–11–1111→111–11100–11–1111
...	...	...
CD N ..	...	...

As a result, after the synthesis of conclusion, we shall obtain subset $D^{*} = \left\{D_{1}^{*}, \ldots, D_{a}^{*}\right\}$. The conclusion is accepted if there is at least one decision $D_{a}^{*} \in D^{R^{*}}$ that is more preferable than $D_{a} \in D^{R}$, which were obtained while solving the INPR for the initial configuration of situation with OBCP IS.

5. Program realization of the decision support system

DSS is realized in the programming environment Rad Studio XE. User interfaces include the modules, which realize the operation of subsystems, demonstrated in Fig. 3. The methods employed in DSS, as well as models and algorithms, were described in papers [17, 22, 24].



Subsystem of representation of initial information (Interfaces): Initial information of the state of IS (previous estimation); Entry and editing of attributes; Entry of attributes scales.

Subsystem of extraction of experts' preferences (Interfaces): Direct assessment; Pair comparison; Assigning functional dependence.

Subsystem of solving: Direct problem; Inverse problem.

Subsystem of representation of simulation results (Interfaces): Graphic representation of predictions (scripts); Tabular representation of the situation development.

Subsystems for decision support; Support of expert's analytical activity; Explanation of predictions of the situation development; Advising subsystem; Script study of the situation.

Fig. 3. Subsystems and user interfaces of DSS

Interface for the formation of initial information is intended for setting "A", which reflect the situation, as well as the corresponding scale of estimating "A". A visualization of the transformation of the situation is represented in the form of sign DG (SI, AM), Fig. 4. Dark blue color denotes edges of DG, structurizing the fragments of the situation "Part – Whole", red color denotes fragments of the situation "Class – Sub–class".

A subsystem of DM preferences provides the possibility to reveal the degree of influence of each of "A" of anomalies or cyberattacks on other factors of IS. As the initial data, we used scale of informativeness "A" ML_{ij} [17, 24]. Furthermore, DSS analyzes current values ml_{ijk}, obtained based on DG (SI, AM).

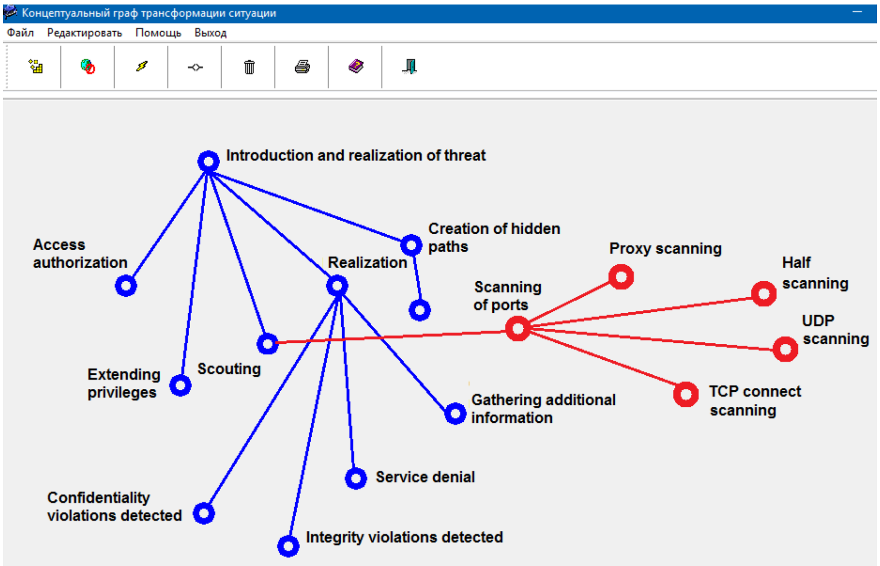


Fig. 4. Form of DSS for the visualization of transformation of the situation

If the variant of direct evaluation is selected, then degree of influence of "A" of cyberattack on the indicators of IS was calculated as follows: $am_{ijsl} = v^{c}_{ij} / v^{r}_{sl}$, where v^{c}_{ij}, v^{r}_{sl} is the addition of "A" characteristics of reason ("RE") and consequence ("CO"), respectively; i,s is the number of concept, j, l is the number of "A".

Fig. 5 shows a form for the interpretation of results of simulation of the indicator, which determines the degree of influence of the attributes of cyberattack on the current estimation of OCP IS. The form includes components that make it possible to formulate a question for an expert in the natural language, as well as components for changing the values of attributes of cyberattack in the context of bond of cause-effect ("RE-CO") and the degree of fuzziness in the answers.

