УДК 519.816+338.24 **doi: 10.26906/SUNZ.2019.4.082**

O. Milov, O. Korol, V. Khvostenko

Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine

DEVELOPMENT OF THE CLASSIFICATION OF THE CYBER SECURITY AGENTS BOUNDED RATIONALITY

The **subject** are the bounded rationality agents of cyber security system. The **purpose** of this work is is to build a classification system for agents of a cybersecurity system with limited rationality. The **tasks**: consideration of the decision-making process by agents in cybersecurity systems, analysis of various manifestations of bounded rationality of agents of the cybersecurity system, introduction of classification features of bounded rationality, formal presentation of bounded rationality of various types, combining agents with various types of bounded rationality into a whole classification system. **Results.** Presents approaches to the classification of the concept of rationality in relation to cybersecurity systems. Such types of rationality are considered as strong, semi-strong, weak. Further classification of types of rationality is carried out on the basis of the place of manifestation of rationality. For this, the decision-making process in the cybersecurity system has been considered, formal relations have been introduced, which characterize its various stages. Such types of bounded rationality as informational, methodological, predictive, evaluative and conditional are considered. The ratio of the considered types of rationality is presented. **Conclusion:** A comparison of various types of bounded rationality, based primarily on its place in the decision-making process, made it possible to propose a classification scheme of bounded rationality characteristic of agents of the cybersecurity system. The result of the formalization of the description of bounded rationality is presented, which can be used as the basis for the development of models of behavior of interacting agents of cybersecurity systems.

Keywords: cyber security, decision making process, decision maker, bounded rationality.

Introduction

In recent years, in the literature on decision-making in cybersecurity systems and the behavior of participants in cyber conflict in particular, it is increasingly said that the behavior of decision-makers (DM) can only be partially characterized as rational. The concept of bounded rationality, originally introduced in [1], is also found in studies on the interaction of participants in teams of cybersecurity systems [2, 3].

Modeling bounded rationality [4] is becoming increasingly relevant due to the increasing interest in shaping and making decisions on ensuring the security of critical infrastructure systems.

The behavior of a decision maker may be far from perfect rationality, either because of its internal motivating factors, or because it is impossible to act rationally due to external factors beyond its control. In the first case, we should speak of intentionally irrational or irrational behavior, which becomes quite rational if we consider it from an alternative position. In modern studies on the so-called "minority games" [5-8], an intentionally irrational strategy of behavior promises the player a much greater gain than the average, which the majority adheres to. The second case of imperfectly rational behavior is more likely associated with objective reasons, it is this option that corresponds to the concept of bounded rationality. The limited rationality is connected, first of all, with the lack of any resources (temporary, material, physical) for the decision maker to make a completely rational decision.

Research results

To determine possible approaches to modeling, it is necessary first of all to identify the forms of rationality, in particular limited, and to classify them. Consider the options for the classification of rationality, highlighting the following forms: strong, semi-strong and weak.

A strong form of rationality involves the maximization of utility in one form or another. However, the traditional interpretation of maximization often simplifies the conditions: the role of organizational structures is minimized, the participants in cyber conflict are represented by their utility functions, the distribution of functions between the various participants in the cyber security system is treated as given, and optimization is common. This approach ensures the applicability of formal optimization methods, however, it turns out to be very far from real practice.

A semi-strong form of rationality is limited rationality. This form of rationality suggests that cybersecurity agents tend to act rationally, but in fact they only have this ability to a limited extent. In such a definition, there is both a desire for rationality and its limitations. Modern behavioral sciences recognize that human rationality is limited, and argue that both parts of the definition are essential. The pursuit of rationality means a focus on the economical use of limited resources, and the recognition of limited cognitive abilities serves as an incentive to explore the functioning of cybersecurity systems in general. If the assumption of bounded rationality is made, then making decisions that fully cover all possible cases is a non-realistic assumption in the study of security systems. On the other hand, if intelligence is a limited resource, then the desire to save on its use is quite understandable. There are two ways to save on intelligence in the framework of the bounded rationality model: firstly, during the decision-making processes themselves, and secondly, using the help of governing structures. In this case, it is necessary to distinguish between situations of choice in terms of limited information (uncertainty or low probability of events) and situations in which the decision maker does not have an idea of the full set of possible states of choice when we are dealing with limited cognitive activity in one form or another.

