

"Smart Habitat": Features of Building It Infrastructure, Main Problems of Building Data Networks Using 5G (6G) Technologies

Alexander Bogdanov[1,2], Nadezhda Shchegoleva[1,2], Gennady Dik[3(✉)], Valery Khvatov[4], and Aleksandr Dik[1]

[1] Saint Petersburg State University, St. Petersburg, Russia
{a.v.bogdanov,n.shchegoleva}@spbu.ru, st087383@student.spbu.ru
[2] St. Petersburg State Marine Technical University, St. Petersburg, Russia
[3] LLC "System Technologies", St. Petersburg, Russia
g.dick@systechnologies.ru
[4] DGT Technologies AG, Toronto, Canada

Abstract. The main issues of digitalization of settlements in Russia based on the "Smart Habitat" (SH) technology are considered, an analysis of security problems and possible risks of 5G and 6G networks used for receiving and transmitting information is carried out, ways of organizing the protection of the used cellular networks are proposed.

Keywords: Network protection · Smart habitat · 6G networks · IoT · Data transmission systems

1 Introduction

One of the significant factors in improving the quality of life of the population in modern conditions is the use of the so-called "Smart Home"' technology, which, for the purpose of further development, develops into a whole strategic direction of building the infrastructure of the habitat called "Smart Habitat" (Fig. 1). The well-known technology "Smart Home", and then "Smart City" (SC) (hereinafter referred to as technology) has long been used in the modern world, but at the same time, the aspect of introducing these technologies in small summer cottages and villages is of increasing interest. In these settlements (habitat fragments - HFbit) there is also a need to automate life processes and ensure the personal and technical safety of residents (Fig. 1). This raises the question of SHF as a more universal and scalable option for using an interconnected system of information and communication technologies with IoT (Internet of things), which simplifies the management of the internal processes of the environment and makes the life of residents more comfortable and safer.

Within the framework of this article, SHF is considered as an environment in which engineering infrastructure, IT infrastructure, social infrastructure and business infrastructure are combined in order to improve the quality of life of the population through the digitalization of various spheres of life HFbit [1].

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2022
O. Gervasi et al. (Eds.): ICCSA 2022 Workshops, LNCS 13380, pp. 628–638, 2022.
https://doi.org/10.1007/978-3-031-10542-5_43



Fig. 1. SHF - integrated technology of a new standard of living

As for the goals and priorities of the development of the SHF, it is advisable to take as a basis six basic principles for constructing the SC, expanding and applying them to the considered HFbit according to [2]:

1. The principle of creating a comfortable environment for all SC residents;
2. The principle of coordination and interaction of all participants in the development of SC;
3. The principle of additional designation of the SHF infrastructure (priority of endowing the existing elements of the infrastructure with new functions and obtaining new results due to this);
4. The principle of sustainable development based on monitoring, analysis and forecasting;
5. The principle of sustainable development based on monitoring, analysis and forecasting;
6. The principle of forming a digital environment for self-organization of residents and businesses;
7. The principle that implies a priority orientation towards the creation of positive emotions of residents from interaction with the SC environment.

In accordance with the above principles, the SHF technology is generalized by the concept that declares different approaches to the development of a settlement of any scale.

Despite the absence of a generally accepted definition of SHF, it should be noted that the technology under consideration is a concept declaring various approaches to the development of a settlement of any size and the expected effects from the introduction of those technologies. This approach includes solving the following tasks:

– obtaining significant an economic effect;
– improving the quality of life of the population through effective management the life cycle of the settlement;
– ensuring the safety of living, life, work processes.

All these tasks should be solved by open interaction of all stakeholders (the population, government and authorities, business structures, etc.) and the use of

high-tech IT infrastructure, which includes specialized equipment for retrieving and transmitting data using high-speed communication channels, as well as software and hardware systems for processing circulating information. At the same time, in the modern world there is no sufficient awareness of the principles of creating an SHF and, as a result, a unified approach for constructing both the architecture itself and the issue of organizing data transmission networks, control signals, etc. (hereinafter referred to as - information transmission networks (ITN) [2].

Within the framework of this article, it is proposed to dwell on the problems of choosing a ITN for the formation of the most effective variant of the IT infrastructure of the SHF, while paying special attention to the analysis of the architecture of building networks of the 5G standard (in the future - 6G standard) and the landscape of security threats directly related to it.

