European Proceedings of
Multidisciplinary Sciences
EpMS

www.europeanproceedings.com
e-ISSN: 2421-826X

DOI: 10.15405/epms.2024.09.92

MTMSD 2022
I International Conference «Modern Trends in Governance and Sustainable Development of Socio-economic Systems: from Regional Development to Global Economic Growth»

DIGITAL TECHNOLOGIES AND INNOVATIONS APPLICATION IN PENITENTIARY ACTIVITY OF THE RUSSIAN FEDERATION

Shadid Sh. Mutsalov (a), Oleg G. Kovalev (b)*, Irina I. Krasnyanskaya (c),
Olga E. Mikhailova (d), Andrey V. Shcherbakov (e)
*Corresponding author

(a) Chechen State University named after A. A. Kadyrov, Grozny, Russia, Shadid_rshb@mail.ru
(b) Pskov Branch of the Academy of Law Management of Federal Penal Service of Russia, Pskov, Russia, okovalev66@gmail.com
(c) Pskov Branch of the Academy of Law Management of Federal Penal Service of Russia, Pskov, Russia, krasnyanskayirina@mail.ru
(d) Pskov branch of the Academy of Law Management of Federal Penal Service of Russia, Pskov, Russia, ostanina545@mail.ru
(e) Pskov branch of the Academy of Law Management of Federal Penal Service of Russia, Pskov, Russia, Andrey-Sherbakov-1973@yandex.ru

Abstract

In the article are observed theoretical, organizational and legal basis of modern informational technologies and innovation's introduction and use in penal activity. They are able to ensure security of penal institutions. Legislative and other regulatory legal acts on the topic are analyzed. It is pointed that the main aim of government and executive authorities' development is a total digital transformation. This process involves penal system of Russia. At the same time the experience reflected in international regulatory legal acts, the Concept for the development of the penal system for the period up to 2030 is actively applied. The results of a comprehensive theoretical and empirical 5 years study, methodology and special applied methods have shown that decision-making based on artificial intelligence in terms of penitentiary institutions location, their security, and control over persons who are punished by non-custodial measures is a priority and promising area of activity for bodies of the Federal Penitentiary Service of Russia. The development of a methodological and technological basis for the formation and development of personnel competencies in order to carry out digital transformation and innovation activities will allow them to exercise professional activities at a higher level. Creation of a single secure managed information space of the Federal Penitentiary Service of Russia is aimed at introducing information systems and resources for processing official and confidential information, interdepartmental electronic interaction with federal executive authorities, law enforcement and judicial authorities.

Keywords: Digital transformation, digital technologies, innovations, penal system

https://doi.org/10.15405/epms.2024.09.92
Corresponding Author: Oleg G. Kovalev
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

1. Introduction

Information and telecommunication technologies are actively developing in all spheres of the modern state and change the human life. They act as the main engine of progress development.

The national security strategy of the Russian Federation approved by Decree of the President of the Russian Federation dated July 2, 2021 No. 400 refers to the national interest in developing safe information space, protection of Russian society from destructive informational and psychological impact. The resources of public authorities, organizations and institutions of civil society act as a mechanism for implementing the protection: (Rossiyskaya Gazeta, 2020, July 22).

One of the priority national development goals of the Russian Federation for the period up to 2030 is digital transformation which affects all social spheres of state bodies including the prison department.

Digital technologies and innovations are actively used in domestic penitentiary practice. International legal provisions for ensuring security have a positive effect on the Russian penitentiary system development. A significant part of them is accepted in the current Russian legislation and is implemented in law enforcement practice in constitutional and legislative provisions: (Shcherbakov et al., 2017).

At present the international legal component takes an important place in the legal security of the penitentiary system. This fact is explained by active participation of Russia in the integration processes of the penitentiary sphere, constitutional and legislative provisions. They determine the parameters for the perception of international law in the legal Russia. The progressive nature of the provisions are contained in international legal acts serve as legal guidelines for the development of criminal – executive system and ensure its security in a democratic society: (Shcherbakov et al., 2020). In this context scientists analyze the regulatory framework, international and domestic standards for digital technologies and innovations use in the field of information security. This is very relevant for penitentiary practice at the present time: (Rodichev, 2019). At the same time scientists focus on the introduction of modern automated systems that are able to identify and eliminate threats to the information cyberspace including security objects: (Bondarev, 2016). There were studied various aspects of information crimes, the detection, disclosure and prevention of crimes in digital spheres: (Bykov & Cherkasov, 2015).

