Information Security Aspects in a Smart City

Anton D. Nazarov[a]
Ural State University of Economics, Yekaterinburg, Russia

Keywords: Smart City, Information Security, Data Protection.

Abstract: The article considers the specifics of the functioning of smart cities in terms of ensuring their security. Typical risks and vulnerabilities of large settlements of the digital future are mentioned. The key aspects of the process of ensuring confidentiality, integrity, availability of socially and economically significant information are identified. The ways of solving certain problems of protecting the infrastructure of modern smart megalopolises are outlined.

1 INTRODUCTION

Regarding the long-term upfront growth in resources used in production, in comparison with the growth rate of final product in the modern economy, there is a replacement in technological systems, a complete restructuring of all outdated systems. The basic foundations of the state economies are changing radically. In our country, the position of the enterprise as a key element of the economy is being replaced by a municipal entity.

More than 40% of the world's population currently lives in cities. The need for sustainable and high-quality management of the metropolis infrastructure requires significant technological innovations in all systems of functioning of huge human settlements. For this purpose, it is necessary: a) to modify the exploit and control of social and economic structures; b) to re-evaluate the country's resources in accordance with the new circumstances; c) to develop high-quality strategies to achieve the objectives set (Kuznetsova et al., 2017).

From about 2015, in Western America and Northern Europe, in order to ensure a modern level of population quality of life, the development of smart cities projects commenced. It is expected that the most efficient utilization of available resources through the use of innovative technologies will allow:

- to use urban life systems economically;
- to provide a high standard of environmental protection, maximum life safety of citizens;
- to provide thigh quality services to the people.

According to experts, a smart city is, first of all, people living in comfortable conditions due to intelligent management of transport systems, street lighting, the interaction of citizens with the authorities, receiving medical and educational services, and ensuring the personal safety of individuals.

2 MATERIAL AND METHODS

The implementation of smart technologies into the urban environment will allow: to significantly improve the procedure for the production, distribution, consumption of electricity; to reorient the transport system towards the pedestrian; to redirect any contacts of people between themselves and with the authorities online; to reduce the burden on the environment; to provide an instant exchange of information about the treatment of a patient by a large number of doctors; to receive by learners and students knowledge from teachers from anywhere in the world.

Abroad, projects to create smart cities are being actively implemented in the USA, Spain, England, France, Singapore, and Japan.

The first studies show: more than 9 billion euros in electricity savings per year in Barcelona; a noticeable increase in the efficiency of street lighting in New York in comparison with traditional types; an

[a] https://orcid.org/0000-0002-8299-1834

Nazarov, A.
Information Security Aspects in a Smart City.
DOI: 10.5220/0010619800003170
In *Proceedings of the International Scientific and Practical Conference on Computer and Information Security (INFSEC 2021)*, pages 132-135
ISBN: 978-989-758-531-9; ISSN: 2184-9862

increase in the quality, rate of interaction between the population and the authorities in London; almost one hundred percent consistency in the work of public services in Nice; creative application of transport management systems in Singapore.

3 RESULTS AND DISCUSSIONS

Particular attention in the smart megalopolises of the Land of the Rising Sun is paid to ecology: only the energy of daylight is used for heating and lighting dwellings, public transport is represented mainly by bicycles and electric vehicles (Tsakanyan, 2017).

Several universities in the United States of America and the United Kingdom have studied and compiled data on the results of the use of "smart" electricity, water, gas counters (30% resource savings), motion sensors and energy-saving lamps (70% savings), the implementation of energy-saving technologies in the construction of buildings on the territory of universities (up to 30% savings), the implementation of video monitoring systems for the territory (20% savings on the maintenance of the protection service), intelligent transport management systems (reducing the bus travel time on campus, reducing the emission of pollutants from them).

In our country, there are attempts to implement the smart city system elements in Moscow, St. Petersburg, and Kazan. Interesting projects are being developed in Siberia. Digital management of housing and communal services and transport is being introduced in Moscow. A unified city information system is being formed. In St. Petersburg, smart services are being introduced into the security management systems, management of municipal structures of the city. The capital of Tatarstan is being equipped with a unified urban video surveillance network and Wi-Fi, intelligent control of the urban environment and ecology. The city is equipped with traffic flow sensors, controlled traffic lights.

A smart city is a complex social and technical object that requires a multi-stage, extensive system to ensure the uninterrupted functioning of the infrastructure, of each individual citizen: as a consequence of the informatization of production processes and living conditions, information security threats of all areas of life are changing.

The threat is understood as the potential possibility of impeding the concealment of integrated, self-sufficient, autonomous data, information, preventing information leakage, which harms the smooth functioning of the infrastructure of a smart city (Denisov, 2016).

