International Journal of Engineering & Technology, 7 (4.38) (2018) 82-85

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Cognitive Information Systems for Protection of Museum Complexes

Aleksey Valentinovich Bogdanov[1,2]*, Igor Gennadievich Malygin[3]

[1] *State Hermitage Museum, 33 Palace Embankment, Saint-Petersburg, 190000, Russian Federation*
[2] *Saint-Petersburg University of State Fire Service of EMERCOM of Russia, 149 Moskovsky Avenue, Saint-Petersburg, 196105, Russian Federation*
[3] *Solomenko Institute of Transport Problems of the Russian Academy of Sciences,13 12th Line VO, Saint-Petersburg, 199178, Russian Federation,*
**Corresponding author E-mail: bogdanov.aleksey.v@mail.ru*

Abstract

The paper considers the conceptual provisions of building a promising cognitive information security system of the museum complex on a cyber-physical basis. The stratified model of cognitive information security system of the museum complex was presented. It was shown that the key technological platform for the security of the museum complex is information and network technologies integrated (converged) with the technologies of industrial artificial intelligence. The generalized structural scheme of the cognitive cycle of the information security system of the museum complex was considered. The characteristic of the basic processes realized in a cognitive contour was given.

Keywords: *security system, cognitive system, cognitive cycle, information system, cyber-physical system, museum complex, industrial revolution*.

1. Introduction

Industrial revolutions that started two hundred years ago (Figure 1) had and continue to have a significant impact on all spheres of society (modes of production, economy, politics and life) [1]. To a large extent, industrial revolutions find their new manifestation in the level of security assurance.

During the first industrial revolution, the physical security systems mainly dominated. During the second industrial revolution, electromagnetic security systems were widely used. After the third industrial revolution, a feature of which is the widespread use of computer technology, software and network technologies, the new, computerized security systems appeared, and they generated new problems of information and network security (security in the cybernetic sphere).

Currently, a new (fourth) industrial revolution is coming, one of the distinctive features of which is the widespread use of intelligent security systems (Figure 1).

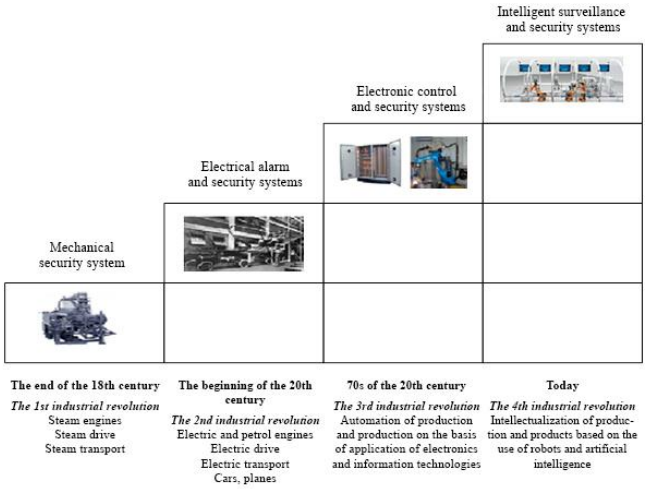

Fig. 1: Co-evolution of industrial technologies and security technologies

However, the fourth industrial revolution leads to the emergence of new security threats in various spheres. This is primarily due to the fact that the new industrial strategy envisages not only the intellectualization of industry, financial institutions and trade, education and culture, but also their information network and intellectual interaction [1]. In other words, the security assurance acquires an integrated (interrelated) and global nature (Figure 2). At the same time, each area of activity has its own characteristics of vulnerability and the need for protection, both in the physical and cybernetic levels [2], [3].

