Journal of Theoretical and Applied Information Technology
30th April 2018. Vol.96. No 8

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

SYSTEM OF DECISION SUPPORT IN WEAKLY-FORMALIZED PROBLEMS OF TRANSPORT CYBERSECURITY ENSURING

[1]AKHMETOV B., [2] LAKHNO V.

[1]Yessenov Caspian state university of technologies and engineering, Kazakhstan
[1]Department of Cyber Security, European University, Ukraine

E-mail: [2]007berik@mail.ru, [1]lva964@gmail.com

ABSTRACT

This paper resolves the actual task of the development of mathematical software decision support systems (DSS) cyber security mission-critical information systems of transport (CRIST) in poorly structured and difficult tasks of formalizing the information security and information risk assessment. The paper presents developed system for decision support in weakly formalized problems of CRIST and the cyber security of objects of Informatization of the industry. The system is based on models of information security tasks description, risk assessment and cyber defense of transport in conceptual and functional aspects. Also the article presents the description of the process of forming the DSS knowledge base for circumstances related to the identification of hard-to-explain signs of anomalies and attacks.

Keywords: *system of support of decision-making, cyber security, poorly formalized tasks, the interpretation of the situation.*

1. INTRODUCTION

In connection with the increased number of complex targeted cyber-attacks (C–A) on critical information systems for transport (CRIST) [1–4], one of the most pressing problems of public and private transportation companies became cyber security (CS). The most serious security issues CS CRIST is to protect it from unauthorized access (UAA). The magnitude of the problem says at least the fact that even one person who has access to the data CRIST, in a short time can completely paralyze the work of any strategic railway hub, seaport, gas or oil transport enterprises, logistics center, etc. For this purpose it is enough to enter only several tens of code lines of the virus program into the software (SW) CRIST. During targeted attacks, cybercriminals often use unique malicious programs and methods of penetration into the CRIST (cyber defense facilities – CDF) [5, 6]. To withstand the constant growth of complexity of illegitimate influences on OBCS is possible, in particular using the system for the intelligent recognition of C–A (SIRCA), equipped with modules of decision support (DS) for complicated structured and formalized problems of information security (IS). Even the initial problem of designing integrated systems for the protection of information (ISPI) for CRIST can be attributed to poorly formalized tasks with incomplete information. Such tasks include situations associated with the recognition of long target of C–A on OPKS, not accompanied by obvious signs. Therefore, the scope of the research devoted to the development of models of DS systems (DSS) in poorly structured and difficult to be formalized to ensure information security CRIST, seems relevant.

2. ANALYSIS OF LITERARY DATA AND PROBLEM STATEMENT

The increase in the number of C–A on CRIST in recent years sparked interest in the development of effective systems of intellectual recognition of C–A (SIRCA) and anomalies [7, 8]. A separate direction of research in this area began work on the development of methods, models and software (SW) for DSS [9, 10] and expert systems (ES) [11, 12] region IS CR [13, 14], in particular, transport, energy, industry etc.

In [15, 16] analyzed the methodology of intelligent simulation for analysis and decision-making in poorly structured situations, the IP. Research has not brought to the hardware or software implementation.

The poorly amenable to formalization and structuring of the task of providing the CS with the appearance of new classes of attacks are difficult to

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

analyze and support decision-making concerning IS CRIST (or CDF) are [17]. In this case, the status parameter IS CDF, can be represented by quality indicators [18], which is not always appropriate.

As the authors [19, 20], analysis of the security of CRIST and the development of countermeasures to counter targeted C–A, should be preceded by a stage of identifying the major threats and vulnerabilities. At the same time, as pointed out by the researchers themselves, it is problematic to describe not regular formalized relationships between threats and vulnerabilities in the conceptual and functional aspects IS OBCS without appropriate DSS.

A significant drawback of the works [21, 22] is the lack of an architectural implementation of a DSS for the difficult formalized tasks IS OBCS. As the authors acknowledge [22], most of these DSS and ES are currently in the testing phase.

The works [23, 24] show that the disadvantages of many DSS and ES in the field of IS are: the need for experts of high qualification in the formation of the knowledge base (KB); inability to assess the effectiveness of specific DSS, etc.

Thus, taking into account the debate in the reviewed works, there is obviously a need to continue research on viable solutions for DSS in the field IS CDF. Such studies, in particular, should be aimed at the decision of difficult formalized tasks atypical of IP, for example, in the process of implementation of the multi-stage targeted attacks.

3. STATEMENT OF THE PROBLEM

The aim of this work is the development of models for the DSS for the information security management and information risk assessment in difficult formalized atypical situations, in implementing of multi-stage targeted attacks on CRIST. The article examines the decision based on the development of models describing the transformation of the situation when assessing IS CRIST in the conceptual and functional aspects. The problem solution of information risks reducing countermeasures selection includes the minimization of costs of measures for the protection of information (IP) in CRIST, while ensuring acceptable level of risk, presented as: $C_{\sum} \to \min$ for $AR \le AR_r$, where $C_{\sum}$, A, AR_r – accordingly, allocations to CSIP (countermeasures), and allowable total risk value of IS.

The motivation for our study was the desire to improve the security of information systems in various fields. Also there were taken into account the situations where cyber security experts and analysts have to deal with poorly formalized problems with incomplete information about the signs of anomalies, cyberattacks and threats to critical computer systems.

4. MATERIALS AND METHODS

The procedure of structuring a situation associated with the task of supporting the building IS CRIST (or OBCS) considered in functional and structural contexts of the concept – the field of knowledge (FN) cyber security.

We introduce the following notation (in the form of concepts – concepts of cyber security) threats IS for CRIST in FN: destabilizing factors (DF); target (targeted) factors (TF); intermediate factors (INF).

The structural approach version enables the decomposition of the situation. It enables to perform structural-functional relationships of its constituent component (se_i). The component selection (se_i), implemented in the course of interaction DSS and SIRCA [8, 11, 14, 23]. The result of such interaction is represented by a hierarchical component of the "Part – Whole", $\langle PA, WH \rangle$, where $PA = \{pa_i\}$ – integer (the set or alphabet (se_i)), WH – the relation "Part – Whole" in the alphabet PA, $i = 1,...,n$.

