

RESEARCH FRAMEWORK FOR SYSTEM SECURITY OF TECHNOLOGICAL & INNOVATION SYSTEMS

Olha Kudrina¹

*Sumy State Pedagogical University named after A.S. Makarenko, Ukraine;
Centre for European Reforms Studies, Grand Duchy of Luxemburg*

Vitaliy Omelyanenko²

Sumy State Pedagogical University named after A.S. Makarenko, Ukraine

Abstract. *The purpose of this study is to consider the main aspects of system security theoretical concept and practical aspect within the technological & innovation systems research methodology development according to their considering as structurally complicated systems. Methodology.* In this study, we propose to use the concept of technological & innovation systems, in which it is analysed the development of the technological field in terms of structures and processes that support or impede its development. So this approach can be considered as an expanding to techno-socio-economic analysis, considered for the innovation system in our previous studies. *Results.* The problem of study comes from the national security and defence objectives, which can be achieved within the national innovation systems, considering new meaning and problems in the age of globalization and high technologies development. We can underline that the important factor of technological & innovation systems system security consists in system identification within the management theory as the determination of the structure of the system and its parameters by analysing input data and system outputs. At the same time, we can note the system specifics, e.g. the identification of industrial systems security deals with the establishment of the identity of production facilities an ecological security etc. The most important relationships of innovation & technological systems designing that allow establishing appropriate adaptive management decisions were proposed. For the development of combined models of innovation & technological systems security, the main aspects of this type of systems were considered. *Practical implications.* Based on this, the author proposed to use system indicators for security providing process. Using these indicators, we can identify system synchronous development speed and autonomous of speeds of security providing process. The technological & innovation systems security management is proposed to be analysed in two interrelated subsystems: self-organizing subsystems and technological subsystem. The main activities for the system security of highly complicated system providing were proposed. *Value/originality.* Based on the foregoing, the authors proposed to use security relationships adaptive management as a set of methods that can generate management systems, able to change the security-related parameters of regulator or controller structure according to the change of control object parameters or external disturbances acting on the control object.

Key words: system security, technological & innovation system, national security, national innovation system, technology, analysis.

JEL Classification: C51, O14, O32

1. Introduction

Today the problem of security is the main from the list of nation's strategic importance development priorities. It includes the complexity of transformation processes at the beginning of XXI century and is the condition and the objective of development policy because it requires

the concentration of all forces and resources on problems solving. Their distraction from threats neutralizing makes difficult or sometimes makes it impossible for the successful realization of development strategy.

Security management system in different innovation systems can be considered as a set of methods and

Corresponding author:

¹ Business Economics and Administration Department, Sumy State Pedagogical University named after A.S. Makarenko. Centre for European Reforms Studies, Grand Duchy of Luxemburg.

E-mail: olya.dina@gmail.com

² Business Economics and Administration Department, Sumy State Pedagogical University named after A. S. Makarenko.

E-mail: omvitaliy@gmail.com

instruments of ensuring the maintenance of safe state of the object (system), prevention, detection, and elimination of threats, health, environment, property, and information, having common means of collecting and information processing, and management. In this general definition, the security is considered in terms of its functionality and is a common case of an integrated security system. The necessity for further innovation system analysis of methodology development through the improvement of existing and developing the new tools for security assessment and providing is caused by the fact that with the growth of complexity of human-made systems and numerous links in them, and the more elements are in them, the greater the potential danger and risks and accordingly processes of analysing and forecasting system condition become more difficult.

A brief literature review has shown that the problem of our study comes from the national security and defence objectives, which can be achieved within the national innovation systems, considering new meaning and problems in the age of globalization and high technologies development.

In this framework, the main purpose of “technological & innovation system” conceptualization and analysing according to (Hekkert, 2009) is to “analyse and evaluate the development of a particular technological field in terms of the structures and processes that support or hamper it.” Within this analysis, such basic steps are highlighted:

- analysis of innovation system structure (actors and rules, which make up the system);
- analysis of how the system is functioning (functions and interaction between the functions analysis);
- analysis of system problems, which block of system well-functioning.

