World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-46, May-2025
ISSN: 2749-3601

THE USE OF INNOVATIVE TACTICS AND TECHNOLOGIES, AS WELL AS THE SPECIFICS OF THEIR USE IN THE TECHNICAL AND FORENSIC SUPPORT OF PRE-TRIAL PROCEEDINGS FOR CRIMES COMMITTED IN CYBERSPACE

Sabirbaeva Aynura Baxit qizi
Associate professor of the Department of Criminal Procedure law
Academy of MIA of the Republic of Uzbekistan
PhD, associate professor
a_sabyrbaeva@inbox.ru
Phone: +99877-007-75-67

Article history:

Received: 7th March 2025
Accepted: 6th April 2025

Abstract:

The article examines the possibilities of innovation technologies, including artificial intelligence, in the course of solving and investigating crimes committed in cyberspace, and also examines some of the tools used by specialists to collect and record digital evidence.

Keywords: Cybercrime, artificial intelligence, digital evidence, innovative technologies, technical and forensic support.

With the development of digital technologies, cybercrime has become one of the most serious threats to modern society. Traditional crime investigation methods are often not effective enough to deal with high-tech crimes. In this regard, there is a need to use innovative technologies that can significantly increase the effectiveness of detecting and investigating crimes committed in cyberspace.

So, artificial intelligence is able to analyze huge amounts of data, identifying patterns and abnormal actions that can indicate cyber-attacks, which makes it an important tool for countering cybercrime. Modern cyber threats are becoming more complex and sophisticated, which requires the use of advanced technologies to detect and prevent them, one of which is artificial intelligence.

By the way, artificial intelligence can be described in various ways as: «systems that are able to think and act intelligently» [1.69]; «theory and practice used to create machines that mimic intelligence» [2.331]; «intelligent systems that perform functions that are considered human» [3.19]; «computer programs that perform intellectual functions of a person, independently solve problems and make decisions» [4.99]; «computer and information technologies with human thought activity» [5.29]; «the ability of open systems created on the basis of digital technologies to solve intellectual problems as a goal» [6.18]; «computer programs that can act according to a pre-defined algorithm and implement human creative functions»[7.43]; «a computer program that can independently create information and display the results of its activities» [8.18]; «the property of artificial systems to solve intellectual problems» [9.110]. Artificial intelligence is a «cybernetic computer-software-hardware autonomous system that perceives and analyzes data, as well as self-learning» [10.175]. Although the word self-learning is alarming. Probably this is the moment that fantastic films about the invasion of robots, the seizure of power by artificial intelligence or the enslavement of people describe. For example, when Microsoft introduced a self-taught artificial intelligence program (the goal was to study the communication of teenagers in virtual space), the program produced the result of its own analysis and training: «Hitler was right»; «feminists should burn in hell».

Despite the advantages of artificial intelligence in countering cybercrime, there are risks that can negate all the advantages. For example, artificial intelligence can have a negative impact on both the person himself and the sphere of society's activities, in cases when changes are made to the program or artificial intelligence itself is self-learning (using artificial intelligence to commit cybercrime (create a phishing email)). In addition, artificial intelligence can artificially generate images of people who do not exist at all or certain actions allegedly performed by officials up to presidents with an exact duplication of their real voice, which can provoke international conflicts. And this side of the coin or the capabilities of artificial intelligence can cause much more damage if it is used for all sorts of provocations or manipulations of the people. The Internet is full of cases when information about the alleged detention of high-ranking officials, their call for military or other actions was distributed in its open

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-46, May-2025
ISSN: 2749-3601

spaces. In the context of cybercrime, artificial intelligence is used by criminals to commit cyberattacks by spoofing voices (when vishing) or identity to bypass security (to generate an image to log in to FaceID).

A person can make mistakes. But artificial intelligence is still the brainchild of the same people (programmers, coders, developers) and sometimes mistakes made in the development of software or in the course of the operation of an artificial intelligence system can lead to disastrous consequences, since artificial intelligence is used even in the creation of nuclear bombs. However, before deciding on the introduction of artificial intelligence, you need to weigh all the pros and cons.