For the variant of the functional approach to the definition of the situation defines a baseline assessment of illegitimate interference in the work of CRIST. Made for all the components of the situation $SI_i = \{si_{ij}\}$, $j = 1,...,m$ – many peaks, AM_i – the adjacency matrix (MS) directed graph (DG), which specifies for each component (se_i) situation (pa_i) its functional structure. Using experts, construct cognitive maps (COGM) (SI_i, AM_i), which reflect the subjective interpretation of the laws of functioning of the element of the EOQ. Then received COGM grouped (SI, AM), where $SI = \cup SI_i$ – a set of attributes ("P") describing the change in the situation.

The developed DSS uses a model of representation of knowledge in the form of the iconic OG, as well as fields of knowledge (FN) [25, 26]. FN is defined and the input data (factors X) of tasks for DSS; conclusions (output – *Y*); module (*MO*), used to transform the original data in the output. The model described by the system SC_{pa}, FS_{si}, which display, respectively,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the structure of the situation and the regularities of the implementation of PB OBCS.

COGM (SI, AM) described in the functional system (FS) FN for concepts (*DF*), (*TF*) (*INF*). In the process descriptions, COGM applied scale of informativeness "P" [27, 28]. To describe COGM also used methods to identify the preferences of the expert (or decision makers – decision makers), analyzing the transformation scenarios situations (pa_i).

Using the method of [23] obtained ordered set $ML_{ij} = \{ml_{ijz}\}$ linguistic knowledge (LK) $j-$th «P» $i-$th judgment for $z-$th number LM whose elements are displayed in the range [0,1]. For each "P" judgments there determined the scale X_{ij}. The scale division has a linguistic interpretation $ml_{ijz} \in ML_{ij}$.

The indirect effect from the influence of the DF concept (concepts) INF – concept can be described as follows:

$$EF_n\left(CO^i_{DF} \to CO^j_{TF}\right) = \min_{k.l}\{COM_{kl}\}, \quad (1)$$

where CO_{DF}, CO_{TF} – concepts (concepts) and the task of destabilizing factors IS CRIST, respectively, $\{COM_{kl}\}$ – many links in the transformation of the situation from destabilizing threats to the target.

The direct effect of the influence of the *DF* concept for INF – concept can be described as follows:

$$EF\left(CO^i_{DF} \to CO^j_{TF}\right) = \\ = \max\left(EF_1, EF_2, ..., EF_k, ..., EF_N\right), \quad (2)$$

where $k = 1,2,..., N$, N – indirect effects of the concepts *DF* on *INF*.

The resulting risk of impact *TF* for all threats KRIST CS can be described as follows:

$$R = \sum_{i,j}\left(\begin{matrix} EF\left(CO^i_{DF} \to CO^j_{TF}\right)\cdot \\ \cdot CI_j \cdot IM_j \end{matrix}\right), \quad (3)$$

where CI_j, IM_j – the cost and value of j –th information asset in CDF.

For situations where there needed to script the transformation of the original data is the situation: many factors $SI = \{si_i\}$; scale(s) of factors X_{ij}; the initial state of the CDF prior to the occurrence of the situation being evaluated $X(t_0) = (x_{11}, ..., x_{nm})$;

CM $AM = \left|am_{ij\,sl}\right|$, where i, s – number of a notion (concept), j, l – the number "P" judgments, with the numbers $i \vee s$, respectively.

Generally it is required to define the vector of addition "P" (VA) $V(t), V(t+1), ..., V(t+n)$ and track the state change of the CDF for the input parameters $X(t), X(t+1), ..., X(t+n)$ in moments of $t, ..., t+n$.

To solve the problem using the method of successive iterations in which VA was determined from the expression $V(t+1) = V(t) \circ AM$.

The state of CDF at the moment $t+1$, is characterized by the ratio of $X(t+1) = X(t) + V(t+1).$ Each CM $AM = \left|am_{ij\,sl}\right|_{n\times n}$ for positive and negative component was converted under the following conditions:

$$\begin{aligned} &if\ am_{ij\,sl} > 0\ \ then\ \ am'_{i(2j-1)s(2l-1)} = \\ &= am_{ij\,sl},\ am'_{i(2j)s(2l)} = am_{ij\,sl}; \\ &if\ am_{ij\,sl} < 0\ \ then\ \ am'_{i(2j-1)s(2l-1)} = \\ &= -am_{ij\,sl},\ am'_{i(2j)s(2l)} = -am_{ij\,sl} \end{aligned} \quad (4)$$

to double positive definite CM $AM' = \left|am'_{ij\,sl}\right|_{2n\times 2n}$.

Therefore, AV $V(t)$ and predictive values of the indication(s) $V(t+1)$, also have dimension *2n*. There are rules of synthesis of primary AV $V'(t)$ with the dimension *2n*:

$$\begin{aligned} &if\ v_{ij}(t) > 0\ \ then\ \ v'_{i(2j-1)}(t) = v_{ij}(t), \\ &v'_{i(2j)}(t) = 0\ \&\ if\ v_{ij}(t) < 0\ \ then \\ &v'_{i(2j)}(t) = v_{ij}(t), v'_{i(2j-1)}(t) = 0. \end{aligned} \quad (5)$$

In vector $V'(t) = (v^-_{11}, v^+_{11}, ..., v^-_{nm}, v^+_{nm})$ the significance of "P" si_{ij} is determined by two components with the index $2j$, characterizing v^+_{ij}, and with the index $2j-1$, determining v^-_{ij} addition si_{ij}.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

AV $V'(t+1)$ for positive definite CM AM' represented as – $V'(t+1)=V'(t)\circ AM'$.

In the result of the transposition of components of the AV for the moments of time $V'(t+1),...,V'(t+n)$ the block matrix (BM) is received. In BM of a line – addition "P" at the moments *t*, columns – addition "P" in timepoint which corresponds to a column: $V^t=\left|V'(t+1)^T,...,P'(t+n)^T\right|$.

BM V^t was used in DSS in a subsystem of forecasting of transformation of a situation with IS CRIST.

The degree of mismatch of elements fields of knowledge (FK) – $dis_{ij}(t)$, taking into account the works [23, 27, 28], is defined by expression:

$$dis_{ij}(t)=\frac{\left|v_{ij}^{+}(t)-v_{ij}^{-}(t)\right|}{v_{ij}^{+}(t)+v_{ij}^{-}(t)}, \quad (6)$$

$$0\le v_{ij}(t)\le 1,$$

where $v_{ij}^{+}(t),\quad v_{ij}^{-}(t)$ – adding positive and negative "P" in the points t, respectively.

