ORIGINAL ARTICLE

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE

ISSN: 2692-5206, Impact Factor: 12,23
**American Academic publishers, volume 05, issue 04,2025**

Journal: https://www.academicpublishers.org/journals/index.php/ijai

# THE ROLE OF ARTIFICIAL INTELLIGENCE IN THE INVESTIGATION OF CYBERCRIMES

***S.Yusupova***
*Master's student of*
*Tashkent State University of Law*

**Abstract:**This article provides a comprehensive analysis of the growing importance of artificial intelligence (AI) technologies in the investigation of modern cybercrimes. In the context of the exponential growth of digital data and the complication of cybercrimes, traditional investigative methods are losing their effectiveness. The article examines in detail the application of AI-based solutions in areas such as data mining, analysis, threat identification, and criminal identification. In addition, legal, ethical, and confidential issues related to the implementation of AI technologies by law enforcement agencies, as well as the future prospects of these technologies, will be discussed. According to the research results, AI can significantly increase the effectiveness of cyber investigations, but appropriate legal and ethical frameworks are necessary to address confidentiality, data security, and ethical issues.

**Keywords:**Artificial intelligence, cybercrime, international cooperation, digital forensics, data recovery.

## Introduction

Cybercrimes are becoming increasingly complex, rapidly changing, and difficult to detect. Traditional investigative methods are no longer sufficient, as the volume of digital evidence grows exponentially, and criminals use more sophisticated methods to conceal their activities. This situation forces law enforcement agencies and security specialists to seek new, effective solutions.

Artificial intelligence (AI) technologies have begun to play an important role in solving these problems. AI algorithms are capable of processing huge amounts of data in a short time, identifying complex patterns, and finding relationships that the human eye cannot perceive. These features are very valuable in the process of investigating cybercrimes.

This article discusses in detail the application of artificial intelligence in the investigation of cybercrimes, its advantages and limitations, as well as legal and ethical issues existing in this area. The article presents the current state of cybercrime investigation, including the practical application of AI technologies in real investigations, existing solutions, and future trends.

## Main areas of application of artificial intelligence in the investigation of cybercrimes

Modern cyber investigations require the processing and analysis of data in the amount of exabytes. These include files of various formats, network data, social media content, emails, and many other digital data. Artificial intelligence algorithms allow automating and accelerating this process.

Machine learning methods, especially deep learning algorithms, are very effective in processing large volumes of unstructured data. For example, AI platforms like IBM Watson

ORIGINAL ARTICLE

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE

ISSN: 2692-5206, Impact Factor: 12,23
**American Academic publishers, volume 05, issue 04,2025**

Journal: https://www.academicpublishers.org/journals/index.php/ijai

allow investigators to expedite access to data in various formats, respond to inquiries, and highlight information relevant to the investigation[1].

Thematic modeling algorithms can identify thematic relationships among a large number of documents, which helps investigators identify criminal schemes or suspicious actions. For example, the Latent Dirichlet Allocation (LDA) algorithm is used to identify topics that may be related to criminal activity from emails or social media posts[2].

Technologies of intelligent text processing (NLP) are of particular importance in cyber investigations. They help extract important information related to criminal activity from emails, chat correspondence, forum discussions, and social media posts. Transformer-based models such as BERT and GPT show high results in understanding contextual meanings within the text and highlighting information important for criminal investigation[3].

Image recognition and video analysis technologies also play an important role in cyber investigations. Algorithms based on the Convolutional Neural Network (CNN) architecture are used to identify objects and persons in images, as well as to detect information hidden in data (steganography). These technologies are important for identifying criminals, finding evidence supporting criminal activity, and identifying suspicious activities[4].

Artificial intelligence algorithms are very effective in detecting unusual, suspicious activity or anomalies. This allows for the early detection of cyberattacks, fraud, and other cybercrimes.

Uncontrolled learning algorithms, including methods such as k-means clustering, DBSCAN, and isolation forest, are widely used to identify deviations from normal activity. For example, these algorithms may detect unusual login attempts, suspicious file downloads, or unusual patterns in network traffic[5].

Time series prediction algorithms (ARIMA, Prophet, or LSTM-based neural networks) are used to predict future cyberattacks using historical data. They allow you to identify potential attack vectors based on system vulnerabilities and prevent them[6].

Automation of threat intelligence is also one of the important areas of application of AI technologies. Algorithms such as Graph Neural Network (GNN) are used to identify links between cyber threats and attackers, predict new attack vectors, and build networks of cybercriminals. This information provides investigators with valuable information about criminal groups or government-supported hackers[7].

AI algorithms are also widely used for monitoring dark web and cryptocurrency transactions. They help identify suspicious activities in hidden markets, track cryptocurrency payments, and identify dark web resources that may be associated with criminal activity. For

[1] IBM. (2023). “IBM Watson for Cybersecurity.” https://www.ibm.com/security/artificial-intelligence
[2] Blei, D. M., Ng, A. Y., & Jordan, M. I. (2003). “Latent dirichlet allocation.” Journal of Machine Learning Research, 3, 993-1022. https://dblp.org/rec/journals/jmlr/BleiNJ03.html
[3] Devlin, J., Chang, M. W., Lee, K., & Toutanova, K. (2019). “BERT: Pre-training of deep bidirectional transformers for language understanding.” https://arxiv.org/abs/1810.04805
[4] Koonce, B. (2021). “Convolutional Neural Networks with Swift for Tensorflow: Image Recognition and Dataset Creation for iOS Applications.” Apress® https://link.springer.com/book/10.1007/978-1-4842-6168-2
[5] Liu, F. T., Ting, K. M., & Zhou, Z. H. (2008). “Isolation forest.” https://dl.acm.org/doi/10.1109/icdm.2008.17
[6] Hochreiter, S., & Schmidhuber, J. (1997). “Long short-term memory.” https://direct.mit.edu/neco/article-abstract/9/8/1735/6109/Long-Short-Term-Memory?redirectedFrom=fulltext
[7] Kipf, T. N., & Welling, M. (2016). “Semi-supervised classification with graph convolutional networks.” https://arxiv.org/abs/1609.02907

ORIGINAL ARTICLE

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE

ISSN: 2692-5206, Impact Factor: 12,23
**American Academic publishers, volume 05, issue 04,2025**

Journal: https://www.academicpublishers.org/journals/index.php/ijai

example, Chainalysis's special AI algorithms are used to analyze cryptocurrency transactions and identify transactions related to criminal activity[8].