In accordance with the concept of the penitentiary system of the Russian Federation development for the period up to 2030 approved by the Decree of the Government of the Russian Federation dated April 29, 2021 No. 1138-r it is planned to carry out digital transformation and implement digital technologies in all spheres of the system.

The analysis of normative legal acts allows the authors to pay attention to such priority areas as

i. creation and development of data collection,
ii. decision-making based on the results of artificial intelligence use in institutions of the penitentiary system, security and control over persons who are punished by non-custodial measures,
iii. creation of a single protected managed information space of the Federal Penitentiary Service to ensure the implementation and operation of information systems and information resources involving the processing of confidential information and to ensure interdepartmental electronic

https://doi.org/10.15405/epms.2024.09.92
Corresponding Author: Oleg G. Kovalev
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

interaction with information systems of federal executive authorities, law enforcement and judicial authorities.

2. Problem Statement

The introduction and use of modern informational technologies and innovations in penal activity are essential for ensuring the security of penal institutions. However, the effective implementation of these technologies requires a strong theoretical, organizational, and legal basis. In this context, it is important to analyze the legislative and other regulatory legal acts related to the topic to identify the challenges and opportunities for their practical application.

3. Research Questions

The authors' collective, for the most part, aimed to find answers to several questions, namely:

i. What is the current state of the theoretical, organizational, and legal basis of modern informational technologies and innovation's introduction in penal activity?
ii. What are the major challenges and opportunities for implementing these technologies in penal institutions?
iii. How can decision-making based on artificial intelligence be utilized in terms of penitentiary institutions' location, security, and control over persons who are punished by non-custodial measures?
iv. What are the competencies required for personnel to carry out digital transformation and innovation activities in the penal system?
v. What are the benefits of creating a single secure managed information space for the Federal Penitentiary Service of Russia?

4. Purpose of the Study

The purpose of this study is to examine the theoretical, organizational, and legal basis of modern informational technologies and innovation's introduction and use in penal activity with the aim of identifying the challenges and opportunities for their practical application. The study aims to provide insights into the practical implementation of these technologies, including the use of artificial intelligence in decision-making, the development of competencies required for personnel to carry out digital transformation and innovation activities, and the creation of a single secure managed information space for the Federal Penitentiary Service of Russia. Ultimately, the study seeks to contribute to the total digital transformation process involving the penal system of Russia through the development of a methodological and technological basis for the formation and development of personnel competencies.

5. Research Methods

The comprehensive study of information technologies in the penitentiary system has been carried out over the past five years. Domestic and foreign experience in the use of information and

https://doi.org/10.15405/epms.2024.09.92
Corresponding Author: Oleg G. Kovalev
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

telecommunication technologies and security systems has been analyzed. A content analysis of the main definitions and concepts proposed by scientists and practitioners in this field has been carried out. The results of digital technologies and innovations introduction have been studied by the comprehensive analysis method in eight territorial bodies of the Federal Penitentiary Service of Russia. Trends in the subject matter have been identified throughout the prison administration of the Russian Federation.

The methodological bases for the study of legal and organizational aspects of information technology and computer security introduction in the institutions of the penitentiary system were the fundamental provisions of domestic legal science, comparative legal and statistical methods. Methods of systemic and structural analysis, interviews with employees of engineering and technical departments and security departments and the participant observation method were used. Various approaches were considered in the ways of implementation information technologies and subsequent security in the field of cyber threats, ways to prevent them and identify the difficulties of stable operation at the facilities of prison infrastructure.

6. Findings

The results of the study were discussed by the authors at international round tables, scientific and practical conferences. More than 20 scientific articles have been published in journals annotated by the Higher Attestation Commission, Scopus, Web of Science. There was conducted a study by the Research Institute of the Federal Penitentiary Service of Russia. More than 2.5 thousand employees of the penitentiary system took part in the implementation of effective information technology tools to ensure the safety of staff and special contingent of the penitentiary department. The results of the survey of 2819 convicted persons from places of liberty deprivation was conducted in 60 constituent entities of the Russian Federation and allowed to assess information technology processes modernization in correctional institutions of the Federal Penitentiary Service of Russia. 54.9% of convicted persons noted that the introduction of new information technologies is effective for their safety and it prevents them from committing further crimes. This information was obtained from the Central Prisoner Monitoring System: (Central Inmate Monitoring System, 2007, December 31).