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

Tracking the dynamics of transformation of the situation during the implementation of illegitimate actions by an attacker in the moments $X(t),...,X(t+n)$, in the DSS are displayed in the process of transformation of the term:

$$\left\langle v_{ijk}(t+1),\, dis_{ij}(t+1)\right\rangle, \quad (7)$$

where

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

It is accepted that if it is true inequality $v_{ij}^{+}(t+1)>v_{ij}^{-}(t+1)$ that sign $v_{ij}(t+1)$ is positive. If it is true inequality $v_{ij}^{+}(t+1)<v_{ij}^{-}(t+1)$, is negative. Consequently, the transformation of the situation in the course of prediction, to determine a tuple:

$$\left\langle X(t+1),\, DIS(t+1)\right\rangle, \quad (8)$$

where $X(t+1)=X(t)+V(t+1)$ or $x_{ij}(t+1)=x_{ij}(t)+v_{ij}(t+1)$;

$dis_{ij}(t+1)\in DIS(t+1)$.

In the developed DSS, the transformation of the situation represented by the matrix $X^t=\left|X(t+1)^T,...,X(t+n)^T\right|$. The matrix X^t is used for visual representation of results generated in the search for solutions.

The solution of the inverse problem (INPR) forms for ADP recommendations, allowing to transform the current situation in the target state CDF. While in subsystem of search of conclusions (SSC) there was used transitive closure AM^* double adjacency matrix $AM'=\left|am'_{ij\,sl}\right|$.

In SSC, in particular, when there are set AM^* and the target vector $P=(p_1,...,p_n)$, sets of vectors of entrance influences are defined – $\Psi=\{D\}$. It is accepted that for all $D\in\Psi$ there implemented the expression $D\circ AM^*=P$.

The versions of the decision of INPR for $D_{\max}$ and $D_{\min}$ are presented in works [27, 28]. Control actions D_i, on "P" si_{ij} are established by parameters v_{ij} and dis_{ij}, i.e. $D=(v_{11},dis_{11},...,v_{nm},dis_{nm})$. Parameters of dis_{ij} and v_{ij} in DSS are determined by using relations (6) and (7), respectively.

The current status FS FN is defined by the tuple: $\langle SI,\, X,\, X(0),\, AM\rangle$.

The conceptual system (CONS) of FK in the part of the DSS allows you to perform structural and functional decomposition of the situation $\langle PA, WH\rangle$. It is also used in the processes of interpretation of findings related to the scenarios of the transformation of the status of CDF, for example, in the course of the implementation of targeted C–A.

Components of the situation are defined by the following parameters:

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$\langle pa_i, SI(pa_i), CV(pa_i)\rangle$, where pa_i – the identifier of the notion (concept); $SI(pa_i)$ – the intension of the concept ($SI_i = \{si_{ij}\}, SI(pa_i) = (x_{11},...,x_{nm})$); $CV(pa_i)$ – the scope of the concept (a component of the situation described in the model).

The concept pa_i in DSS displayed in the space coordinates of the values "P". The feature space of concepts formed by the Cartesian product of the scales of all "P" – $U(pa_i)$.

In the model of CONS the identifier of the concepts $pa_i \in PA$ are presented in meaningful (semantic [29]) space $U(pa_i)$. CONS allows to define a set of semantic spaces $U(PA) = \{U(pa_1),...,U(pa_n)\}$, and hierarchical component WH (« Part–Whole »). So, a couple of the concepts $U(pa_i)$ and $U(pa_q)$ are connected by the relation WH i.e. $U(pa_i)\ WH\ U(pa_q)$.

In the field of CS for the developed DSS there carried out the structuring of the semantic space for key concepts pa_i in a format of representative clusters CL^i [30]. Clusters and concepts are interfaced by the relations "Classes – Subclasses".

In DSS it is accepted that pa_i^1 represents a class pa_i^2, if conditions are satisfied $\left(SI\left(pa_i^1\right) \subset SI\left(pa_i^2\right)\right)$ and $\left(CV\left(pa_i^1\right) \supset CV\left(pa_i^2\right)\right)$.

Conceptual clusters (CCL) in semantic space of IS are defined in interpretation of basic concepts pa_i^B (BC). BC defines a class of the objects analyzed by means of SIRCA and DSS (for example, an attack class), and category of a situation to which the element is carried pa.

The interval of values is established by an expert way $X_{ij}^B = [x_{ijb}, x_{ijc}]$, $x_{ij} \in X_{ij}^B$, $\forall j$, which sets the bounds of object classes under consideration SIRCA and DSS for CRIST.

Within the meaningful (semantic) concepts IS belonging to the space of terms (ST), i.e. $U(pa^o) \subseteq U(cv^0)$, there are areas of the allowed semantic values $U(pa^o)$ for «P» si_{ij}, for example, vulnerabilities are found, partially found, not found, etc.

BC is defined by parameters: $\left(pa_i^B, SI\left(pa_i^B\right), CV\left(pa_i^B\right)\right)$, where pa_i^B – the identifier of BC; $SI\left(pa_i^B\right)$ – the intension of BC; $CV\left(pa_i^B\right)$ – the scope of BC. The scope of BC can be presented as a set of objects of ST for which values "P" belong to acceptable. Acceptable values from the point of view of the analyst of information security (ISA or the employee of department of cyber security) belong to area of the allowed BC parameters $AC(pa_i^B)$.

The procedure of generalization of BC is realized by removal of the repeating "P" or their combinations.

It is accepted that BC for IS have for m number of abstractions – $A = 2^m - 1$. The universalized BC are classified 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 in admissible values of the generalized concepts of the alphabet of IS BC values are implemented. Thus, $AC\left(pa_i^B\right) \subset AC\left(pa_i^{Ba}\right)$ and $CV\left(pa_i^B\right) \subset CV\left(pa_i^{Ba}\right)$.

The intension of BC and its abstractions form 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 represents a conceptual cluster of BC – PA^i. Formed CCL allow to structure the semantic space of CS. The transitions from BC are determined in clusters pa_i^B to generalized pa_i^{Ba}. At CONS the navigation is set to a tuple of vectors:

$$\langle CN(t), CC(t), SV(t)\rangle, \quad (9)$$

where $CN(t) = \left(pa_1^{Ba},..., pa_n^{Ba}\right)$ – identifiers of concepts within the description of situations; $CC(t) = \left(SI\left(pa_1^{Ba}\right),..., SI\left(pa_n^{Ba}\right)\right)$ – the intention of CONS $pa_i^{Ba} \in CN(t)$; $SV(t) = \left(CV\left(pa_1^{Ba}\right),..., CV\left(pa_n^{Ba}\right)\right)$ – the scopes of the concepts $pa_i^{Ba} \in CN(t), \forall i$.

