DOI: https://doi.org/10.34069/AI/2023.61.01.31

How to Cite:
Kaduk, S., Shulha, A., Svoboda, I., Varyvoda, I., & Mykytyn, Y. (2023). The use of automated information systems in the investigation of criminal offences. *Amazonia Investiga*, *12*(61), 307-316. https://doi.org/10.34069/AI/2023.61.01.31

The use of automated information systems in the investigation of criminal offences

Застосування автоматизованих інформаційних систем при розслідуванні кримінальних правопорушень

Received: January 15, 2023 Accepted: February 19, 2023

Written by:
Svitlana Kaduk[132]
https://orcid.org/0000-0002-5300-9987
Andriy Shulha[133]
https://orcid.org/0000-0001-5524-5433
Ivo Svoboda[134]
https://orcid.org/0000-0002-0941-4686
Iryna Varyvoda[135]
https://orcid.org/0000-0002-6728-3696
Yurii Mykytyn[136]
https://orcid.org/0000-0002-9354-3586

Abstract

The aim of the study was to develop recommendations for the most effective and safe use of automated information systems in the investigation of criminal offences. The study involved the following methods: anamnestic method; descriptive analysis; forecasting method. The society uses an automated information system, which is defined as an ordered complex (system) of actions designed to implement a specific information technology for the performance of specified functions, which involves personnel and a complex of automation tools. They help to create databases, which are used in the investigation of criminal offences. The following measures are proposed for increasing the efficiency and expanding the scope of automated information systems in the investigation of crimes: ensure the protection of databases from external intrusions (cyber-attacks); ensure the internal security of the data contained in the respective databases in order to prevent privacy violations; ensure the

Анотація

Метою дослідження було вироблення рекомендацій щодо забезпечення максимально ефективного та безпечного використання автоматизованих інформаційних систем при розслідуванні кримінальних правопорушень.У дослідженні використовувалися такі методи: анамнестичний метод; метод описового аналізу; метод прогнозування. Автоматизована інформаційна система діє у суспільстві, і визначається як упорядкований комплекс (система) дій, спрямований на реалізацію конкретної інформаційної технології виконання визначених функцій, в процесі чого задіяні персонал та комплекс засобів автоматизації. За допомогою них створюються бази даних, які і використовуються у процесі розслідування кримінальних правопорушень. З метою підвищення ефективності та розширення сфери використання автоматизованих інформаційних систем у розслідуванні злочинів пропонується: забезпечити захист баз даних від зовнішніх

[132] PhD of Law Sciences, Associate Professor, Department of Politics in the Sphere of Combating Maliciousness and Criminal Law, Primary Scientific Law Institute, Precarpathian National University named after Vasyl Stefanyk, Ivano-Frankivsk, Ukraine.
[133] PhD of Juridical Sciences, Associate Professor, Department of State and Legal Disciplines and Public Administration, Faculty No. 4, Donetsk State University of Internal Affairs, Kropyvnytskyi, Ukraine.
[134] Associate Professor, Guarantor of Security Management Studies, Department of Security and Law, University of Regional Development and Banking Institute, AMBIS, Prague, Czech Republic.
[135] Postgraduate Student, Department of Policy in the Field of Crime Control and Criminal Law, Educational and Scientific Law Institute, Vasyl Stefanyk Precarpation National University, Ivano-Frankivsk, Ukraine.
[136] PhD of Law Sciences, Associate Professor, Director, Professor, Department of Politics in the Field of Fighting Crime and Criminal Law, Vasyl Stefanyk Precarpathian National University, Ivano-Frankivsk, Ukraine.

organization of specialized training for law enforcement officers; automate a number of tactical operations using information systems; develop and adapt all possible information resources and technologies for the set procedural tasks; create unified databases of forensic data at the international and national levels. This study opens up prospects for further research for the most effective protection of databases from illegal use, which will contribute to the development of this direction in international and national criminal justice.

Keywords: information systems, artificial intelligence, investigation, proceedings.

