UDC 004.056 **doi: 10.20998/2522-9052.2019.1.22**

O. Milov

Simon Kuznets Kharkiv National Univrsity of Economics, Kharkiv, Ukraine

ADAPTIVE DECISION SUPPORT SYSTEMS FOR CYBER SECURITY

The subject of the research is the principles and models of adaptive decision support systems in cyber security. **The purpose** is to develop basic principles and models underlying the operation of adaptive decision support systems in the field of cybersecurity. **The methods of research** are methods of system analysis, control theory, decision theory, and artificial intelligence. **The result of the study.** The basic principles and models are proposed, the consideration and use of which in decision support systems will allow the formation of adaptive properties of the described systems. It is shown that the properties of adaptability can be formulated as a learning task. Presents optimization algorithms that underlie learning processes. **Conclusion.** The combined use of mathematical modeling methods, the theory of adaptation and artificial intelligence methods (training, pattern recognition and problem solving planning) with the corresponding creation of ontologies of cybersecurity systems that ensure the filling of databases, models and knowledge will allow you to implement an effective adaptive decision support system that will be useful a tool for managers at any level at all stages of decision making and implementation. The presented approaches can be used as a basis for building and operating decision support systems, increasing the area of application of such systems due to the formation of their adaptability properties.

Keywords: adaptability; decision support systems; cybersecurity; information security; learning; search for solutions.

Introduction

Nowadays it is almost impossible to find a branch of human activity where there is no information technology (IT).

Due to the rapid growth of IT technologies, companies often face the need to increase information security. However, information security is a complex system that is very difficult to manage. As a result, in most organizations there is a risk of information system security.

Modern decision-making for most people and organizations depends on online information. In addition, the professional, individual and social life of many ordinary people is connected with networks and the information available in them. The infrastructure for these networks is usually the Internet. Such dependence on an open source of information creates new opportunities for opponents. Cyber incidents, when opponents affect or control communication and information systems to influence human behavior, have become commonplace.

As a rule, malware, such as viruses, worms, trojans and botnets, are used to attack:

- accessibility: reduce communication / computing power or prevent the availability of information and communication systems;
- confidentiality: compromise confidential information;
- confidentiality: get detailed information about individuals and organizations;
- integrity: creating uncertainty about information.

It should be noted that the task of improving the security of information systems and technologies in modern conditions is characterized by complexity and uncertainty associated with a large number of internal and external factors affecting information security. To solve the problem of information security, it is especially important to identify assets and establish the initial level of information system security. The identification process should take into account the basic characteristics of information assets: the value of information, the sensitivity of assets to threats, the presence of protective measures.

The carrier of knowledge about this subject area, which allows to form various databases (data, models, scenarios, knowledge) is the ontology of cybersecurity. It is the ontology that reflects the domain-specific knowledge in a form that a computer can use to work effectively [1, 2].

The ontology of the DSS should contain the following concepts as basic ones:

- threat - a potential cause of an unwanted incident that could harm the system or organization;
- vulnerability - physical, technical or administrative weakness that can be exploited by threats.
- management control is used to mitigate vulnerabilities by implementing organizational or physical measures.
- asset - all that matters to the organization.

An ontology should also reflect:

- problem area of complex security tasks;
- concepts that define the essence of cybersecurity and the relationship between them;
- external and internal objective factors, external and internal subjective factors;
- measures and technologies to ensure integrated security of information systems;
- heuristic knowledge of the security status of information systems, integrated security strategies;
- identification of information system assets, determination of criteria and safety indicators, development of procedures for evaluating criteria and indicators for developing an integrated information security support model, etc.
- principles of integrated information security (consistency, adaptability, transparency and confidentiality, continuity, training and experience, etc.).

Thus, the solution of the problem area provides comprehensive security (a set of basic concepts that define the nature of the research and the relationship between them), including:

the subject area,

the purpose of the research,

the tasks, the possible tactics, the strategies used to achieve this goal.

It should be noted that among the factors affecting safety, a special place is occupied by subjective factors that are potentially the most dangerous [3].