We believe that this approach can be useful for system security analysis because it provides possibilities for extended analysis.

Necessary for innovation systems efficient models development is caused by a clear understanding that innovation component becomes the main part of the global economic competition (New Challenges, 2008).

Experts (OECD, 1997) have noted that there are different approaches to national innovation systems analysing. For example, innovation firm-level surveys consider enterprise’s sources of knowledge most relevant to innovation and rank of different linkages of industrial sector and country. Cluster analysis focuses on interactions between particular types of firms and sectors, which can be grouped according to some technological and networking characteristics (OECD, 1997). But all these approaches consider innovation system as a separate object without answering the list of questions concerning system dynamics, different types of influences and impulses, subsystems dynamics etc.

Among studies, devoted to problems of national security and defence objectives, we can name research

(Mowery, 2009) focusing, in particular, on the USA during and after the Cold War, including a brief description of post-9/11 trends in related to defence and national security investments using R&D strategy. Also, systems security issues can be defined from the confidentiality & trade secrets as a part of the innovation process. In general, we need to identify vulnerability as a weakness in the target, which potentially can be exploited by security threats. For example, in the term “security economy” OECD experts describe a cluster of activities concerned with preventing (reducing) risk of deliberate harm to life or property (OECD, 2004).

In NPR 8715.3 C system safety is defined as “application of engineering and management principles, criteria, and techniques to optimize security ... within the constraints of operational effectiveness, time and cost throughout all phases of system life cycle” (NASA, 2011). This definition gives a base for security management of various systems.

The complexity of modern technological & innovation systems necessitates carrying out their depth analysis using system approach, methods and algorithms for structural and parametric synthesis based on technology package approach (Artyukhov et al., 2016) as a set of technologies and additional elements that provide efficiency of innovation & technological system. This approach is consistent with Benner L. (1997), who has suggested that any system definition describes dynamic interactions among people, procedures, and things and their influences on outcomes.

The technology package approach can be applied based on different management approaches. E.g. in 2007 International Organization for Standardization has released ISO 28000 “Specification for Security Management Systems for the Supply Chain”. Although in the title supply chain is included, given Standard specifies the requirements for security management system, including those aspects critical to security assurance for any organization or enterprise wishing to manage the security of organization or its activities.

The purpose of this study is to consider the main aspects of system security theoretical concept and practical aspect within the technological & innovation systems research methodology development according to their considering as structurally complicated systems.

2. The methodology of technological & innovation systems study review

The complexity of modern technological & innovation systems leads to the necessity of carrying out their depth analysis using system approach, methods and algorithms for structural and parametric synthesis, based on technology package concept as a set of technologies (industrial, social, organizational) that provide expected efficiency in the relationship of innovation & technological system.

In this study, we propose to use the concept of technological & innovation systems (Hekkert, 2009), in which it is analysed the development of the technological field in terms of structures and processes that support or impede its development. So this approach can be considered as an expanding to techno-socio-economic analysis, considered for the innovation system in our previous studies (Marekha, Omelyanenko, 2016; Omelyanenko, 2014; Prokopenko, Omelyanenko, 2013; Omelyanenko, 2015a; Omelyanenko, 2015 b).

That's why through the review of previous studies and according to rational approach, given in (Chechkin, 2009), we consider as a base for our study the concept of "system security of complex (complicated) system" that means an unconditional preservation of its main functions, main components of complex system and their relationships in solving any particular problem for the system life cycle ensuring the proper functioning of the complex system (i), as well as its system integrity within its metasystem (ii).

In respect that the main characteristic of technological innovation system approach is its focus on system dynamics (Suurs, 2009), we propose to analyse it in terms of its system components and (or) in terms of its general dynamics. That's why we can apply virtuous circle (also referred as a vicious cycle) that refer to complex chains of events, which reinforce themselves through the feedback loop (Webel, 2012).

In our research, we also use approach for the identification of system security of technological & innovation systems based on system protection by reducing the risk of loss of its integrity and availability of information for decision-making to an acceptable level.