правопорушень (кібер-атак); забезпечити внутрішню безпеку даних, що містяться у відповідних базах, щоб не допустити порушення їх конфіденційності; забезпечити організацію спеціалізованого навчання працівників правоохоронних органів; автоматизацію за допомогою інформаційних систем низки тактичних операцій; розробити та пристосувати для поставлених процесуальних завдань усіх можливих інформаційних ресурсів та технологій; створити об'єднані бази криміналістичних даних на міжнародному і національному рівнях. Дане дослідження відкриває перспективи для подальших пошуків найефективнішого захисту баз даних від незаконного використання, що сприятиме розвитку цього напрямку у міжнародній та національній кримінальній юстиції.

Ключові слова: інформаційні системи, штучний інтелект, розслідування, провадження.

Introduction

The need to use the latest means of response to certain actions of people around the world determined the introduction of the latest information technologies in criminal justice (Ritchie et al., 2021). Accordingly, the investigation of criminal offences requires a widespread use of automated information systems, which is determined by the need for timely, complete and reliable information (Thompson, 2010) and the potential of artificial intelligence in this area is difficult to overestimate (Rigano, 2019). The use of these technologies is accompanied by a number of problems that must be solved in the near future. In particular, the matter is about the ethics of using certain human databases (biometric data to create facial recognition technology) (Smith & Miller, 2022); legality of using information from mobile phones of persons involved in a specific criminal offence as evidence (Alatawi et al., 2020). There can also be complications when police reports from different structural parts are combined to create and maintain a single database (Carnaz et al., 2020). On the other hand, the issue of protecting such electronic databases from theft and distribution of confidential information arises (Uzlov & Strukov, 2017).

The aim of this study, in view of the relevance of the issue under research, as well as the unresolved issues related to the use of automated information systems in the investigation of crimes, will be to develop recommendations to ensure their most effective and safe use by law enforcement agencies in the investigation of criminal offences. The aim involved the following research objectives:

- identify and describe the largest and most important forensic databases;
- analyse the powers of international organizations in the field of information exchange between law enforcement agencies;
- establish basic methods of studying forensic data

This article will consist of the following sections:

- Introduction – the relevance of the research and its purpose and tasks are highlighted;
- Review of the literature - the latest studies of the selected issues are analyzed in the sources, and little-researched problems and unresolved issues in this area are identified;
- Methodology and methods – the research methods are defined, and the empirical material used in the article is indicated;
- Results – data and theoretical propositions are displayed, and facts are given in the author's interpretation, including tables and figures;
- Discussion – the opinions of individual researchers are presented regarding the prospects and shortcomings of the use of automated information systems in the investigation of crimes and the author's attitude towards them;

- Conclusions – the author's vision of the practical and legislative achievement of the set goal and the implementation of the set tasks is presented;
- Sources - a list of literary sources used in this study is provided.

Literature review

Individual issues of implementation and use of automated information systems in the activities of relevant bodies are the subject of quite a large number of theoretical and practical studies in view of the importance of this direction of modernization of the process of investigation of criminal offences. Bulgakova et al., (2019) studied the use of large databases in the investigation of criminal offences in general. Pramanik et al., (2017) conducted research on the use of technological data analysis in the activities of investigative bodies. Rigano (2019) studied the possibilities of using certain technical devices and developments in order to collect relevant information to improve the investigation of criminal acts, such as artificial intelligence to meet the needs of criminal justice, are being studied.

A number of studies deal with the issue of the use of separate databases for the investigation of criminal offences. In particular, they focus on the possibility of using information systems which contain data on fingerprints and palms to identify persons who have committed a criminal offence (Haraksim et al., 2019); appropriateness and possibility of using biometric databases in criminal proceedings (Smith et al., 2018), as well as different types of information contained on electronic media. The issues of appropriateness of using data contained in social networks (Arshad et al., 2020) and mobile content or other information from mobile phones in the investigation (Alatawi et al., 2020), as well as the inclusion of this type of data in certain information systems were covered. Solovyeva and Frantsiforov (2020) separately studied the peculiarities and specifics of the investigation of some types of crimes using electronic and digital databases as automated information systems.

The question of protecting relevant databases containing forensic analytical information to ensure the investigation of criminal offences logically arises against the background of an extended use of automated information systems in the investigation of crimes and in criminal procedural activities in general (Uzlov & Strukov, 2017). The reason is that the theft of such information will have a negative impact on the work of law enforcement and judicial bodies both at the national and at the international level.