Hereby we propose the variant of an IT infrastructure for SHF technology, while paying special attention to the analysis of the architecture of building 5G networks (in the future - 6G) and the directly related landscape of security threats.

2 A Modern Approach to Organizing of Information Transmission Networks for the Concept of "Smart Habitat"

It should be noted that in practice quite often there are cases when already implemented solutions did not bring the expected effect in terms of changing the quality of life of the population. In a number of situations, the introduction of new technologies has complicated the management processes and even created an additional burden in terms of maintaining and operating the IT infrastructure itself. An example is the already well-known and widely discussed Korean city of Songdo, where the support of "smart" infrastructure has become a barrier to the development of the city. This is due to the complexity of the environmental processes, when, as a result, the introduction of individual technical solutions may affect other areas of life, and the effects of fragmented informatization are quite difficult to predict. Thus, first of all, it is necessary to identify the main shortcomings of the implemented solutions, which must be taken into account during the selection and further evaluation of the effectiveness of the proposed solutions.

In addition, if within the city there is a fairly developed switching infrastructure, then in settlements outside the city it is practically absent. Thus, there is a need for faster and broadband communication channels with wireless properties, because when introducing the SHF technology, it is not always and not everywhere possible to organize a wire cable economy.

In order to resolve this issue, 5G and 6G wireless networks are expected to provide global coverage of the surface of the entire Earth, so that users and connected IoT can access the Internet anywhere and at any time. In this case, wireless terrestrial networks must be combined with air and water (not located

on the surface of the Earth) access nodes (satellites, drones, high-altitude platforms (HAP), surface signal broadcast stations, etc.). The seamless 3-D (land, sea and sky) coverage constructed in this way will form a global integrated communication network (Fig. 2). Thus, all terrestrial and non-terrestrial networks will be comprehensively integrated at the system level, providing convergence of services, wireless interfaces, various types of networks and connected user devices.

It should be noted that such a network construction will allow users and connected IoT to be in a single information space, regardless of their mode of movement or location. In addition, the failure of a network fragment will not have a significant impact on the performance of the entire SHF IT infrastructure as a whole.

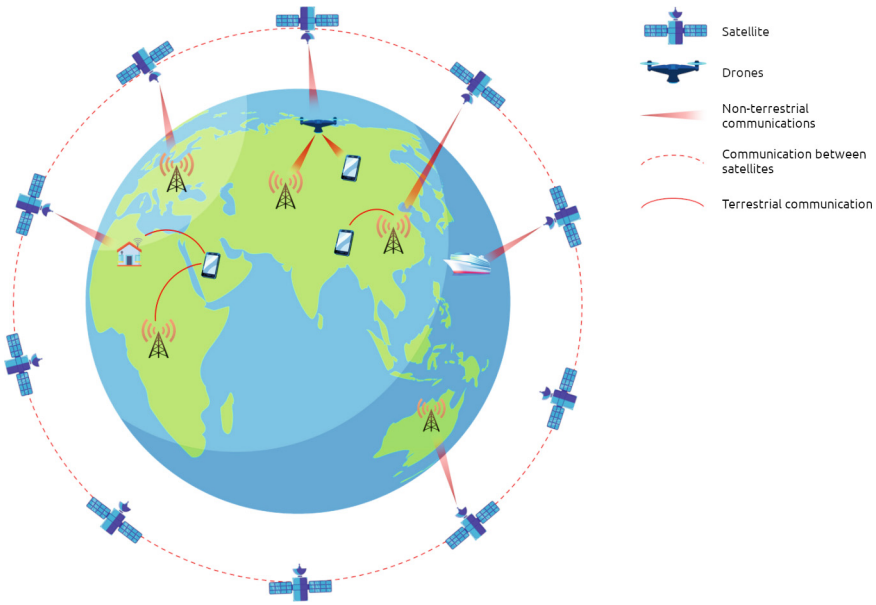

Fig. 2. Converged multilayer heterogeneous network

The presented network construction will allow not only a broadband wireless connection anywhere and on the move, but also to organize the connection of the following vital SHF processes:

1. Communications and disaster relief. This option is essential in response scenarios as it provides not only disaster forecasting, but also warning and emergency response and emergency communications. In some cases, duplication of terrestrial networks through the operation of non-terrestrial networks will provide continuity of service and support for emergency management, including

transmission of voice, data and using a video system for operational communication with the command post;
2. High-precision positioning and navigation, which will provide high-quality V2X services for vehicles, both in the urban environment, and accurate positioning and navigation services for vehicles in remote and hard-to-reach areas;
3. Monitoring of the earth's surface in real time. In this case, optical filming using visible light and partial infrared cameras, as well as radio frequency scanning, will avoid the limitations of transmitting and receiving communication channels;

