Threats to information security in a highly organized system of the "Smart city"

G I Kurcheeva¹, V V Denisov¹, V A Khvorostov¹

¹ Novosibirsk State Technical University, 20, Karla Marksa Ave., Novosibirsk, 630073, Russia

E-mail: xvorostov@corp.nstu.ru

Abstract. The article discusses issues related to comprehensive development and introduction of technologies such as "Smart city". The urgency of accelerating the development of such highly organized systems, primarily in terms of reducing threats to information security, is emphasized in the paper. In accordance with authors' analysis of the composition and structure of the threats to information security, "Accessibility", "Integrity" and "Confidentiality" are highlighted. Violation of any of them leads to harmful effects on the information and other system resources. The protection of "Accessibility" mobilizes one third of all efforts to ensure information security that must be taken into account when allocating protective actions. The threats associated with failure of the supporting infrastructure are also significantly reduced. But the threats associated with failures of the system itself and failures of users are clearly increasing. There is a high level of society and production informatization, and the threats to information security are changing accordingly.

Introduction

Urban population growth in the world has amounted to about 40% over the past 10 years. This growth increases the load on all services for the operation of the urban economy. However, many technologies that provide vital functions of Russian cities have exhausted their ability to service the rapidly growing urban population.

One of the world-wide known technology trends is the development of highly organized systems, often named "smart" - smart home, smart district, smart city. And the "Smart City", as a system, is recognized as the most safe in terms of the development of information systems.

As the world practice shows, achievement of this goals requires the implementation of new information technologies, which are an important element in the functioning of "smart cities". We are talking about implementation of automated management and control systems of various spheres of city life, such as housing and utilities, urban traffic, public transport, tourism, public safety, education, health, energy, water and environmental situation.

Comprehensive implementation of modern information technology contributes to a significant increase in the quality and efficiency of education, health and other social services, and to the level of information security.

The heads of major Russian cities are seeking the ways to optimize the urban environment, transport streams, to create a more efficient system of urban infrastructure management. There are sectoral projects, for example in the energy sector, to improve production, distribution and...
consumption systems that require sensors, "smart" devices connected to the Internet or to the "cloud." They allow one to better organize production, consumption and distribution of electricity, reduce the negative impact on the environment of urban and rural areas.

1. Threats to information security

Computerization of industrial and household processes reaches a new, higher level. Considering the positive dynamics of development of the systems, we should not forget the protection of information. Threats to information security changes are not less active. We should take into account the principle of extremality technologies, namely the use of high technology inevitably leads to strengthening of the existing threats and the emergence of new ones (along with the disappearance of some of the vulnerabilities).

Threat is the potential to violate the security of the information, which is usually regarded as a combination of three aspects: accessibility, integrity and confidentiality [1].

Violation of any of them affects the system information and other resources. Within production and information systems, there is a simple and equal distribution of protective actions among the three aspects. That is, in such systems, to ensure information security, one third of all efforts is used to protect accessibility, one third - to ensure integrity and one third - to provide confidentiality.

High organization of "smart systems", the movement of technologies along the chain “Smart system - Smart Home - Smart district - Smart City” shifts this distribution towards accessibility, making it the most important. Figure 1 shows a variant of such a bias based on a study of expert reports. End users and information security professionals were involved in the analysis of the importance of threats. Accordingly, the protective activities keep the same proportions.

![Figure 1. The distribution of protective actions [2].](image)

Enhancing the role of Accessibility is due to the change of the list of threats. For example, "Internet things" in highly organized information systems interact in an automatic mode - any failure in communication leads to misalignment of the whole system. For sensors and other devices, accessibility is vital because this is a data property, providing the possibility of their timely use in solving problems.

The list of risks associated with the human factor is greatly reduced. The most powerful stream of "Unintentional errors of end users" threats is limited to the users’ possible errors to detect signals and respond to the message. This type of threats, based on risks surveys, now reaches 65%, and the "smart system" significantly reduces this level at least twice [3, 4].
Table 1 summarizes the results of the analysis of the list of generic threats and their harmful effects (Table 2 shows the designation of the malicious activity). One can see a distinct change of activity. The numbers of threats marked with (*) disappear in the "smart" systems. The threats marked with (**) activate the attacks on availability.

**Table 1.** The list of threats to information security with the attacking aspects (*) (compiled by the authors)

| №  | Name of threat                                      | Trivial systems |   | "Smart" systems |
|----|-----------------------------------------------------|-----------------|---|-----------------|
|    |                                                     | A   | I  | C  | A  | I  | C  |
| 1  | Theft of material                                   | +++ | -  | +  | +++| -  | -  |
| 2  | Theft of intangible (copying, assignment of rights ...) | -   | -  | ++ | -  | -  | ++ |
| 3  | Loss                                                 | ++  | +  | +  | ++ | -  | -  |
| 4  | Accidental data corruption                          | -   | +  | -  | -  | -  | -  |
| 5* | Deliberate data corruption                          | --- | +++| -  | -  | +  | -  |
| 6* | Accidental data distortion, entry errors            | -   | +  | -  | -  | -  | -  |
| 7**| Deliberate data distortion, allowing access         | --- | +++| ++ | +++| -  | -  |
| 8**| Data distortion, unauthorized access                | --- | +++| +++| +++| -  | -  |
| 9* | Forgery, substitution                               | -   | +++| +  | -  | -  | -  |
| 10*| Destruction of data on a carrier                    | +++ | -  | -  | -  | -  | -  |
| 11 | Destruction of hardware and carriers                | +++ | -  | -  | +++| -  | -  |
| 12**| Destruction of infrastructure (elements)           | +++ | -  | -  | +++| ---| -  |
| 13 | Blocking (setting interference) communication channels | +++ | -  | -  | +++| -  | -  |
| 14 | Latency (delay, pause ...)                          | +++ | ++ | +  | +++| ++ | +  |
| 15 | The denial of the authenticity, availability, completeness | +++ | -  | +  | +++| -  | -  |
| 16 | The imposition of false information                 | --- | ++ | -  | ---| ++ | -  |
| 17*| Illegal actions (forced)                            | ++  | ++ | +++| -  | -  | -  |