It is necessary to consider those studies that express an ambiguous attitude to the use of automated information systems in criminal justice in general and in procedural activities in particular. Willis et al., (2020) note that the impact of the use of information technologies on the work of police officers is ambiguous and causes different attitudes among the police officers themselves. Thornton (2016) criticizes attempts to create unified databases for the work of police officers.

It should be noted that currently insufficient attention is paid to such problematic aspects of the use of automated information systems in the investigation of crimes as the protection of personal data (confidentiality) contained in these databases. The issue of general protection of the databases created by automated information systems against the theft of confidential information is not fully resolved. In the current context, these issues require an urgent theoretical and practical solution, and their legislative enshrinement.

Methods

This study was carried out in stages based on the logic of the presentation of the material to achieve the aim of achieving the aim set in the article and fulfilling the relevant objectives. These stages were the following:

- formulating the topic and defining the scope of the research;
- search and selection of literature and sources;
- selection and study of statistics;
- analysis of the material presented in the selected sources, and evaluation of the results of these studies;
- identification of unresolved problems related to the use of automated information systems in the investigation of criminal offences;
- determining the aim of the article;
- drawing conclusions and providing practical recommendations for solving the problems selected for research;
- outlining the prospects for further research in the specified area.

This study was based on the data on the types of information systems and databases, areas of activity for obtaining information, as well as the information exchange between law enforcement

agencies of different states aimed at fighting crime. A number of national and international databases used by law enforcement agencies in criminal proceedings (The National Crime Information Center Database, FBI Uniform Crime Database, Interpol International Criminal Databases, Stanford Open Policing Project, Combined DNA Index System Crime Database), twenty databases used in forensic investigations that are created and owned by the United States; nineteen Interpol databases used by police around the world were analysed.

The legal framework of the study consisted of the provisions of international legal acts, in particular, the Convention on the establishment of a European Police Office (Europol Convention) of 1995, Council Decision of 6 April 2009 establishing the European Police Office (Europol), Council of Europe Committee of Ministers Recommendation No. R(87) 15 to the Member States on regulating the use of personal data in the police sector of 17 September 1987, Council Decision 2005/681/JHA of 20 September 2005 establishing the European Police College (CEPOL) and repealing Decision 2000/820/JHA.

The study involved the following methods to achieve the aim of the research:

- the *information analytical method* was used to analyse information sources and draw conclusions on the importance of using automated information systems in the investigation of criminal offences, as well as outlining prospects for further research in this area;
- the *system approach* was used to analyse the conclusions on the need to use the latest information technologies in the investigation of criminal offences;
- the *anamnestic method* was used to collect data on international and national cooperation in the investigation of criminal offences;
- the *descriptive analysis* was used to study the literature and information sources on the use of automated information systems in the investigation of crimes;
- the *forecasting method* was used to develop proposals and recommendations for improving the mechanism of using automated information systems in the investigation of criminal offences and ensuring their protection.

Results

An automated information system is a component of the overall concept of an automated system used in society. It is defined as an ordered complex (system) of actions aimed at the implementation of a specific information technology for the performance of specified functions, which involves personnel and a complex of automation tools (Black, 2023). Automation tools include software, computer hardware, a processing system, storage of information and texts, networks and other relevant special equipment.

The relevant databases are created by automated information systems, which are used in the investigation of criminal offences. Almost every country has such databases at the current stage of scientific and technical development. For example, they distinguish between such basic databases for forensics as anthropological, ballistic, biometric, domestic violence data, firearms, digital crimes, banditry, human trafficking, etc. in the US (Uncovered, 2022).

In general, there are five world largest and the most important in terms of the collected materials of individual countries and international databases, which are used in forensics for the investigation of criminal offences (see Table 1 for more details).

Table 1.
Top 5 forensic data sources

1	NCIC (The National Crime Information Center) Database	It has been used since 1967; a comprehensive database that contains forensic information from all US law enforcement agencies, and is accessible to every criminal justice agency and court in the country.
2	FBI Uniform Crime (UCR) Database	A massive FBI managed database which contains data on past crimes, divided into four large databases; it is accessible to law enforcement officers as well as the public for full information free of charge.
3	Stanford Open Policing Project	Contains data on daily detentions (stops of transport and individual citizens); it was created for the purpose of establishing cooperation between citizens and law enforcement agencies; it is publicly available and used for statistical research
4	Interpol International Criminal Databases	Database of the International Criminal Police Organization; it contributes to the investigation of international crimes; combines 19 separate databases; has a secure system for law enforcement officers to communicate through a database; open to law enforcement agencies worldwide
5	CODIS DNA (Combined DNA Index System) Crime Database	The database exists since 1990 and is provided by the FBI; it contains information about biological evidence; contributes to the identification of missing persons and detection of complex cases; available in the USA and 90 laboratories in more than 50 countries; it is based on a special software

Source: Kovacevic (2020).