Researchers note that the introduction of complex integrated systems at protected facilities of penitentiary institutions is a qualitatively new approach to security at a higher modern hardware and software and technological levels: (Belkin, 2015).

The most important elements of the integrated security system are biometric technologies that allow people to be identified by one or more physical or behavioral traits: (Bochkarev, 2016) and a security television system designed to control restricted areas, secure locations and increase the service efficiency of penitentiary officers in terms of ensuring security requirements: (Berdnikov, 2016).

It is significant that the employees of the penitentiary system highly appreciate these technical means. They control supervision in the system of crimes prevention.

According to the results of the study with 2.5 thousand participants conducted by the Research Institute of the Federal Penitentiary Service of Russia 75% of respondents consider video recorders to be the most effective means of supervision in the system of crime prevention, 65.4% of respondents consider video surveillance to be the most effective, 26.3% consider the access to control systems to be the most

https://doi.org/10.15405/epms.2024.09.92
Corresponding Author: Oleg G. Kovalev
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

effective and 15.8% consider light and sound alarms (a total excess is of 100% due to the fact that respondents marked different answers at the same time).

According to the results of a survey the majority of convicted persons serving their sentences in places of liberty deprivation consider the installation of video surveillance cameras as a factor contributing to the observance of internal regulations and in general they evaluate this fact positively.

66.8% of the respondents noted that installation of video surveillance cameras in correctional institutions is conductive to internal order control. 24.5 % noted that video surveillance system in residential and locked premises contributes to ensuring the safety of convicted persons. 10.3% of respondents noted that video cameras installation keep employees from being rude. 9.7% of respondents noted that video cameras installation prevent the convicts from committing illegal actions. At the same time 52.3% of the respondents pointed video surveillance as a factor invading their privacy. 58.8% of the respondents indicated video surveillance equipment as the best mean of safety. 25.8% indicated alarms, 11.4% indicated security lighting systems. 60.1% of the respondents believe that video surveillance cameras installed in premises contribute to their personal safety. At the same time many convicts noticed that each camera has got "blind zones". Results of the survey of 2819 convicts serving sentences in places of liberty deprivation was conducted in 60 constituent entities of the Russian Federation in the period from July to September 2017

Majority of the convicted persons noticed the technical means such as alarms, video surveillance and integrated security systems of restricted areas as a barrier to escape.

54.9% of the surveyed convicted persons said that fences and technical means of the restricted areas are a deterrent to escaping. 31.8% consider the possibility of using weapons by sentries as a deterrent to escaping. Results of a survey of 2819 convicted persons serving sentences in places of liberty deprivation was conducted in 60 subjects of the Russian Federation in the period from July to September 2017.

The given empirical data testify the importance of digitalization, introduction of innovations, the equipment of penitentiary institutions and planned decisions reflected in the federal programs of penitentiary department development. While preparing these regulatory legal acts the experience of developed foreign countries in the field of digital technologies and innovations application in penitentiary institutions of open and closed types was in demand: (Kovalev et al., 2022).

This fully applies to the introduction of modern digital technologies and innovations in the field of computer or cyber security in the penitentiary system. In conducting the study the authors took into account the experience of this work organization in the EU states where over the past years the cybersecurity strategy has been actively implemented, its legal and organizational structures have been created: (Kovalev & Skipidarov, 2021). The strategy is enshrined in the legislation of the European Union and individual member states: (Europol Europa, 2022). While developing the trend representatives of Germany state structures propose to introduce digital technologies into the activities of state law enforcement agencies not only at the federal level but also at the level of specific lands, subjects of the federation. Italian experts in the field of digital technologies application in cybersecurity suggest to concentrate on the use of specific techniques that allow timely digitization of the received data, its classification and eliminating emerging cyber threats in cyberspace.

https://doi.org/10.15405/epms.2024.09.92
Corresponding Author: Oleg G. Kovalev
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

The materials of the study allowed the authors to conclude that the internal equipment of the penitentiary, the level of modern information and computer technologies use, innovations in the field of digital technologies has a significant influence on the state of law and order in places of liberty deprivation. Penitentiary institutions with digital technologies and innovations, modern integrated security systems and engineering and technical equipment have a two times lower level of violations.