Finally, organic rationality is the weakest form. This is the rationality of some process occurring in the cybersecurity system. At the same time, within the framework of the evolutionary approach, it considers the rationality of the whole process from the point of view of the goals of the system, which to some extent resembles the well-known thesis “the goal justifies the means”.

Obviously, this classification should be supplemented with two other forms of behavior: irrational and irrational. However, the decision on whether behavior can be attributed to these two types substantially depends on what is known about the decision makers ’motivations, its goals and its consistency with each other and the goals of the cybersecurity system as a whole.

The above classification exhaustively exhausts the possible types of rationality, however, the concept of bounded rationality should be considered in more detail.

Since rationality is ultimately realized by the adoption of a decision, then the classification should be associated with the decision-making process. External constraints affecting the rationality of the choice of decision n makers can manifest themselves at different stages of the decision-making process and in various ways. Therefore, the place of occurrence of limited rationality in the decision-making process can be considered as the basis of classification.

Consider the basic model of the decision-making process (Fig. 1).

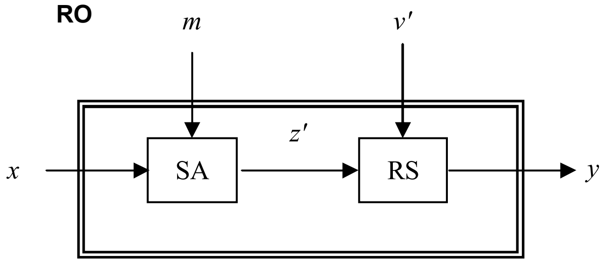

Fig. 1. The basic model of the decision-making process

The decision maker receives input information x from its environment and uses it at the situation assessment (SA) stage to determine the specific value of the variable *z*, which indicates the situation. Information from the rest of the safety management team (RO) - *m* - may change the assessment of the situation and result in a different value from the previously accepted value for *z*'. Possible alternatives for action will be evaluated at the stage of selecting an answer (RS). The result of this process is the choice of action or response decision *y*. The control input *v*' from the rest of the organization (external environment) can influence the selection process.

At the stage of obtaining input information from the environment, the limited resources of decision makers lead to a lack of information about the external environment and the situation of the confrontation as a whole. This option should be distinguished from decision making under conditions of uncertainty, which arose due to the fundamental impossibility of obtaining complete information, for example, because of the presence of stochastic elements in the decision making problem. The rationality of decision-makers may be limited at this stage also because the information coming to it depends on other persons in whose interests to hide or distort complete information about the state of the external environment and the situation. In this case, we can talk about decision-making in conflict situations, where the limitation of decision makers is manifested in the form of insufficient data on reliable and complete information.

In contrast to the previous case, there is no fundamental impossibility of obtaining information; however, obtaining it may require a significant investment of time and resources. It can be assumed that with sufficient time and material resources, the decision makers would conduct a thorough research (exploration) and receive additional information. Therefore, this situation can be characterized as information limited rationality.

At the stage of assessing the situation (SA), one of the following problems may arise before the DM: the lack of assessment methods for this class of situations, the absence or lack of algorithms that implement assessment methods, incompleteness of information for applying certain algorithms, computational complexity of assessment algorithms, and .P. The problem of incomplete information returns us to the previous stage of decision making.

The most significant from the point of view of bounded rationality is the absence of methods and algorithms for evaluation. This problem becomes even more complicated than the more specific is the decision-making task, which may be characteristic of hybrid threats. It is characteristic of single (single) choice tasks in which the decision maker deals with a new threat. The limited rationality of the decision maker may lead to the choice of an inadequate method of assessing the situation or obtaining an unreliable assessment of *z*. Thus, at the stage of assessing the situation, we are dealing with methodological and estimated limitations of rationality.

At the next stage of evaluating possible alternative actions, lack of resources leads to two options for limitation: the limited number of alternatives and the limited knowledge of the consequences of choice. The limited rationality associated with a multitude of alternatives is manifested in the fact that the decision maker may in principle be unaware of the existence of such an alternative, or exclude from consideration those alternatives that seem to him impracticable or for studying which will have to spend too many resources. The limitedness of alternatives returns us to the first stage of informational limitation, since it speaks of the insufficient study of the situation. But limited knowledge about the consequences is an independent option, because besides the lack of information it can also be associated with limited possibilities of forecasting certain elements of the situation, both for objective reasons and because of targeted actions by RO elements (for example, in the face of conflicts of interests of various LPR). So, at this stage predictive limited rationality arises.