In the specialized literature, threats to the information security of smart cities include:

- unlawful non-repayable seizures of an intangible nature made for personal gain: copying data, assigning rights to a resource;
- illegal acquisition of personal data, intellectual property;
- loss, intentional, unintentional damage to information and data;
- intentional or unintentional input errors, distortion, falsification, data substitution;
- destruction of information carriers or information on them;
- blocking communication by creating interference, setting bookmarks;
- compulsion to use false information;
- destruction of technical means, digital infrastructure;
- deliberate or accidental deviation from the procedure for the operation of technical resources;
- breach of the normal operation of the system, due to certain actions of users or persons serving the structure: an increase in the number of requests to indicators higher than the calculated norms, too large amounts of information to be processed;
- occurrence of errors as a result of configuration of the structure;
- malfunctions in the operation of software or hardware;
- violation of data integrity;
- failure to respect the principles of work by users: unwillingness to master new skills, acquire new skills required to work with the system (Chipiga, 2017).

To solve the above problems, it is necessary to know and to understand the popular demands as accurately and in detail as possible; to combine physical and digital planning methods; to predict, quickly identify problems; to respond quickly to emergencies; to improve the quality and rate of service delivery systematically and regularly, thus increasing their productivity. To know and be able to prevent the causes of the vulnerability of digital resources: a) massive amounts of generated, collected, stored, used data, intellectual property, commercially significant information; b) a diversity of contractual instruments, mechanisms for managing information interaction between enterprises and organizations. To predict emerging risks: quantum technologies, by means of which it will be possible to process information millions of times faster than now; cheap satellite Internet delivery from near-earth orbit; IoT Internet connection for consumer electronics, cars, environmental sensors and many other devices; displaying information into text, contextual views out of text, audio and video formats; the emergence of new ways to exploit the service of determining precise location of an electronic device using the Internet, new ways to provide for personal needs of users, new ways of requests and analytics based on public identity; minimal or complete absence of human intervention in the operation of machines to identify and process data, to use them for various purposes; the possibilities of biometrics to penetrate into a person's personality and its functional changes.

Analysis of possible risks in the system of functioning of smart cities resulting in the identification of key aspects for their minimization or complete elimination to ensure digital security (Vladimirova et al., 2015).

Distribution of efforts on three levels: services (education, medicine, tourism, public safety); objects (residential buildings and premises, offices, trading floors, clinics, schools, preschool educational institutions); infrastructure (energy and water resources, transport, waste disposal, information and communication technologies).

Compliance with key requirements: focus on providing the basic needs of the individual; manufacturability of interconnected objects of the city, ensuring its functioning; increasing the level of resource management of the urban environment, as well as its comfort and safety; commitment of economic efficiency.

Widespread implementation of innovative electronic and engineering solutions.

Regular, integrated accounting of public incidents, forecasting non-standard situations, developing ways to respond to them.

4 CONCLUSION

Compliance with the established rules for the work of structures and their management.

Systematic monitoring and control of data received from devices, sensors, stationary and mobile tracking objects, broadcasting the results to the appropriate subsystems in order to anticipate non-standard situations, quick response to incidents.

Tracking the crime situation in real time.

The use of biometric platforms, intelligent surveillance, recognition and location detection systems for shots from firearms.

Identification of weaknesses in the security system of infrastructure facilities.

Instant interagency information interaction.

Advanced training of personnel providing information security in smart megalopolises.

Legislating owners and users of information in smart cities.

Educating the population in a reasonable, conscious, careful use of digital resources, and in taking personal responsibility for the security of personal data.

Improving the nature of the interaction between police authorities, service providers, and other products in smart cities.

Knowledge, appreciation, timely prevention and prompt overcoming of cyber threats will allow actively resist aggressive, harmful effects on the functioning of "smart" cities of various negative phenomena and factors, improve the quality and standard of living of the population in modern megalopolises (Kupriyanovsky, 2017).

REFERENCES

Abid, A., Abbas, A., Khelifi, A., Farooq, M. S., Iqbal, R., & Farooq, U. (2020). An architectural framework for information integration using machine learning approaches for smart city security profiling. *International Journal of Distributed Sensor Networks*, 16(10). doi:10.1177/1550147720965473

Berkel, A. R. R., Singh, P. M. and van Sinderen, M. J. (2018). An information security architecture for smart cities. doi:10.1007/978-3-319-94214-8_11

Chipiga, A.F. (2017). *Information security of automated systems*, 336 p. M.: Helios ARV

Cilliers, L. and Flowerday, S. (2014). Information security in a public safety, participatory crowdsourcing smart city project. *World Congress on Internet Security*, pages 36-41. doi:10.1109/WorldCIS.2014.7028163

Daniel, T. S. E., Li, R. and Zheng, H. (2019). Risks facing smart city information security in hangzhou. *ACM International Conference Proceeding Series*, pages 29-33. doi:10.1145/3374549.3374552

Denisov, V.V. (2016). Identification of data security vulnerabilities in the informatization of production processes. In the book: Youth and the XXI century – 2016. *Materials of the International Youth Scientific Conference: in 4 volumes.* Managing editor: A.A. Gorokhov, pages 287-292.