In accordance with the "Smart Habitat" concept [1], one of the main tasks for creating a complex socio-technical system is to build an IT infrastructure with distributed communication support (DICS). This DICS should include a complex of information systems, consisting of local automation equipment using artificial intelligence technology (sensors, sensors, video cameras, thermal imagers, etc., the so-called "Internet of things" or "IoT") and metacognitive control technologies complex socio-cyber-physical systems based on a neural network, as well as high-performance wireless data networks, etc. (Fig. 3).

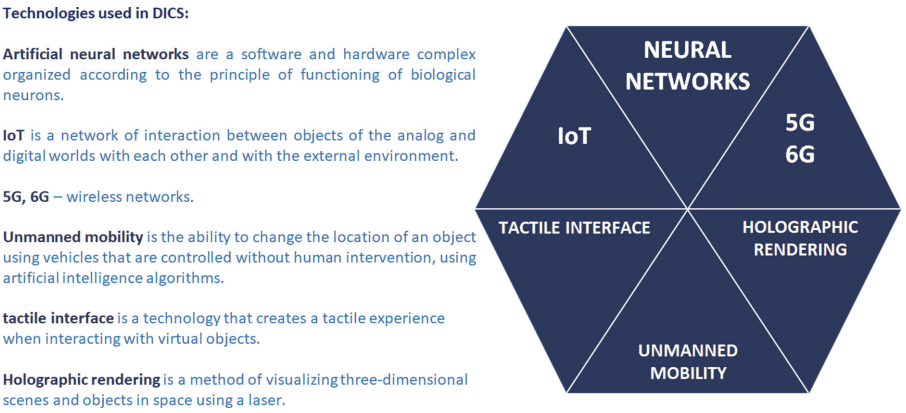

Fig. 3. The use of modern technologies in the construction of DICS

IoT is a set of different devices and sensors united by wired and wireless communication channels and largely connected to the Internet to better integrate the real and virtual worlds, when, in fact, communication is carried out between people and devices. It is assumed that with the development of IoT technology, "things" will become active participants in business, information, and social processes, where they will be able to interact and communicate with each other, exchanging information about the environment, reacting and influencing processes occurring in the world around them, without human intervention. Thus, it can be assumed that this IoT construction is a self-organizing network of many sensors and actuators, interconnected via a radio channel. Moreover, the

coverage area of such a distributed wireless sensor network can range from several meters to several kilometers due to the ability to relay messages from one element to another. The interaction under consideration is impossible without the active and comprehensive use of ITN, which ultimately leads to considering IoT as a "network of networks", where compact, loosely connected networks form larger, and then global networks (Fig. 4). At the same time, it should be noted not only the variety of primary data collection devices (gas, water, heat, electricity meters, security and fire sensors, etc.), but also the need for centralized transmission to the server through base stations and processing of incoming information. In the future, the information received is displayed in your personal account on a computer or smartphone, but it should be possible at any time to receive data from devices or send control commands to them (such as turning off the device, switching the operating mode, time synchronization, etc.) via a wireless network [3].