Finally, at the last stage of decision making - the stage of choosing the option of action y - limited rationality can be associated with the lack of a method of choice, that is takes the form of a methodological, or appears as a modification of the original decision-making task by introducing additional constraints, i.e. conditional. From this point of view, it seems useful to us to use the classification proposed in [9].

Let the interests of the decision maker reflect its objective function *f(y)*, defined on a set of possible actions: $y \in \mathrm{A}$, f: $\mathrm{A} \to \Re^1$. Then the set of rational choice will be a set of actions that deliver the maximum of the objective function:

$$P^0(f(\cdot),A)=\left\{Arg\max_{y\in A} f(y)\right\}. \qquad (1)$$

Principle (1) corresponds to rationality in a strong form. Models of bounded rationality imply the abandonment of the aim of the decision maker to achieve the absolute maximum, replacing it with the assumption of striving to achieve a certain level of utility, perhaps, depending on the magnitude of the optimum.

So far, we have not imposed any specific restrictions on the aims of the decision maker and their presentation. However, this becomes necessary when building a formal description. We introduce the following assumption about the objective function and the admissible set: let $f()$ be continuous and concave, and the set A be convex and compact. Within the framework of these assumptions, the set $P^0(f(\ ),\ A)$ is non-empty.

Let $y^* = \arg\max_{y\in A} f(y)$.

For simplicity, we assume that $f(y^*) \geq 0$.

Three types of bounded rationality, corresponding to the decision-making stage, describe possible easing of the maximization requirements.

Minimum sufficient solution. Suppose that the decision maker seeks to provide some minimum level of individual utility U, that is, a set of rational choice can be considered

$$P^1(f(\cdot),A,\bar{U})=\{y\in A/ f(y)\geq \bar{U}\}. \qquad (2)$$

Rational absolute losses. Suppose that the agent is ready to accept the loss of a fixed value $\varepsilon \geq 0$ compared with the absolute maximum. Then the rational choice set is

$$P^2(f(\cdot),A,\varepsilon)=\{y\in A/ f(y)\geq f(y^*)-\varepsilon\}. \qquad (3)$$

Note that this method of taking into account the “insensitivity” and thresholds for distinguishing is most common in game-theoretic models and, when used in the construction of generalized solutions, makes it possible to achieve stability of the solution by the model parameters. In addition, this type of presentation of rational behavior is consistent with models that take into account uncertainty, including the uncertainty of the goals of decision makers.

Rational relative loss. Suppose that the decision maker is ready to accept the losses that are no more than a fixed part $\delta \in (0,1]$ of the maximum possible result for him. Thus, the set of rational choice depends on the optimal value:

$$P^3(f(\cdot),A,\delta)=\{y\in A/ f(y)\geq (1-\delta)f(y^*)\} \qquad (4)$$

or equivalent

$$P^3(f(\cdot),A,\delta)=\{y\in A/ f(y^*)-f(y)\leq \delta f(y^*)\}. \qquad (5)$$

The introduced three types of bounded rationality cover most of the tasks encountered in practice and can be used in the case of multicriteria decision-making problems.

Note that the optimization of absolute and relative losses is associated with finding the optimal solutions, and the possibilities of this search are limited due to the limitation of decision makers in the previous stages of the decision-making process. Therefore, this classification can only be considered an integral part of the more general one considered earlier.

Constructed version of the classification of bounded rationality should be presented in the form of a diagram (Fig. 2), which shows the types of bounded rationality relating to the various stages of the decision-making process.

Stages of the decision process	**Types of bounded rationality**				
	informational	**methodological**	**estimated**	**forecast**	**conditional**
Receiving the information	▨				
Assessment of the situation		▨	▨		
Evaluation of alternatives	▨	▨		▨	
Decision making		▨			▨

Fig. 2. Classification of bounded rationality

The proposed classification makes it possible to formalize the concept of bounded rationality as follows.

Let us denote by x^D information about the situation accessible by the decision maker. This information may be complete and relevant to the actual state of affairs, in this case $x^D = x$, where x is complete and reliable information about the decision-making situation. If the information is incomplete, but all its components are reliable, then we get: $x^D \subset x$, and, finally, the presence of unreliable information leads to the case $x^D - x \neq \varnothing$. The latter option is most fraught with the adoption of not just irrational, but obviously wrong decision. Thus, informational bounded rationality can have three degrees: absence or unboundedness, partial boundedness, and fundamental boundedness. The same degrees can be distinguished in all other types of bounded rationality.