3. Technological & innovation systems security

Modern technological & innovation systems can be referred as structurally highly complicated systems, which in the mathematical description cannot be reduced to simple serial, parallel or tree structures but can be described by complex network scenarios with cycles and repeatability arguments in formalization. The complex phenomenon of these type of systems, which include, for example, information and computing systems, nuclear power stations, space stations, space vehicles, etc., in scientific terms are not known until the end and their security is not solved satisfactorily in an applied sense.

For the system security detailed analysis, we need such three basic points' acknowledgment:

1) in the macroeconomic and international levels the security of structurally complicated innovation & technology systems, we propose to consider as a classical situation, when the "impact of factors (external and internal) does not lead to system deterioration or impossibility of its operation or development" (Zaplatinskiy, 2006);

2) system's security analysis is aimed at the identification and assessment of factors that determine the undesirable internal incidents probability, the study of incident and development of preventive measures to reduce their probability (internal security of system);

3) system's security analysis is also connected with the identification and evaluation of external factors that determine the probability of undesirable incidents (conflicts, events etc.) inside of it, the study of an incident's nature and, recently, the development of preventive measures to reduce an incident's probability (external security of system).

So, according to the mentioned points and definitions, the system security of the highly complicated system can be provided through such main activities:

- monitoring and elimination of conflicts between its components (subsystems) and their linkages that appear throughout the system life cycle stages;
- monitoring and elimination of conflicts between the complex system and other external systems (its metasystem).

Based on methodology, given in (Hekkert, 2011), and our previous studies, we can underline that the important factor of technological & innovation systems system security consists in system identification within the management theory as the determination of the structure of the system and its parameters by analysing input data and system outputs. At the same time, we can note the system specifics, e.g. the identification of industrial systems security deals with the establishment of the identity of production facilities' ecological security etc.

Similar in formulation and meaning is the task of calculating the reliability of the systems, i.e. analysis of system's ability to maintain the properties, necessary to comply with the specified purpose, during normal operation. But in the case of innovation & technological systems, we are facing with different external impulses (competitors, macroeconomic dynamics) that do not correspond to its normal (initial) conditions. Analytical description of all above-mentioned issues can be conducted in two directions:

1. Identification and description of different types of improper actions and incorrect management decisions according to different interrelations;

2. Identification of consequences of malfunction, which causes other problems (or not cause), which ultimately leads to undesirable incidents and evaluate their probability.

To solve these tasks from the standpoint of classical cybernetics, the technological & innovation management we propose to consider as function-oriented activity (i) for maintenance system basic properties (set of properties or functions (subsystems), loss of which entails the destruction of system or losing of its capacity or safety) in the environmental conditions change and (ii) for certain actions implementation,

ensuring the stability of its functioning and development to achieve some target.

In the context of function-oriented system analysis of objectives and appropriate optimization of technological & innovation systems, we propose to consider mechanism of complex transformation of a wide range of initial resources into the final results using the tools complex based on humanity-established skills and knowledge, as well as adequate information and management system of necessary resources and sub-system of dissemination various economic, social, environmental, and other results, which are related to this system (Fig. 1).

Function-oriented security approach significantly expands the tasks of traditional factor analysis since provides that the object of security analysis should be systematic (integrated) and accordingly involve a number of sub-supply systems (scientific, technical, information, logistics, personnel, organizational, etc., that separately can be considered as a subsystems) must be function agreed through the set of different types of flows (material, energy, information flows, states changing etc.). From this perspective, the innovation & technological system's structure can be considered as a set of restrictions on flows system in space and time.

So we can apply system security approach to the consideration of the role of international relations in technological & innovation systems development within political and economic associations' framework. This means that the necessity to manage

of different resources (including valuable and limited resources) flows led to international integration processes development from simple economic and trade associations to interstate political, economic alliances and networks, as well as to different kinds of economic and technological wars.

System security also corresponds to "technological economy" concept that characterizes "social technological" systems, their transforming socio-natural character with the predominance of economic and scientific-technical development and rationalizing landmarks. So the technological & innovation systems security management according to the selected object is proposed to be analysed in two interrelated subsystems:

- first deals with the characteristic of self-organizing subsystems;
- second deals with the technical (technological) subsystem.

