www.volsu.ru

ИННОВАЦИИ В ИНФОРМАТИКЕ, ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКЕ И УПРАВЛЕНИИ

DOI: https://doi.org/10.15688/jvolsu10.2017.2.1

УДК 681.3
ББК 32.973

THE ANALYSIS OF METHODS AND APPROACHES FOR MODELING COMPONENTS OF THE COMPLEX ORGANIZATIONAL AND TECHNICAL SYSTEMS “SMART CITY”

Yulia Sagidullovna Bakhracheva

Candidate of Technical Sciences, Associate Professor, Department of Information Security,
Volgograd State University
bakhracheva@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Amanulla Azizovich Kadyrov

Doctor of Technical Sciences, Professor,
Director of Center for Strategic Innovations and Informatization
amanulla.kadirov@innovation.uz
Universitetskaya St., 2, 100095 Tashkent, Republic of Uzbekistan

Aziza Amanullaevna Kadyrova

Candidate of Technical Sciences,
Deputy Director of Center for Strategic Innovations and Informatization
amanulla.kadirov@innovation.uz
Universitetskaya St., 2, 100095 Tashkent, Republic of Uzbekistan

Elena Aleksandrovna Maksimova

Candidate of Technical Sciences, Associate Professor, Head of the Department of Information Security,
Volgograd State University
infsec@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Abstract. The article discusses issues related to comprehensive development and introduction of technologies such as "smart city". The authors justify the need of reducing the threats for information security of "Smart city". In case of implementing smart city technologies, it is necessary to take into account the costs of research of threats from new technologies. Now the universal gateway with a large number of wire and wireless interfaces which performs work on collection and normalization of data from heterogeneous sources is developed. The universal gateway is an infrastructure basis of a network in "the smart city". In this gateway support of special industrial data interfaces (PLC, DI/DO, etc.), characteristic of SCADA systems is integrated. An integrated approach to development and deployment of smart city projects in Russia will promote increase in information security.

Key words: smart city, organizational and technical systems, mathematical modeling, information flows, information security.

1. Introduction

Among the trends of development of technologies in Russia and worldwide at the forefront is the development of highly organized systems, often called "smart" – smart home, smart city.

As world practice shows, the achievement of this goal requires the introduction of new information technologies, which are one of the important elements of smart cities functioning. We are talking about the introduction of automated systems of management and control of various aspects of city life such as housing and communal services, urban traffic, public transport, tourism, public safety, education, health, energy, water and environmental situation. A comprehensive introduction of modern information technologies promotes quality and efficiency in the provision of educational, health and other social services and increases the level of information security.

2. Trends in the development of information security "Smart city"

Large cities seek to optimize the urban environment, traffic flows, to create a more effective system of urban infrastructure management. For the operation environment of highly organized systems the main aspects should be highlighted: a network of data centers, information resources over large dimensions, the analyst take into account processes and objects, development of embedded systems, communications and infrastructure for the telecommunications industry.

The information collected inside houses may be used to optimize the operation of public utilities. Research Agency Gartner believes that in 2016 the number of different sensors and devices in cities reached several billion.

Threats to information security change at the same pace. The principle of extreme technologies should be taken into account, namely the use of highly efficient technologies inevitably leads to the amplification of existing threats and the emergence of new ones (along with the disappearance of some vulnerabilities) [4].

The list of threats related to human factor is greatly reduced. The most powerful stream of threats "Unintentional errors regular users" is limited to possible errors of users to configure, to detect signals, to respond to messages. This type of threats according to the materials of the related risks currently reaches 65 % of the "smart system" to significantly reduce this value at least twice.

Consider the threats associated with failures. Cracks users:

– unwillingness to work with the information system (is most often seen when you need to master a new);

– the inability to operate the system, as there is no appropriate training;

– the inability to operate the system due to the lack of technical support (incomplete documentation, failure to receive information).

The failure of the system itself for internal reasons:

– retreat (accidental or intentional) from the regulations;

– the output of the system from nominal mode of operation due to accidental or intentional actions of users or staff (in excess of the estimated number of requests that an excessive amount of processed information, etc.);

– error when (re) configuring the system;

– failures of software and hardware;
– destruction of data;
– destruction or damage to the equipment.