In the operation of DSS there defined the rules of transformation CONS: 1) if in the course of forecasting the results of development of C–A, the value "P" of the concept went beyond the permitted

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

BC, formed a new concept; 2) new concepts summarize the primary BC for the characteristics whose values deviate from the permissible.

Formally rules are submitted as display of a condition of FS $X(T)$ in a condition of CONS, i.e.

$$\langle CN(t), CC(t), SV(t)\rangle, UM: X(t) \rightarrow \rightarrow (CN(t), CC(t), SV(t)), \quad (10)$$

where $UM = (UM_i)$ – vector transformation rules BC pa_i^B in common $pa_i^{Ba}, \forall i.$

The expression (10) gives ADP the ability to interpret and generalize the concept IS characterized by a set of "P".

Thus, taking into account (10), a model for the representation of PZN is determined by the tuple:

$$\langle SC_{pa}, FS_{si}, UM\rangle, \quad (11)$$

where SC_{pa} – CONS FK, FS_{si} – FS FK, i.e. $\langle U(PA), WH, PA^i, (CN(t), CC(t), SV(t))\rangle$.

The problem of search of a conclusion and obtaining the decision is reduced to development of strategy of transformation of a situation from current state of IS in target. Thus, INPR decides. During the decision are defined $X(0) = (x_{11}^0, ..., x_{nm}^0)$ and $X^P = (x_{11}^p, ..., x_{nm}^p)$ FK. Further the target vector of additions is defined $P = (v_{1j}, ..., v_{nm})$, where $v_{11} = x_{11}^p - x_{11}^0$, $v_{12} = x_{12}^p - x_{12}^0$, etc. The target vector specifies the direction and size of the changes the "P" attack from an initial state $X(0)$ CDF in target X^P. The operating SIP resources for CRIST are defined so: $V^R = (v_{11}^r, ..., v_{nm}^r)$.

Set of conclusions $D = \{D_1, ...D_{cv}\}$ formed in the process of solving INPR i.e. the situation that arose during the implementation of the C–A from its current state to the target.

In some situations, there are precedents, when there is no solution. However, changing the structure of the cognitive model situation, you can find a solution, using a heuristic approach, in particular, attracting experts IS.

Finding solutions involves the following stages: generation of insights; structuring insights for functional mapping; outlining the findings in a conceptual format.

Generating insights is performed in the process of solving INPR to the respective control circuits IS. The result is a set of solutions $\{D_1, ..., D_{cv}\}$, forming a vector of control actions (VCA). VCA corresponds to VAS, taking into account cognitive consonance (c) [27, 31-33], i.e. $(v_{11}, c_{11}, ..., v_{nm}, c_{nm})$. Thus, to each conclusion $D_{cv} \in D$, is to be put in compliance a condition of CDF after change of a situation in the functional FK display $X_{cc} = (x_{11}^0 + v_{11}, ..., x_{nj}^0 + v_{nj})$.

For structurization of conclusions of functional display the following criteria were used: feasibility of the decision within, the available SIP; conflictness of the decision.

In DSS the decision is made $D_{cc} = (v_{11}, c_{11}, ..., v_{nm}, c_{nm})$ realizable, if $\forall v_{ij} \in D_{cc}$ and $v_{ij} \le v_{ij}^r$, $v_{ijk}^r \in V^R = (v_{1j}^r, ..., v_{nj}^r)$.

Criterion feasibility, in relation to $\{D\}$, has allowed to divide conclusions to subsets of realized D^R and unrealizable D^N decisions.

Decision component D_{cv} is set by parameters v_{ij} and c_{ij}. In [27, 28, 31], the level of consonance in problems of decision-making IS specified in the range $c_{ij} = 0{,}5 - 0{,}65$. Values below $c_{ij} < 0{,}5$ for decision-making D_{cv} rely conflict [27, 31].

Structurization of conclusions in a conceptual format is realized by model of representation of knowledge (expression (11)). We will believe that to each conclusion $D_{cv} \in D$ there corresponds dynamics of transformation of a situation X_{cv}. It is displayed by structure of CONS, i.e. $UM: X_{cv} \rightarrow (CN_{cv}, CC_{cv}, SV_{cv})$. Therefore, to a set of decisions *D* in FS there corresponds the set of conclusions of CONS, i.e. $\Delta = \{D_{pa1}, ..., D_{pacv}\}$, where $D_{pacv} = (CN_{cv}, CC_{cv}, SV_{cv})$ – state CONS DSS.

It is accepted that in semantic space of CS of coordinate of the points defining acceptable characteristics of BC are set by a condition of a situation X_{cv}, and decision D_{cv}. Perhaps at once several BC values and the decisions corresponding to them, get to the area allowed by ADP. At the

Journal of Theoretical and Applied Information Technology
30th April 2018. Vol.96. No 8

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

same time combination of various decisions is possible $D_{cv} \in D$. Therefore, in CONS DSS classes are formed D_{pa}^{q}. Class solution is characterized by the tuple $D_{pa}^{e} = \langle CN^{q}, CC^{q}, SV^{q} \rangle$, where Q – quantity of classes in CONS. The content of classes $\{CC^{1},...,CC^{Q}\}$ forms the conceptual graph of decisions (DG), fig. 1. The root vertex of DG (0, Y0) contains insights $D_{v} \in D$, in which any of the signs ("P") doesn't go beyond, limited BC for IS CDF. On U1 solutions are found D_{v}, in which outside the area ST came out no more than one "P". On U2 are solutions D_{v}, in which outside the area ST came out no more than two "P". Conclusions summarize the conclusions U2 U1 "P", etc. For the situation when the values of "P" beyond the limits set ST, defined new feature class with non-basic ST structure and actions [10, 12, 23].

Search for structural solutions includes the steps of: evaluation of alternative solutions; evaluation of prospects; the formation of solutions. The conclusion about the prospects of the course of action starts from the root node of the DG gas. ADP should imagine a situation, abstracting from the "P" that it is a generalization.

The formation of output is based on the assessment of alternatives to individual decisions. Evaluation is performed during the introduction of the structural transformation in the situational model $\langle SI, X\ X(0)\ AM \rangle$ and the subsequent decision INPR for structure $\langle SI^{*}, X^{*}\ X(0)\ AM^{*} \rangle$.