If AIS considers it appropriate to conduct a paired comparison of the informativeness of attributes of cyberattack, for example, in the situation, which requires the refinement of attributes-reasons si_{tl}, si_{sd} and their influence on the bond of attribute-consequence ("A– CO"), the rank scale is used [5, 8, 24]. A degree of influence of "A" of the attack on the indicators of OBCS IS was determined as follows:

$$am_{ij\,tl} = am_{ij\,sd} \cdot \left(\beta_{tl} / \beta_{sd} \right),$$

where β is the parameter that describes a degree of influence of the bond "A-RE" on "RE-CO".

In the situation when the contradictions are revealed while estimating IS, the module of correction is activated, which makes it possible to react in real time to the occurring errors in the assessment of state of the MCCS cyberprotection. DSS implies both manual and automated correction of the situation, for example, when an expert's estimation does not coincide with the estimation of the level of DSS IS and SIRCA. When corrected manually, an expert may change his choice, assigned at the previous step of paired estimation. A heuristic algorithm is employed during automated correction [3, 5].

In the situation when quantitative characteristics of the bonds "A-RE" and "A-CO" are known, as well as functional correlations of "RE-CO" on the set "A-RE", DM may use a mode of functional dependence.

It is accepted:

$$si_{ij} = \Theta\left(si_{tl}, si_{sd}, \ldots, si_{ze}\right)$$

and

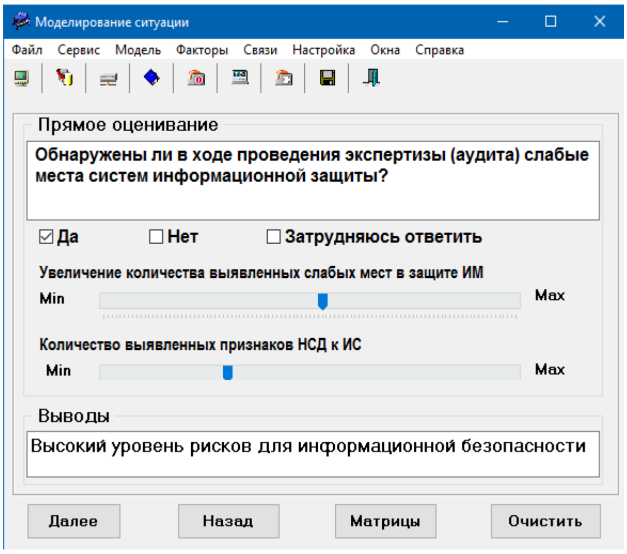
$$x^{0}_{ij} = \Theta\left(x^{0}_{tl}, x^{0}_{sd}, \ldots, x^{0}_{ze}\right).$$

The force of influence of factors on IS is determined as sensitivity index for each of the arguments:

$$am_{tlij} = \frac{\left(x^{0}_{ij} - \Theta\left(x^{0}_{tl} + x^{0}_{tl} \cdot \lambda, x^{0}_{sd}, \ldots, x^{0}_{ze}\right)\right)}{\left(\lambda \cdot x^{0}_{tl}\right)},$$

$$am_{sdij} = \frac{\left(x^{0}_{ij} - \Theta\left(x^{0}_{tl}, x^{0}_{sd} + x^{0}_{sd} \cdot \lambda, \ldots, x^{0}_{ze}\right)\right)}{\left(\lambda \cdot x^{0}_{sd}\right)},$$

where $0 < \lambda < 1$.



Прямое оценивание

Обнаружены ли в ходе проведения экспертизы (аудита) слабые места систем информационной защиты?

☑ Да □ Нет □ Затрудняюсь ответить

Увеличение количества выявленных слабых мест в защите ИМ

Min Max

Количество выявленных признаков НСД к ИС

Min Max

Выводы

Высокий уровень рисков для информационной безопасности

Fig. 5. Form for the interpretation of results of simulation

DSS contains interfaces that ensure:
– entry of DM preferences;
– determining the force of influence of attributes;
– detection of export errors.

