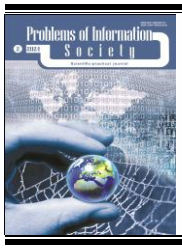

www.jpis.az

15 (2)
2024

Smart socio-technological infrastructures: cyber security risks and the human factor

Rasmiyya Mahmudova

Institute of Information Technology, B. Vahabzade str., 9A, AZ1141 Baku, Azerbaijan

rasmahmudova@gmail.com

https://orcid.org/0000-0002-5816-9373

ARTICLE INFO

http://doi.org/10.25045/jpis.v15.i2.06

Article history:
Received 19 February 2024
Received in revised form
22 April 2024
Accepted 24 June 2024

Keywords:

Socio-technical infrastrukture
Smart city
Cybersecurity problems
Smart infrastructure
Smart sitizen
Information security culture
Human factor

ABSTRACT

Smart socio-technological infrastructure is a new approach to the design and creation of complex systems, based on the integration of technological and social elements. Currently, smart socio-technological infrastructures are applied in all spheres of life, from business and industry to healthcare and medical facilities. The implementation of these infrastructures creates new opportunities for the development of various fields. However, it causes a number of problems. The reasons for new information security problems arising from the characteristics of smart socio-technological infrastructures may include the increase in the number of devices (the number of devices interacting with each other increases, which expands the potential attack plane), the complexity of integration (the integration of social and technological components leads to the creation of new vulnerabilities), data heterogeneity (where the processing and storage of various types of information, including confidential information, make them an attractive target for cybercriminals), the dynamism of the environment (smart socio-technological infrastructures are constantly evolving and adapting, which makes it difficult to ensure their security). This article examines information security problems of smart socio-technological infrastructures. New threats arising from the introduction of these infrastructures are classified. The development of information security culture is justified as one of the main factors of combating these threats, and recommendations are given on the principles and methods of its formation.

1. Introduction

Infrastructures are of strategic importance in any country and some of them are called critical infrastructures. Therefore, the condition and development of infrastructures is always under the control of the state. Well-planned and developed infrastructure has a positive impact on people's living conditions. It forms the foundation of the social and economic life of the society.

Infrastructures ensure the uninterrupted operation of the basic systems which our lives depend on. The way people live and function (for example, to move, access information, meet their needs for clean water or electricity) would not be possible without infrastructures.

Infrastructure is explained as a set of enterprises, institutions, management systems, communication tools, etc. that ensure the activity of society or any of its areas (Kuznetsov S.A., 2000).

In a general sense, infrastructure refers to a complex of measures, as well as enterprises and structures, that ensure the operation of all departments and organizations, regardless of their organizational-legal form and ownership form, located both on the territory of the state and beyond its borders.

For example, the fuel and energy complex, transport complex, healthcare, finance, information, engineering, scientific research and production, military, space, law enforcement, customs, social, tourism and other infrastructures belong to the infrastructure of the state. Recently, in addition to physical assets, intangible, virtual assets (for example, services, product supply cycle, websites, etc.) are also considered infrastructure.

Infrastructure is defined as objects, institutions, structures and systems that provide the necessary economic basis for the functioning of society. Infrastructure is classified in different ways. For example, infrastructure is grouped into technical and social infrastructure. Here, technical infrastructure refers to supply and disposal (water supply, sewage, energy supply, waste disposal), transport (automobile, railway, air and sea transport) and information and communication technologies (telecommunication, Internet, radio and television).

Social infrastructure is determined as the areas of physical social infrastructure (e.g., schools, fire departments, hospitals, etc.), personnel social infrastructure (e.g., social workers, kindergarten teachers, and police officers), and institutional social infrastructure (e.g., standards, laws, and guidelines).

In recent times, there has been a rapid increase in public demand for infrastructure assets. This is due to high expectations of productivity and service delivery (Annaswamy et al., 2016).

The importance of infrastructure is usually best understood when it is disrupted due to natural disasters. An example of this is violations in the infrastructure of the country, as well as in the city. For example, interruptions in gas, water and electricity supply, infrastructure disruptions as a result of traffic accidents.

Digital transformation also affects infrastructure development. It covers all spheres of human life, from business and public administration to personal information and daily communication. While creating many new opportunities that increase comfort and quality of life, it also brings certain dangers. Thus, as a result of the increase in digitalization, the security of people's personal data and data stored in various information systems, as well as people's privacy, are emerging.

The development of information technologies, the use of sensors, artificial intelligence, the Internet of Things, big data, and robotics have led to the wide application of the concepts of "smart infrastructure", "smart city", "smart village", and "smart home". In recent years, the concept of smart infrastructure has been applied in a number of areas, including electricity distribution, water supply and sanitation, automatic toll collection, intelligent transport systems, emergency services and monitoring of critical infrastructure assets such as tunnels, bridges and dams. (Hoult et al., 2009; Venkatasubramanian et al., 2014).

Smart socio-technological infrastructures are characterized as complex systems that connect people, technologies and physical objects to achieve a common goal. The main feature of these systems is that all its elements are constantly interacting with each other. Artificial intelligence and other advanced technologies are also used to achieve the common goal. In this regard, building and developing smart infrastructures requires society to be "smart" as well.

Currently, smart socio-technological infrastructures are becoming more and more widespread. This leads to increased cyber security risks that can have serious consequences for society. The study of the cyber security risks of smart socio-technological infrastructures, as well as the information security culture as one of the methods of preventing these risks, is very relevant for a number of reasons.

First, these infrastructures, applied in all areas of life, from healthcare to transportation to finance, are extremely complex and consist of a large number of interconnected devices and systems. This feature makes them more vulnerable to cyber-attacks.