Din, Z., Jambari, D. I., Yusof, M. M. and Yahaya, J. (2019). Challenges in managing information systems security for internet of things-enabled smart cities. *International Conference on Research and Innovation in Information Systems*, ICRIIS. doi:10.1109/ICRIIS48246.2019.9073661

Dong, N., Zhao, J., Yuan, L. and Kong, Y. (2018). Research on information security system of smart city based on information security requirements. *Journal of Physics: Conference Series*, 1069(1). doi:10.1088/1742-6596/1069/1/012040

Ferraz, F. S. and Ferraz, C. A. G. (2014). More than meets the eye in smart city information security: Exploring security issues far beyond privacy concerns. Paper presented at the Proceedings - 2014 IEEE International Conference on Ubiquitous Intelligence and Computing, 2014 IEEE International Conference on Autonomic and Trusted Computing, 2014 IEEE International Conference on Scalable Computing and Communications and Associated Symposia/Workshops, UIC-ATC-ScalCom 2014, pages 677-685. doi:10.1109/UIC-ATC-ScalCom.2014.143

Hui, P. (2020). Construction of information security risk assessment model in smart city. *IEEE Conference on Telecommunications, Optics and Computer Science*, TOCS 2020, pages 393-396. doi:10.1109/TOCS50858.2020.9339614

Jameel, T., Ali, R. and Ali, S. (2019). Security in modern smart cities: An information technology perspective. *2nd International Conference on Communication, Computing and Digital Systems*, C-CODE 2019, pages 293-298. doi:10.1109/C-CODE.2019.8681021

Karasevich, A. M., Tutnov, I. A., & Baryshev, G. K. (2016). The prospects of application of information technologies and the principles of intelligent automated systems to manage the security status of objects of energy supply of smart cities. *ACM International Conference Proceeding Series*, pages 9-14. doi:10.1145/3014087.3014111

Kupriyanovsky, V.P. et al. (2017). Intelligent mobility and mobility as a service in Smart Cities. *International Journal of Open Information Technologies*, 5(12).

Kurcheeva, G. I., Denisov, V. V. and Khvorostov, V. A. (2017). Threats to information security in a highly organized system of the "smart city". *Journal of Physics: Conference Series,* 803(1) doi:10.1088/1742-6596/803/1/012086

Kuznetsova, A. V., Samygin, S.I. and Radionov, M.V. (2017). Artificial intelligence and information security of society, 64 p. *M: Rusays*

Lakhno, V., Kasatkin, D. and Blozva, A. (2019). Modeling cyber security of information systems smart city based on the theory of games and markov processes. *IEEE International Scientific-Practical Conference: Problems of Infocommunications Science and Technology*, pages 497-501. doi:10.1109/PICST47496.2019.9061383

Li, X., Li, H., Sun, B. and Wang, F. (2018). Assessing information security risk for an evolving smart city based on fuzzy and grey FMEA. *Journal of Intelligent and Fuzzy Systems*, 34(4): 2491-2501. doi:10.3233/JIFS-172097

Toapanta, M., Mafla, E. and Orizaga, J. (2017). An approach to information security by applying a conceptual model of identities in smart cities projects. *Journal of Engineering and Applied Sciences*, 12(6): 7765-7770. doi:10.3923/jeasci.2017.7765.7770

Tsakanyan, V.T. (2017).The role of cybersecurity in world politics. *Bulletin of the Peoples' Friendship University of Russia. Series: International Relations*, 17(2): 339-348.

Vladimirova, T.A., Sokolov, V.G. and Sokolov, S.A. (2015). Reliability of functioning and development of economic systems with a high technological order // Siberian financial school, 6 (113): 7-12.

Wang, D., Bai, B., Lei, K., Zhao, W., Yang, Y. and Han, Z. (2019). Enhancing information security via physical layer approaches in heterogeneous IoT with multiple access mobile edge computing in smart city. *IEEE Access,* 7: 54508-54521. doi:10.1109/ACCESS.2019.2913438

Wu, S. M., Guo, D., Wu, Y. J. and Wu, Y. C. (2018). Future development of taiwan's smart cities from an information security perspective. *Sustainability (Switzerland)*, 10(12). doi:10.3390/su10124520

Zhu, N. and Zhao, H. (2018). IoT applications in the ecological industry chain from information security and smart city perspectives. *Computers and Electrical Engineering*, 65: 34-43. doi:10.1016/j.compeleceng.2017.05.036