In the future, we will mark with an index *D* the components of the decision-making process related to DM.

At the stage of assessing the situation in terms of the methodological and evaluative limited rationality of the decision maker, only a fraction of the entire set of adequate algorithms for assessing the situation $\{SA\}$ is available $\{SA^D\}$, i.e.

$$\{SA^D\} \subseteq \{SA\}. \tag{6}$$

The application of a full set of assessment algorithms to the information available to the decision maker gives an assessment, generally speaking, different from that which can be obtained on the basis of complete information, and even more different from the one that the decision maker will receive, operating with its own set of algorithms:

$$\begin{gathered} z = SA(x), \\ z^a = SA(x^D), \\ z^D = SA^D(x^D), \\ z \gtreqless z^a, \; z^a \gtreqless z^D, \; z \gtreqless z^D. \end{gathered} \tag{7}$$

It is obvious that in this sequence the assessment corresponding to absolute rationality (optimality) may differ significantly from that used by the decision maker.

If the process of assessing the situation is also affected by the rest of the team, then the result will undergo certain changes and, therefore, we will

$$\begin{gathered} z' = SA(x,m), \; z'^D = SA^D(x^D,m), \\ z' \gtreqless z'^D, \; z'^D \gtreqless z^D, \end{gathered} \tag{8}$$

where *m* – information from the external environment,

z' – assessment of the situation, taking into account external influence based on complete information,

z'^D – the same for evaluating decision makers. Next, the decision maker acts on the basis of this assessment.

Further, let $\{RS\}$ - the whole set of methods and algorithms for choosing a solution adequate to this task of choosing a solution $\{RS^D\}$ is the set of available decision makers due to the informational, methodological and predictive boundedness of algorithms and methods for choosing a solution, while

$$\{RS^D\} \subseteq \{RS\}. \tag{9}$$

The final choice of the solution - y, made in the framework of a rational campaign and in conditions of independence, is the result of transformations:

$$y = RS(z) = RS(SA(x)). \tag{10}$$

Assuming that the selection process itself is also influenced by the external environment in the form of information *v'*, then the result will be different

$$y' = RS(z',v') = RS(SA(x,m),v'). \tag{11}$$

As for the choice made by the decision maker, its result is

$$y^D = RS^D(z^D) = RS^D(SA^D(x^D)) \tag{12}$$

in conditions of independence, or, in the presence of external influence

$$y'^D = RS^D(z'^D,v') = RS^D(SA^D(x^D,m),v'). \tag{13}$$

The relationship between these choices is the same as for the situation assessments (7), which can be represented by the scheme:

$$\begin{tikzcd} & y & \\ y^D & < \arrow[l] \arrow[r] \arrow[u] \arrow[d] & y'^D \\ & y' & \end{tikzcd}$$

Thus, considering any pair of choices, we obtain an inequality, the specific form of which depends on the conditions of choice.

Combining all of the above, we can present the effect of bounded rationality in the form of the following diagram (Fig. 3).

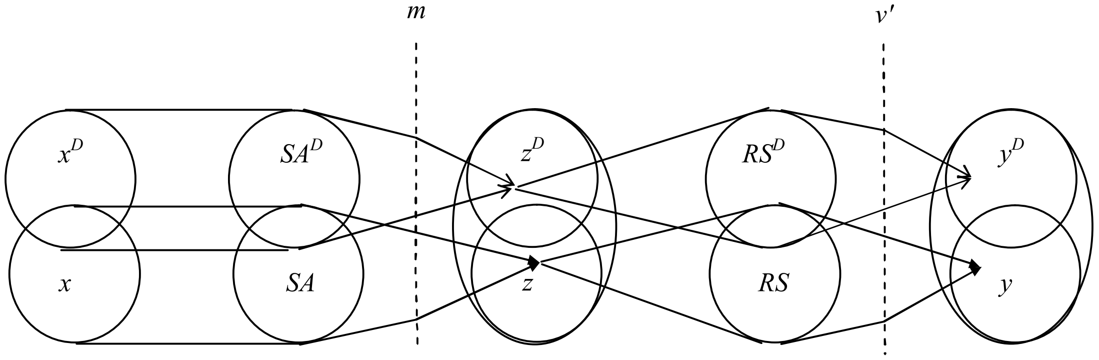

Fig. 3. The ratio of unlimited and limited rationality in decision making

The scheme can be used to build mathematical and simulational decision-making models in conditions of bounded rationality.