In recent years, cooperation between police officers at the international level has been developing rapidly. The relations between police officers are not bilateral, but multi-channel, where interaction is established simultaneously with many countries.

The EU is one of the bright examples of such cooperation between police officers of different countries. The EU created a special police service — Europol (like the international organization Interpol) — on the basis of the Convention on the establishment of a European Police Office (Europol Convention), which was adopted in 1995 and ratified by EU member states in 1998 (Council Act of 26 July 1995 No 95/C 316/01). This organization coordinates the activities of law enforcement agencies of the EU member states, as well as non-member states, cooperates with other international organizations in providing forensic data. The main function of Europol is the organization of interstate cooperation in combating crime and the implementation of relevant criminal policy. The scope of this organization includes ensuring detection and investigation of criminal offences committed on the territory of member states based on the main standards of combating crime. The direct function of Europol is to provide information (see Figure 1for more details).

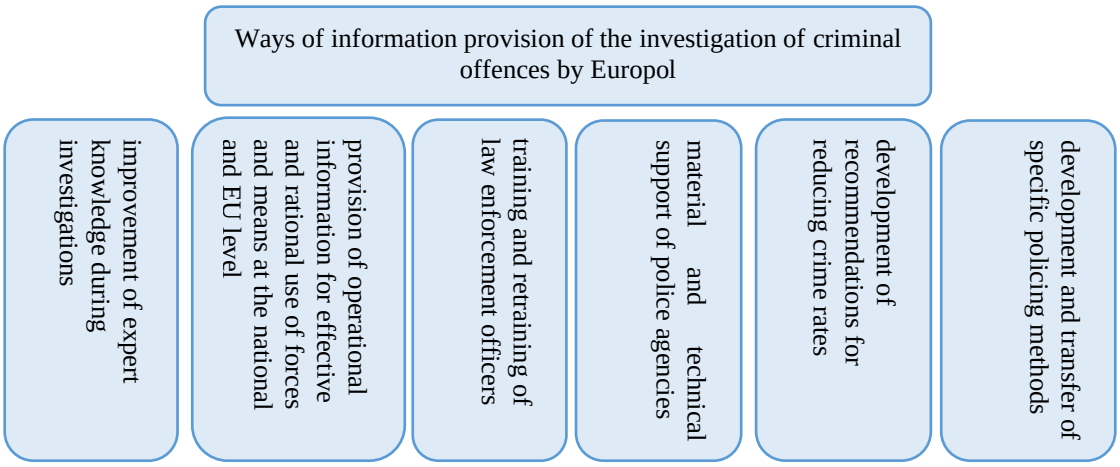

Figure 1. Powers of Europol in information provision
Source: Sirant (2016)

As the international cooperation in the field of crime investigation is developing and strengthening, there are international databases that form the basis of an international automated information system. According to Interpol's definition, these include databases of personal data on offenders, forensic databases, data on travel (movements) and official documents, on stolen property, etc. (see Table 2 for more details on international databases). At the same time, it is indicated that these 19 databases contain 124 million police reports and are used daily by 20 million people who are looking for data (the response time to a request is less than a second).

