

THE IMPORTANCE OF INFORMATION TECHNOLOGIES IN THE DEVELOPMENT OF THE PUBLIC SAFETY SYSTEM

<https://doi.org/10.5281/zenodo.15626437>

A. A. Saitkhanov

*Senior Lecturer (PhD) of the Department of "Philosophy and national idea"
of Fergana State University*

The article examines the importance of information technology in the development of the public security system. Emphasis is placed on using video surveillance, smart cities, big data analytics, and cybersecurity to enhance the effectiveness of law enforcement agencies, emergency services, and other structures ensuring citizens' safety. The article analyzes the opportunities and challenges associated with the introduction of new technologies, including issues of. It is expected that with the development of IT systems, the public safety system will be significantly improved, however, it is also necessary to consider the ethical and legal aspects of their use.

Information technology (IT) has become an integral part of all spheres of human activity, and the public security system is no exception. Technologies are changing approaches to crime prevention, ensuring law and order, and protecting citizens from various threats. The development of IT in the field of security is related to the application of modern solutions that make it possible to more effectively manage situations, respond quickly to incidents, and prevent crimes. However, the implementation of such technologies is also associated with a number of problems, such as the protection of personal data, privacy, and legal issues, which require attention from government bodies and society[1;57].

One of the most obvious and important areas of IT application in the field of public safety is video surveillance. In recent years, surveillance cameras have become an important tool in maintaining public order[2;64]. However, traditional video surveillance systems no longer meet modern security requirements. The implementation of intelligent systems with facial recognition and big data analysis capabilities makes cameras much more efficient[3;7].

Moving from traditional video surveillance methods to more modern solutions, it can be noted that modern cameras not only record what is happening but can also analyze information in real time, identifying anomalous events. For example, facial recognition systems can identify suspicious individuals in public places such as airports, railway stations, or stadiums and immediately send an alarm signal to relevant authorities. This significantly speeds up the law enforcement response process and can help prevent crimes before they occur. In some cities, such systems have already been implemented that can track citizens'

behavior, allowing for quick response to suspicious actions and prompt identification of criminals[4;32].

An example of the successful application of such technologies is China, where a system of video surveillance with facial recognition is used in a number of large cities. These systems allow tracking people's movements, quickly identifying offenders, and preventing potential threats. The impact of such systems on the level of crime in cities has become noticeable - thanks to high-tech solutions, the number of crimes in public places has been reduced.

Along with the development of video surveillance, the concept of "smart cities" is becoming increasingly important. In such cities, more and more infrastructure elements, including transport, energy supply, water and waste management, are connected into a single system, where data is collected and analyzed for more effective management. Smart cities are actively using various technological solutions to improve citizens' safety and quality of life. Moving on to the next aspect, it can be noted that in smart cities, data coming from various sensors, cameras, and IoT devices is used not only to monitor the environment but also to quickly respond to emergencies. For example, devices can monitor parameters such as air quality, pollution level, temperature, and humidity, which helps to respond promptly to potential threats such as gas leakage or fire[5;8]. This allows not only to increase the level of safety, but also to improve the overall comfort of life in cities.

In addition, smart cities use innovative technologies to improve transport systems and ensure road safety. For example, intelligent systems can automatically adjust traffic lights, optimizing traffic flow and minimizing the likelihood of accidents. In case of an accident, the system can immediately notify emergency services so they can arrive at the scene as quickly as possible.

In addition to surveillance cameras and smart cities, one of the most significant technologies changing the public safety system is big data analytics. In a situation where the volume of information coming from various sources is rapidly increasing, the use of such technologies has become necessary for effective management of situations. Data analytics allows for the collection and processing of large amounts of information from video cameras, sensors, social networks, and mobile devices, which helps to predict threats and respond to them quickly[6;9].

Moving from technological solutions in the field of video surveillance and smart cities, it can be emphasized that the analysis of big data gives law enforcement agencies a unique opportunity to predict crimes. By examining patterns and patterns, such systems can predict where and when violations may occur. This allows patrols to be sent to potentially dangerous areas in advance, as well as to respond to calls promptly. As a result, the safety of citizens is improved, and the response time of emergency services is reduced. An example of the successful use of data analytics is the "PredPol" system in the USA, which predicts possible crimes based on historical data[7;5]. This allows the police to take measures in advance to prevent crimes in hot spots.

With the increasing use of information technologies in the field of public safety, the threat of cybercrime also arises. As seen from previous points, technologies such as video surveillance and data analysis play a key role in ensuring security, but they also become vulnerable to cybercriminal attacks. Therefore, to ensure the reliability of the security system, it is important to develop and strengthen cybersecurity.

Unlike physical threats, cyber threats can pose a real danger to the entire society. Hacking attacks on emergency services or law enforcement agencies can paralyze the work of these structures, leading to catastrophic consequences[8;6]. Therefore, protection from such threats has become a priority for all countries developing national and international security systems.

Among the technologies used to protect against cyber threats, one can highlight data encryption, the use of multi-layer authentication, and security systems against hacking. Modern governmental and private organizations are obligated to continuously update their security systems, train specialists, and implement the latest information security solutions.

With the development of IT in the field of public safety, there is also a need for legal and ethical regulation of its use. As previous sections showed, technologies such as video surveillance and data analysis can significantly enhance citizens' security, but at the same time, they raise issues related to personal data protection and human rights compliance.

Moving from the technical aspects to the issues of legal norms, it is important to note that the use of these technologies requires the implementation of strict data protection mechanisms, as well as their transparent and fair application. It is necessary to ensure a balance between the effectiveness of technologies and the observance of citizens' rights to privacy and personal inviolability. For this, international standards and laws regulating the use of such technologies, as well as the creation of independent bodies to monitor their application, are necessary. Information technology has a profound impact on the development of the public security system. Video surveillance, smart cities, data analytics, and cybersecurity technologies open up new opportunities to improve security levels and effectively respond to threats. Nevertheless, with the introduction of these technologies, serious challenges arise related to the protection of personal data and human rights, which requires clear legal frameworks and ethical standards.

The future of information technology in the field of security is linked to its further development and improvement, but this also requires a careful approach from society to the issues of its use so that these technologies serve the benefit of society without violating the fundamental rights of citizens.

LIST OF USED LITERATURE:

1. Kotenkova, E. V. Information Technologies in Law Enforcement Agencies. - M.: Yuridicheskiy mir Publishing House. 2021

2. Ivanov, I. A. Video surveillance as a safety tool in modern cities. - Saint Petersburg: "Security" Publishing House. 2020.
3. Smirnova, N. V. Artificial Intelligence in Video Surveillance: Opportunities and Challenges. - "Security Technologies" journal.2022.
4. Vedeneyev, I. M. Modern Video Surveillance Systems. - M.: "Security of the XXI Century" Publishing House. 2023.
5. Petrova, T. V. Internet of Things in Smart City Systems. - Journal "Smart Cities and Innovations." 2021.
6. Vlasova, I. P. Big Data and its Role in Crime Prevention. - Journal "Society Safety." 2022.
7. Nabiyeu, A. S. PredPol System: How Crime Prediction Works. - "Police Practice" magazine. 2019.
8. Dmitriev, I. K. Cybercrime Risks in the Public Security System. - Journal "Cyber Threats and Protection." 2021.