For each of these subsystems security, two basic approaches can be used: activity analysing approach and process analysing approach. Selection of specific approach depends upon the nature and complexity of object of management and focuses on the appropriate range of methods of analysis and decision-making (qualitative or quantitative). Within the management of technological & innovation systems, which, as it was already mentioned above, are the most complicated types of systems, the first approach currently is dominant, and methodological spectrum share of qualitative methods of analysis and decision-making significantly exceeds the share of traditional quantity methods.

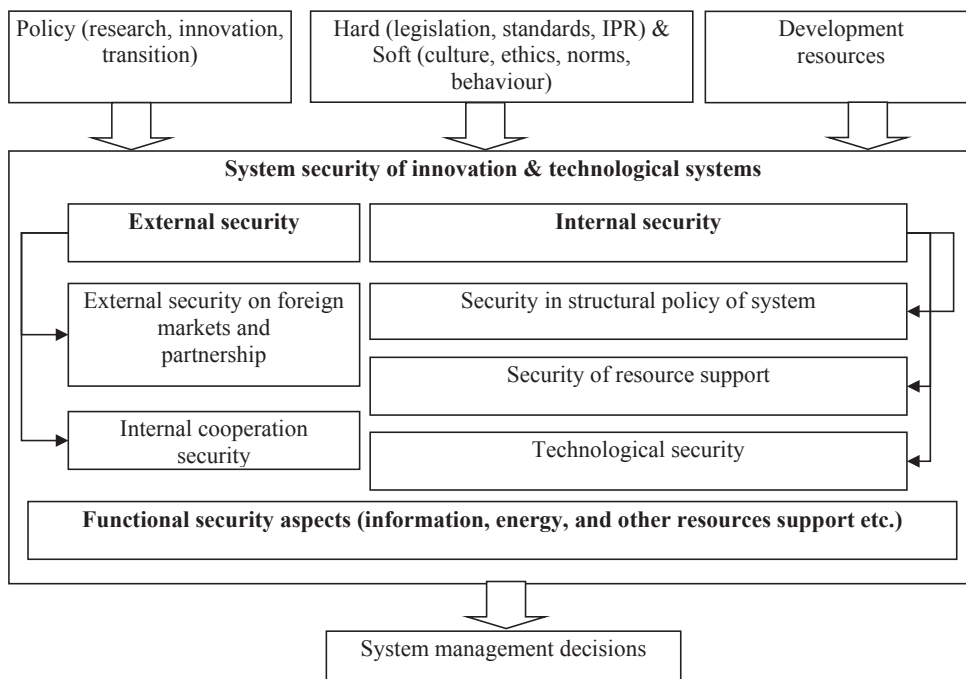


Fig. 1. System security of technological & innovation

The author's approach

4. Technological & innovation systems development management

The mentioned methods in the application for the technological & innovation systems should be considered as a part of system controlled evolution, which we offer to understand as a process of formation and implementation of such target impacts on technological & innovation system, as a result of which the system will turn to the target condition. As a part of the evolutionary management of technological & innovation systems, we offer to consider such analysis:

- 1) analysis of a variety of purposes based on potential and resource capabilities of the system;
- 2) analysis of internal environment of system formation processes;
- 3) data envelopment analysis, based on external factors (impulses and requests).

Therefore, for innovation & technological systems security analysis, we propose to use adapted evolutionary models in compliance with the dialectics principles and systematic approach. These models are based on the combination of constant (hereditary) part and variable component, which reflects the changes in the system and its environment. We also should underline the presence in evolutionary models of the efficiency concept as the dominance of one group of objects over another. This predominance can be achieved through the use of innovations and their interaction with other elements (technologies) in the system or the consequences of a technological innovations impact on the other areas. So with this understanding, we can identify causal relationships in a security context.