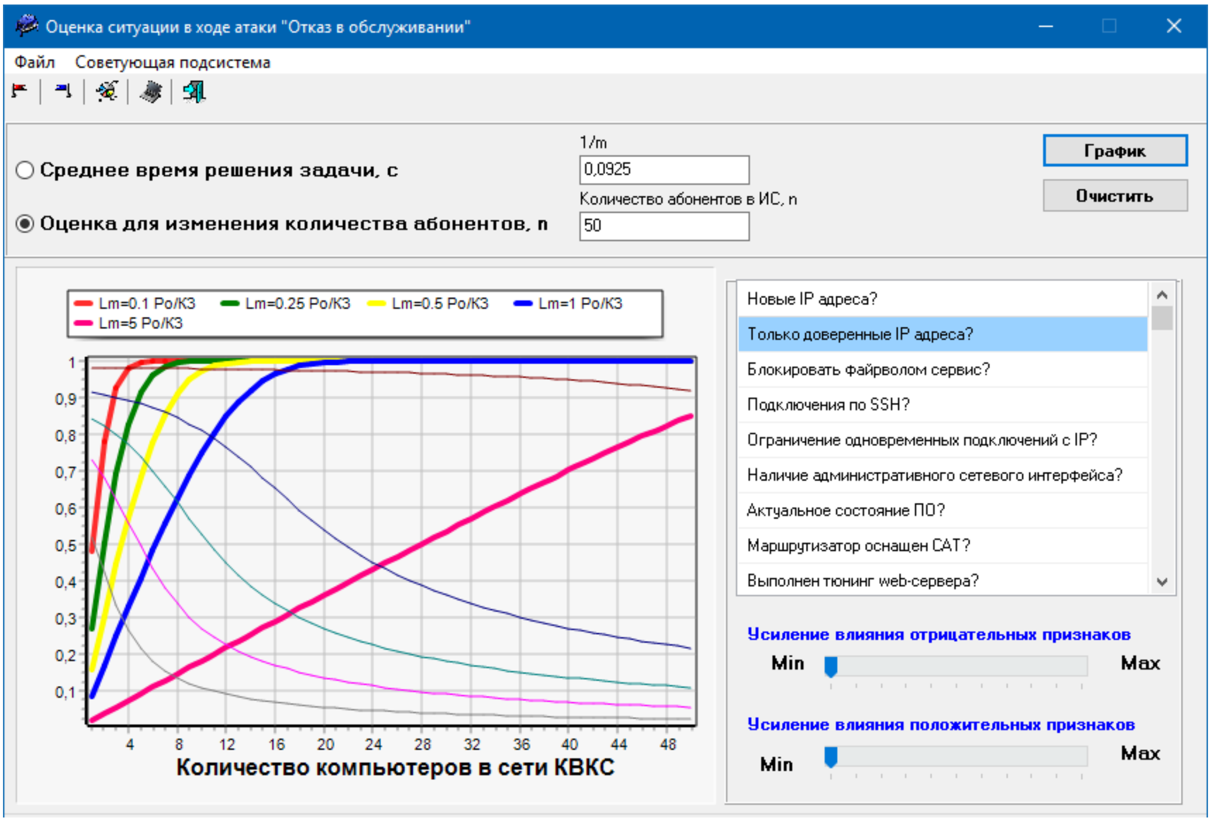
Results of operation of the module for predicting the transformation of situation are represented by two-dimensional arrays. The first one contains data on additions V^t. The second one reflects the changes in states of IS X^t. The described arrays are used by the subsystems of representation of the results of simulation, as well as in the process of supporting the decisions of DM.

The forms, shown in Fig. 6–8, visualize summarized results obtained in the process of simulation. The forms contain tables with parameters of increments from ml^{0}_{ijk} to ml^{v}_{ijk}. The forms also reflect the charts of dynamics in the transformation of values of attributes si_{ij}. For example, Fig. 6 shows a chart of the change in situation in the course of assessing the development of DDoS attack on the resources of MCCS. The charts in Fig. 6 demonstrate results of evaluating the probability of service denial for several scripts of development of the situation in the course of DDoS attack. Additional option of DSS is the capability of generating a report that contains "RE-CO" diagrams. The diagrams reflect the changes that CS undergoes in the course of realization of different classes of attacks. The algorithm of diagrams formation is based on the isolation of zone with the registered max increments in the values of si_{ij} for matrix V^t. Thus, a fragment of maximum additions si_{ij} creates causal connections, which make it possible for DM to interpret the transformations of bond "RE-CO", Fig. 7.

Fig. 8 shows an example of the interface of subsystem for the simulation of situation for the script of MCCS network virus infection. The form contains a digital indicator, which provides for the convenient format of representation of probabilistic parameters of the situation assessment based on an analysis of existing "A".

Intelligent support of DM decisions is provided by "Advising subsystem", Fig. 9.

In this case, DM is given a possibility, based on own knowledge and experience, to select governing "A" from the set of data, obtained while solving INPR. In the course of evaluating IS strategy, the search for solution D_v is realized by the iterative process, which consists in the successive determining the elements of decision vector. Such an iterative search allows DM to form a set of variants of alternative decisions.



○ Среднее время решения задачи, с

● Оценка для изменения количества абонентов, n

1/m 0,0925

Количество абонентов в ИС, n 50

Новые IP адреса?
Только доверенные IP адреса?
Блокировать файрволом сервис?
Подключения по SSH?
Ограничение одновременных подключений с IP?
Наличие административного сетевого интерфейса?
Актуальное состояние ПО?
Маршрутизатор оснащен CAT?
Выполнен тюнинг web-сервера?