Table 2.
Interpol's 19 databases used by police around the world

Database	What is includes
Note: Interpol Criminal Information System (Colour-Coded International Dangerous Persons Alert System)	
Individuals	Nominal data: personal data and criminal histories of people for whom international police cooperation is requested Violence against children and the victim: an international database that provides data for establishing the connection between the victim, the perpetrator and the crime scene; contains images of child sexual exploitation; aims to locate and detain criminals
Criminalistics	Fingerprints: an automated fingerprint identification system DNA: database of DNA profiles of criminals, missing persons, unidentified bodies I-Familia: a database that identifies missing persons by matching them with family DNA Facial recognition: a database providing a specialized platform for storing and cross-checking images to identify missing persons, escapers
Travel and official documents: border checkpoints databases	Travel and Identity Documents Database (INTERPOL's SLTD): contains information on travel and identity documents known to be illegal Stolen Administrative Documents (SAD): contains records of stolen official documents that serve to identify objects Counterfeit documents: provides police and border guards with information on the main identification markers of falsified or forged documents Comparison of authentic and forged documents: includes examples of genuine travel documents to identify fake ones
Stolen property	Vehicles: contains advanced identification data for all types of vehicles and parts that can be identified from a stolen report Vessels: Stolen Vessels is a centralized database for tracking stolen vessels and engines Works of Art Database: contains descriptions and images of cultural objects reported as stolen by Member States and international partners
Circulation of firearms	Firearms Identification: an interactive online tool that provides standardized methods for the most accurate identification and description of firearms for tracking them in cross-border investigations Firearms Tracing: a single global law enforcement platform to support transnational tracking of illegal, lost or stolen firearms, terrorism and other firearm-related crimes. Ballistic Data Comparison: the world's only large-scale international ballistic data exchange network.
Organized Crime Networks — a database that helps to improve the efficiency of gathering and sharing intelligence, investigations and analysis of criminal networks that facilitate the identification and arrest of their leaders and financiers.	
Maritime Piracy: stores intelligence on incidents of piracy and armed robbery at sea, including details of individuals, their location, etc.	

Source: Our 19 databases. Interpol (2022).

The use of databases created by automated information systems can have various directions. But the main ones, which relate to the collection and analysis of data necessary for the investigation of criminal offences, are distinguished. These include the most effective intellectual methods for synthesis and analysis, such as link analysis, intelligent agent, text mining, neural network, machine learning (see Figure 2 for more details).

The creation and development of databases with the help of automated information systems to make procedural activities in the investigation of criminal offences and their further use in this area more efficient is accompanied by certain complications and threats. They require an urgent solution.

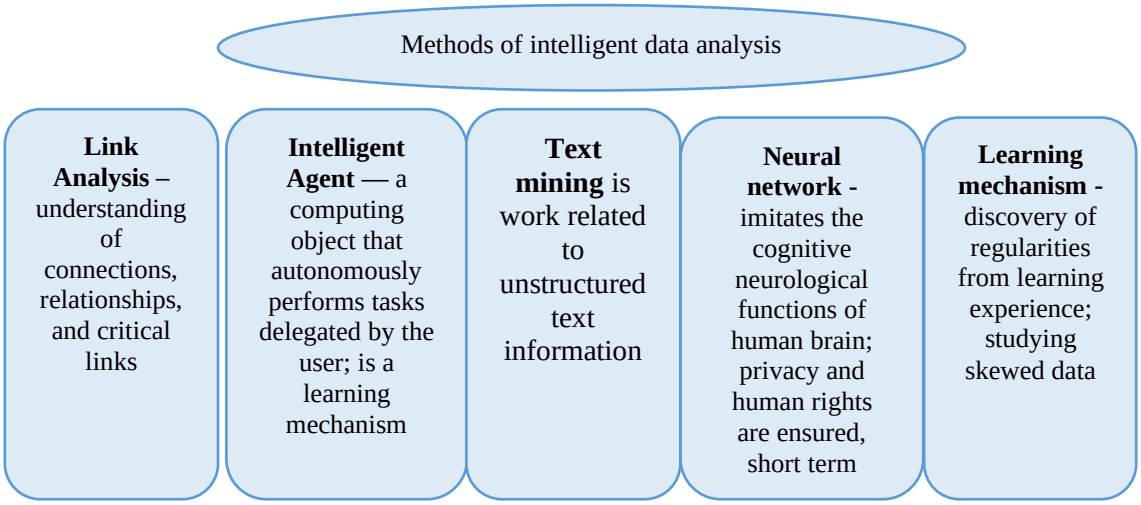

Figure 2. Five methods of intelligent data analysis
Source: Pramanik et al., (2017)

The risk of theft or damage of such data as a result of specially targeted cyber-attacks is one of the most dangerous. Different methods are offered for the protection of such systems, where the following ones are distinguished as the most effective:

- a method of monitoring the parameters of variable software components of the trusted information environment, which ensure the stability and integrity of the system (Kalinin, 2010);
- a method of multi-stage identification of users, which can be based on entering a login and password that changes from time to time; entering a set of user-specific data; recognition of biometric data; using radio code devices; chip authentication (Kirilchuka et al., 2022);
- accreditation and certification method, where the Ministry of Defence in provides access to databases of a particular country subject to the submission of relevant documents (Dawson et al., 2013).