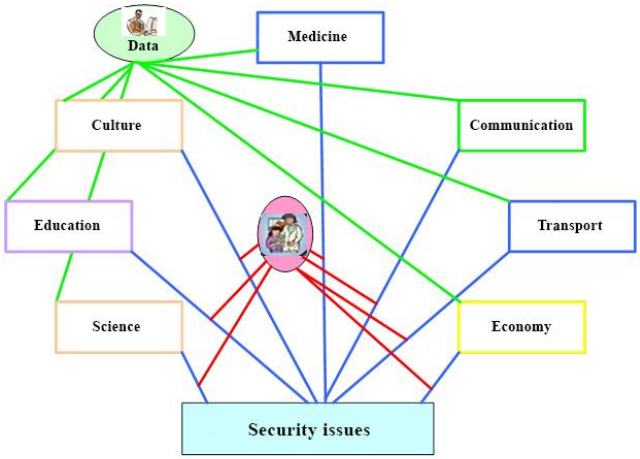

Fig. 2: Modern security issues

Another feature of the coming 4th industrial era is the expansion of the role of cybernetic space in all spheres of life and activity of society. Not only material objects of the physical world but also mental objects find their digital reflection in cybernetic space. Recently, manifestations of various actions (including those related to the security of museum complexes) are often reflected in both physical and cybernetic levels. Moreover, cybernetic space is increasingly being used by various criminal elements to damage physical objects (and vice versa). In other words, by observing the behavior of the subject or the object of a potential threat in one of the impact areas (for example, physical), it becomes possible to independently assess its behavior in the other level – cybernetic, while opening up new opportunities for significantly improving the quality of information systems to ensure the security of museum complexes.

2. Cognitive Information Security Systems and their Stratified Representation

People are an essential part of any security system. They intuitively understand the goals and objectives of an intentional offender and form an idea of the behavior that he/she may demonstrate when trying to achieve his/her goals in the physical sphere. At the same time, people use all five senses to detect signs of such behavior in order to assess the severity of the threat, so that an effective protective reaction can be initiated in advance. In order to increase the observability of the security of the physical level, it is in some cases equipped with various sensors (including video sensors), which allow one to quickly identify the place and time of the threat and respond to it in a timely manner [1]. The use of various types of sensors actually provides a significant expansion of the observation space with the help of technical systems (based on the transfer of "disturbances" in the cybernetic sphere) with the subsequent notification of violation of the human operator or protecting the automatic technical device.

Information security system operators are able to form threat profiles related to the targets of a specific offender (e.g., obviously different profiles of terrorist threat, robbery, vandalism, insurance fraud, casino fraud, etc.). Even a highly skilled operator isn't able to analyze the initial data provided by a very small number of security peripherals deployed in a network environment. Thus, the main drawback of the current approach is that the operator is often not able to process in real time a large amount of data supplied from the peripheral security infrastructure. The complexity of the problem of observation, identification of dangerous situations and timely response to them simultaneously at both levels (physical and cybernetic) increases significantly. The reason for this is the high complexity and speed of change of the situational danger, which often becomes so difficult that an operator (a group of operators) lacks the opportunities given by nature for a timely response.

One of the key approaches to solving the ever-increasing problems of security (in a variety of areas) is the creation of cognitive information security systems. The peculiarity of cognitive information security systems on a cyber-physical basis is the partial transfer of intellectual functions of the human operator (only those with which the operator cannot cope fully) to technical cognitive systems [4], [5].

The generalized stratified representation of the cognitive information security system of museum complexes on a cyber-physical basis is presented in Figure 3.

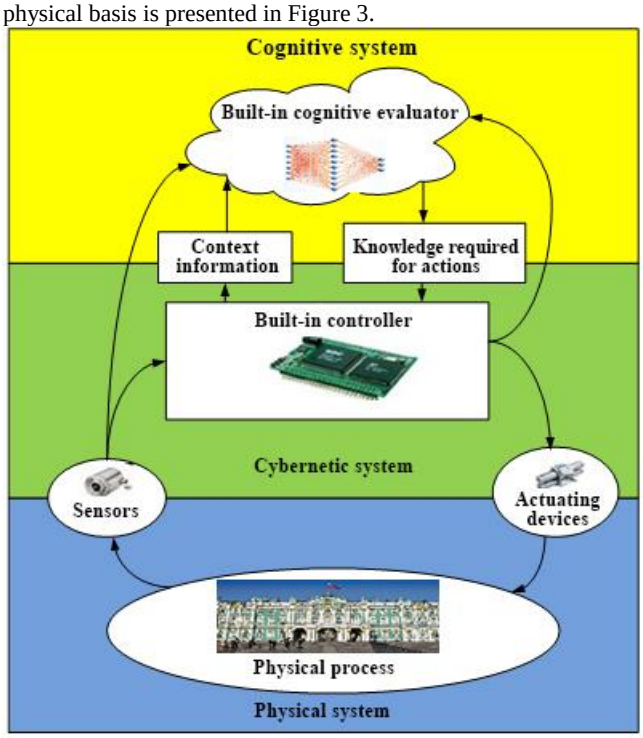

Fig. 3: Cognitive information security system of the museum complex

On the first stratum (in the physical system) there are protected material systems and physical processes. Physical systems and processes are equipped with sensors (providing an assessment of their states) and actuators (capable of influencing physical systems, their processes and their environment).