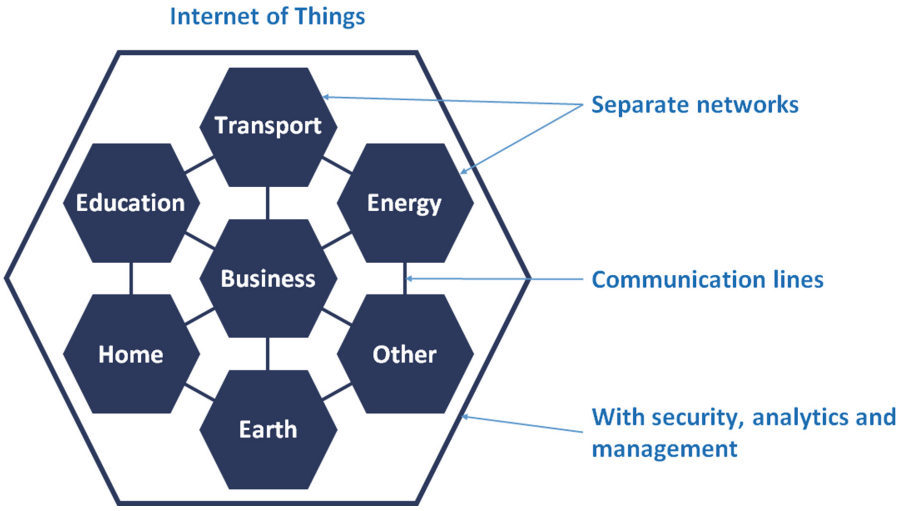

Fig. 4. IoT networks

The main advantages and disadvantages of building of an ITN based on Bluetooth, ZigBee, Z-Wave, NFC, RFID, Wi-Fi, LTE were widely illuminated in various sources [4–8]. As for the networks of remote range, i.e. cellular, then the introduction of networks of the fifth (5G), and then the promising sixth generation (6G), in contrast to the LTE network (Fig. 5), will significantly expand the ITN, taking into account three main scenarios for its use, namely:

1. Enhanced mobile broadband-eMBB: up to 25 Gbps peak data rate. Application: 4K, 8K, 3D live streaming, AR (Augmented Reality)/VR (Virtual Reality) services, cloud gaming and other high-traffic services.

2. Ultra-Reliable and Low-Latency Communication-URLLC: Reducing data transfer delays up to 1 ms and always having a connection. Application: unmanned vehicles (Vehical to Everything, V2X), remote technologies (automation of production lines, robotic surgery).
3. Mass machine-to-machine communication (enhanced Mobile BroadBand-MBB): support up to 1 million connections to the base station per 1 square kilometer with data transfer rates up to tens of gigabits per second. Application: development of consumer and industrial IoT (power supply, manufacturing, smart city, Smart living environment, etc.).

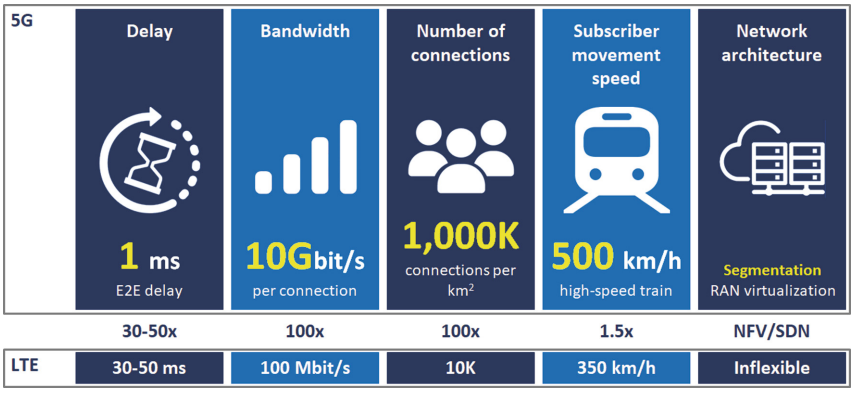

Fig. 5. Main differences between LTE and 5G networks

The 5G communication network is based on the new 5G NR (New Radio) standard and consists of the following main components:

– subscriber equipment with USIM cards;
– radio access networks (RAN), including backhaul and fronthaul networks;
– network core (5GC).

The promising 6G network is based on a similar structural one, but at the same time there are several significant differences.

3 Security Issues and Possible Risks of 5G and 6G Networks

Despite the positioning of the fifth and sixth generation ITNs as secure, the analysis below shows several security problems. [9]:

1. Significantly increased attack surface. This circumstance is primarily due to the ever-increasing number of IoT, which in turn leads to a proportional

increase in entry points for organizing targeted attacks. In addition, according to the concept of converged architecture, WiFi radio access networks, 4G-LTE, etc. must also connect to a single core 5G or 6G network, making connected devices less resistant to outside hacking. This will allow more IoT devices to be harvested and used for DDoS attacks by hackers, causing an increase in the frequency of such attacks. As a result, many connections and high bandwidth increase the attack surface, while the number of IoT devices that are less resistant to hacking is growing.