Guaranteeing human rights and freedoms enshrined in international and national regulatory legal acts is another problematic aspect of using such databases in the investigation of criminal offences. This applies to ensuring the minimum standards of information protection enshrined in the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 1981, and the Convention on Cybercrime of 1987. The relevant international and national bodies apply the principle of personal data protection as part of a partial solution to this problem. It prescribes that data contained in separate databases and information systems can be transferred and used only by the competent authorities of the member states to the Convention and only for the purpose of preventing and combating crime in general and investigating individual crimes in particular. Their other use must be coordinated with the states that own the database, but on the condition that the information is used only for the stated purposes, which do not contain a potential threat of violation of individual rights and freedoms.

At the national level, the vast majority of states have separate legal acts, including norms aimed to protect personal data from their illegal use or distribution. On the other hand, prosecution is associated with certain complications. It should be, however, noted that certain effective steps in this direction have already been taken. In particular, individual countries established a system of fines for the mentioned offences. The EU adopted the General Data Protection Regulation (GDPR) in 2018, which not only clearly regulates the collection, processing and use of personal data, but also provides quite significant fines for legal entities for violating the regulations. About EUR 360 million of fines were collected under this Regulation for 2 years (Fisun, 2020). Therefore, the establishment of

appropriate penalties in the future will have an appropriate effect for personal data protection.

The process of creating and using special databases for the investigation of criminal offences depends on scientific and technological development. The future of law enforcement is likely to continue to evolve rapidly, as artificial intelligence and automated information tracking become more common. But this process is also complicated by a certain incompetence of law enforcement officers in using databases created by automated information systems. Therefore, the promising directions in the process of improving the use of information databases in the investigation of crimes are the following:

- the organization of specialized training of law enforcement officers in order to develop the skills of detection, preliminary study, research, recording of intellectual, material and virtual traces of criminal offences;
- independent work with databases, electronic media and means of recording information;
- conducting investigative actions with the introduction of information technologies and the capabilities of artificial intelligence.

One of the promising areas should be the automation of a number of tactical operations by using information systems, which include the search and identification of persons involved in a crime, identification of suspects, exposure of the criminal, identification of accomplices, study and analysis of the obtained evidence, establishment and identification of traces of a criminal offence etc.

There are the following promising directions of fulfilling the specified objectives and improving the use of automated information systems:

- development and adaptation of all possible information resources and technologies for the set procedural tasks, as well as the development of a mechanism (algorithm) for their use in criminal proceedings, in particular for the investigation of criminal offences;
- creation of unified databases, which will contain forensic information in the most complete volume, at the international and national levels, which will allow speeding up individual stages of criminal proceedings and increasing their efficiency.

Discussion

There is no doubt about the need to develop new and improve existing mechanisms for the use of automated information systems and created databases in law enforcement activities in general and in the investigation of crimes in particular. This is determined by the potential of artificial intelligence, which will be used in the fight against crime and, in particular, in detecting crimes, much more widely (Rigano, 2019). There is a need to protect information systems (geo-information systems) used in crime investigations, as well as forensic analysis and analytics (Uzlov & Strukov, 2017).

At the same time, it is difficult to fully agree with the reasoning regarding the unethical use of biometric data and technologies for recognizing faces or other parts of the human body, because this artificial intelligence technology has great potential for investigating crimes provided proper data protection (Smith & Miller, 2022). The same applies to the analysis of mobile content, which can be used as evidence. Given the needs of law enforcement agencies, is quite permissible also under the condition of maintaining confidentiality (Alatawi et al., 2020).

On the other hand, it is indicated that the use of information systems in the investigation of crimes does not always bring positive results, as they can break the interaction between the employees of investigative bodies and the police (Willis et al., 2020). Although, such interaction will be re-established as soon as a single database is created. One cannot agree with those who believe that the procedural technology is not promising and will not bring the expected results (Thornton, 2016).