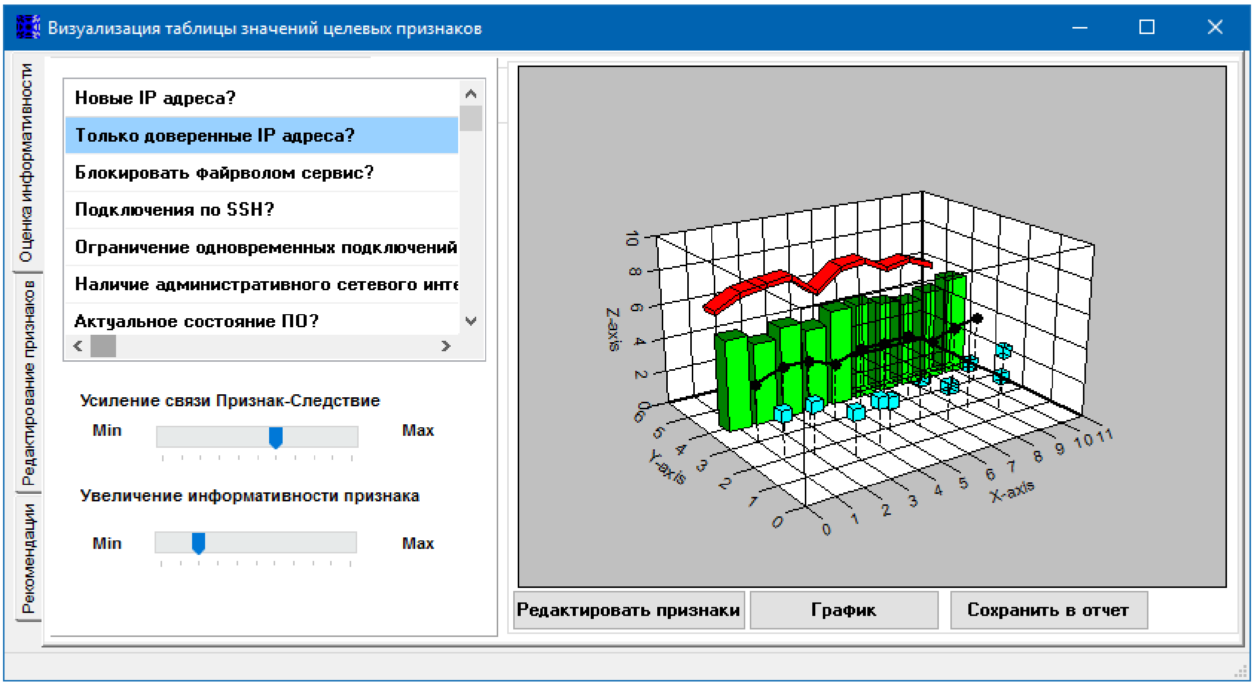
Усиление влияния отрицательных признаков

Min Max

Усиление влияния положительных признаков

Min Max

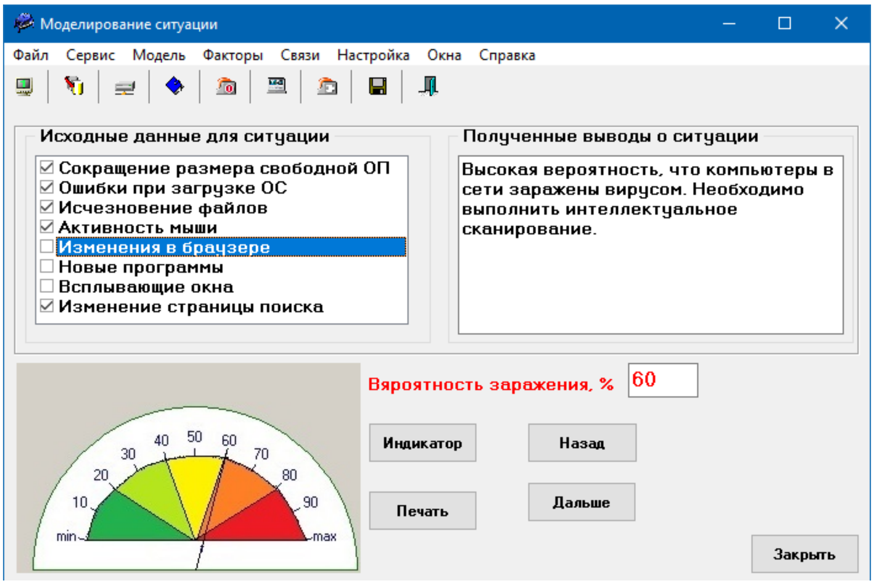
Fig. 6. Form for evaluating the transformation of situation at a change in the attributes



Визуализация таблицы значений целевых признаков

Новые IP адреса?
Только доверенные IP адреса?
Блокировать файрволом сервис?
Подключения по SSH?
Ограничение одновременных подключений
Наличие административного сетевого инте
Актуальное состояние ПО?