The second stratum includes built-in controllers, which form an internal digital model of the physical environment (a physical object, physical processes and the external environment) on the basis of the data received from a variety of sensors. The digital model of the environment is used to form commands to the actuators, and its contextual part is directed to the built-in cognitive calculator.

On the third stratum there is a cognitive calculator, which processes the flow of digital information models obtained from the cybernetic level, forms knowledge about the dynamics and direction of changes occurring in the physical level, thus, self-learns and directs them to the built-in controller to develop a plan of the most effective actions implemented by the executive devices together with the staff of the museum complex.

The process of functioning of the information security system is cyclic, the frequency of its repetition depends on the degree of dynamism of the processes occurring in the physical environment. The generalized block diagram of the working cycle of the cognitive information security system of the museum complex is shown in Figure 4.

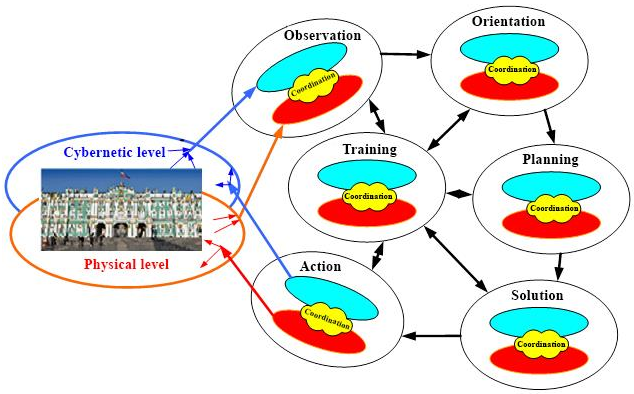

Fig. 4: Generalized block diagram of the working cycle of the cognitive information security system of the museum complex

Any physical system (for example, an intellectualized museum building) can act as a protected object. In this case, the building can be logically divided into thr cybernetic level (in which network, information, software and intellectual processes take place) and the physical level (in which physical movements and actions of the maintenance personnel and actuating mechanisms take place) [1].

The cognitive security information system work cycle includes contextual security processes of observation, orientation, planning, solution, training and action [6].

Observation is carried out in a coordinated manner at the cybernetic and physical levels. Surveillance at the cybernetic level is carried out by software aimed at collecting data that can display zero-day attacks, the presence of bot traffic, questionable behavior of visitors or staff, etc. The decision-making procedures for notifying the security system operator at the cybernetic level are based on the application of threat detection profiles, abnormal traffic models, etc., which are provided by the training area and are consistent with it. Observation at the physical level is based on the use of various contextual possible threats sensors (video, acoustic, location, movement, chemical, radioactivity, etc.).

Orientation is performed in real time on the basis of cognitive analytics (a set of modern software applications that simulate the work of the human brain to process observations, the formation of conclusions and the codification of instincts and experience in the learning process). Orientation is based on the processing of the collected data programmatically (at the cybernetic level) and is supplied from many peripheral security devices (at the physical level), mining, aggregation and processing of these data for the detection and identification of different security events related to the threat profile. Orientation supplies a leading cognitive signal through the security management interface to intelligent systems and the operator and helps them in predicting and responding to security breaches in real time.

The orientation process uses data in their current context and knowledge gained from previous experience (as it accumulates), then develops knowledge about behavior and opportunities, and responds to unexpected changes. In the orientation process, the task to distinguish really malicious actions from anything that is just anomalous is solved.

Planning is carried out dynamically and flexibly as the results of orientation are obtained and clarified, and with the active use of knowledge from the field of training. For example, if an e-mail or a message with threats is registered as a result of observation at the cybernetic level, the result of planning can be the identification of the sender, the search for his/her image, the task for surveillance cameras in the physical level, the search for the person and his/her escorting.

Solution assumes the development of several strategies for the implementation of the developed plan and the choice (by specified criteria) of the best of them. Decisions are formed dynamically as new or adjusted action plans become available. The decisions taken must ensure the prevention of the offender's actions before the occurrence of possible negative consequences.

Actions are carried out in accordance with the decisions made and can be carried out both at the physical and cybernetic levels at the same time.