At the same time, we fully agree with the proposal regarding the need for constant comparison of techniques and methods, choosing the necessary methodology depending on the type and severity of crimes in order to improve the use of databases in the investigation of criminal offences (Pramanik et al., 2017). The proposition regarding the appropriateness of improving the automation of the investigation process itself and other forensic processes is essential (Jadhav et al., 2020).

Conclusions

The above study demonstrated the potential and high efficiency of using automated information systems in the investigation of criminal offences.

The development of digital technologies and the implementation of artificial intelligence in law enforcement activities in relation to the investigation of criminal offences, an increasing number of spheres of social life and activity require the development of mechanisms that will facilitate the rapid and high-quality use of its achievements in certain spheres. It is proposed to improve the following areas of this activity in order to improve efficiency and expand the scope of the use of automated information systems in the investigation of crimes:

- protection of databases from external intrusions (cyber-attacks) by monitoring the parameters of variable software components of the trusted information environment, multi-stage identification of users and the method of accreditation and certification;
- ensuring the internal security of the data contained in the relevant databases in order to prevent violations of their confidentiality by imposing appropriate fines, as well as other types of liability;
- organization of specialized training law enforcement officers to develop their skills of studying intellectual, material and virtual traces of criminal offences, independent work with databases, conducting investigative actions with the introduction of information technologies;
- automation of a number of tactical operations using information systems;
- development and adaptation of all possible information resources and technologies for the set procedural tasks;
- creation of unified databases of forensic data at the international and national levels.

It is proposed to develop a special document (Recommendations) at the international level on the basis of the specified recommendations, which will contain these provisions and propositions for their most effective implementation in procedural activities by individual states.

This study opens up prospects for further research for the most effective solution to problematic aspects in this area. This includes, in particular, ensuring the protection of databases and confidential information from illegal use, which will contribute to the development of this area in international and national criminal justice.

Bibliographic references

Alatawi, H., Alenazi, K., Alshehri, S., Alshamakhi, S., Mustafa M., & Aljaedi, A. (2020). Mobile Forensics: A Review. In: 2020 International Conference on Computing and Information Technology (pp. 1-6). Tabuk, Saudi Arabia. https://doi.org/10.1109/ICCIT-144147971.2020.9213739

Arshad, H., Omlara, E., Oludare Abiodun, I., & Aminu, A. (2020). A semi-automated forensic investigation model for online social networks. Computers & Security, 97. https://doi.org/10.1016/j.cose.2020.101946

Black, K. (2023). What is an Automated Information System? Easytechjunkie. Retrieved from https://www.easytechjunkie.com/what-is-an-automated-information-system.htm

Bulgakova, E., Bulgakov, V., Trushchenkov, I., Vasilev, D., & Kravets, E. (2019). Big Data in Investigating and Preventing Crimes. In: A. Kravets (Ed), Big Data-driven World: Legislation Issues and Control Technologies. Studies in Systems, Decision and Control (vol. 181). Cham: Springer. https://doi.org/10.1007/978-3-030-01358-5_6

Carnaz, G., Beires Nogueira, V., Antunes, M., & Ferreira, N. (2020). An Automated System for Criminal Police Reports Analysis. (vol. 942, pp. 360–369). Cham: Springer. https://doi.org/10.1007/978-3-030-17065-3_36

Council Act of 26 July 1995 No 95/C 316/01. Drawing up the Convention based on Article K.3 of the Treaty on European Union, on the establishment of a European Police Office (Europol Convention). Official Journal of the European Communities, C 316/1. Retrieved from https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:1995:316:0001:0032:EN:PDF

Dawson, M. E., Crespo, M., & Brewster, S. (2013). DoD cyber technology policies to secure automated information systems. International Journal of Business Continuity and Risk Management, 4(1), 1–22. https://doi.org/10.1504/ijbcrm.2013.053089

Fisun, V. (2020). Problems of personal data protection: experience of Ukraine and other countries. Yurydychna hazeta Online, 10(716). Retrieved from https://yur-gazeta.com/publications/practice/informaciyne-pravo-telekomunikaciyi/problemi-zahistu-personalnih-danih-dosvid-ukrayini-ta-inshih-krayin.html