Cyber attacks primarily affect human behavior, creating confusion and information overload, stimulating irrational behavior.

However, the issues of modeling the impact of cyber attacks on human behavior has not been adequately reflected in the literature.

Instead, most research focuses on modeling attacks and technical solutions, as well as measures to prevent, detect, and recover from an attack.

Taxonomies are provided for attacks, attackers and human effects of cyber attacks, as well as simulating the relationship between cyber attacks and the decision-making process [4–6].

It should be recognized that effective opposition to cyber-attacks cannot be performed exclusively by people or machines working individually. Rather, they should cooperate. In particular, these tasks not only require computing power to cope with the complexity of the information that is generated during various kinds of incidents, but also require a person to understand the situation that unfolds, which allows them to prioritize tasks and monitor the operation of autonomous objects [7–14].

Under these conditions, a possible solution is the creation and use of a decision support system (DSS), which allows for:

- collection and integration of information about the facility and management environment;
- processing and storage of this information with acceptable degrees of aggregation;
- assessment of the state of the object and the control environment with the prediction of a possible change of states;
- search for management solutions initiated by assessments of the state of the object and the management environment or unfavorable forecasts of the development trends of the controlled processes;
- optimization of found and recommended solutions;
- decision making with challenge capabilities to analyze both the data underlying the search for recommended solutions, and the logic and mathematical methods used, on which the search for proposed solutions was based.

Methods and Approaches

The current approaches to automating decision-making in the management of complex objects are based on game-theoretic, semiotic principles and methods of the theory of identification and experiment design.

In the first case, a scheme is studied in which the control body Y always knows a set of mutually exclusive solutions

$$R = \{r_1, r_2, \dots, r_m\}.$$

He needs to take one of them; the environment and the control object are in one of the mutually exclusive states

$$Z=\{z_1, z_2, \dots, z_n\},$$

when Y at the moment of making decisions not all the information is known; there is always an evaluation functional $F=\{f_{ik}\}$, which characterizes the assessment of the degree of acceptability of the decisions made in terms of "winning" or "losing" Y in the event that he chooses a solution $r_k \in R$ for the state $z_j \in Z$. When implementing such a scheme, the quantitative side of the decision-making procedure in the conditions when the object and the environment "behave" antagonistically with respect to decision-making by the governing body implement methods of game theory [15, 16].

In the case of "passive" object and control environment, about which the control body knows the probability distribution $P=\{p_1, p_2, \dots, p_n\}$ on $Z=\{z_1, z_2, \dots, z_n\}$, they implement the methods of the theory of statistical solutions. The disadvantage of this approach in relation to decision-making systems is the laboriousness of the a priori study of all relationship options, taking into account the power of their sets, determined by the dynamic world of complex control objects. The resulting selection problem is difficult to implement on modern computers, especially for real-time control processes [17].

In the semiotic approach, a scheme is studied in which the control body knows: not always a certain set of parameters $\{x\}$ characterizing the current state of the object and the control environment; many ways of splitting $\{x\}$ into classes of states that require decisions; a set of models for finding solutions $\{M\}$; a set of mechanisms for finding solutions on models $\{\varphi\}$.

When such a scheme is implemented, the sets $\{k\}$ and $\{M\}$ are dynamically formed, their capabilities allow us to obtain the necessary solutions in an acceptable time, but the nature of the solutions obtained is qualitative [18].

Methods of the theory of identification and an experiment design can be applied only to the extent that statistics can be collected on the response of the control object to control actions in the mode of its operation. This makes it difficult to use them directly in the systems under consideration.

Taking into account the many functions assigned to the system, existing approaches to automating decision-making processes, as well as the presence of decision-makers, it is necessary to develop the concept of human-machine control [19].

Such systems possessing "own knowledge" and allowing automatically or by communicating with a person to find control solutions or to develop and substantiate logical facts that are not laid a priori, to engage in dialogue with decision makers will be referred to as a class of decision-making systems with intelligent automatic search engines.

Rapid changes in the organizational environment require that the DSS not only plays an active role in the management process, but also be able to adapt to changes in the environment.