A - Accessibility, I – Integrity, C – Confidentiality

**Table 2.** Legends for effects in Table 1

| №  | Symbols | Characteristic                          |
|----|---------|----------------------------------------|
| 1  | +       | Not necessarily, but there is a small probability |
| 2  | ++      | There are possible negative consequences |
2. Foreign experience in the implementation of new information technologies

International practice shows that promising direction is the implementation of new information technologies in the leading cities of the country. Such projects have successful experience in the US and the EU, the results of which are shown in Table 3.

| №  | City      | Features                                                                 |
|----|-----------|--------------------------------------------------------------------------|
| 1  | Barcelona | The highest rank in this city belongs to the intelligent control system of traffic and parking, as well as the intelligent lighting system. Analysts at Juniper Research have concluded that the intelligent control system of energy efficiency implemented in the city will be saving approximately 9.5 billion euros a year by 2019. In the city, a lot of attention is paid to transparency of public and social services and processes. |
| 2  | New York  | New York has the highest results in street illumination and transportation system management. At the same time, analysts note, referring to the advantages of technology and interaction with the public, that the weak point is the preservation of the environment. |
| 3  | London    | London has the highest scores in the criterion of technology and interaction with the public. |
| 4  | Nice      | The French town won the Environment, as well as the consistency of services. Nice is the only city among the top 5, which has a population of less than 1.5 million. |
| 5  | Singapore | Singapore has the highest results in the intelligent management of the transport system and the creative use of technology. |

There are attempts of implementation of "smart services" in major metropolitan areas of our country. For example, in Moscow, "smart services" are successfully functioning in the field of housing and communal services, control of transport services, the formation of a unified information system of the city. In Saint Petersburg and Kazan they started the project to implement the security systems and efficient management of urban public utilities. At present, Kazan is implementing a large-scale project "Smart and safe city of Kazan", which provides a unified city Wi-Fi network, and video surveillance for control of the urban and ecological environment, the intellectual transport system representing a set of sensors of traffic, a processing center and controlled traffic lights.

The largest international IT-companies such as IBM, Cisco and others are engaged in the implementation of "smart" technologies in Russian cities. [5]

Thus, the idea of "smart city" includes the following basic concepts (Table 4).

| Areas of technology | Traditional urban economy | «Smart city» |
|---------------------|---------------------------|-------------|
| 1 Energy efficiency | Reduced energy consumption| Improving the system of production, distribution and consumption |
2 Public health Provision of health services The use of high-tech medical equipment with simultaneous exchange of information on the method of treatment of all professionals

3 Transport Control of all modes of transport on the basis of the "GLONASS" system A smart technology in transport is building a pedestrian-oriented city, with the focus on public transport

4 Green Planet Implementing environmental programs Implementation of the system of "green" technologies

5 Communications The introduction of remote access systems All communications are transferred to the online mode.

6 Infrastructure Development of an integrated system of urban services The implementation of new technologies that reduce the burden on the environment, ensuring the necessary quality of life

7 Education The implementation of distance education The union of students, teachers and knowledge from around the world

8 Security The individual, disparate technologies, personal security, home or business An integrated approach that includes technology to ensure urban safety

3. Conclusion
To achieve the required objectives and ensure the urban security, we need a completely new integrated approach combining technical and humanitarian aspects of solving the problem. Safe technologies of critical infrastructures, secure telecommunications and security of every citizen, including their personal information and moral education are the basis upon which we must build a physical entity of such a complex socio-technological object as a "safe smart city".

The essence and structure of the threats associated with malfunctioning of the municipal services supporting the infrastructure are changing due to the development and implementation of modern technologies. First of all, it refers to the threats related to failures of the system and user failures. A non-systemic approach, the implementation of detached modern technologies, the lack of communication between municipal services technologies lead to an increase in security threats.

When planning investments related to the development and introduction of the technology, "smart city" must take into account the costs of protecting the accessibility to a greater extent, ensure the neutralization of these threats, study the costs of potential threats from new technologies. It is a comprehensive approach to the development and implementation of projects of "smart city" in Russia which will enhance information security.

References
[1] Vladimirova T. A., Sokolov V. G., Sokolov S. A. 2015 The efficient operation and development of economic systems with a high technological structure. Siberian financial school 6 (113) pp 7 – 12
[2] Galatenko, V. A. 2006 The Basics of information security: a course of lectures: textbook (Moscow) p 208
[3] Kurcheeva G. I., Aletdinova A. A. 2015 To the question about the development of a model management the promotion scientific and technological innovation. The Restructuring of the
Russian economy and industrial policy. Proceedings scientific-practical conference with foreign participation (St. – Petersburg) pp 241-245

[4] Bakaev M. A 2015 Quantitative measure for information transfer in human-machine control systems. *International Siberian conference on control and communications (SIBCON–2015)* (Omsk : IEEE)

[5] Sharafutdinova E., AvdeenkoT., Bakaev M. 2014 Design and implementation of the integrated information system for the russian ministry of emergency situations. *The 9 international forum on strategic technology (IFOST)* (Bangladesh : IEEE) pp 238-241