Second, cyber-attacks on smart infrastructures can lead to serious consequences such as information theft, system disruption, financial loss and even threat to human life.

Third, it is observed that the level of information security culture is insufficient in many enterprises, as well as among the population. This makes them more vulnerable to cyber-attacks. Because criminals can use this factor to bypass technical security measures.

The purpose of the study is to analyze the new cyber security risks created by smart socio-technological infrastructures, including the risks related to the human factor, and to develop proposals and recommendations for their prevention.

2. Related work

In the scientific literature, cyber security problems of smart cities are explored from different aspects. (Elmaghraby and Losavio, 2014) state that advanced information technologies create new economic and social opportunities, as well as risks related to security and confidentiality. In smart cities, access to more information about the location and activities of citizens and privacy is compromised. According to the authors, collecting this data on any device or in the cloud raises questions about rights, responsibilities and risks. Analysts can use this information to create various services, which in turn can be used for beneficial or harmful purposes. The

article analyzes the problems related to the safety of data collected by recorders installed in vehicles, GPS navigation systems, including location data.

(Habibzadeh et al., 2019) states that the implementation of cyber-physical systems in smart cities can significantly improve healthcare, transportation services, utilities, security, and environmental protection. However, the efficiency gains and service improvements come at the cost of increased risks and gaps. This article provides a general summary of the theoretical and practical challenges of implementing smart cities from a technical, political, and organizational perspective. The authors believe that despite its many advantages, the implementation of smart cities increases infrastructure risks. According to (Baker et al., 2002), infrastructure risks are defined by three parameters: threats, gaps and consequences.

The services that make cities smart are selected by using the city's data flows (i.e., information about the location of residents, information about transport, the environment and digital interactions with local government bodies). The collection and processing of these data streams raises security and privacy issues at both the individual and societal levels (Zaheer Khaan et al., 2017). According to the authors, although various measures are taken to ensure the security and privacy of residents, these problems of smart cities are not only related to residents. Service providers and local governments have their own caveats, that is trust in service providers, reliability of data obtained, and ownership of data. In the study, researchers identify a list of stakeholders and model their participation in smart cities using an onion model approach. Based on this model, the authors present a security and privacy framework for service provisioning in smart cities, namely Smart Secure Service Provisioning (SSServProv).

(Mahmudova, 2023) mentions the security problems of cyber-physical systems, as well as the importance of the human factor in ensuring the information security of cyber-physical systems. The difficulties faced by the enterprises regarding the information security of the employees and the formation of the culture of information security in them are analyzed. Appropriate training methods for developing employees' necessary knowledge and skills related to information security are interpreted and recommendations are given.

In (Alguliyev R., Mahmudov R., 2021), the authors classify the human factor as one of the main pillars of cyber-physical systems.

Smart city technologies are promoted as an effective way to prevent uncertainties and urban risks through efficient services, however, creating new weaknesses and threats by making urban infrastructure and services more vulnerable, open to wider forms of crime (Kitchin, R., & Dodge, M., 2019). Here, researchers identify five forms of vulnerabilities in smart city technologies, and interpret the scale of cyber-attacks on network infrastructure and services based on examples.

In (de Bruijn, H., & Janssen, M.,2017), the authors describe cyber security as an ongoing battle between criminals and those who protect people and organizations from them. Because it is impossible to predict new attack types and technologies in advance. Correspondingly, those who create smart infrastructures do not fully know in advance what threats these infrastructures will face. Therefore, it is impossible to determine in advance the tools necessary to fight against unknown threats.

On the other hand, neither organizations nor individuals ever think that they will be attacked by hackers. It seems to them that these attacks do not concern them. In fact, there is always a risk of cyber security, and it applies to everyone. Recently, it has been rightly believed that people are the weakest link in the security chain. Criminals who influence people's weak points by using psychological methods convince employees to do what they need (Mahmudova, 2022).

People play an important role in updating and maintaining systems. They are responsible for detecting attacks and taking measures to prevent them. At the same time, it is very important to have an information security policy so that people know what is required of them (de Bruijn, H., & Janssen, M., 2017). Deliberately giving the password to someone by an employee working with information systems or carelessly handing it to someone else makes it possible for the data collected here to be stolen and fall into the hands of criminals (Mahmudova, 2021).

The analysis of the literature shows that the application of smart socio-technological infrastructures has many advantages in terms of improving the quality of services provided to the population, improving management, control, and promoting the living conditions of the population. At the same time, these infrastructures pose a number of security risks.

In the current study, the cyber security risks of smart infrastructures are analyzed and the issues of information security culture formation as one of the main methods in their prevention are discussed and suggestions are made. Section four analyzes the

cyber security risks of smart socio-technological infrastructures (smart city, smart healthcare, smart home systems). Section five examines the role of the "smart citizen" in smart city infrastructure and defines the necessary competencies. Section six classifies the new risks arising from the application of smart infrastructures and the necessary measures for their prevention. Moreover, recommendations are given on the principles and methods of information security culture formation.

3. "Smart infrastructures": essence and advantages

The rapid development and wide application of information technologies (IT) has led to the emergence of the concept of "smart infrastructure". There is no common definition of smart infrastructure. This term is used in different contexts according to different socio-technical conditions.

A specific feature of smart infrastructure systems is the continuous collection, analysis and feedback of large amounts of data to improve performance. Thus, supportive technologies such as connected sensors and big data analytics are integrated with physical infrastructure to enable real-time monitoring, efficient decision-making, and improved service delivery (Weiss, 2009).

Smart infrastructures have benefits such as reducing maintenance costs, minimizing damage and costs due to failures (congestion or power outages), increasing the quality and cost of services (on-demand usage and flexible tariffs), as well as protecting human life (reducing traffic accidents), or better responding to natural disasters (Morimoto, 2010).