We will refer to the class of adaptive decision-making systems systems that have knowledge of management technology, allow automatically or by communicating with a person to find management decisions, to develop and substantiate decision-making logic, not laid down a priori, to automatically select the necessary mathematical model to model the management process, and also to carry out adaptation (parametric, functional, structural) to changing conditions. Such systems will be considered as software and hardware and information and analytical technologies designed specifically to assist in solving problems of search, analysis and selection of the best possible options. In this case, the decision maker (DM) must be provided not only information and computing, but first of all technological and intellectual support of the procedure for choosing the best solution.

Results of studies

Currently, there is no complete general theory of systems of this class, and therefore there is no general model of such systems that have management knowledge and can use it to organize support for the targeted behavior of the management system in order to achieve specified quality criteria.

At the same time, an analysis of the tasks to be solved in decision-making systems with intelligent automatic search mechanisms shows that:

a formal apparatus describing the processes of recognizing situations, developing and making decisions in a rapidly changing situation with elements of uncertainty, must be extremely flexible;

decision-making and decision-making processes are based not only on quantitative characteristics, but also on factors that do not always have quantitative measures (psychological, moral, etc.) [20];

Special attention should be paid to the decision-making procedure itself, i.e. It is important to know which components of the decision-making and decision-making process should be controlled by the decision maker and which can be performed by computers;

an important place is occupied by the problem of human and machine communication;

the problem of learning or adapting the developed system to the subject area of management requires the development of a special procedure that allows the release of information presented formally (algorithmically) and informally (expertly);

the problem of designing and generating software implementation of different versions of mathematical models requires the development of a special design technology within this class of systems.

Adaptive support systems should be considered as intelligent systems. The model of an adaptive decision support system should be based primarily on the ideas of structural adaptation, learning theory, methods of pattern recognition (situations), and problem solving planning [21].

Management tasks are characterized by incomplete specifications. This suggests that the learning process should be the basic process that provides adaptation in the DSS, since it is the learning theory that deals with similar tasks and provides a tool for solving them.

Learning as a mathematical problem can be assigned to the class of *optimization problems of descriptions searching*. Optimization problem L is a quintuple

$$\left\langle X_L, Y_L, \rho_L, F_L, J_L \right\rangle$$

where X_L and Y_L – a set of input and output records; $\rho_L \subseteq X_L \times Y_L$ - relation (or function $\rho : X_L \to Y_L$); F_L – a set of relations ($f_L \subseteq X_L \times Y_L$ for all $f_L \in F_L$), called descriptions; J_L - quality operator for F_L, showing for each $f_L \in F_L$ the degree of its proximity to ρ_L. The task is to find an optimal J_L description f_L^* from F_L.

Depending on the method of specifying problems, the type of algorithms allowed, the class of problems studied, the criterion for evaluating synthesis, etc., the teaching methods in the DSS can be implemented in three approaches:

1) *the theory of statistical hypotheses* considering the set M of realizations of a random object with a probability distribution $p(x)$ on M. Let W be an arbitrary subset of M and $\{H\}$ be a set of fixed-type hypotheses associated with probability $p(x \in W)$ and characterizing it. It is required, based on a sample of M obtained in accordance with $p(x)$, to choose the most appropriate hypothesis from $\{H\}$. Statistical methods for random variables reveal their specific, statistical characteristics, which are often symptomatic with respect to the basic deep-seated patterns of the phenomena studied;

2) *the theory of parametric adaptation*, assuming that the set F of descriptions among which it is searched f_L^* for can be characterized by a vector of parameters and the choice is reduced to the search f_L^* for the extremum of the quality operator specified by the functional of the form

$$J(c) = \int_x Q(x,c)\, p(x)\, dx = Mx\{Q(x,c)\}$$

Here $x = (x_1, ..., x_l)$ is the vector of a discrete or continuous random process with a distribution density $p(x)$; $c = (c_1, ..., c_m)$ - vector, the components of which characterize the selected solution (description); $Q(x,c)$ is a functional of c depending on x; Mx is the mathematical expectation. The extremum $J(c)$ is found from the equation grad $J(c)$=0, or from the difference equation

$$c[t] = c[t-1] - \Gamma[t]\, grad_c L(c[t-1]),$$

where Γ – matrix $m \times m$, elements of which, generally speaking, depend on the current value *c*[*t*-1], elements of which, generally speaking, depend on the current value of *c*[*t*-1]. Proper selection of the matrix Γ should ensure the convergence of *c*[*t*] to the optimal value of *c**.