2. he architecture of the core network (network core or 5G Core) is based on cloud technologies and virtualization of network functions - software-defined network, Network Functions Virtualization (NFV), allowing you to create many independent segments and thus support services with a different set of characteristics. In addition, sharding will allow operators to provide network infrastructure as separate services. At the same time, the network infrastructures used will depend on 5G, and then on 6G, much more than on their predecessors, and a security breach in any area can become critical, and the consequences can be catastrophic. Thus, the risks should include the fact that such a construction of a network infrastructure leads to more serious consequences in case of failures and cyber-attacks, considering the scale of use.
3. Ample opportunities are opening for more aggressive conduct of various types of so-called "espionage". As you know, any IoT device with the ability to capture video or audio information (the presence of cameras and microphones) can be used by cybercriminals or software and hardware manufacturers to view and listen to uninformed users. In this case, the risks are obvious.
4. An analysis conducted by an international team of security researchers from Purdue University and Iowa State University (USA) found almost a dozen vulnerabilities in the fifth generation (5G) mobile communication standard [12]. The exploitation of the vulnerabilities allowed for several attacks, such as location tracking, the transmission of false alarms, and the complete disconnection of the phone's 5G connection from the network. A group of researchers was able to track and fix the location of the device in real time. Moreover, experts were able to intercept the phone's paging channel to broadcast fake emergency alerts, which, according to the research team, could cause "artificial chaos." It should also be taken into account that a new kind of security threat can exploit vulnerabilities in all AKE protocols, including 5G protocols, and invade the privacy of mobile device users, causing more serious damage than before. These "spyware" attacks use fake base station attacks that attackers have used to target vulnerable AKE protocols and security leaks in 3G and 4G networks, as well as an encryption vulnerability for SQNs (sequence numbers). Although the AKE protocols used in 5G and 6G networks have improved protection against base station spoof attacks, researchers have shown that relay attacks can break the SQN security of cellular networks, making it useless. These attacks are much more dangerous than the previous attacks. have an important feature: previously a user could avoid an intrusion by leaving the attack zone, but now hackers can continue

to monitor the user's activity even if he left the range of a fake base station using a new fake attack. In this case, the risks include attacks such as "monitoring the activity of subscribers", which, in addition to physical tracking of the subscriber or certain devices, create prerequisites for the security of encryption protocols.

5. 5G networks, and then 6G, involve the active use of edge computing technology (MEC - Mobile Edge Computing or Mobile Edge Computing). These can be corporate applications running on the network of operators: intelligent services, financial services, multimedia. It should be added that in this case, the operator's 5G and 6G networks are being integrated into the corporate infrastructure. At the same time, one of the advantages of 5G and 6G networks is a significantly low latency, which can be "successfully" used in the same DDoS attacks, because hackers will be able to strike faster - in seconds, not minutes. To confirm the theory, the researchers created a malicious base radio and, using the 5G Reasoner tool, successfully carried out several attacks on a smartphone connected to 5G. In one of the scenarios, a DoS attack on a phone resulted in a complete disconnection of the connection from the cellular network [10]. Thus, the risks include new opportunities to penetrate corporate networks, the placement of MEC equipment outside the protected perimeter of the organization, as well as the fact that the speed of a malicious attack becomes significantly higher.
6. The centralized network management infrastructure (O&M - Operations & Maintenance or Operation and Maintenance) used in 5G and then 6G networks is complicated by the need to simultaneously support a large number of service segments. In this case, risks can be attributed to the more serious consequences of misuse of resources and O&M configuration errors.

4 Measures for Protecting 5G and 6G Networks

Based on the analysis of possible security problems of 5G and 6G networks, it is proposed to define several levels of protection.

The first level is protection at the level of implementation of technical solutions, building the network infrastructure and equipment distribution options:

1. The use of a powerful firewall between users and the outside world, multi-level isolation and protection of the integrity of the SDN and VNF components - the hypervisor, virtual machines, OS, controllers and containers;
2. Authentication of MEC applications, use of an additional authentication factor when accessing the corporate network, whitelisting of devices and services, authorization of API requests;
3. Ensuring high availability of virtual machines for fast recovery after attacks;
4. Trusted hardware environment - secure boot devices, application of technology TEE (Trusted Execution Environment);
5. Real-time attack detection on network nodes and virtual infrastructure elements using artificial intelligence algorithms.

The second level is protection at the level of network infrastructure management:

1. Secure management of not only user data, but service, technical, analytical and other types of information involved in ensuring the solution of SHF tasks (the so-called attack on the subscriber and attack on the mobile operator), using encryption, anonymization, depersonalization and etc.;
2. Centralized management of identified vulnerabilities, as well as policies and levels of information security, the use of information during the ongoing analysis of big data to detect anomalies and quickly respond to attacks;
3. Comprehensive use of counterfeit base station detection tools based on real-time monitoring of operation and maintenance events;
4. Application of multi-factor authentication algorithms and organization of access control to segments by O&M.