"Smart infrastructures" are often referred to in the literature as "intelligent infrastructures", "digital infrastructures", etc. Intelligent infrastructures use modern information and communication systems such as sensor technologies and artificial intelligence to autonomously manage the execution process.

UN ECOSOC (2016) states that smart infrastructures underpin all key areas related to smart cities, including smart people, smart mobility, smart economy, smart lifestyles, smart governance and smart environments. In addition, smart transportation systems, smart energy management systems, smart water supply, smart waste management, and smart health services are identified as important types of smart infrastructure for smart cities.

Smart infrastructures offer additional benefits to citizens, simplifying daily life in many ways and ultimately improving the quality of life. For example, in smart cities, connections between citizens, governments and businesses are better established and important preconditions are created for the prudent use of resources.

Currently, there is an increase in interest in the concept of smart cities in the world, the main reason for which is the rapid increase in the number of urban populations. This forces cities to look for more efficient, intelligent solutions to adapt to population growth, save resources and money, and improve the living conditions of residents by using their infrastructure and assets more efficiently. To this end, smart city applications are used and they serve to improve the quality of life of residents. These programs allow cities to develop existing infrastructure and create new value. Existing infrastructure in smart cities is equipped with sensors. They collect information and transfer it to the "cloud" where the data is stored in real time. This data is then processed to analyze certain processes and make decisions based on it. Figure 1 presents the phases of this process:

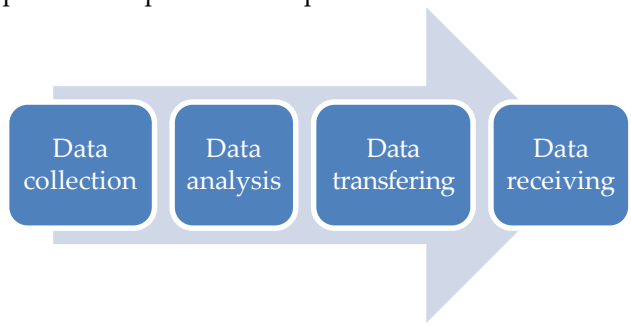

Fig. 1. Decision making in smart cities

- In phase 1, smart sensors collect data on the entire city in real time;
- In phase 2, the data collected by smart sensors are analyzed to obtain useful information;
- In phase 3, the information obtained as a result of the analysis is transmitted to decision-makers through reliable communication networks;
- In phase 4, the information obtained from the analysis is used to make decisions, optimize operations, manage assets and improve the quality of life of residents.

Ambitious projects are launched in a number of countries for the development of modern urban infrastructure based on the use of modern technologies. To overcome the shortcomings of modern cities, new IT systems using Big Data

analytics (analysis of data arrays about city residents), complex computer modeling, the results of the latest scientific research in the field of sociology and human behavior are produced and tested. Therefore, smart city projects take into account different approaches, from the study of human behavior to the management of resources and infrastructure.

A smart city is a common network connection, smart IoT devices, artificial intelligence and machine learning. Through these technologies, various types of data are collected and analyzed in real time. In general, they generate a complex of devices that increase the efficiency of the urban infrastructure of housing and utilities, transport, health and emergency services.

Harrison et al. (2010) believe that a smart city in terms of information technology should be understood as a combination of physical infrastructure, IT infrastructure, social infrastructure and business infrastructure to harness the collective intelligence of the city.

Smart cities cover all aspects of modern life (transportation, healthcare, entertainment, work, business, social interaction, governance).

The smart city concept includes smart solutions in a number of areas.

Smart parking. It is an automated, complex information-navigation system for parking management. The presence of vacant spaces in parking lots equipped with sensors and modern technologies is determined through the program. Important elements of modern smart parking include real-time information about free spaces in the parking lot; building a route to that place; automatic payment for space; parking space reservation etc.

Smart waste management. Different methods are used to solve the problem of waste management. In a number of European cities, garbage cans and containers are equipped with sensors, which inform the garbage companies about the amount of waste. Using visual recognition technologies, machine learning and cloud computing, IBM experts developed Wastenet - a waste sorting system. This system shows which type of waste should be put in which box. The user places the item next to a special scanner in the trash can, and the system directs it to the appropriate trash can (Stepanova I.A., Stepanov A.S., 2020).

Smart transportation. This concept envisages the creation of a single intelligent transport system. The goal here is to manage traffic and pedestrian flows of the city, ensure traffic safety, reduce traffic jams, create safe and convenient bus stops, and prevent environmental pollution using ICT. For example, the smartphone applications of transportation companies allow you to find the fastest route, as well as hail a taxi, book plane and train tickets electronically, and pay electronically. This also contributes to saving time for residents and protecting the environment.

Smart lighting. Through ICT, economic benefits can be obtained by automatic redistribution based on the collection and analysis of information related to the production and use of electricity. For example, in the management of city lighting, the application of smart LED lights that monitor and adapt to the current lighting level, thereby consuming less electricity, gives a great effect. Smart street lights that use smart sensors turn off when there are no cars or pedestrians on the road. In smart cities, both residential buildings and business buildings use less energy due to the installation of smart electricity meters and solar panels, better management of the grid, and the use of different energy sources.

Digital processes help to improve the image of the city, and at the same time strengthen the interaction between citizens and governing bodies.

4. Smart socio-technological infrastructures and cyber security risks

*Smart cities and security risks.*Smart city is a new trend expected to develop more in the coming years. From Singapore and Oslo to Auckland and Amsterdam, smart cities are emerging all over the world. New information and communication technologies, such as artificial intelligence (AI) and the Internet of Things (IoT), are expected to revolutionize the management of infrastructure and people.