Fig. 7. Form for the visualization of tables of values of target attributes for the transformation of bond “RE-CO”



Моделирование ситуации

Исходные данные для ситуации

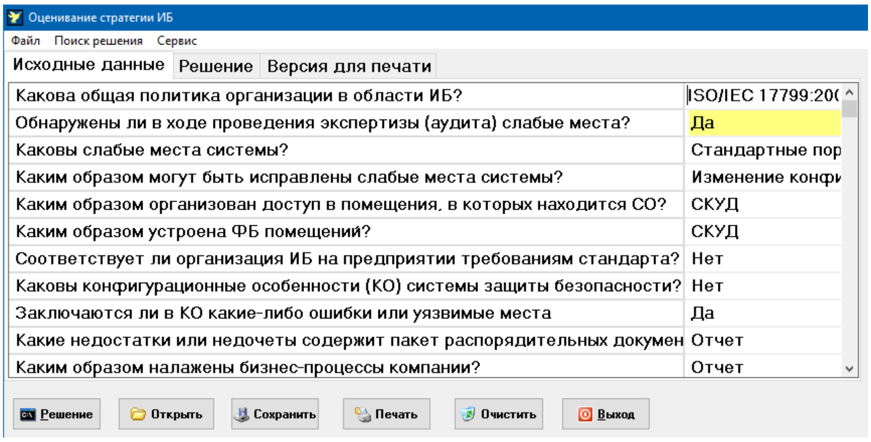
☑ Сокращение размера свободной ОП
☑ Ошибки при загрузке ОС
☑ Исчезновение файлов
☑ Активность мыши
□ Изменения в браузере
□ Новые программы
□ Всплывающие окна
☑ Изменение страницы поиска

Полученные выводы о ситуации

Высокая вероятность, что компьютеры в сети заражены вирусом. Необходимо выполнить интеллектуальное сканирование.

Вяроятность заражения, % 60

Fig. 8. Example of a form for the subsystem of situation simulation in case of MCCS network virus infection



Оценивание стратегии ИБ

Какова общая политика организации в области ИБ?	ISO/IEC 17799:20(
Обнаружены ли в ходе проведения экспертизы (аудита) слабые места?	Да
Каковы слабые места системы?	Стандартные пор
Каким образом могут быть исправлены слабые места системы?	Изменение конфи
Каким образом организован доступ в помещения, в которых находится СО?	СКУД
Каким образом устроена ФБ помещений?	СКУД
Соответствует ли организация ИБ на предприятии требованиям стандарта?	Нет
Каковы конфигурационные особенности (КО) системы защиты безопасности?	Нет
Заключаются ли в КО какие-либо ошибки или уязвимые места	Да
Какие недостатки или недочеты содержит пакет распорядительных докумен	Отчет
Каким образом налажены бизнес-процессы компании?	Отчет

Fig. 9. Form of “Advising subsystem” when assessing strategies for the provision of IS

The form contains components for the visualization of table of values of target "A". The form also contains a list of controlling "A" and a diagram that reflects the results of applying the actions, initiated by DM.

The interfaces of analyses of different scripts of the transformation of situation enable comparison of the results, in this case providing DM with convenient tabular or graphic variant of conclusions representation.

6. Results of testing the DSS

The testing of DSS "Decision Support System of Management protection of information – DMSSCIS" was carried out for MCCS of several transportation enterprises, the cities of Alma Ata, Astana (Republic of Kazakhstan), Kiev and Dnepr (Ukraine).

In the course of testing, we analyzed possibilities of supporting the decisions related to the probabilities of realization of actions by the intruder, who realizes cyberattacks on MCCS, Table 2. It was established that the application of DSS made it possible to reduce the predicted value of risk of overcoming IS contours by 5.5–6 %.