So we came to the conclusion that the effectiveness of technological & innovation systems security instruments depends on balance (level of synchronization) of system's development and relevant processes, caused by the introduction of specific elements (activities) into

the system within the controlled evolution. Assessment of system security, based on synchronization processes, we propose to realize according to a comparison of indicators, which characterize the systems development and development of investigated processes. Based on these indicators, we can identify system synchronous development speed and autonomous of speeds of security providing process. The most important relationships when designing innovation & technological systems, which allow decisions making, can be:

- the hierarchical relationship between the main system's function (a function of quality, a cost function) and sub-functions;
- managing relationship, reflecting the dependence of one system's function (subsystem) from another as a way out of control directed to another;
- functional (technological) relationship, which provides the fact that one output function (subsystem) is input to the next function (i.e., this relationship shows the actual technology). In the case of security models of technological & innovation system development, we propose to distinguish the direct connection for the input, when the output is transferred from the higher to the lower subsystem, and feedback on input, when output is transferred from lower to the higher subsystem. These aspects are relevant especially for technology cycles independency from the foreign or external suppliers;
- consumer (resource) relationship, when the output of one system's function (subsystem) is a mechanism (input) for the other (others);
- logical relationship between homogeneous functions (subsystems) that performs the same activity but by the different (alternative) ways or uses different data (resources);
- resource relationship that occurs between the functions (subsystems) that are used for their activities the same resources;

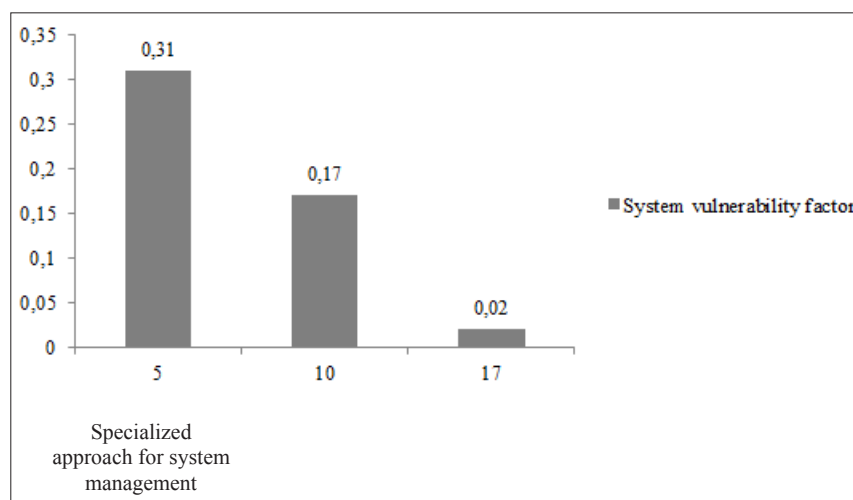


Fig. 2. Comparative analysis of system security providing approaches

The author's calculations

– information relationship that takes place between the system's functions (subsystems) that are used as input of the same information;

– time relationship occurs between the system's functions (subsystems) that are performed simultaneously after another function results obtaining.

Fig. 2 illustrates comparative analysis of application of three main approaches for system security providing (specialized approach, which orients only on the system main function, innovation approach, which orients on the innovation development of the system main function and proposed system security approach), which for the management of IT project for the e-governance.

Based on the foregoing, we propose to use security relationships adaptive management, which can be defined as a set of methods that can generate management systems, which are able to change the security-related parameters of regulator or controller structure according to the change of control object parameters or external disturbances acting on the control object. Model of adaptive management based on precedents contents of possible outcomes (precedents) database that can occur before the start of adaptive management actions based on real or simulated precedents, after processing of control action results.

The precedent structure for technological & innovation systems adaptive management can be written as:

1. Status of the system before the action. Description of the system (a set of agents, processes and their features, belonging to some class of states (situations));
2. Control action. Influence description (where possible formalization, in particular, the classification of control actions);
3. State after impact. Description of the object system (a set of agents, processes and their features, belonging to some class of states);
4. Outcome (positive outcome / negative outcome / controversial outcome).

In the context of initial technological & innovation system subsystems adaptive management at different

levels (company, cluster, sector), we propose to use the similar to IDEF0 methodology for functional modelling and graphical notation, which is intended for the business processes formalization, based on the hierarchical ranking of objects.