If *p*(*x*) is unknown and it cannot be pre-reconstructed, and also in the absence of an explicitly given functional *J*(*c*), one passes to another difference equation, which, using the observed values of *x*, *c* and grad$_c$ *Q*(*x*,*c*), allows determining the change in the vector *c*[*t*]:

$$c[t] = c[t-1] - \Gamma[t]\, grad_c Q\left(x[t], c[t-1]\right).$$

In this case, the corresponding iterative algorithms are called *adaptive* or *learning*;

3) *the theory of inductive inference*, which is a discrete mathematical model of learning by examples. The sets *X* and *Y* are countable, the desired description of *ρ* is generally specified by (potentially infinite) sequences of triples of the form

$$(x_1, y_1, \alpha_1), (x_2, y_2, \alpha_2), \ldots$$

such as if $\alpha_i \in \{0,1\}$ and $x_i \rho y_i$ only if $\alpha_i = 1$ (i.e., triples (x_i, y_i, α_i) represent examples and counterexamples *ρ*).

For real cases of using DSS, an approximate (partial) structured description of the situation is typical. This is a fundamental property of the situation, which allows us to consider it as an image.

The main purpose of pattern recognition is to build on the basis of systematic theoretical and experimental research effective computational tools for classifying formalized descriptions of situations to the corresponding classes.

The basis of such an assignment (recognition, classification) is to obtain some aggregated assessment of the situation from its description.

Provided that a correspondence is established between equivalence classes defined on a set of decisions and a set of situations, the automation of recognition procedures becomes an element of the automation of decision-making processes.

In adaptive cyber security DSS, various recognition tasks can be implemented, the relevance of which is determined by the fact that there can be many different situations corresponding to the implemented attacks, especially considering the emergence of new types, and the number of effective countermeasures is limited and determined largely by the class of attack.

Based on this, classes of recognition tasks have the following typification:

1) training with a teacher, which consists in classifying the situation according to its formalized description to one of the specified classes;

2) learning without a teacher (taxonomy, cluster analysis), which implements automatic classification of situations according to their formalized descriptions into a system of non-overlapping classes;

3) the formation of the information space describing the recognizable situation and reducing its dimension;

4) reduction of the initial data to a form suitable for recognition (construction of a formalized description of a recognizable situation).

Conclusion

The combined use of mathematical modeling methods, the theory of adaptation and artificial intelligence methods (training, pattern recognition and problem solving planning) with the corresponding creation of ontologies of cybersecurity systems that ensure the filling of databases, models and knowledge will allow you to implement an effective adaptive decision support system that will be useful a tool for managers at any level at all stages of decision making and implementation.