To determine relevant threats we have the equation:

$$Y = \frac{Y_1 + Y_2}{20}, \quad (1)$$

where Y_1 – the degree of initial security; Y_2 – the likelihood of threats.

A list of relevant threats is based on a common list of threats and the degree of initial security company. In compiling this list each degree of source protection is defined in accordance with the numerical factor Y_1: 0 for high degree of initial security; 5 – to a medium degree of initial security; 10 for low level of initial security. For our security $Y_1 = 10$.

Under the frequency (probability) of realization of the threat is understood to be defined by experts measure of how likely is the implementation of specific security threats in the current circumstances. We introduce four verbal gradations of this indicator:

1) unlikely there are no objective prerequisites for the implementation of the threat;

2) low probability – objective preconditions for the realization of threats, but the measures are a significant obstacle for its implementation;

3) average probability – objective preconditions for the realization of existing threats, but the measures taken to ensure the security are insufficient;

4) high probability of objective preconditions for the realization of the threats, and measures to ensure safety are not taken.

In the compiled list of relevant security threats every probability of threat is assigned a numerical coefficient Y_2: 0 for unlikely threats; 2 – low probability threats; 5 for medium probability threats; 10 for high probability threats.

Table summarizes all the data about the threats on the basis of which the relevance of a particular threat is to be judged.

The basic principles of information security "smart city":

1) the emergence of new threats to information security during the transition to the information system "smart city" meets the principles of extreme technology development;

2) while planning investments related to the development, you need to consider the cost of remedies availability to a greater extent, to ensure the neutralization of the listed threats, the costs of investigating potential threats from new technologies.

3. Role and place of big data in implementation of the concept of Smart city

The transition of the city into the category of smart puts another requirement to the system – automation – as the ability to predict future energy consumption. Mode upcoming of energy consumption compared with the schedule of its planned output. This allows time to address possible gaps and to smooth peak loads. Energy producers are adjusting the schedule of generation in accordance with the expected demand. Users prepare a reasonable scenario of consumption from centralised sources and the transition to local alternative sources. Between the two sides is information sharing. The role of automation

The calculation of the relevance of threats

№	Name of the threat	Probability	Rate implementation	Possibility	Actuality
1	The threat of leakage through technical channels	2	0,6	medium	actuality
2	The threat of introducing malicious programs	5	0,75	high	actuality
3	The threat of "network traffic Analysis" with the interception of the transmitted in the external network and from external networks information	5	0,75	high	actuality
4	Threat scan	2	0,6	medium	not actual
5	The threats of obtaining data by substitution of the trusted object	2	0,6	medium	not actual
6	Threats such as "Denial of service"	2	0,6	medium	not actual
7	Threats running remote applications	5	0,75	high	actuality

increases. Increasing the level of automation of life-support systems, the level of its integration with information infrastructure building. Standardized database and open protocols allow for the exchange of information between different systems in real time to maintain comfort, energy efficiency and control operating costs. They also support interaction between the building and its users. This increases the efficiency of building maintenance, on the one hand, and improves the quality of life and productivity, on the other hand. While the human factor can play both a positive and a negative role. Therefore, a smart city uses intelligent solutions that attract the attention of users to a reasonable use of energy and motivating them to save.

It is possible to allocate four basic elements in the technological structure of "smart city":

– the Internet of things is a technological concept that allows you to gather information from objects and provides feedback to them;

– infrastructure data transmission that connects the application with the urban infrastructure;

– system of data analysis allows to extract from large volumes of data to useful information;

– system aggregation and harmonization of data, designed to organize and synchronize huge data streams.

Information flow in systems of "smart city" is very large. Some of the information is duplicated or is not valuable. System work data play a crucial role: it is necessary to properly filter and cluster the data to analyze and identify dependencies, in particular, on the correctness of the prediction and accuracy of reaction to emerging events.

There is a number of impediments to the rapid development of "smart cities". One of the reasons is a lot of old systems with disparate interfaces of the data and the old protocols are unclear as to integrate with each other. Such networks are slow, have many security issues.