5. Conclusions

In our study, we have shown that the modern technological & innovation systems are structurally complicated systems, which are not reduced to simple serial, parallel or tree structures but can be described with complex network scenarios with cycles and repeatability arguments in their formalization. Based on this, we have considered system security concept as an analytical approach that can be an efficient base for innovation and economic policy efficiency assessment. As a framework for system security, we use function-oriented security approach, which significantly expands the traditional factor analysis. We came to the conclusion that the effectiveness of technological & innovation systems security instruments depends on balance (level of synchronization) of system's development and relevant processes. In the development of innovation & technological systems security adapted evolutionary models, we proposed the main aspects of this type of systems (general laws, external system's trends, internal system's trends, trajectories of development).

In the further our studies, we will consider the system security of technological & innovation systems development indicators in conditions of objective processes of rapprochement, interlacing and integration of national economies into the global economy and global innovation system.

6. Acknowledgements

The research was publicly funded by Ministry of Education and Science of Ukraine for developing of research project № 0117U003855 "Institutional and technological design of innovation networks for Ukraine's national security systemic providing".

References:

- Hekkert, M. (2011). *Technological Innovation System Analysis. A manual for analysts*. Utrecht University, *innovation-system.net*. Retrieved from http://www.innovation-system.net/wp-content/uploads/2013/03/UU_02rapport_Technological_Innovation_System_Analysis.pdf
- New Challenges for Germany in the Innovation Competition (2008). Fraunhofer Institute for Systems and Innovation Research.
- OECD (1997). *National Innovation Systems*.
- Mowery, D. C. (2009). National security and national innovation systems, *Journal of Technology Transfer*, 34, 455. <https://doi.org/10.1007/s10961-008-9100-4>
- OECD (2004). *The Security Economy*.
- NASA (2011). *NASA System Safety Handbook. Vol. 1, System Safety Framework and Concepts for Implementation*.
- Artyukhov, A. Ye., Omelyanenko, V. A., Artyukhova, N. O. (2016). Strategic framework and methodical bases of technological package development management. *Marketing and Management of Innovations*, 3, 170-179.
- Benner, L. (1997). System safety analysis pitfalls. Proceedings of the 15th International System Safety Conference Washington, DC August 13-17.

- Marekha, I., Omelyanenko, V. (2016). Cultural aspect of innovation strategies' ecologization // *Economic Annals-XXI*, Vol. 162, Issue 11/12, 9-12. <https://doi.org/10.21003/ea.V162-02>
- Omelyanenko, V. (2014). Analysis of Potential of International Inter-Cluster Cooperation in High-Tech Industries. *International Journal of Econometrics and Financial Management*, Vol. 2, No. 4, 141-147.
- Prokopenko, O., Omelyanenko, V. (2013). Role of international factor in innovation ecosystem formation. *Economic Annals – XXI*, 3-4(2), 4-7.
- Omelyanenko, V. (2015a). Preconditions analysis of using of technological package concept for development strategy of space metallurgy. *Metallurgical and Mining Industry*, 8, 508-511.
- Omelyanenko, V. (2015b). Analysis of strategical aspects of technology transfer in metallurgy. *Metallurgical and Mining Industry*, 12, 394-397.
- Chechkin, A. V., Pirogov, M. V. (2009). Intellectualization of a complex system as a means of maintaining its information system safety. *Fundamental and applied math*, vol. 15, no. 3, pp. 225-239.
- Suurs, R. A. (2009). *Motors of sustainable innovation. Towards a theory on the dynamics of technological innovation systems*, Utrecht University, Utrecht.
- Webel, Ch., Galtung, J. (2012). *Handbook of Peace and Conflict Studies*. Routledge.
- Zaplatinskiy, V. M. (2006). Terminologija nauki o bezopasnosti [Safety Science Terminology]. *Zbornik prispevkov z medzinarodnej vedeckej konferencie «Bezhecnostna veda a bezpecnostne vzdelanie» [Proceedings of the international conference «Security science and security education»]*. Liptovsky Mikulas: AOS v Liptovskom Mikulasi. [in Russian].