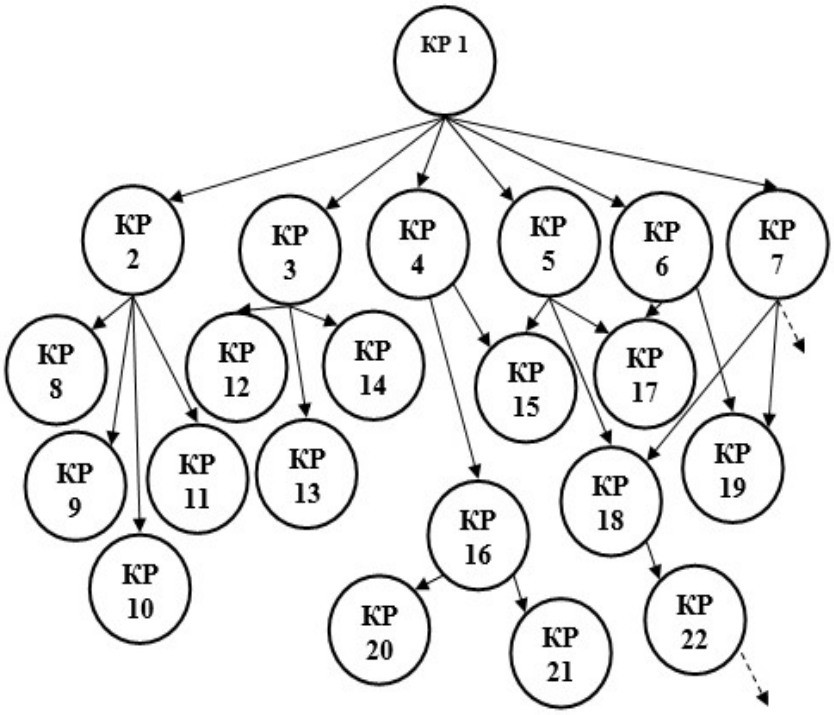


Figure 1: Conceptual graph of solutions

As a result after synthesis of a conclusion we will receive a subset $D^{*} = \{D_{1}^{*},...,D_{a}^{*}\}$. The conclusion is made if there is at least one decision $D_{a}^{*} \in D^{R*}$ preferable, than $D_{a} \in D^{R}$, which have been received during the solution of INPR for an initial configuration of a situation with IS CDF.

The efficiency of the counter-measures offered DSS for protection of CRIST is defined so:

$$EF = \left(R - R' \middle/ R\right) \cdot 100\%, \quad (12)$$

where R, R' – initial and final (after implementation of countermeasures) risk value for the IS CDF, respectively.

The task of selecting countermeasures to reduce information risks to CRIST DSS is solved iteratively.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

DSS is implemented on the algorithmic high-level language. User interfaces include modules that implement the operation of the subsystems, which are described in works [23, 28, 30, 32].

Interface to generate baseline information to define "P", showing the situation and corresponding rating scale "P". Visualization of the transformation of the situation presented in the iconic DG (SI, AM), Fig. 2. Blue color indicates fragments of a situation "Part–Whole", and red "Class–Subclass".

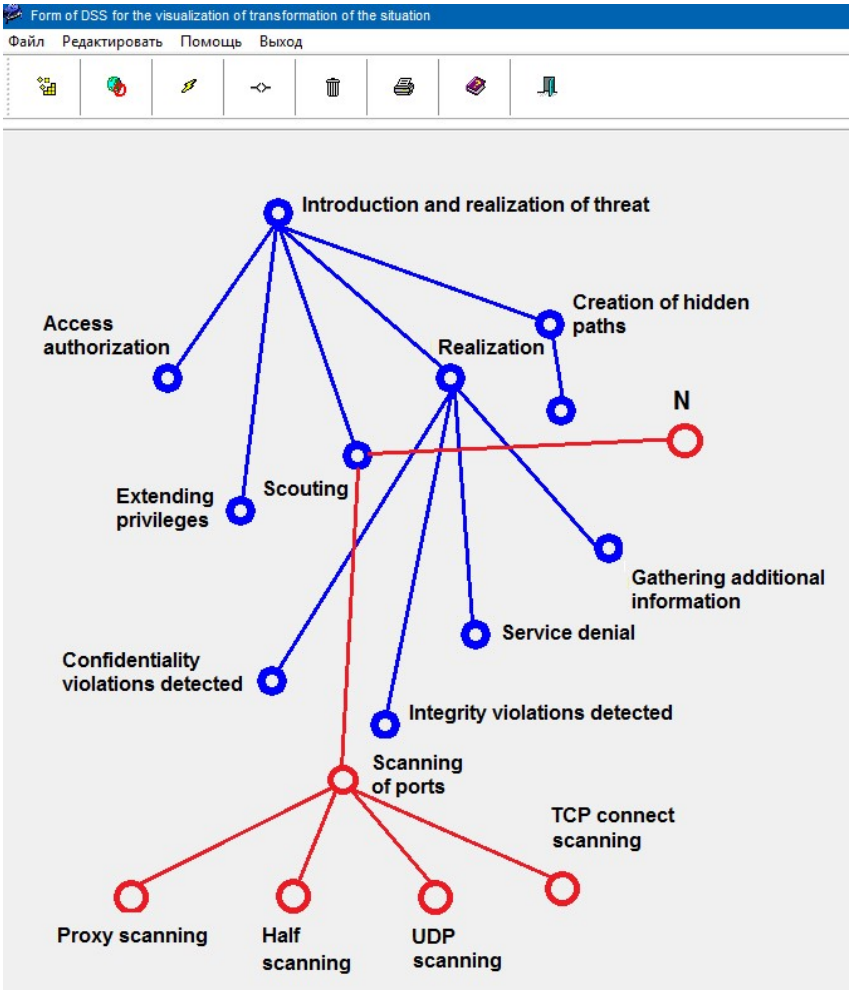


Figure 2: DSS form to visualize the transformation of the situation when assessing CS CRIST

If there selected the direct assessment, the degree of influence of the P cyber-attacks on the indices IS computed so: $am_{ij\,sl} = v^c_{ij} / v^r_{sl}$, where v^c_{ij}, v^r_{sl} – addition of the characteristics "P" of the reason ("R") and consequence ("C"), respectively; *i,s* – number of the concept, *j,l* – number «P».