However, one of the main challenges arisen in smart cities is data protection and confidentiality. How will the data continuously collected for the functioning of smart cities affect citizens? Is it possible to achieve true data privacy in a smart city environment?

Therefore, today it is important to understand not only the achievements of smart technologies, but also the problems and risks associated with their widespread application in smart cities.

Obviously, a smart city cannot function without the use of geospatial technologies. A smart city is equipped with a large number of smart devices (smart meters, intelligent building

management, motion and street lighting sensors, and millions of smartphones), all of which generate enormous amounts of data. This data collected from sensors and stored digitally is extremely useful for real-time decision making. However, the issue of privacy and security of the use of collected data is considered one of the main risks of smart cities. How this data is processed, who processes it, and whether it is transferred to a third party is a concern. (Zobova, 2016).

Smart cities use artificial intelligence to manage transport infrastructure and optimize human flow. However, these, in addition to increasing the efficiency and comfort of management, create new threats for society. Because the malfunction of such a management system can cause serious damage.

One of the biggest obstacles to the effective use of big data in city management is the lack of necessary skills at different levels of management. It is believed that the problem of smart cities cannot be solved without smart people who can use smart planning [World Economic Forum, 2012].

Cloud computing, the Internet of Things, mobile networks, and artificial intelligence are technologies that cities are using to improve the efficiency and quality of life of their citizens, but they also expose us to privacy and security risks.

Faulty sensors or hardware crashes, software errors, incomplete data and incorrect analytics can all lead to obstacles in people's access to emergency services or other authorities. As a result of an undetected data leak, system failure or system hacking, the privacy of citizens' data can be violated, and sensitive information can be captured.

Smart health and safety risks. Smart healthcare, based on the use of the capabilities of modern technologies such as IoT, artificial intelligence and machine learning, is a rapidly developing field. The application of these technologies has many advantages in terms of creating a more effective healthcare system and providing access to medical care.

In the last few decades, ICT has been widely applied in the health sector to facilitate the population's access to health services and to provide medical care more quickly and economically. The introduction of ICT has led to the development of electronic health record (EHR) systems. EHRs store information about the patient's entire medical history, i.e., the diagnosis given to the patient, the drugs taken, the results of laboratory tests, information about vaccinations, etc. They improve the interaction between doctor and patient.

Intelligent devices enabling the patient to be continuously monitored and assisted, when necessary, regardless of where he/she is, is now being used. Thus, the joint use of ordinary mobile devices with portable medical devices (tonometer, glucometer, smart watches, smart lenses, etc.) and IoT makes it possible. For example, wearable sensors (temperature sensor and heart rate sensor, etc.) collect physiological signals from the patient's body, and then transmit this data to a local server via a Wi-Fi network so that the end user (e.g., a doctor) can receive this data. Constantly updated servers allow doctors to access patient information in real time. The joint work of these devices allows creating a single medical report. Moreover, these data are useful for studying and predicting health trends across countries (Zeadally et al., 2020).

"Smart healthcare" is expected to reduce hospital costs and ensure timely treatment of various diseases (Sharma et al., 2017).

On the other hand, IoT devices can also pose a threat to users' security and privacy. Thus, unauthorized intervention in IoT devices can create a serious risk for the health of patients as well as their privacy (Zeadally et al., 2020).

Information about patients in healthcare institutions is collected and stored in various databases. Ensuring the security of this information is a matter of cyber security. Exposure to danger of medical data, leakage of personal information of patients, and wrong diagnosis of patients can lead to negative consequences. Furthermore, it can have a negative impact on the physical and mental health of patients (A. Razaque et al., 2019)

An analysis of reports on cyberattacks registered in the field of medical care organization and provision in different countries shows that, according to their essence, they are divided into the following types:

– Attacks on healthcare institutions (medical, diagnostic, scientific and medical educational structures, pharmaceutical laboratories, healthcare management institutions, etc.);

- Attacks on medical IoT devices, gadgets, local networks of healthcare organizations, as well as medical digital platforms;

- Theft and disclosure of confidential medical information available in digital format by employees of medical institutions who have access to such information.

Unquestionably, smart healthcare is a complex system that ensures the interaction of various devices and data. This interaction creates a number of cybersecurity risks:

- **Data leakage**. Patient information, including medical history and financial information, is very valuable to cybercriminals. Security breaches can lead to the theft of patients' personal information and blackmail.
- **Hacking of medical devices**. Hackers can take control of implantable devices or other medical equipment, putting patients' lives at risk.
- **Violations in the provision of medical services**. Ransomware attacks or "denial of service" attacks can disrupt hospital networks. As a result, patient care becomes more difficult and critical medical procedures may be compromised.
- **Vulnerabilities in artificial intelligence**. Artificial intelligence algorithms used for diagnosis and treatment can be tampered with by criminals, which can lead to inaccurate diagnoses and wrong treatment.

Preventing the cybersecurity risks of smart healthcare requires a comprehensive approach. This approach should cover prioritizing security functions during the design of medical devices, cooperation between stakeholders (health care workers, technology companies and cyber security experts), regular security monitoring by health care facilities, training for medical staff and patients, etc.

Experts and security companies analyzing the ransomware WannaCry attack occurred in 2017, infected thousands of computers in several countries around the world and caused huge financial losses, found that some of the reasons for this were systematically associated with the lack of backing up data and updating the operating systems installed on computers.

Verizon (2023) found that 68% of security breaches in 2023 were due to human factors. The report notes that people continue to play a major role in both incidents and security breaches. Malware and stolen data allow criminals to easily gain access to any information. Therefore, the necessity of programs raising information security awareness in organizations is emphasized.