References

1. Adiel, Aviad, Krzysztof, Węcel and Witold, Abramowicz (2018), “A Concept for Ontology-Based Value of Cybersecurity Knowledge”, *International Journal of Management and Economics*, No. 54 (1), pp. 50–57.
2. Md Mehedi Hassan Onik, Nasr Al-Zaben, Hung Phan Hoo and Chul-Soo Kim (2018), “A Novel Approach for Network Attack Classification Based on Sequential Questions”, *Annals of Emerging Technologies in Computing*, Vol. 2, No. 2, pp. 1–14, available at: http://aetic.theiaer.org/archive/v2n2/p1.html.
3. Atymtayeva, L., Kozhakhmet, K. and Bortsova, G. (2014), “Building a Knowledge Base for Expert System in Information Security”, *Chapter Soft Computing in Artificial Intelligence,* Vol. 270, pp. 57–76, DOI: http://doi.org/10.1007/978-3-319-05515-2_7
4. Bezerra, S., Cherruault, Y., Fourcade, Y. and Verron, G. (1996), “A Mathematical Model for the Human Decision-Making Process”, *Elsevier Mathematical and Computer Modelling*, No. 24 (10), pp. 21–26.
5. Kotenko, I.V. (2005), “Agent Based Modelling and Simulation of Cyber Warfare between Malefactors and Security Agents in Internet”, *Proceedings of 19th European Simulation Multiconference.*
6. Stytz, M.R. and Banks S.B. (2010), “Addressing Simulation Issues Posed by Cyber Warfare Technologies”, *SCSM&S Magazine,* No. 3.
7. Sarvapali, D. (2016), “A Disaster Response System based on Human-Agent Collectives”, *Journal of Artificial Intelligence Research*, No. 57, pp. 661–708.
8. Kulikova, O., Heil, R., Berg, J. and Pieters W. (2012), “Cyber Crisis Management: A decision-support framework for disclosing security incident information”, *2012 International Conference on Cyber Security*, IEEE Society, pp.103–112.
9. Gabriela del Rocío Roldán Molina (2017), *A Decision Support System for Corporations Cyber Security Risk Management*, Dissertation Master´s Degree in Computer Engineering, Leiria, September 2017, 101 p.
10. Amin Salih, M., Yuvaraj, D., Sivaram, M. and Porkodi, V. (2018), “Detection And Removal Of Black Hole Attack In Mobile Ad Hoc Networks Using Grp Protocol”, *International Journal of Advanced Research in Computer Science*, Vol. 9, No 6, pp. 1–6, DOI: http://dx.doi.org/10.26483/ijarcs.v9i6.6335

11. Roldan, G., Almache, M., Rabadao, C., Yevseyeva I. and Fernandes V. (2017), “A Decision Support System for Corporations Cybersecurity Management”, *12th Iberian Conference on Information Systems and Technologies*, Lisboa.
12. Amin Salih M. and Potrus M.Y. (2015), “A Method for Compensation of Tcp Throughput Degrading During Movement Of Mobile Node”, *ZANCO Journal of Pure and Applied Sciences*, Vol. 27, No 6, pp. 59-68.
13. Saravanan, S., Hailu, M., Gouse, G.M., Lavanya, M. and Vijaysai, R. (2019), “Optimized Secure Scan Flip Flop to Thwart Side Channel Attack in Crypto-Chip”, *International Conference on Advances of Science and Technology*, ICAST 2018. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 274, Springer, Cham, DOI: https://doi.org/10.1007/978-3-030-15357-1_34
14. Porkodi, V., Sivaram, M., Mohammed, A.S. and Manikandan, V. (2018), “Survey on White-Box Attacks and Solutions”, *Asian Journal of Computer Science and Technology*, Vol. 7, Issue 3, 2018, pp. 28–32.
15. Ravishankar, M., Rao, D.V. and Kumar, C.R.S. (2018), “A Game Theoretic Software Test-bed for Cyber Security Analysis of Critical Infrastructure”, *Defence Science Journal*, Vol. 68, No. 1, pp. 54-63, DOI: https://doi.org/10.14429/dsj.68.11402
16. Ibidunmoy, E.O., Alese, B.K. and Ogundele, O.S. (2014), “A Game-theoretic Scenario for Modelling the Attacker-Defender Interaction”, *J. of Comp. Eng. and Information Technology*, Vol. 2, No. 1, DOI: https://doi.org/10.4172/2324-9307.1000103
17. Konkarikoski, K. and Ritala, R. (2009), “Elements of Statistical Decision Making”, *XIX IMEKO World Congress Fundamental and Applied Metrology 11*, Lisabon, Portugal, September 6, pp. 1042–1047.
18. Massel, L.V. and Massel, A.G. (2017), “Intelligent system of semiotic type for decisionmaking support in Russia energy sector based on situational management conception”, *Advances in Computer Science Research* (ACSR), Vol. 72, pp. 423–429.
19. Gachet, A. and Haettenschwiler, P. (2003), “Distributed Decision Support Systems - A Federalis Model of Cooperation”, *Human Centered Processes - Distributed Decisio Making and Man-Machine Cooperation*, proceedings of the 14th MINI EURO Conference, Luxembourg, pp. 211–216.
20. Akhmetov, B., Lakhno, V., Boiko, Y. and Mishchenko A. (2017), “Designing a Decision Support System for the Weakly Formalized Problems in the Provision of Cybersecurity”, *Eastern-European Journal of Enterprise Technologies*, No. 1/2 (85), pp. 4–15.
21. Lakhno, V.A. (2017), “Development of a System for Supporting Solutions for Managing Cyber Security”, *Radio Electronics, Computer Science, Control,* No. 2, pp. 109–116.