The preferences subsystem of the ADP provides an opportunity to identify the degree of influence of each of the "P" anomalies or C–A on other factors IS. As basic data the scale of informational content of "P" was used ML_{ij} [23, 30]. Besides, DSS are analyzed the current values accepted on the basis DG(SI, AM).

Earlier in [32] it was proposed to use as the evaluation indicator of the effectiveness of teaching DSS modified condition information of functional performance (MICFP), which is based on entropy and information and remote criteria Kullback – Leibler. Use of MICFP has allowed to build correct decisive rules for the developed DSS [6, 2].

Journal of Theoretical and Applied Information Technology
30th April 2018. Vol.96. No 8

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

5. EXPERIMENT

To verify the practical applicability of the proposed model the program complex (PRCOM) was developed – a system of decision support "Decision Support System of Management Cyber security – DSSMCS" [12, 21, 27]. In the process of experimental verification DSSMCS and simulation in Matlab variants generation and analysis of countermeasures recommended by the DSS for different classes of C–A were investigated. During the experimental verification DSSMCS for CRIST four kinds of countermeasures (or combinations thereof) was tested: 1) notice ISA (ADP); 2) reconfiguration of services IS (for example, router); 3) limiting attempts to connect to the network; 4) connection and sending the alert to the subscriber. Additionally consider blocking access to the modules CRIST, which recorded incidents IS.

If the ISA considers it appropriate to perform a paired comparison of the informativeness of the signs of a C–A, for example, in a situation requiring specification of signs-reasons for si_{tl}, si_{sd} and their impact on a bunch of sign–consequence ("S–C"), use the ranking scale [11, 14, 30]. The degree of influence of the "P" of attack on the performance IS CDF was determined as:

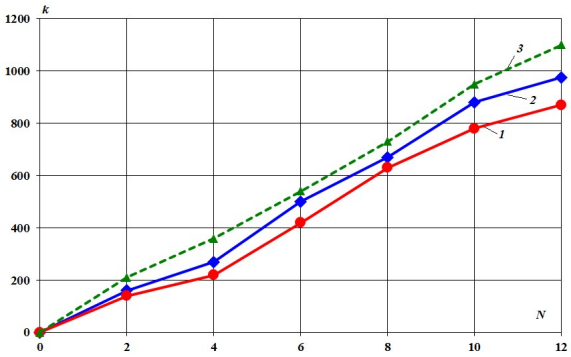
$$am_{ij\,tl} = am_{ij\,sd} \cdot \left(\beta_{tl} \Big/ \beta_{sd} \right),$$

where β – the parameter describing a level of influence of a linking of "S-C" on "R–C".

At the same time minimization of costs of IP is provided in CRIST in case of support of the allowed level of risk, i.e. $C_{\Sigma} \to \min$ for $AR \le AR_r$.

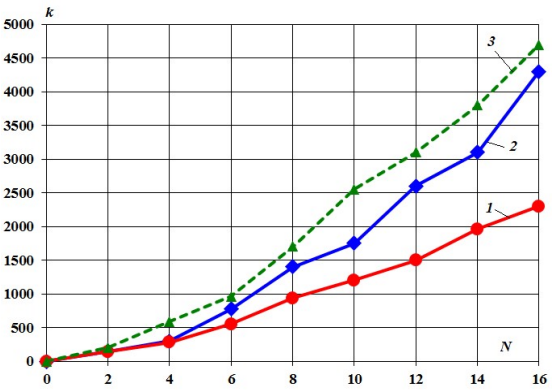
6. RESULTS

The Fig. 3 shows examples of the results of testing the DSS for the decision of problems of cyber security CRIST in poorly structured and difficult to be formalized situations.

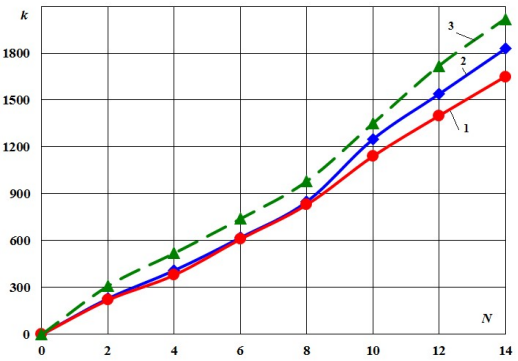


a) decision support by detecting the virus infection CRIST

b)



c) decision support in detecting attacks on SCADA transport company



c) decision support in detecting attacks class network intelligence in CRIST

N *– the number of analyzed bundles of sign–consequence («S–C»),* ***k*** *– the number of consecutive iterations during which the vector of addition of signs (VAS) is formed*

1 – DSS DSSMCS; 2 – methods of forecasting of states; 3 – consecutive search of signs

Figure: 3 Comparative efficiency of the offered model

During testing, it was analyzed the possibility of

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

supporting the decisions regarding the probabilities of realization of actions of the malefactor that implements the C–A on CRIST, table 1. It is established that application of DSS has allowed to reduce the predicted value of risk of overcoming contours of IS by 5.5–6%.

Approbation of the decision support system (DSS) "DSSMCS" has been performed for real cyber security situation centers for transport information systems in Ukraine and Kazakhstan [5, 24, 34, 35].

In comparison with the methods of sequential search signs and statistical algorithms conditions [7, 12], the proposed model allowed to reduce the amount of required rules for making effective decisions on cyber defense CRIST.

Table 1: Results of testing the DSS

Types of attacks	**Parameters of the information environment CRIST / Options of reaction ISA and DSS**			
	The accepted designations: AC – number of abnormal network events; AX – number of abnormal events on a host; AE – number of abnormal events on SIP CRIST perimeters, P_a – probability of C-A to the CRIST components			
An attack through illegitimate connection to Wi – Fi networks (For example, railway stations, airports, etc.)	AC=3, AE=3, P_a= 0,68	AC=3, AE=3, P_a = 0,82	AC=1, AE=2, P_a = 0,4	AC=1, AE=1, P_a = 0,3
	U2R	***R2L***	***DOS/DDoS***	***Probe***
	Blocking access to service to network / Blocking access and restriction of attempts to be connected to network	Blocking to network / Blocking access and restriction of attempts to be connected to network	Reconfiguring of the IS services for the purpose of blocking IP / Reconfiguring of the IS services	Sending of warning on the IP address / Reconfiguring of the IS services for the purpose of IP blocking
	The average time of assessment of the situation (The employee of department of cyber security without/with DSS), min.			
	(15–20)/(7–10)			
The remote attack through perimeter of system of information security in CRIST	AC=3, AX=4, AE=2, P_a = 0,74	AC=3, AX=4, AE=2, P_a = 0,82	AC=1, AX=1, AE=1, P_a = 0,24	AC=1, P_a = 0,08
	U2R	R2L	DOS/DDoS	Probe
	Blocking access to service in networks	Restriction of attempts to be connected to network	Reconfiguring of the IS services for the purpose of IP blocking	Disconnection and sending warnings to an IP address
	The average time of assessment of the situation (The employee of department of cyber security without/with DSS), min.			
	(12–18)/(7–9)			

In the process of testing, it was determined that the implementation of the DSS "DSSMCS" allows to provide increase of level of automation and centralization of monitoring of security of the CDF, and also to reduce the time of information about incidents responsible for information security individuals at 6.75–7.15 times

7. DISCUSSION

DSS "DSSMCS" has the following advantages compared to similar systems previously used for problems of decision support ISA analyze the transport companies.