Table 2

Results of testing the DSS

Types of attacks	Parameters of information environment / Variants of AIS and DSS reaction			
	Adopted designations: AC is the number of anomalous network incidents; AH is the number of anomalous incidents at host, AP is the number of anomalous incidents along the perimeters of MCCS SPI, P_a is the probability of cyberattack			
Attack through the illegitimate connection to the Wi-Fi network of the enterprise	AN=3, AP=3, P_a=0,678	AN=3, AP=3, P_a=0,82	AN=1, AP=2, P_a=0,4	AN=1, AP=1, P_a=0,3
	U2R	R2L	DOS/DDoS	Probe
	Blocking the access to service in the network / Blocking the access and restriction of attempts to connect to the network	Blocking to the network / Blocking the access and restriction of attempts to connect to the network	Reconfiguration of IS services for the purpose of blocking IP / Reconfiguration of IS services	Sending a warning to the IP-address / Reconfiguration of IS services IS for the purpose of blocking IP
	Mean time of the situation assessment (IS dept. staffer with or without DSS), min.			
	(15–20)/(7–10)			
Remote attack through the perimeter of the information protection system of the enterprise	AN=3, AH=4, AP=2, P_a=0,74	AN=3, AH=4, AP=2, P_a=0,82	AN=1, AH=1, AP=1, P_a=0,24	AN=1, P_a=0,08
	Blocking the access to service in the network	Restriction of attempts to connect to the network	Reconfiguration of IS services IS for the purpose of blocking IP	Break-up of connection and sending a warning to the IP-address
	Mean time of the situation assessment (IS dept. staffer with or without DSS), min.			
	(12–18)/(7–9)			

It was established in the process of testing that the realization of DSS "DMSSCIS" makes it possible to ensure an increase in the level of automation and centralization of the OBCP protection monitoring, as well as reduce the time required to inform persons, responsible for the information security, about the incidents by 6.9–7.2 times.

7. Discussion of results of DSS testing and prospects for further studies

DSS "DMSSCIS" has the following advantages when compared to the similar systems, which were previously used for the tasks of supporting AIS decisions at the analyzed enterprises.

First, the DSS provides DM with a convenient format for mapping the changes that OBCP IS undergoes in the course of realization of different classes of attacks. Second, the DSS enables intelligent support for the AIS decisions and the possibility to form alternative variants of decisions to counter attacks.

A specific shortcoming of the DSS is the fact that at the initial stage of operation, each MCCS – OBCP requires manual introduction of initial rules that describe conceptual clusters of IS.

Conducted research is the continuation of studies that were previously carried out by the International Kazakh-Turkish University named after H. A. Yassavi (Kazakhstan), by the European University and by the National Aviation University (Ukraine). Further development of research might be directed at improving the interaction of traditional mechanisms of OBCP IS, which, in particular, process primary information, and the DSS modules for decision making in the weakly formalized problems on the provision of cybersecurity.

As a whole, the studies conducted confirmed effectiveness of the proposed models and DSS program package for improving the level of protection of the examined enterprises.

8. Conclusions

We devised a model for describing in the conceptual and functional aspect the process of formation and application of DSS KB for the circumstances related to the detection of specific hard-to-explain attributes of anomalies and attacks, which makes it possible to improve understanding of the analyzed processes of MCCS cyberprotection.

We designed and tested the DSS "DMSSCIS" software package that realizes the structurization of complex situation for MCCS IS. DSS "DMSSCIS" makes it possible to visualize and interpret results of the current assessment of the revealed hard-to-explain attributes of anomalies and cyberattacks, as well as, based on a cognitive model, describe current situation in the course of realization of a multistage targeted cyberattack. It was established that the application of DSS "DMSSCIS" in combination with other systems for the intelligent recognition of illegitimate interference in the MCCS operation allows an increase in the quality of decisions in the field of cybersecurity.