Smart home systems and security risks. As a result of equipping IoT with various devices, the home environment becomes a smart hub, and public acceptance of the smart home ecosystem is increasing. Undoubtedly, the combination of the physical and digital world through smart home devices has a significant impact on the convenience and efficiency of everyday life (Guhr et al., 2020).

The smart home concept can be seen as an environment equipped with sensors, cloud computing and user directives. A smart home works on the principle of collecting all information about the house and its inhabitants from the bottom up, that is, sensors monitor all the behavior of people in the house and around (Alakbarova, 2023). The data collected by these sensors is collected and processed to identify and predict the daily activities of people in the house.

Using location data and other contextual information, users can control their home (lighting and heating), perform tasks (e.g., set reminders), communicate with others (e.g., make audio and video calls). Users taking advantage of using these technologies in their daily life, sometimes do not consider the security and sustainability aspects related to it.

As the number of smart devices increases, security and privacy risks also increase. The main obstacle to the implementation of "smart home" technologies is the concern about the confidentiality of information (Lowry et al., 2017). To use its full potential, smart home technologies require access to a lot of information about the home and the user's personal life. At the same time, smart home devices are usually designed with always-on hardware sensors, that is, they constantly collect information about offline activities occurring in the user's home (Acquisti and Grossklags, 2005). The collection of this type of information often occurs as a result of the user's lack of knowledge and disregard for the confidentiality of information. As a result, the host's information is exposed to a number of risks (acquisition, falsification, sharing, trading, analysis, loss, theft) by fraudsters and/or third parties for illegal use.

Thus, although the interconnection of devices in smart home systems is useful on the one hand, the low level of awareness of smart home owners in terms of cyber security may expose them to a number of external threats (Bringhenti et al., 2022).

Moreover, the smarter devices are deployed in a home network, the more devices a homeowner can accidentally lose their current security status. AVAST found that 40.8% of digital homes worldwide have at least one device vulnerable to cyber-attacks, putting the entire smart home at risk (Avast, 2019). Their report shows that the built-in security of devices is not always enough, as the security factor is often secondary to manufacturers.

Manufacturers of smart home systems note that the number of people interested in installing

these systems is constantly growing. The reason for this is due to the wide range of possibilities that the system gives to the owner. But they are not fully aware of the risks associated with the installation of such systems, while these risks are quite real. But what kind of unpleasant surprises can the Smart home owner face?

Such systems include many devices, and each of these devices collects and processes information. The exchange of information between them takes place through the network or directly, which makes them vulnerable.

Smart home devices connected to the network are typically controlled by an app on a mobile phone. Although this is very convenient for users, they pose a vulnerability. Criminals who gain access to the management of a smart home system can not only easily open the front door or window of the home, but also gain access to bank accounts, harm people living in the home whose health is monitored through a medical device, by disabling this device.

There are a number of problems with the security of modern intelligent systems, which allow criminals to easily enter the system. Hackers entering the system can obtain information about the lifestyle of residents, and even gain access to audio and video recordings by accessing the video surveillance system. This will make their work much easier.

Obviously, smart home systems often include these devices: smart refrigerators, smart cooling and heating systems, smart assistants, smart lighting, smart locks, smart alarms and sensors, IP cameras, smart washing machines, etc.

Not only smart home systems, but individual devices can also transmit information. For example, Samsung TVs with voice control function listen to everything that happens at home. This is explained by consumers that otherwise the device may ignore some necessary command and not respond. This is mentioned in the agreement with the user, and at the same time, the issue of giving this information to a "third party", for example, those dealing with voice recognition problems, is also reflected. It can also be hijacked by hackers.

Hackers attacking the control system of smart homes can take control of the IoT. This can lead to life-threatening situations. For example, hacking a car's smart control system would allow hackers to hack into any system, unlocking, locking, parking the car, etc.

The most dangerous threats to smart home systems are unauthorized access to information, threats of interception of data transmitted over a computer network, including bank data during transmission over the Internet. Because fraudsters who gain access to a smart home owner's personal information or bank accounts can use them for their own personal purposes or fraudulent transactions. Threats such as attacks from information and telecommunications networks and the introduction of malicious code by visiting infected sites on the Internet are also serious threats. They are dangerous both because the information can be obtained by third parties and because they can lead to taking control of the entire system.

Furthermore, the loss of the power supply can lead to the failure of all devices that do not have a backup power supply. For example, if the front door lock is electronic, the door can be opened automatically in the event of a power failure. In this case, the security alarm will also not work, which may lead to the theft of the property of the system owner.

For example, Kaspersky (kaspersky, 2024) explains the risks posed by networked household devices as follows:

1. The device regularly sends a lot of data to the manufacturer. For example, smart TVs can detect what you're watching, even if the content is from a flash drive or external player. Manufacturers make a lot of money by chasing customers. Even simpler devices like washing machines collect and send data.
2. If a smart device is protected by a weak password, uses a factory-installed configuration, is not modified by anyone, or has loopholes in the control system, hackers can gain control over them. The result will be diverse for different devices. For example, the washing machine can be stopped by mischief. With the help of the video monitor, you can track and even scare the owners of the house. Based on interference with smart home systems, the home's electrical and heating systems can be shut down or disabled.
3. If a smart device is hacked by hackers, malicious code can be used to attack both home computers and devices on the Internet. Very powerful DDoS attacks are known to be launched from infected video cameras. For owners of infected gadgets, this results in a decrease in Internet speed at home and various blacklists.
4. If the manufacturer does not adequately protect the data transmitted from the device, it can be intercepted and published. Sometimes recordings from video cameras

and video cameras are stored in poorly protected cloud environments, which makes it possible for information to fall into the hands of outsiders.

According to statistics provided by smart device manufacturers, about half of smart devices are never connected to the network, but such devices pose a number of security risks. It is quite possible that it will try to connect to the network in open Wi-Fi zones without a password.