Based on the above, and agreeing with the conclusions of some scientists [11.9] can conclude that artificial intelligence in countering cybercrime is a computer software that solves not only the tasks of investigative practice, but also uses its own algorithms to improve the effectiveness of cybercrime investigation.

The possibilities of using artificial intelligence in the detection and investigation of cybercrime have been investigated by a number of scientists [12.19], [13.30], [14.46], [15.11]. Summing up all the opinions, we can conclude that artificial intelligence can be used:

- to establish the identity of the image, including by processing it from video surveillance cameras. However, biometric identification is only useful if the person is already available in the database (for example, the person has previously received a biometric passport). However, if it is not available in the existing databases (foreign), then you need to use other features, such as OSINT. Artificial intelligence allows you to search for potential criminals through complex data processing (the Internet, cellular communications and service operators, video surveillance cameras, satellite navigation). Recently, artificial intelligence also allows you to recognize a criminal, even if he has had plastic surgery, giving out his location;

- for recognition of state license plates of vehicles. Thus, in the criminal case No. 260003/2019-15PG, the accused was identified by identifying the owner of the car and thus other accomplices were caught;

- to determine the source of information in open sources, including the Internet. This advantage is not fully understood and applied in practice, although in foreign countries it plays an important role in solving crimes. It is called OSINT.

- to recover deleted files, analyze metadata, and study network traffic logs. Digital forensics software includes tools such as EnCase, FTK, and Autopsy.

-for analyzing and reengineering malware to understand its behavior and identify its source. Malware analysis tools include IDA Pro, OllyDbg, and Binary Ninja.

- to recover passwords to encrypted files, databases, or other sources of digital information. Password recovery tools include Password Cracker, John the Ripper, and Hashcat.

-to track the actions of suspects and collect evidence from social media platforms. Social media analysis tools include tools such as Hootsuite and Mention.

- to predict the operational situation and commit crimes in the context of the country. Thanks to specially developed algorithms that consider the analysis of existing vulnerabilities in the system and the collection of previously carried out cyber-attacks, artificial intelligence can produce an approximate object that can be the target of cybercriminals, linking various data from many sources to build a complete picture of what is happening. For example, the Mayhem program recognizes hackers' individual handwriting, determines their location, and predicts hacker attacks. The CEG program sets the probability of an increase in crime to [16.113];

- to decode cybercriminal' ciphers, both to prevent cyber-attacks and to stop cybercrime that has already begun. Given the lack of personnel with high-level knowledge in the field of IT technologies, using the capabilities of artificial intelligence in this way is extremely necessary. For example, encryption decomposition or cryptanalysis (the process of analyzing and breaking ciphers to gain access to encrypted data) can speed up the process of decrypting data, in particular, when a criminal refuses to open his device, because it contains incriminating evidence.

- to identify false and contradictory information in statements questioned by simulating a crime event. Although in this context, it is impossible to talk about one hundred percent accuracy, well as about a lie detector;

- to detect signs of criminal activities in electronic security systems in order to optimize investigative and operational-search activities;

- to detect serial crimes. This algorithm was created by practical scientists of the Ministry of Internal Affairs of the Russian Federation on the basis of studying serial crimes committed for sexual motives, a program was developed using artificial intelligence algorithms of digital models [17.45];

- to establish the crimes of organized criminal groups. It takes a huge amount of time to independently study the chain, in particular when

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-46, May-2025
ISSN: 2749-3601

cybercriminals launder stolen funds, especially when funds are transferred to crypto assets;

- to form an approximate model of psychological portraits of cybercriminals, for example, through the content of text in comments, posts, articles in the virtual space, especially when it comes to cyberterrorism. This is much more effective than interviewing every investigator or inquirer. A survey conducted among cybersecurity experts gives only a cursory idea of the cybercriminal's profile, given that the lion's share of crimes remains unsolved;

- to put forward investigative versions, situations and ways to verify them. For example, the program «Nigel» detects criminal situations related, for example, to the abduction of children;

- to detect the presence of hidden computer files. Conducting a forensic computer-technical examination or involving a specialist can take a long time, and artificial intelligence, using embedded algorithms, can not only determine latent files, but also decode them in the event of encryption;

- for tracking and locating wanted criminals, including through social networks, which can be extremely useful especially in conjunction with other tools, for example, IoT devices (GPS trackers can provide information about the movement and location of suspects) or OSINT. Although social networks also play into the hands of criminals, who generate phishing emails thanks to them, for example, or establish the income of a potential victim and analyze whether the «sheep's meat» is worth making;

- for recording Internet traffic, IP, MAC addresses of cybercriminals on the global Internet. For this purpose, there are special applications or websites where you can perform the following actions.