References

1. Petit, J. Potential Cyberattacks on Automated Vehicles [Text] / J. Petit, S. E. Shladover // IEEE Transactions on Intelligent Transportation Systems. – 2015. – P. 546–556. doi: 10.1109/tits.2014.2342271
2. Miao, F. Coding Schemes for Securing Cyber-Physical Systems Against Stealthy Data Injection Attacks [Text] / F. Miao, Q. Zhu, M. Pajic, G. J. Pappas // IEEE Transactions on Control of Network Systems. – 2016. – P. 1. doi: 10.1109/tcns.2016.2573039
3. Sawik, T. Selection of optimal countermeasure portfolio in it security planning [Text] / T. Sawik // Decision Support Systems. – 2013. – Vol. 55, Issue 1. – P. 156–164. doi: 10.1016/j.dss.2013.01.001
4. Fielder, A. Decision support approaches for cyber security investment [Text] / A. Fielder, E. Panaousis, P. Malacaria, C. Hankin, F. Smeraldi // Decision Support Systems. – 2016. – Vol. 86. – p. 13–23. doi: 10.1016/j.dss.2016.02.012
5. Atymtayeva, L. Building a Knowledge Base for Expert System in Information Security [Text] / L. Atymtayeva, K. Kozhakhmet, G. Bortsova // Chapter Soft Computing in Artificial Intelligence of the series Advances in Intelligent Systems and Computing. – 2014. – Vol. 270. – p. 57–76. doi: 10.1007/978-3-319-05515-2_7
6. Gamal, M. M. A Security Analysis Framework Powered by an Expert System [Text] / M. M. Gamal, B. Hasan, A. F. Hegazy // International Journal of Computer Science and Security (IJCSS). – 2011. – vol. 4, Issue 6. – p. 505–527.
7. Dua, S. Data Mining and Machine Learning in Cybersecurity [Text] / S. Dua, X. Du. – UK, CRC press, 2016. – 225 p. doi: 10.1201/b10867
8. Buczak, A. L. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection [Text] / A. L. Buczak, E. Guven // IEEE Communications Surveys & Tutorials. – 2016. – Vol. 18, Issue 2. – p. 1153–1176. doi: 10.1109/comst.2015.2494502
9. Larionov, I. P. Problemy sozdaniya i osnovnye zadachi ekspertnoy sistemy podderzhki proektirovaniya kompleksnoy sistemy zashchity informatsii [Text] / I. P. Larionov, P. B. Khorev // Internet-zhurnal «NAUKOVYEDYENIYE». – 2016. – Vol. 8, Issue 2. – P. 1–8. Available at: http://naukovedenie.ru/PDF/117TVN216.pdf
10. Ben-Asher, N. Effects of cyber security knowledge on attack detection [Text] / N. Ben-Asher, C. Gonzalez // Computers in Human Behavior. – 2015. – Vol. 48. – P. 51–61. doi: 10.1016/j.chb.2015.01.039
11. Goztepe, K. Designing Fuzzy Rule Based Expert System for Cyber Security [Text] / K. Goztepe // International Journal of Information Security Science. – 2012. – Vol. 1, Issue 1. – p.13–19.
12. Gamal, M. M. A Security Analysis Framework Powered by an Expert System [Text] / M. M. Gamal, B. Hasan, A. F. Hegazy // International Journal of Computer Science and Security (IJCSS). – 2011. – vol. 4, Issue 6. – p. 505–527.
13. Chang, L.-Y. Applying fuzzy expert system to information security risk Assessment – A case study on an attendance system [Text] / L.-Y. Chang, Z.-J. Lee // International Conference on Fuzzy Theory and Its Applications (iFUZZY), 2013. – p. 346–351. doi: 10.1109/ifuzzy.2013.6825462
14. Kanatov, M. Expert systems for information security management and audit [Text] / M. Kanatov, L. Atymtayeva, B. Yagaliyeva // Implementation phase issues, Soft Computing and Intelligent Systems (SCIS), Joint 7th International Conference on and Advanced Intelligent Systems (ISIS), 2014. – p. 896–900. doi: 10.1109/scis-isis.2014.7044702
15. Lee, K.-C. Sec-Buzzer: cyber security emerging topic mining with open threat intelligence retrieval and timeline event annotation [Text] / K.-C. Lee, C.-H. Hsieh, L.-J. Wei, C.-H. Mao, J.-H. Dai, Y.-T. Kuang // Soft Computing. – 2016. – p. 1–14. doi: 10.1007/s00500-016-2265-0
16. Pan, S. Developing a Hybrid Intrusion Detection System Using Data Mining for Power Systems [Text] / S. Pan, T. Morris, U. Adhikari // IEEE Transactions on Smart Grid. – 2015. – Vol. 6, Issue 6. – p. 3104–3113. doi: 10.1109/tsg.2015.2409775
17. Lakhno, V. Design of adaptive system of detection of cyber-attacks, based on the model of logical procedures and the coverage matrices of features [Text] / V. Lakhno, S. Kazmirchuk, Y. Kovalenko, L. Myrutenko, T. Zhmurko // Eastern-European Journal of Enterprise Technologies. – 2016. – Vol. 3, Issue 9 (81). – p. 30–38. doi: 10.15587/1729-4061.2016.71769
18. Louvieris, P. Effects-based feature identification for network intrusion detection [Text] / P. Louvieris, N. Clewley, X. Liu // Neurocomputing. – 2013. – Vol. 121. – p. 265–273. doi: 10.1016/j.neucom.2013.04.038
19. Wang, Z. Inferring User Search Intention Based on Situation Analysis of the Physical World [Text] / Z. Wang, X. Zhou, Z. Yu, Y. He, D. Zhang // Lecture Notes in Computer Science. – 2010. – p. 35–51. doi: 10.1007/978-3-642-16355-5_6
20. Yeremeev, A. Modelirovanie vremennykh zavisimostey v intellektualnykh sistemakh podderzhki prinyatiya resheniy na osnove pretsedentov [Text] / A. Yeremeev, P. Varshavskiy, I. Kurilenko // International Journal «Information technologies and knowledge». – 2012. – Vol. 6, Issue 3. – P. 227–239.
21. Kulinich, A. Kontseptualnye «karkasy» plokho opredelennykh predmetnykh oblastey [Text]: Mater. III Mezhd. nauch.-tekhn. konf. / A. Kulinich // Otkrytye semanticheskie tekhnologii proektirovaniya intellektualnykh system, 2013. – P. 135–142.
22. Puri, C. Analyzing and Predicting Security Event Anomalies: Lessons Learned from a Large Enterprise Big Data Streaming Analytics Deployment [Text] / C. Puri, C. Dukatz // 26th International Workshop on Database and Expert Systems Applications (DEXA), 2015. – p. 152–158. doi: 10.1109/dexa.2015.46
23. Verma, R. Security Analytics: Essential Data Analytics Knowledge for Cybersecurity Professionals and Students [Text] / R. Verma, M. Kantarcioglu, D. Marchette, E. Leiss, T. Solorio // IEEE Security & Privacy. – 2015. – Vol. 13, Issue 6. – p. 60–65. doi: 10.1109/msp.2015.121