The increase in the number of cyber security incidents around the world is mainly due to the fact that most of the people do not strictly follow the safety rules and instructions given in the workplace. The main security threat that makes the organization's assets vulnerable to external and internal actors are the organization's employees; that is, it is the person who is considered the weakest link in the security chain (Mahmudova, 2023).

Users often accept the option offered by the principle of silence in tuning the device, not paying attention to the complex technical instructions.

However, it also poses serious security risks: valuable data such as passwords, financial accounts and other sensitive information are considered attractive targets for attackers. Cyber-attacks on this infrastructure can not only lead to data leakage, but can also lead to serious financial losses and even loss of life. Therefore, it is extremely important to increase the awareness of people about cyber security to protect themselves from such attacks.

5. Place and role of "smart citizen" in "smart city" infrastructure

In addition to the implementation of the concepts of "smart city" and "smart village", expressions such as "smart citizen" and "smart person" are also often found.

According to (Frank & Fernández-Montesinos, 2020), a "smart person" is a person who is literate in the field of digital technologies, who takes advantage of technologies to be involved in a "smart city" environment, as well as in local problem solving and decision making.

In (Buyannemekh B., 2024), the author analyzes various approaches to the concept of "smart citizen" and summarizes them. According to the source, a smart citizen is a citizen who is able to use the technologies and data that form the basis of smart cities for own benefit and collective benefit.

The concept of "Smart city" is a concept that involves increasing the efficiency of the city economy by using the possibilities of modern ICT by citizens, giving them certain opportunities to be involved in city management. That is, in the "smart city" environment based on "smart technologies", there are real opportunities for the population to participate in the management of the city economy and municipality (Vasilenko L.A., 2021).

The analysis of the literature shows that to be a smart citizen, it is required to actively participate in discussions on "smart solutions" and innovations, in making decisions to improve the quality of life of citizens. Thus, in building smart cities and implementing various smart solutions, educating a smart citizen is of primary importance.

Citizens play an important role in the operation of the smart city, where technologies are integrated into all spheres of human life. To be an effective participant in such an environment, citizens must possess a number of competencies. Table 1 presents the list of these competencies.

6. Discussion

The relationship between smart socio-technological infrastructures and information security culture is becoming more and more important in the modern world. Socio-technological infrastructures such as smart cities, smart grids and smart homes are becoming more widespread and they create new opportunities to improve efficiency, comfort and quality of life. On the other hand, these infrastructures contain many interconnected devices and systems that can be attacked, which creates new cybersecurity risks.

Information security culture can be considered an important component of smart socio-technological infrastructures.

Socio-technological infrastructures combine technological advances and social practices to create efficient and reliable systems. For example, imagine a smart city that integrates smart lighting, energy distribution network, waste management systems, etc. Although this is a very complex technical issue on the one hand, it also has social aspects, such as the training of officials involved in urban management and raising the awareness of citizens for its effective management.

The main risk areas arising from the complex interaction between the technological aspects and the social aspects of smart socio-technological infrastructures can be classified as follows:

Table 1. Competencies required for smart city residents

Competencies	Explanation
Digital literacy	Ability to use various digital devices and online platforms to access information and take advantage of electronic services offered by the government.
Cyber security awareness	Knowing the basics of cyber security to protect information and personal data.
Information literacy	Ability to critically evaluate information obtained from online sources.
Problem solving skills and creative thinking	Ability to identify problems related to urban life and propose innovative solutions
Communicativeness	Collaborative skills to work together with other urban residents and authorities to improve the urban environment
Active citizen position	Understanding the rights and responsibilities as a resident of a smart city, willingness to participate in decision-making related to the development of the city, responsibility for the impact of actions on the urban environment.
Environmental awareness	Understanding the principles of sustainable development and the importance of respecting the environment. Conscious consumption of resources and the desire to minimize the ecological footprint
Adaptation and learning skills	The desire to constantly change and apply new technologies, the desire to develop oneself and increase one's qualifications. Ability to adapt to new living and working conditions in a smart city.

Confidentiality. Smart infrastructures often collect a lot of data about people's movements, behaviors and choices. This data may be used for monitoring, discrimination or advertising purposes.

Security. These interconnected systems can be vulnerable to cyber-attacks, resulting in the disruption of critical services.

For example, a hacked intelligent transportation system can lead to chaos. Or a hacking of an intelligent water supply system may result in a health hazard.

Social inequality. Unequal access to smart technologies can exacerbate existing social inequality. Those who do not have access or the necessary skills to use these systems may be left behind. For example, if public transport use is largely dependent on smart ticketing systems, those without a smartphone or internet access may be left out.

Loss of control. As more and more problem solving is automated by these systems, people risk losing control over critical aspects of their lives.

Algorithmic bias: Algorithms used in intelligent systems can perpetuate biases in society if not carefully designed. For example, face recognition software used in smart security systems may have higher error rates for certain ethnic groups.

Extraordinary Risks. Complex interactions between different components of smart infrastructure can lead to unpredictable and potentially dangerous consequences.

Consequently, the creation of "smart infrastructures" brings new opportunities as well as new threats. In particular, as a result of the digital transformations that occur with the application of Industry 4.0 technologies, countries are sometimes exposed to cyber threats on a global scale.

One of the main factors in the fight against cyber threats is the development of a cyber security culture in society.

Failure to adequately protect important information poses various threats to people's personal safety, government and business organizations' safety, and most importantly, national security. As a result, the problem of information protection becomes a personal, business and national priority and affects every member of society (Malyuk, 2021).

Therefore, cyber security measures must be understood and supported by every member of society. Everyone should know about the factors that threaten information security and the possible preventive measures that are important to avoid, understand their responsibility and take measures to ensure security.