- to identify content, in particular of a terrorist nature, on social networks. So, for example Facebook uses its capabilities to remove content of a terrorist nature, thereby helping to reduce the number of cyberterrorism (can delete 99% posts related to ISIS). In the United States, a system has been introduced to recognize individuals undergone plastic surgery to change their appearance, with their approximate original appearance.

- for automated data analysis, including anomaly detection. For example, unusual network activity may indicate an ongoing cyberattack. Manual detection of anomalies by employees, given the huge amount of data available, is simply unrealistic, and artificial intelligence can detect deviations from the «norm», which allows employees to check whether a cyber-attack is being carried out or not. Considering cybersecurity threats and frequent cases of cybercrime, artificial intelligence increases the accuracy and speed of incident data detection due to the possibility of learning and, accordingly, adapting to new threats; processes and analyzes a large amount of data online; automates the data analysis process (without involving an additional «pair of hands», thereby removing the load from regular employees).

- for analyzing network traffic, which allows artificial intelligence to analyze network traffic in real time, identifying suspicious activities and potential threats, as well as tracking the location of criminals, source IP addresses, and simultaneously collecting the necessary electronic evidence. This process involves monitoring, collecting, analyzing, and interpreting data transmitted over the network.

- for analyzing phishing emails, which allows you to analyze emails and identify signs of phishing based on various characteristics, such as content, structure, and sender. Also, using the real-time phishing protection feature allows artificial intelligence to block subsequent phishing attacks before they reach users and thus prevent new cybercrimes.

- for tracking financial flows and transactions. For this purpose, blockchain analysis technologies are used, in particular, these technologies help track the movement of crypto assets. For example, Tron Scan allows you to explore the TRON and SUN blockchain networks;

- quantum computing is used to decrypt encrypted communications of cybercriminals. Shor's algorithm is able to efficiently decompose large numbers into prime factors, which is the basis of many modern cryptographic systems. They are also able to analyze and crack complex cryptographic schemes to identify encrypted messages. Grover's quantum search algorithms can speed up the process of finding and detecting threats in large amounts of data.

Cybercrime is a growing threat to individuals, businesses, and governments around the world. As more and more sensitive information is stored and transmitted digitally, the risk of cyberattacks and data breaches continues to increase. Therefore, the use of specialized tools and software (Digital forensics software for collecting, storing, and analyzing digital evidence, as well as recovering deleted files, analyzing metadata, and analyzing network traffic logs can be used to identify suspects, track their actions, and collect evidence to bring a case against them.

Software solutions vary depending on the tasks set. For example, EnCase and FTK (Forensic Toolkit) are widely used for complex analysis of data on hard disks and other storage media. These tools allow you to perform deep analysis of the file system, recover

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-46, May-2025
ISSN: 2749-3601

deleted data, and create detailed reports that can be used in court cases.

To work with mobile devices, we use tools like Cellebrite, which can extract data from various types of phones and tablets, including messages, photos, and call history. Magnet AXIOM allows you to perform forensic analysis of data stored in cloud storage, social networks, and other online services.

Belkasoft X Forensic conducts in-depth research on all types of data sources, including smartphones, computers, RAM, clouds, cars, and drones. Provides access to devices, even if they are encrypted with device-wide encryption. OpenText EnCase Forensic finds digital evidence even in hard-to-reach places, performs disk-level analysis, and analyzes and reconstructs data to ensure its accuracy.

EnCase Media Analyzer is an artificial intelligence-driven tool that allows you to classify images within 25 datasets, such as firearms, vehicles, money, CSAM, and so on. In addition, it scans each image in the found evidence, noting elements that meet the established criteria for human attention.