The observed information and technological changes and the process of their integration allows the authors to talk about the modernization of the systems in the penitentiary department which is necessary for collecting and processing data, recording violations of convicted persons, predicting possible illegal actions of convicted persons and other persons on the regime territory.

As it was mentioned above the effectiveness of implementation involves digitalization and intellectualization of the information systems of the Federal Penitentiary Service of Russia, adoption of innovative solutions for the regime and supervision organization and possibility to control persons punished by non-custodial measures.

Today the Russian state has a national standard in the field of Big Data which describes its characteristics, methods of analysis and security control in this area: (Electronic sinking fund and regulatory and technical information (2021, November 1).

The use of the data analysis received in the penitentiary environment increases the role of the possible interaction of correctional institution services and law enforcement agencies in relation to convicted persons punished by non-custodial measures.

It is necessary to record persistent information about the convicted person for the data implementation. This information includes his way of serving the sentence, the state of his health, his psychological state, his behavior during the period of serving the sentence and many other indicators that were previously not available or were considered as unimportant circumstances.

The whole range of information received during the period of serving a sentence by a special contingent and form Big Data must be processed, structured and analyzed for successful implementation in correctional facilities.

Employees of the penitentiary department receive information for predicting and automating decision-making in case of order violation by convicted persons, employees of the administration and other persons located in the regime area.

Big Data received by the Federal Penitentiary Service of Russia can represent various kinds of information that has special volume, speed of its receipt, analysis of processing and reliability. In order to analyze the received information it is necessary to use technologies of Data Science, NoSQL, SAP HANA, MapReduce and Hadoop, other services and hardware.

7. Conclusion

Under the circumstances of the foregoing and taking into account the presented positive scientific and practical research the authors came to the following conclusions.

i. Information technologies development will solve such problem as inability to process big data promptly.

https://doi.org/10.15405/epms.2024.09.92
Corresponding Author: Oleg G. Kovalev
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

ii. By means of programming languages such as SQL and Python Big Data Science analytics can reach a new level in the field of detecting deviant behavior of a convicted person. Analyzing the large data volumes of the special contingent behavior it is possible to find unexpected correlations of the convicted person and prevent his further crimes or illegal actions.

With regard to the use of video surveillance of special contingent, administration and other persons located in the regime area it is necessary to focus on video analytics. The information received through video cameras will be able to promote methods of the so-called computer vision which allows obtaining data by processing and analyzing image sequences.

The basis of software in correctional institutions processing video analytics is a set of machine vision algorithms without the direct participation of penitentiary institution employee.

The above examples are related to information security of the penitentiary department and they illustrate the following tasks

to include Data Science in computer vision tasks,

to observe a convicted person in the correctional institution, track his behavior throughout the day, classify his actions, to identify convicted persons and employees in the correctional institution,

to extract data from images and subsequent provision of the obtained information to special services,

to analyze received information by the use of artificial intelligence.

i. The applied information technologies will represent a set of methods and tools for processing structured and unstructured information in order to obtain specific results. In this case it is possible to use big data analysis in the security systems of correctional facilities, monitor the quality of work of the special contingent in the production area and detect the location of the convicted person and the administration employee.
ii. Decision-making by officials will be based on the results of artificial intelligence use. This means the use of video analytics and predicting the behavior of convicted persons and staff, control over persons punished by non-custodial measures and behavior of the released persons.
iii. Registration of a single protected managed information space of the Federal Penitentiary Service of Russia involves the creation of a specialized database to secure service information protected by the law of the Russian Federation. It is necessary to provide appropriate certified equipment to suppress attempts of unauthorized access to this information, protect personal data of personnel, suspects, accused and convicted persons.
iv. The introduction of digital technologies and innovative products involves interaction with information systems of law enforcement agencies that provide control over persons after they have served their sentence, obtain documents required for the resocialization of convicted persons in society, send electronic submissions to the courts on issues of sentence serving order, requests for parole, hold videoconferences, webinars, material and medical support for detainees, etc.
v. Creation of a methodological and technological basis will allow employees of penitentiary institutions to perform their functional duties at a higher level and ensure safety of special contingent.