In order to prevent the risks caused by smart infrastructures, it is important to implement the following measures first:

- The Information Security Policy should be developed, which includes the specific features of smart infrastructures;
- Threats related to smart devices and networks should be taken into account in the information risk management system;
- Technical protection methods should be

updated to protect against new types of attacks;
- Procedures and instructions should be adapted to new technologies and operations;
- Information security awareness and training should focus on emerging risks and threats.

Until recent years, more attention was paid to the development of technological methods for solving the problem of information security (Mahmudova, 2022). However, practice shows that without taking into account the human factor, the measures taken in the field of ensuring information security do not have the necessary effect. Building and developing an information security culture can help smart cities protect their critical infrastructure and keep their citizens safe.

Formation of information security culture in enterprises and organizations should be based on the following principles:

Responsibility: every employee must be responsible for the data protection.

Awareness: employees must be aware of information risks and know how to minimize them.

Vigilance: employees must be vigilant and report any suspicious activity or events.

Confidentiality: employees must maintain the data confidentiality.

Ethics: employees must follow ethical requirements when using information.

7. Conclusion

Thus, in parallel with the creation of smart socio-technological infrastructures, information security culture should be formed in the society.

From a technical point of view, information security threats include unauthorized access to information systems, information leaks, disruption of information systems or their separate subsystems, unauthorized mass collection of information, etc.

One of the important factors during the development of the mechanism of formation of information security culture in the society is that the measures to be taken should cover all citizens. Educational programs for all age groups should be prepared, and people should be ensured to be involved in education using various methods. The goal here is that when using information technologies, including smart devices, users should be responsible, avoid behavior that will cause security violations, be able to react in time during any security-related incident, be able to restore the operation of the computer, information system in the country, to be informed about the institutions responsible for data safety within the organization, so that they know who to contact regarding the incidents that occur.

For the formation of information security culture of citizens:

1. It is important to educate people about the fundamentals of information security so that they can protect themselves from cyber-attacks and identity theft. This should include knowledge and skills such as creating strong passwords, using antivirus software, and how to recognize phishing attacks.

2. People should be aware of the risks associated with using smart infrastructures and how to protect themselves from these risks. This can be implemented through awareness campaigns and educational programs.

3. Government agencies and companies must take steps to protect the information they collect about people. This includes developing strong security measures and ensuring data to be used only for legitimate purposes.

4. New laws and regulations should be developed to regulate the implementation of smart infrastructures. These laws must protect the confidentiality of personal data and ensure the safe and responsible use of smart infrastructures.

5. Cyber threats have no borders, subsequently it is important for countries to cooperate in the field of information security. This includes sharing information about cyber threats and developing joint strategies to combat them.

Formation of information security culture of citizens is very important to protect people from risks related to smart infrastructures. Education, information, information protection measures, legal regulation and international cooperation are important steps in this field.

References

Acquisti A., Grossklags J. (2005). "Privacy and rationality in individual decision making", IEEE Secur. Privacy, vol. 3, no. 1, pp. 26-33.

Alakbarova İ. (2023). Development of a model for the analysis of human behavior in a smart home environment. Problems of Information Society, 14(1), 75-84.

Alguliyev, R., & Mahmudov, R. (2022). Formation of Cyber-Physical Systems in Azerbaijan and Some Topical Problems of Their Complex Security. In Cybersecurity for Critical Infrastructure Protection via Reflection of Industrial Control Systems (pp. 81-89). IOS Press.

Alharbi, Talal, and Asifa Tassaddiq. (2021). "Assessing Cybersecurity Awareness Among Majmaa University

Students." Big Data and Cognitive Computing 5, no. 2: 23. doi:10.3390/bdcc5020023. (in Russian)

Annaswamy A., Ahmadpour A., Baros S. (2016). Emerging research topics in control for smart infrastructures. Annual reviews in Control, Volume 42, p. 259-270. doi:10.1016/j.arcontrol.2016.10.001

Avast, (2019). Avast smart home security report.

Baker, A. B., Hutchinson, R. L., Eagan, R. J., Moonka, A. K., Falcone, P. K., Swinson, M. L., ... & Hines, W. C. (2002). A scalable systems approach for critical infrastructure security (No. SAND2002-0877). Sandia National Lab.(SNL-NM), Albuquerque, NM (United States); Sandia National Lab.(SNL-CA), Livermore, CA (United States).

Bringhenti D., Valenza F., Basile C. (2022). Toward cybersecurity personalization in smart homes. IEEE Secur. Privacy, 20 (1), pp. 45-53, doi:10.1109/MSEC.2021.3117471

Bulletin of Tomsk State University. (2021). No. 468. P. 243–252. DOI: 10.17223/15617793/468/28 UDC 343.3/.7 L.R. Klebanov, S.V. Polubinskaya DIGITAL HEALTHCARE, THE COVID-19 PANDEMIC, AND CYBERSECURITY PROBLEMS. (in Russian)

Buyannemekh B, Gasco-Hernandez M, Gil-Garcia JR. (2022). Fostering Smart Citizens: The Role of Public Libraries in Smart City Development. Sustainability, 16(5):1750. doi:10.3390/su16051750

C. Harrison, B. Eckman, R. Hamilton, P. Hartswick, J. Kalagnanam, J. Paraszczak, P. Williams. (2010). Foundations for smarter cities IBM Journal of Research and Development, pp. 1-16.

de Bruijn, H., & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. Government Information Quarterly, 34, 1-7.

Elmaghraby A.S., Losavio M.M. (2014). Cyber security challenges in Smart Cities: Safety, security and privacy J. Adv. Res., 5 (4), pp. 491-497.