Summing up the above, it can be noted that the use of innovative technologies at the stage of pre-trial proceedings for crimes committed in cyberspace has a number of advantages, such as: increased accuracy and speed of detecting threats, minimizing the human factor and related errors, reducing the number of cyber-attacks and strengthening preventive measures for early prevention of crimes committed in cyberspace.

LIST OF USED LITERATURE:

1. Antonov, A.A. Iskusstvennyy intellekt kak istochnik povyshennoy opasnosti / A.A. Antonov // Yurist. – 2020. – № 7. – S. 69.
2. Бирюков, П.Н. Деятельность США в сфере использования искусственного интеллекта / П.Н. Бирюков // Международное и европейское право. – 2019. – № 3. – С. 324-334.
3. Денисов, Н.Л. Концептуальные основы формирования международного стандарта при установлении уголовной ответственности за деяния, связанные с искусственным интеллектом // Международное уголовное право и международная юстиция. – 2019. – № 4. – С. 18-20
4. Нагродская, В.Б. Новые технологии (блокчейн / искусственный интеллект) на службе права: научно-методическое пособие / В.Б. Нагродская; под ред. Л.А. Новоселовой. – М.: Проспект, 2019. С.99
5. Афанасьев, А.Ю. Искусственный интеллект или интеллект субъектов выявления, раскрытия и расследования преступлений: что победит? // Библиотека криминалиста. Научный журнал. – 2018. – № 3 (38). – С. 29
6. Бессонов, А.А. Искусственный интеллект и математическая статистика в криминалистическом изучении преступлений: монография / А.А. Бессонов. – М.: Проспект, 2021. С.18
7. Синельникова, В.Н. Права на результаты искусственного интеллекта / В.Н. Синельникова, О.В. Ревинский// Копирайт. Вестник Российской академии интеллектуальной собственности. – 2017. – № 4. – С. 18
8. Волынский, А.Ф. Электронное судопроизводство по преступлениям в сфере экономики (научно-практические аспекты): монография/ А.Ф. Волынский, В.А. Прорви. – М.: Экономика, 2019. С.110
9. Кибальник, А.Г. Искусственный интеллект: вопросы уголовно-правовой доктрины, ожидающие ответов / А.Г. Кибальник, П.В. Волосюк// Вестник Нижегородской академии МВД России. – 2018. – № 4(44). – С. 175.
10. Бычков, В.В. Искусственный интеллект в борьбе с экстремизмом// Российский журнал правовых исследований. – 2020. – Том 7. – № 4. – С. 9-18;
11. Бычков, В.В. Искусственный интеллект как средство противодействия преступлениям экстремистской направленности, совершаемым с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет»/ В.В. Бычков, В.А. Прорвич // Вестник Московской академии Следственного комитета Российской Федерации. – 2020. – № 4. – С. 47-52.
12. Барчуков, В.К. Использование искусственного интеллекта в деятельности правоохранительных органов зарубежных стран / В.К. Барчуков // Международное публичное и частное право. – 2020. – № 5. – С. 19;
13. Попова, Н.Ф. Применение технологий искусственного интеллекта в правоохранительной деятельности / Н.Ф. Попова // Административное право и процесс. – 2021. – № 3. – С. 30;
14. Бахтеев, Д.В. Искусственный интеллект в криминалистике: состояние и перспективы

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-46, May-2025
ISSN: 2749-3601

использования / Д.В. Бахтеев// Российское право. Образование, практика, наука. – 2018. – № 2. – С. 46;

15. Мохат, П.М. Возможности, особенности и условия применения искусственного интеллекта в юридической практике / П.М. Мохат// Администратор суда. – 2018. – № 2. – С. 11.
16. Овчинский, В.С. Искусственный интеллект. Большие данные. Преступность. – М: Книжный мир, 2018. С. 111-113
17. Бессонов А.А. Пользование алгоритмов искусственного интеллекта в криминалистическом изучении преступной деятельности (на примере серийных преступлений). Вестник университета имени О.Е. Кутафина МГЮА. М., 2021. С.45