Currently, the universal gateway with a large number of wired and wireless interfaces, which performs the work to collect and normalize data from disparate sources. Universal gateway is actually infrastructure-based network in the "smart city". This IoT-router is made in an industrial case and is designed to work on the street, protected from adverse weather conditions.

This gateway integrates support for industrial data interfaces (PLC, DI/DO, etc.), are more characteristic of SCADA systems than for telecommunications infrastructure.

REFERENCES

1. Anisimov I., Ivanov A., Chikishev E., Chainikov D., Reznik L. Assessment of gas cylinder vehicles adaptability for operation at low ambient temperature conditions. *WIT Transactions on Ecology and the Environment*, 2014, vol. 1, pp. 685-695.

2. Genon G., Torchio M.F., Poggio A., Poggio M. Merging of energy and environmental analyses for district heating systems. *Energ. Convers. Manage*., 2009, vol. 50 (3), pp. 522-529.

3. Gitelman L.D., Ratnikov B.E., Kozhevnikov M.V. Demand-side management for energy in the region**.** *Economy of Region*, 2013, vol. 2, pp. 78-84.

4. Karnaukhov N., Reznik L., Kholyavko V. Speckle effects in adaptive optical systems. *Adv. Transport*, 2000, vol. 6, pp. 439-443.

5. Panepinto D., Senor A., Genon G. Environmental balance study for the construction of a biomass plant in a small town in Piedmont. *WIT Trans. Ecol. Envir.*, 2014, vol. 180, pp. 479-490.

6. Poggio A., Maga C., Benedetti P., *Provincia di Torino. Piano di sviluppo del teleriscaldamento nell'area di Torino, Rapporto finale*. Tecnoapi, Torino, 2009. 325 p.

7. Senor A., Panepinto D., Genon G. Building an eco-effective district heating management system in a city. *WIT Trans. Built Env.*, 2016, vol. 168, pp. 651-662.

8. Torchio M.F., Genon G., Poggio A., Poggio M. Biomass-fired CHP and heat storage system simulations in existing district heating systems. *Energy*, 2009, vol. 34 (3), pp. 220-227.

9. Vasilyev A. Simulation of valve gear dynamics using generalized dynamic model. *Mechanika*, 2006, no. 2, pp. 37-43.

10. Vasilyev A.V., et al. Valve Cam Design Using Numerical Step-by-Step Method. *Vestnik Volgogradskogo gosudarstvennogo universiteta. Seriya 10, Innovatsionnaya deyatelnost* [Science Journal of Volgograd State University. Innovations], 2014, no. 1 (10), pp. 26-32.

АНАЛИЗ МЕТОДОВ И ПОДХОДОВ К МОДЕЛИРОВАНИЮ КОМПОНЕНТОВ СЛОЖНЫХ ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИХ СИСТЕМ «УМНЫЙ ГОРОД»

Юлия Сагидулловна Бахрачева

Кандидат технических наук, доцент кафедры информационной безопасности,
Волгоградский государственный университет
bakhracheva@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аманулла Азизович Кадыров

Доктор технических наук, профессор,
директор Центра стратегических инноваций и информатизации
amanulla.kadirov@innovation.uz
ул. Университетская, 2, 100095 Ташкент, Республика Узбекистан

Азиза Амануллаевна Кадырова

Кандидат технических наук,
заместитель директора Центра стратегических инноваций и информатизации
amanulla.kadirov@innovation.uz
ул. Университетская, 2, 100095 Ташкент, Республика Узбекистан

Елена Александровна Максимова

Кандидат технических наук, доцент,
заведующий кафедрой информационной безопасности,
Волгоградский государственный университет
infsec@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. В статье проводится анализ методов и подходов к моделированию компонентов сложных организационно-технических систем «умный город». Показано, что в случае внедрения технологий «умного города» нужно учитывать расходы на научные исследования угроз от новых технологий. Комплексный подход к разработке и внедрении проектов «умный город» в России будет способствовать повышению информационной безопасности.

Ключевые слова: умный город, организационно-технические системы, математическое моделирование, информационные потоки, информационная безопасность.