Conclusion

A comparison of various types of bounded rationality, based primarily on its place in the decision-making process, made it possible to propose a classification scheme of bounded rationality characteristic of agents of the cybersecurity system. The result of the formalization of the description of bounded rationality is presented, which can be used as the basis for the development of models of behavior of interacting agents of cybersecurity systems.

References

1. Herbert A. Simon (1955) / A Behavioral Model of Rational Choice // The Quarterly Journal of Economics, Vol. 69, No. 1 (Feb., 1955), pp. 99-118
2. Lempert, R. (2002). Agent-based modeling as organizational and public policy simulators. Proceedings of the National Academy of Sciences 99(3): 7195–7196.
3. Tuomas W Sandholm and Victor R Lesser (1995). Coalition formation among bounded rational agents. Technical report, University of Massachusetts at Amherst Computer Science Department, 1995.
4. Rubinstein, Ariel, Modeling Bounded Rationality (Cambridge, MA: MIT Press, 1998).
5. Gabaix, Xavier, ‘‘Some Game Theory with Sparsity-Based Bounded Rationality,’’ Working Paper, New York University, 2013.
6. Amin Salih M., Yuvaraj D., Sivaram M., Porkodi V. 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. P. 1–6, DOI: http://dx.doi.org/10.26483/ijarcs.v9i6.6335
7. Saravanan S., Hailu M., Gouse G.M., Lavanya M., Vijaysai R. 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
8. Manikandan V, Porkodi V, Mohammed AS, Sivaram M, “Privacy Preserving Data Mining Using Threshold Based Fuzzy cmeans Clustering”, ICTACT Journal on Soft Computing, Volume 9, Issue 1, 2018, pp.1813-1816. **DOI:** 10.21917/ijsc.2018.0252
9. Новиков Д.А. Сетевые структуры и организационные системы. М.: ИПУ РАН, 2003. – 102 с.

Рецензент: д-р техн. наук, проф. С. Г. Семенов,
Національний технічний університет “ХПІ”, Харків
Received (Надійшла) 17.06.2019
Accepted for publication (Прийнята до друку) 24.07.2019

Розробка класифікації агентів кібербезпеки з обмеженою раціональністю

О. В. Мілов, О. Г. Король, В. С. Хвостенко

Предметом є класифікація агентів з обмеженою раціональністю системи кібербезпеки. **Метою** роботи є побудова системи класифікації агентів системи кібербезпеки з обмеженою раціональністю. **Задачі:** розгляд процесу прийняття рішень агентами в системах кібербезпеки, аналіз різних проявів обмеженої раціональності агентами системи кібербезпеки, введення класифікаційних ознак обмеженої раціональності, формальне подання обмеженої раціональності різних типів, об'єднання агентів з різним типом обмеженої раціональності в єдину систему класифікації. **Висновок.** Порівняння різних типів обмеженої раціональності, заснованої, перш за все, на її місці в процесі прийняття рішень, дозволило запропонувати класифікаційну схему обмеженої раціональності, характерну для агентів системи кібербезпеки. Представлений результат формалізації опису обмеженої раціональності можна використовувати в якості основи для розробки моделей поведінки взаємодіючих агентів систем кібербезпеки.

Ключові слова: кібербезпека, процес прийняття рішень, ОПР, обмежена раціональність.

Разработка классификации агентов кибербезопасности с ограниченной рациональностью

А. В. Милов, О. Г. Король, В. С. Хвостенко

Предметом является классификация агентов с ограниченной рациональностью системы кибербезопасности. **Целью** работы является построение системы классификации агентов системы кибербезопасности с ограниченной рациональностью. **Задачи:** рассмотрение процесса принятия решений агентами в системах кибербезопасности, анализ различных проявлений ограниченной рациональности агентов системы кибербезопасности, введение классификационных признаков ограниченной рациональности, формальное представление ограниченной рациональности различных типов, объединение агентов с различным типом ограниченной рациональности в единую систему классификации. **Заключение.** Сравнение различных типов ограниченной рациональности, основанной, прежде всего, на ее месте в процессе принятия решений, позволило предложить классификационную схему ограниченной рациональности, характерную для агентов системы кибербезопасности. Представлен результат формализации описания ограниченной рациональности, который можно использовать в качестве основы для разработки моделей поведения взаимодействующих агентов систем кибербезопасности.

Ключевые слова: кибербезопасность, процесс принятия решений, ЛПР, ограниченная рациональность.