First, DSS ADP provides a convenient display format changes IS CRIST during the implementation of the various classes of attacks. Second, the DSS provides intelligent decision support ISA and the ability to generate alternative solutions to counter the attacks.

Eliminate the drawback of DSS is that at the initial stage of operation for each CRIST must be in manual mode to set initial rules descriptions of conceptual clusters IS.

Further development of research could be improving the interaction of the traditional mechanisms IS that, in particular, treated with primary information, and units of DSS for decision-making in weakly-formalized problems of cyber security CRIST.

Overall, studies have confirmed the effectiveness of the proposed models and software complex DSS to improve security of the considered companies.

The work was carried out within the framework of the grant competition for scientific and scientific and technical projects for 2018-2020 of the Republic of Kazakhstan registration number

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

AP05132723 "Development of adaptive expert systems in the field of cyber security of critical information objects".

A temporary shortcoming of the software implementation of the decision support system (DSS) "DSSMCS", which was identified as a result of testing, has become quite a long time to update the knowledge base on the signs of cyberattacks. This applies only to situations with incomplete information. Now work is under way to optimize the developed software (DSS) "DSSMCS", which will eliminate this drawback.

This work continues the research of authors whose results were previously partially published in international publications [5, 23, 34, 35].

8. CONCLUSIONS

This paper resolves the relevant task of mathematical software DSS CS CRIST development in poorly structured and difficult formalization of the information security task.

The developed model descriptions in the conceptual and functional aspect of the process of formation and use of a KB DSS for the circumstances associated with detection of certain inexplicable signs of anomalies and attacks, which improves the understanding of the analyzed processes of cyber defense CRIST.

The software complex DSS "DSSMCS" that implements the structurally difficult situation IS for CRIST Developed and tested. DSS "DSSMCS" allows to visualize and interpret the results of the current evaluation revealed signs of difficult to explain the anomalies and C–A, but also to describe the current situation in the implementation of the multi-stage targeted attacks, on the basis of the cognitive model. The use of DSS "DSSMCS" in interaction with other systems for the intelligent recognition of illegitimate interference in the work of CRIST, allows to improve the quality of solutions in the field of cyber security.

The article presents improved model for describing situations related to the terminology of information and cybersecurity in the conceptual and functional aspects of the problem under consideration. This problem consists in the formation of adequate knowledge bases for decision support systems in situations of detection of anomalies and cyber attacks on the basis of insufficient descriptive characteristics. The proposed approach has made it possible to increase the understanding of the analyzed cyberprotection processes in computer systems for situations where signs of anomalies, attacks and threats are poorly formatted.

REFERENCES:

[1] U. S. Department of Transportation, Research and Innovative Technology Administration, "Intelligent Transportation Systems (ITS) Strategic Plan: Background and Processes" (2010). Available at: http://www.its.dot.gov/strategic_plan2010_2014/ppt/strategic_backgroundv2.ppt

[2] A. W. Sadek, B. Park, B., & M.Cetin. Special Issue on Cyber Transportation Systems and Connected Vehicle Research. *Journal of Intelligent Transportation Systems*, Vol. 20, no. 1, 2014, pp. 1–3.

[3] Transportation & Logistics 2030. Vol. 4: Securing the supply, pp. 254–286.

[4] V. P. Kharchenko, Ju. B.Chebotarenko, O. Gh. Korchenko, V Je, S. Pacira, O. Ghnatjuk, (2009). Kyberterroryzm na avyacyonnom transporte, *Problemy informatyzaciji ta upravlinnja*, Vol. 4, no. 28, 2009, pp. 131–140.

[5] V. Lakhno, A. Hrabariev. Improving the transport cyber security under destructive impacts on information and communication systems, *Eastern–European Journal of Enterprise Technologies*, Vol. 1 No 3(79), 2016, pp. 4–11.

[6] V. A. Lakhno, A. S. Petrov, A.V. Hrabariev, Y.V. Ivanchenko, G.S.Beketova. Improving of information transport security under the conditions of destructive influence on the information-communication, *Journal of theoretical and applied information technology*, Vol. 89, Iss.2, 2016, pp. 352–361.

[7] J. Petit, S.E. Shladover. Potential Cyberattacks on Automated Vehicles, *IEEE Transactions on Intelligent Transportation Systems*, Vol. 16, Iss. 2, 2015, pp. 546 – 556.

[8] F. Miao, Q. Zhu, M. Pajic, G.J. Pappas. Coding Schemes for Securing Cyber-Physical Systems Against Stealthy Data Injection Attacks, *IEEE Transactions on Control of Network Systems*, Vol. PP, Iss. 99, 2016, pp. 1.

[9] T. Sawik. Selection of optimal countermeasure portfolio in it security planning, Decision Support Systems, Vol. 55, Iss. 1, 2013, pp. 156–164.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[10] A. Fielder, E. Panaousis, P. Malacaria, C. Hankin, F. Smeraldi. Decision support approaches for cyber security investment, Decision Support Systems, Vol. 86, 2016, pp. 13–23.

[11] L. Atymtayeva, K. Kozhakhmet, G.Bortsova. Building a Knowledge Base for Expert System in Information Security, Chapter Soft *Computing in Artificial Intelligence of the series Advances in Intelligent Systems and Computing*, Vol. 270, 2014, pp. 57–76.

[12] M. M. Gamal, B. Hasan, A.F. Hegazy. A Security Analysis Framework Powered by an Expert System, *International Journal of Computer Science and Security (IJCSS)*, Vol. 4, No. 6, 2011, pp. 505–527.