The third level is protection at the level of the standard:

1. SSeparation of the layers of the protocol for receiving and transmitting data into three planes: User Plane, Control Plane, Management Plane. with complete isolation, encryption and integrity control of these planes;
2. use of encryption methods for subscriber and technological traffic with an increase in the length of the encryption key from 128 bits to 256 bits;
3. The use of a single mechanism for subscriber authentication for various types of wireless communications;
4. Support for flexible security policies for segments;
5. Use of unified standards.

At the same time, it should be noted that in addition to ensuring information security at all levels, a comprehensive approach is needed to protect networks of 5G and 6G standards, which includes an administrative and technical approach from ongoing network audit to continuous improvement of security systems. The rapidly developing technologies of new generation networks will significantly improve the interaction of consumers of ITN services through communication. And here the security issues of all types of network traffic used are most acute, which, having great potential, opens wide opportunities for cyber-attacks, invasion of privacy, serious disruption of not only IoT, but the entire SHF as a whole.

By organically combining these two access environments into one converged multi-layer heterogeneous network spanning the entire globe, 6G will provide users with a consistent experience. Providing global delivery of mobile services will be an important aspect of 6G network development.

The integrated 6G network will expand the range of services provided. For example, by integrating terrestrial and non-terrestrial networks, 6G will provide broadband and IoT services in regions and areas where there is no terrestrial network coverage, including remote farms, and even aboard ships and aircraft. In addition, 6G will help emergence of new applications such as high-precision positioning the development of objects by combined means of satellite and earth

systems and high-precision survey of the earth's surface in real time for agriculture.

From a strategic point of view, this transformation is aimed at ensuring sustainable economic development, effective municipal government, providing high-quality public services to the population of the SHF, etc. But at the same time, the transition to 6G requires comprehensive compliance with more stringent requirements for mobile communication systems, especially for their security. And thus, we can speak about emerging of ecosystem based on new communication technologies, that will change both quality of life and level of control of environment.

5 Conclusions

Thus, the transition to 5G and 6G networks significantly increases the opportunities for cyberattacks and invasion of privacy. The paper discusses a list of measures that should be taken to ensure the secure connection of home devices at high speeds. It is very important that only the creation of multi-layered protection can guarantee the safe and convenient use of the Internet of Things technology for use in private homes and settlements.

The research is partially funded by the Ministry of Science and Higher Education of the Russian Federation as part of World-class Research Center program: Advanced Digital Technologies (contract No. 075-15-2020-903 dated 16.11.2020).

References

1. Argunova, M.V.: The "smart city" model as a manifestation of the new technological mode. Science and School, no. 3 (2016)
2. Mityagin, S.A., Karsakov, A.S., Bukhanovskiy, A.V., Vasil'yev, V.N.: "Smart St. Petersburg": an integrated approach to the implementation of information technologies for managing a metropolis. Control Engineering Russia **1**(79) (2019)
3. Virkunin, A.O., Derevyashkin, V.M., Maksimov, A.S., Rozhentsev, V.L.: Analysis of radio access technologies for the implementation of the "smart home" system. Siberian State University of Telecommunications and Informatics (2018)
4. Wireless networks ZigBee and Thread. http://www.wless.ru/technology/?tech=1. Accessed 06 Nov 2021
5. Tkachenko, V.: WiFi technology. sib.com.ua/arhiv_2014/2014_3/statia_1_4/wifi.pdf. Accessed 06 Nov 2021
6. Bluetooth UR: https://ru.wikipedia.org/wiki/Bluetooth. Accessed 05 Nov 2021
7. LoWPAN: https://ru.wikipedia.org/wiki/6LoWPAN. Accessed 05 Nov 2021
8. Oltorak, S.: Overview of the Z-Wave protocol. https://rus.zwave.me/z-wave-knowledge-base/about-z-wave/z-wave-technical-overview. Accessed 06 Nov 2021
9. www.nttdocomo.co.jp/english/binary/pdf/corporate/technology/whitepaper_6g/DOCOMO_6G_White_PaperEN_20200124.pdf. Accessed 06 Nov 2021
10. www.securitylab.ru/news/502542.php. Accessed 06 Nov 2021