24. Razaq, A. A big data analytics based approach to anomaly detection [Text] / A. Razaq, H. Tianfield, P. Barrie // Proceedings of the 3rd IEEE/ACM International Conference on Big Data Computing, Applications and Technologies – BDCAT '16, 2016. – P. 187–193. doi: 10.1145/3006299.3006317
25. Perlovsky, L. Dynamic Logic Machine Learning for Cybersecurity [Text] / L. Perlovsky, O. Shevchenko // Advances in Information Security. – 2014. – p. 85–98. doi: 10.1007/978-3-319-10374-7_6

Розроблено методи автоматичного аналізу тексту на основі декларативного представлення правил синтаксичної сполучуваності та програмного розподілення аналітико-синтетичної обробки природно-мовного тексту в системах машинного перекладу. Програмна реалізація експерементально доводить, що застосування розроблених методів зменшує кількість помилок семантичного характеру в середньому на 14–16 % у порівнянні з відомими системами машинного перекладу

Ключові слова: система машиного перекладу, автоматичний аналіз тексту, аналітико-синтетична обробка тексту

Разработаны методы автоматического анализа текста на основе декларативного представления правил синтаксической соединяемости и программного распределения аналитико-синтетической обработки естественно-языкового текста в системах машинного перевода. Програмная реализация експерементально подтверждает, что применение разработанных методов уменьшает количество ошибок семантического характера в среднем на 14–16 % по сравнению с известными системами машинного перевода

Ключевые слова: система машинного перевода, автоматический анализ текста, аналитико-синтетической обработка текста

UDC 519.76:81'22
DOI: 10.15587/1729-4061.2017.92021

DEVELOPMENT OF KNOWLEDGE-ORIENTED SYSTEM OF MACHINE TRANSLATION BASED ON THE ANALYTIC-SYNTHETIC TEXT PROCESSING

L. Lytvynenko
Postgraduate student*
E-mail: l.lytvynenko@gmail.com
O. Nikolaievskyi
Postgraduate student*
E-mail: a1.n1@yandex.ru
V. Lakhno
Doctor of Technical Science, Associate Professor**
E-mail: lva964@gmail.com
E. Skliarenko
PhD, Associate Professor*
E-mail: sigma.inet@gmail.com
*Department of Information Systems and Mathematical Sciences***
Department of Managing Information Security*
***European University
Academika Vernadskogo blvd., 16 V,
Kyiv, Ukraine, 03115

1. Introduction

A constant growth of the volume of text information (TI), associated with the use of the Internet, leads to an increase in the need for automatic text processing of TI. The quality requirements for processing, primarily based on the use of modern information technologies, are at the forefront. Unfortunately, high quality software in the tasks of synthetic-analytical processing of multilingual text information in machine translation systems (MTS) exists only for narrow subject areas and cannot be easily adapted to a wide range of tasks. In addition, existing solutions mostly require post-editing and are oriented to professional translators, rather than ordinary users.

The relevance of present work is in the study of method of automatic syntactic analysis (ASA) of the text based on declarative representation of the rules of syntax combinability and on the method of software distribution of analytical-synthetic processing of the natural language text (NLT) at MTS.

2. Literature review and problem statement

As shown by the analysis of theoretical and practical work in the field of MTS development, a lifetime problem of automatic translation is polysemy and uncertainty, the solution to which involves computer modeling of the process of understanding NLT, particularly evident for the Slavic languages due to rich morphology [1].

Today, three complex models for building formal semantics of NLT are known [2–5].

Model [2] was developed at Stanford University (United States) and has the title "semantics of advantages"; it is