[13] S. Dua, X. Du. Data Mining and Machine Learning in Cybersecurity, CRC press, 2016, p. 225.

[14] A. L. Buczak, E. Guven. (2016). A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection, *IEEE Communications Surveys & Tutorials*, Vol. 18, Iss. 2, 2016. pp. 1153 – 1176.

[15] I. P. Larionov, P. B. Khorev. Problemy sozdaniya i osnovnye zadachi ekspertnoy sistemy podderzhki proektirovaniya kompleksnoy sistemy zashchity informatsii, *Internet-zhurnal «NAUKOVYEDYENIYE»,* 2016, Vol. 8, no. 2. available at: http://naukovedenie.ru/PDF/117TVN216.pdf.

[16] N. Ben–Asher, C. Gonzalez. Effects of cyber security knowledge on attack detection, *Computers in Human Behavior*, Vol. 48, 2015, pp. 51–61.

[17] K. Goztepe. Designing Fuzzy Rule Based Expert System for Cyber Security, *International Journal of Information Security Science*, Vol. 1, No 1, 2012, pp.13–19.

[18] M.M. Gamal, B. Hasan, A.F. Hegazy. A Security Analysis Framework Powered by an Expert System, *International Journal of Computer Science and Security (IJCSS)*, Vol. 4, No. 6, 2011, pp. 505–527.

[19] Chang Li-Yun, Lee Zne-Jung. Applying fuzzy expert system to information security risk Assessment – A case study on an attendance system, International Conference on Fuzzy Theory and Its Applications (iFUZZY), 2013, pp. 346 – 351.

[20] M. Kanatov, L. Atymtayeva, B.Yagaliyeva. (2014). Expert systems for information security management and audit, *Implementation phase issues, Soft Computing and Intelligent Systems (SCIS), Joint 7th International Conference on and Advanced Intelligent Systems (ISIS)*, 2014, pp. 896 – 900.

[21] K.C. Lee, C.H. Hsieh, L.J.Wei, C.H. Mao, J.H. Dai, Y.T. Kuang. Sec-Buzzer: cyber security emerging topic mining with open threat intelligence retrieval and timeline event annotation, Soft Computing, 2016, pp. 1–14.

[22] S. Pan, T. Morris, U. Adhikari. (2015). Developing a Hybrid Intrusion Detection System Using Data Mining for Power Systems, *IEEE Transactions on Smart Grid*, Vol. 6, Iss. 6, 2015, pp. 3104 – 3113.

[23] V. Lakhno, S. Kazmirchuk, Y. Kovalenko, L. Myrutenko, T. Zhmurko. Design of adaptive system of detection of cyber-attacks, based on the model of logical procedures and the coverage matrices of features, Eastern-European Journal of Enterprise Technologies, No 3/9 (81), 2016, pp. 30–38.

[24] P. Louvieris, N. Clewley, X. Liu. Effects-based feature identification for network intrusion detection. Neurocomputing, Vol. 121, Iss. 9, 2013, pp. 265–273.

[25] Z. Wang, X. Zhou, Z. Yu, Y. He, D. Zhang. Inferring User Search Intention Based on Situation Analysis of the Physical World, *Chapter Ubiquitous Intelligence and Computing of the series Lecture Notes in Computer Science*, Vol. 6406, 2010, pp. 35–51.

[26] A. P.Yeremeev, P. R.Varshavskiy, I. Ye. Kurilenko. Modelirovanie vremennykh zavisimostey v intellektualnykh sistemakh podderzhki prinyatiya resheniy na osnove pretsedentov, *International Journal «Information technologies and knowledge»*, Vol. 6, № 3, 2012, pp. 227–239.

[27] A.A. Kulinich. Kontseptualnye «karkasy» plokho opredelennykh predmetnykh oblastey. Otkrytye semanticheskie tekhnologii proektirovaniya intellektualnykh sistem: materialy III Mezhdunarodnoy nauchno-tekhnicheskoy konferentsii (Minsk, 21–23 fevralya 2013) / Pod red. Golenkova V.V. – Minsk: BGUIR, 2013, pp. 135–142.

[28] C. Puri, C. Dukatz. Analyzing and Predicting Security Event Anomalies: Lessons Learned from a Large Enterprise Big Data Streaming Analytics Deployment, 26th International Workshop on Database and Expert Systems Applications (DEXA), September 1–4, Valencia, Spain, 2015, pp. 152–158.

[29] R. Verma, M. Kantarcioglu, D. Marchette, E. Leiss, T. Solorio. Security Analytics: Essential

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Data Analytics Knowledge for Cybersecurity Professionals and Students, *IEEE Security & Privacy*, Vol. 13, Iss. 6, 2015, pp. 60 – 65. DOI: 10.1109/MSP.2015.121

[30] A. Razaq, H.Tianfield, P. Barrie. A big data analytics based approach to anomaly detection, BDCAT '16 Proceedings of the 3rd IEEE/ACM International Conference on Big Data Computing, Applications and Technologies, 2016, pp. 187–193.

[31] L. Perlovsky, O. Shevchenko. (2014). Dynamic Logic Machine Learning for Cybersecurity, *Chapter Cybersecurity Systems for Human Cognition Augmentation of the series Advances in Information Security*, Vol. 61, 2014, pp. 85–98.

[32] V. A. Lakhno, Y. N. Tkach, T.A. Petrenko, S.V. Zaitsev, V. M. Bazylevych. Development of adaptive expert system of information security using a procedure of clustering the attributes of anomalies and cyber attacks, Eastern-European Journal of Enterprise Technologies, No 6/9 (84), 2016, p. 32–44.

[33] M. Seijo Simó, G. López López & J. I. Moreno Novella. Cybersecurity Vulnerability Analysis of the PLC PRIME Standard. Security and Communication Networks, 2017.

[34] G. Beketova, B. Akhmetov, A. Korchenko, V, Lakhno, A. Tereshuk. Cyber intelligence systems based on adaptive regression splines and logical procedures of attack recognition. *Computer modelling and new technologies*, Vol. 21, No. 2, 2017, pp. 7–16.

[35] Lakhno V., Petrov Al., Petrov Ant. Development of a Support System for Managing the Cyber Security of Information and Communication Environment of Transport, *Information Systems Architecture and Technology : 38th International Conference on Information Systems Architecture and Technology (ISAT 2017)*, Wroclaw, 17–19 September 2017 : proceedings, Wroclaw : Springer, 2017, pp. 113–127.