Frank, E., & Fernandez-Montesinos, ´ G. A. (2020). Smart city= smart citizen= smart economy?: An economic perspective of smart cities. Social, Legal, and Ethical Implications of IoT, Cloud, and Edge Computing Technologies, 161–180.

Guhr N., Werth O., Blacha P.P.H., Breitner M.H. (2020). Privacy concerns in the smart home context SN Appl. Sci., 2, pp. 2523-3971. doi: 10.1007/s42452-020-2025-8.

Habibzadeh, H., Nussbaum, B. H., Anjomshoa, F., Kantarci, B., & Soyata, T. (2019). A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. Sustainable Cities and Society, 50, 101660.

Hoult N, Bennett PJ, Stoianov I et al. (2009). Wireless sensor networks: creating 'smart infrastructure'. Proceedings of the Institution of Civil Engineers – Civil Engineering 162(3): 136–143, doi:10.1680/cien.2009.162.3.136.

Kaspersky daily. https://www.kaspersky.ru/blog/how-to-secure-smart-home/34849/

Kitchin, R., & Dodge, M. (2019). The (In) Security of Smart Cities: Vulnerabilities, Risks, Mitigation, and Prevention. Journal of Urban Technology, 26(2), 47–65. doi:10.1080/10630732.2017.1408002.

Kuznetsov S.A. (2000). The Large Explanatory Dictionary of the Russian Language / (ed.). - SPb.: Norint, 2000. — C. 397. — ISBN 5-7711-0015-3. (in Russian)

Lowry, P.B.; Dinev, T.; Willison, R. (2017). Why security and privacy research lies at the centre of the information systems (IS) artefact: Proposing a bold research agenda. Eur. J. Inf. Syst. 26, p.546–563.

Mahmudova R. (2021). On some aspects of the culture of information security of an individual and society, Problems of information society, 12(1), 56-66. doi:10.25045/jpis.v12.i1.05.

Mahmudova R. (2022). Analysis of international experience in the formation of a culture of information security in society, Problems of Information Society, 13(1), 75–82. doi:10.25045/jpis.v13.i1.10.

Mahmudova R. (2023). "Cyber-physical Systems: Security Problems and Issues of Personnel Information Security Culture", International Journal of Education and Management Engineering (IJEME), 13(2), 18-26. doi:10.5815/ijeme.2023.02.03.

Mahmudova R. (2024). Voprosi razvitiya chifrovix kompetenciy specialistov dlya Industry 4.0 /Informacionnoye obshestvo, 1, p. 61-70. doi: 10.52605/16059921_2024_01_61.

Malyuk, A.A., Malyuk, Z. P. (2021). Topical issues of creating a mass education system for information security culture. IT Security (Russia), 28(4), 6–21. ISSN 2074-7136. doi: 10.26583/bit.2021.4.01.

Morimoto R. (2013). A socio-economic analysis of Smart Infrastructure sensor technology. Transportation Research Part C: Emerging Technologies 31: 18–29. doi:10.1016/j.trc.2013.02.015.

Ogie, R. I., Perez, P., & Dignum, V. (2017). Smart infrastructure: an emerging frontier for multidisciplinary research. Proceedings of the Institution of Civil Engineers - Smart Infrastructure and Construction, 170(1), 8–16. doi:10.1680/jsmic.16.00002.

Razaque A. et al. (2019). "Survey: Cybersecurity Vulnerabilities, Attacks and Solutions in the Medical Domain," in IEEE Access, vol. 7, pp. 168774-168797.

Sharma, S., Tripathi, M.M. and Mishra, V.M. (2017), "Survey paper on sensors for body area network in health care", The IEEE International Conference in Emerging Trends in Computing and Communication Technologies (ICETCCT).

Stepanova I.A., Stepanov A.S. (2020). Review of waste collection and disposal systems in anthropogenic ecosystems, Samara Scientific Bulletin, v.9, no. 2(31), p. 121-131. (in Russian)

UN ECOSOC: Report on Smart cities and infrastructure (2016), https://unctad.org/system/files/official-document/ecn162016d2_en.pdf

Vasilenko L.A. (2021). Digital breakthrough: will public administration be smart enough in a digital state and how smart are the elite and citizens. Digital sociology, vol. 4, no. 3, pp. 6–15. doi: 10.26425/2658-347X-2021-4-3-6-15).

Venkatasubramanian KK, Mukherjee T and Gupta SK. (2014). CAAC – an adaptive and proactive access control approach for emergencies in smart infrastructures. ACM Transactions on Autonomous and Adaptive Systems (TAAS) 8(4): 1–20.

Verizon Data Breach Report (2023). https://www.verizon.com/about/news/2023-data-breach-investigations-report

Weiss A. (2009). Smart infrastructure matches supply and demand. Networker 13(3): 18–25.

World Economic Forum. (2012). Strategic Infrastructure Steps to Prioritize and Deliver Infrastructure Effectively and Efficiently. Geneva.

Zaheer Khan, Zeeshan Pervez, Abdul Ghafoor Abbasi. (2017). Towards a secure service provisioning framework in a Smart city environment, Future Generation Computer Systems, Volume 77, p. 112-135, ISSN 0167-739X, doi10.1016/j.future.2017.06.031.

Zeadally, S., Siddiqui, F., Baig, Z. and Ibrahim, A. (2020). "Smart healthcare: Challenges and potential solutions using internet of things (IoT) and big data analytics", PSU Research Review, Vol. 4 No. 2, pp. 149-168. doi:10.1108/PRR-08-2019-0027.

Zobova L. L. (2016). The problem of describing geospaces: modern technologies // Bulletin of the Kemerovo State University. Series: Political, sociological and economic sciences. No. 1. p. 51 – 55. (in Russian)