3. Contemporary Museum – as a Cognitive Information System

Digitalization and intellectualization of museums are historically inevitable [7]. The digital museum is a museum that uses digital technologies in its activities [8]. Even today, digital technologies are widely used to support all kinds of museum activities, such as collection, storage, research, exposition, training, historical research of collections and their security assurance.

As a rule, museums perform three types of functions [7]: primary, secondary and the functions of protection of the exhibits.

The main function is to acquire, classify and research the collection.

The secondary function is to organize educational activities using collections, including exhibitions.

The third function is to ensure the safety and security of collections.

As for the primary function, digital modeling (digital scanning and high-precision reproduction of the original) is sometimes the only way to replenish the collection and restore the exhibits, conduct their unmistakable classification and research (based on digital image processing of exhibits and large historical data). Regardless of the conditions of preservation of collections in the museum, the collection will deteriorate over time. The only way to keep the current state of collections is to accurately measure them using different scanners and sensors, record and store measurement data in digital formats. Digital technologies can be used during their restoration. Digital models of exhibits can be stored indefinitely.

The secondary function, especially in the form of museum exhibitions, is expected to undergo significant changes based on the use of multimedia and network technologies. These technologies include virtual museums, museums on the basis of hypermedia in the Internet and network virtual 3D environment. These virtual exhibitions allow one to infinitely expand the exhibition space. In general, the modern digital museum is a cultural information system.

The third function is undergoing radical changes since not only real (physical) exhibits, but also virtual exhibits (museum databases) and their exposition means (computer networks and systems) located in the cybernetic level need protection.

One of the most effective approaches to the protection of information systems is the use of cognitive technologies. It is important to note that cognitive technologies can significantly improve the performance of all three functions performed by museums.

4. Conclusion

A distinctive feature and novelty of the considered cognitive information security systems of museum complexes on the cyber-physical basis is their harmonious compliance with the requirements of protection of various, both traditional and perspective architectures (historical, cultural, industrial, economic, banking, social, etc.) in the context of the changes that they undergo (and will continue to undergo) in the process of deployment of the fourth industrial revolution.

References

[1] Komashinskiy VI, Komashinskiy DV, Mikhalev OA, Cognitive cyberphysical systems for transportation security. *Transport of Russia: problems and prospects in 2016: materials of International*

scientific-practical conference, 29-30 October 2016, Vol 2. Saint Petersburg, Solomenko Institute of Transport Problems of the Russian Academy of Sciences, (2016), 148-153.

[2] Bauernhansl T, Hompel M, Vogel-Heuser B, *Industrie 4.0 in Produktion, Automatisierung und Logistik, Anwendung, Technologie, Migration*. Wiesbaden, Springer Vieweg, (2014).

[3] Bauer J, Schlund P, Marrenbac D, *Industrie 4.0 – Volkswirtschaftliches Potenzial fur Deutschland*. Berlin, BITKOM, (2014).

[4] Malygin IG, Komashinskiy VI, Information technologies and artificial intelligence – basic drivers of the fourth industrial revolution (Industrie 4.0). *Theoretical and applied scientific-technical journal "Information technologies"*, 22(12), (2016), 899-904.

[5] Mertens P, Industrie 4.0 – Herausforderungen auch an Rechnungswesen und Controlling im Uberblick. *Controlling – Zeitschrift fur erfolgsorientierte Unternehmensteuerung*, 27(8-9), (2015), 452-454.

[6] Malygin IG, Komashinskiy VI, Science, technology and education in the period of the 4th industrial revolution. *Scientific and technical problems in the industry: the future of a strong Russia is in high technologies: proceedings of the XI all-Russian scientific readings 19-21 April 2017*. Saint Petersburg, Publishing house "Scythia", (2017), 121-127.

[7] Bogdanov AV, Concept of creating security systems of large museum complexes. *Scientific and analytical journal "Bulletin of the St. Petersburg University of the State Fire Service of EMERCOM of Russia"*, 4, (2013), 39-43.

[8] Bogdanov AV, Features of information security of cloud technologies in a single information space of large museum and exhibition complexes. *Complex protection of information objects and measuring technologies: materials of all-Russian Scientific-Practical Conference with International Participation, 16-18 June 2014 Saint Petersburg State Polytechnic University*. Saint Petersburg, Publishing House of Polytechnic University, (2014), 12-14.