Received (Надійшла) 11.01.2019
Accepted for publication (Прийнята до друку) 13.03.2019

Адаптивні системи підтримки прийняття рішень в кібербезпеці

О. В. Мілов

Предмет дослідження - принципи і моделі адаптивних систем підтримки прийняття рішень в кібербезпеці. **Мета** - розробка базових принципів і моделей, що лежать в основі функціонування адаптивних систем підтримки прийняття рішень в області кібербезпеки. **Методи дослідження.** В якості методів дослідження виступають методи системного аналізу, теорії управління, теорії прийняття рішень і штучного інтелекту. **Результат вивчення**. Запропоновано базові принципи і моделі, облік і використання яких в системах підтримки прийняття рішень дозволить сформувати адаптивні властивості описуваних систем. Показано, що властивості адаптивності можуть бути сформульовані як завдання навченості. Представлені алгоритми оптимізації, які лежать в основі процесів навчання. **Висновок.** Комбіноване використання методів математичного моделювання, теорії адаптації та методів штучного інтелекту (навчання, розпізнавання образів та планування завдань) з відповідним створенням онтологій систем кібербезпеки, що забезпечують заповнення баз даних, моделей та знань, дозволить реалізувати ефективна адаптивна система підтримки прийняття рішень, яка буде корисною інструментом для керівників будь-якого рівня на всіх етапах прийняття та впровадження рішень. Представлені підходи можуть бути покладені в основу побудови і функціонування систем підтримки прийняття рішень, збільшуючи область застосування таких систем за рахунок формування у них властивостей адаптивності.

Ключові слова: адаптивність; системи підтримки прийняття рішень; кібербезпека; інформаційна безпека; навчання; пошук рішень; простір ситуацій; простір завдань.

Адаптивные системы поддержки принятия решений в кибербезопасности

А. В. Милов

Предмет исследования – принципы и модели адаптивных систем поддержки принятия решений в кибербезопасности. **Цель** – разработка базовых принципов и моделей, лежащих в основе функционирования адаптивных систем поддержки принятия решений в области кибербезопасности. **Методы исследования.** В качестве методов исследования выступают методы системного анализа, теории управления, теории принятия решений и искусственного интеллекта. **Результат изучения.** Предложены базовые принципы и модели, учет и использование которых в системах поддержки принятия решений позволит сформировать адаптивные свойства описываемых систем. Показано, что свойства адаптивности могут быть сформулированы как задача обучаемости. Представлены алгоритмы оптимизации, которые лежат в основе процессов обучаемости. **Заключение.** Совместное использование методов математического моделирования, теории адаптации и методов искусственного интеллекта (обучение, распознавание образов и планирование решения проблем) с соответствующим созданием онтологий систем кибербезопасности, обеспечивающих наполнение баз данных, моделей и знаний, позволит реализовать эффективная адаптивная система поддержки принятия решений, которая будет полезным инструментом для руководителей на любом уровне на всех этапах принятия решений и их реализации. Представленные подходы могут быть положены в основу построения и функционирования систем поддержки принятия решений, увеличивая область применения таких систем за счет формирования у них свойств адаптивности.

Ключевые слова: адаптивность; системы поддержки принятия решений; кибербезопасность; информационная безопасность; обучение; поиск решений; пространство ситуаций; пространство задач.