Haraksim, R., Galbally, J., & Beslay, L. (2019). Study on Fingermark and Palmmark Identification Technologies for their Implementation in the Schengen Information

System. Luxembourg: Publication office of the European Union. Doi: 10.2760/852462

Interpol. (2022). Our 19 databases. Retrieved from https://www.interpol.int/How-we-work/Databases/Our-19-databases

Jadhav, E. B., Sankhla, M. S., & Kumar, R. (2020). Artificial Intelligence: Advancing Automation in Forensic Science & Criminal Investigation. Journal of Seybold Report, 15(8). Retrieved from https://www.researchgate.net/publication/343826071

Kalinin, M. O. (2010). Permanent protection of information systems with method of automated security and integrity control. In: Proceedings of the 3rd international conference on Security of information and networks (pp. 118-123). Association for Computing Machinery, New York. https://doi.org/10.1145/1854099.1854125

Kirilchuka, S., Reutova, V., Nalivaychenkoa, E., Shevchenkoa, E., & Yaroshenko, A. (2022). Ensuring the security of an automated information system in a regional innovation cluster. Transportation Research Procedia, 63, 607–617. Retrieved from https://acortar.link/RW4oVv

Kovacevic, A. (2020). The 5 Most Important Criminal DNA And Crime Data Sources. Smart data collective. Retrieved from https://www.smartdatacollective.com/5-important-criminal-dna-and-crime-data-sources/

Pramanik, M. I., Lau, R. Y. K., Yue, W. T., Ye, Yu., & Li, C. (2017). Big data analytics for security and criminal investigations. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 7, e1208. https://doi.org/10.1002/widm.1208

Rigano, C. (2019). Using artificial intelligence to address criminal justice needs. National Institute of Justice, 280. Retrieved from https://www.cep-probation.org/wp-content/uploads/2020/11/252038.pdf

Ritchie, K. L., Cartledge, C., Growns, B., Yan, A., Wang, Y., Guo, K., Kramer, R. S. S. … White, D. (2021). Public attitudes towards the use of automatic facial recognition technology in criminal justice systems around the world. PLoS ONE, 16(10), e0258241. https://doi.org/10.1371/journal.pone.0258241

Sirant, M. (2016). Police cooperation Ukraine and the European Union – legal aspects. Bulletin of Lviv Polytechnic National University. Series: Legal Sciences, 850, 353-360. Retrieved from http://nbuv.gov.ua/UJRN/vnulpurn_2016_850_54

Smith, M., & Miller, S. (2022). The ethical application of biometric facial recognition technology. AI & SOCIETY, 37, 167–175. https://doi.org/10.1007/s00146-021-01199-9

Smith, M., Mann, M., & Urbas, G. (2018). Biometrics, Crime and Security. London: Routledge, https://doi.org/10.4324/9781315182056

Solovyeva, N. A., & Frantsiforov, Y. V. (2020). Specifics of Electronic and Digital Law Enforcement in Crime Investigation. (vol. 110, pp. 449–458). Cham: Springer. https://doi.org/10.1007/978-3-030-45913-0_53

Thompson, T. (2010). Crime software may help police predict violent offences. The Guardian. Retrieved from http://www.theguardian.com/uk/2010/jul/25/police-software-crime-prediction

Thornton, J. (2016). Cost, Accuracy, and Subjective Fairness in Legal Information Technology: A Response to Technological Due Process Critics. 91 N.Y.U. L. Rev. 1821 Retrieved from https://heinonline.org/HOL/LandingPage?handle=hein.journals/nylr91&div=52&id=&page=

Uncovered. (2022). 20 Databases Used in Forensic Science Investigations. Retrieved from https://uncovered.com/20-databases-used-in-forensic-science-investigations/

Uzlov, D., & Strukov, V. (2017). Web-based protected geoinformation system of criminal analysis (RICAS) for analytical support for crimes investigation. In: 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T) (pp. 508-511). Kharkiv, Ukraine. https://doi.org/10.1109/INFOCOMMST.2017.8246450

Willis, J. J., Koper, C. S., & Lum, C. (2020). Technology use and constituting structures: accounting for the consequences of information technology on police organisational change. Policing and Society, 30(5), 483-501. https://doi.org/10.1080/10439463.2018.1557660