https://doi.org/10.15405/epms.2024.09.92
Corresponding Author: Oleg G. Kovalev
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

vi. Security of information technologies should take its place in the educational process and scientific activities of educational and scientific organizations of the Federal Penitentiary Service of Russia so that future employees of the penitentiary department will have an opportunity to perform their tasks at a higher professional level (Nazarov et al., 2021).

vii. It is necessary to teach employees the culture of cybersecurity, algorithmization of the network and cyberspace users' response to possible tricks of cybercriminals such as phishing emails, encryption programs, software viruses, and others. It is important to protect not only confidential and limited distribution of information but also other databases used in penitentiary practice.

viii. It is necessary to carry out systematic explanatory work and annual cybersecurity monthly plans. They will help to increase the knowledge and skills of officials, employees of the penitentiary system in the field of information and computer security.

References

Belkin, V. Y. (2015). Security in the institutions of the penitentiary system. *Bulletin of the penitentiary system, 8,* 27-35.

Berdnikov, N. G. (2016). Features of the use of engineering and technical means of protection and supervision in the penitentiary system at the present stage. *Technology and safety of objects of the penitentiary system: a collection of materials of the International Scientific and Practical Interdepartmental Conference.* Voronezh Institute of the Federal Penitentiary Service of Russia.

Bochkarev, V. V. (2016). Improving the use of engineering and technical means in correctional institutions. *Actual problems of Russian law, 4,* 170-178. https://doi.org/10.17803/1994-1471.2016.65.4.168-175

Bondarev, V. V. (2016). *Introduction to information security of automated systems.* MSTU named after N.E. Bauman Press.

Bykov, V. M., & Cherkasov, V. N. (2015). *Crimes in the field of computer information: criminological, criminal law and forensic problems.* Urlitinform Press.

Central Inmate Monitoring System. (2007, December 31). *28 C.F.R. pt. 524, subpt. F; Program Statement 5180.05*. https://www.bop.gov/policy/progstat/5180_005.pdf

Electronic sinking fund and regulatory and technical information. (2021, November 1). Information Technology. Big Data. Overview and Dictionary. *GOST R ISO/IEC 20546-2021*. https://docs.cntd.ru/document/1200180276

Europol Europa. (2022). *European Union Agency for Law Enforcement Cooperation*. Retrieved 1 October, 2022 from www.europol.europa.eu

Kovalev, O. G., & Skipidarov, A. A. (2021). Legal regulation of the cybersecurity strategy implementation in the states of the European Union. *Stolypin Vestnik, 3*(2), 48-55.

Kovalev, O. G., Vilkova, A. G., & Shvyrev, B. A. (2022). Methodology for the formation of knowledge about information and computer security of penitentiary institutions. *The penitentiary system: law, economics, management, 4,* 25-27. https://doi.org/10.18572/2072-4438-2022-4-25-27

Nazarov, V. L., Zherdev, D. V., & Averbukh, N. V. (2021). Shock digitalisation of education: Education and science. *Education and science, 23*(1), 156-201. https://doi.org/10.17853/1994-5639-2021-1-156-201

Rodichev, Y. A. (2019). *Regulatory framework and standards in the field of information security: international and national standards.* Piter Press.

Rossiyskaya Gazeta. (2020, July 22). *On the national development goals of the Russian Federation for the period up to 2030: Decree of the President Ros*. Federation dated July 21, 2020 No. 474. https://rg.ru/documents/2020/07/22/ukaz-dok.html

https://doi.org/10.15405/epms.2024.09.92
Corresponding Author: Oleg G. Kovalev
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2421-826X

Shcherbakov, A. V., Mikhailova, O. E., Uskacheva, I. B., Bogdanov, M. N., & Shatov, S. A. (2017). Foreign experience the security of the penitentiary system and the possibility of its use in domestic practice. *Bulletin of Tver State University. Series: Law, 3*, 75-93.

Shcherbakov, A. V., Smirnova, I. N., Budanova, L. Y., & Shabanov, V. B. (2020). International legal acts in the field of security and their implementation in the penal system of Russia. *Bulletin of the Kuzbass Institute, 4*(37), 152-161.