Artificial intelligence plays an important role in the field of digital forensics by automating the processes of searching, restoring, and analyzing evidence.

The restoration of deleted data is carried out more efficiently using AI algorithms. Deep learning methods increase the likelihood of restoring data that has been deleted or damaged from hard drives, USB devices, or other storage devices. This is especially important in cases where criminals attempt to destroy evidence[9].

AI algorithms are also used for the validation and authentication of digital evidence. Technologies such as the Generative Adversarial Network (GAN) help to identify falsified or altered digital evidence. This allows investigators to gather reliable evidence that can be used in court[10].

Chronological data analysis and timestamps are performed more accurately and quickly using AI. Algorithms such as Recurrent Neural Network (RNN) and Long Short-Term Memory (LSTM) are used to detect anomalies in time series and determine whether time marks in data have been manipulated[11].

Steganography and the detection of encrypted data are also carried out more effectively using AI algorithms. Deep learning methods allow us to identify information hidden in images, audio files, or other digital data. This is crucial for discovering and decrypting information encrypted or hidden by criminals[12].

**Artificial intelligence-based investigative systems and tools**

Network security and threat identification systems based on artificial intelligence are important for the prevention and detection of cybercrimes.

AI-based cyberattack detection systems, such as Darktrace, are used to monitor network traffic in real time and detect anomalies. These systems, based on Enterprise Immune System technology, study the organization's "normal" network behavior and detect any unusual behavior. This allows for early detection and rapid response to cyberattacks[13].

Security platforms such as FireEye Helix use AI algorithms to identify threats by integrating and analyzing data from various security devices. These platforms allow you to identify, analyze, and respond to cyber threats[14].

Digital forensic tools based on artificial intelligence are used to automate and improve the process of collecting, storing, and analyzing evidence related to cybercrimes.

Digital forensic tools, such as AccessData's FTK (Forensic Toolkit) and Guidance Software's EnCase, allow for the restoration, indexation, and analysis of digital evidence

---

[8] Chainalysis. (2023). “Chainalysis Crypto Crime Report.” https://www.chainalysis.com/
[9] Moustafa, N. (2022). “Digital Forensics in the Era of Artificial Intelligence” https://www.routledge.com/Digital-Forensics-in-the-Era-of-Artificial-Intelligence/Moustafa/p/book/9781032244686
[10] Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., ... & Bengio, Y. (2014). “Generative adversarial nets.” https://arxiv.org/abs/1406.2661
[11] Hochreiter, S., & Schmidhuber, J. (1997). “Long short-term memory.” https://direct.mit.edu/neco/article-abstract/9/8/1735/6109/Long-Short-Term-Memory?redirectedFrom=fulltext
[12] Fridrich, J. (2009). “Steganography in digital media: principles, algorithms, and applications.” Cambridge University Press.
[13] Darktrace. (2020). “Darktrace Immune System Version 5 Redefines Enterprise Security” https://www.darktrace.com/news/darktrace-immune-system-version-5-redefines-enterprise-security-5
[14] FireEye. (2023). “FireEye Helix Security Platform.” https://www.fireeye.com/products/helix.html

ORIGINAL ARTICLE

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE

ISSN: 2692-5206, Impact Factor: 12,23
**American Academic publishers, volume 05, issue 04,2025**

Journal: https://www.academicpublishers.org/journals/index.php/ijai

using AI technologies. These tools allow investigators to automatically process large amounts of information and highlight important information related to the crime[15].

Mobile forensic tools, such as Magnet AXIOM, are used to restore and analyze data on smartphones and tablets using AI algorithms. These tools allow investigators to recover and analyze deleted messages, images, and other data on mobile devices[16].

**Legal and ethical issues**

**Legal status of evidence collected using AI**

The legal status of evidence collected using artificial intelligence is an important issue in the investigation of cybercrimes. This issue is regulated differently in different countries.

In the USA and other Western countries, evidence collected using AI is evaluated using Frey or Doubert's standards, which are used for the acceptance of scientific evidence in court. For the results of AI algorithms to be accepted as evidence in court, they must be reliable and scientifically based. This raises issues of transparency and explanation, since many AI algorithms, especially deep learning models, work like a "black box," and their decision-making process is difficult to explain[17].

In the European Union, laws such as the GDPR (General Data Protection Regulation) impose additional requirements for data collection and analysis using AI. The possibility of explaining the solutions of AI algorithms and issues of personal data protection are of great importance[18].

In the Republic of Uzbekistan, a number of laws have been adopted in the field of information technology and cybercrime. The Law "On Informatization," the Law "On Electronic Document Management," and the Law "On Electronic Digital Signature" define the legal status of digital evidence. The new law "On Cybersecurity," adopted in September 2021, regulates the processes of investigating cybercrimes and collecting digital evidence[19].

In the investigation of cybercrimes using artificial intelligence, issues of personal data protection and confidentiality are of great importance.

In the process of data collection and analysis, citizens' privacy rights may be violated. AI algorithms can disclose personal data by analyzing large amounts of data, which can lead to violations of privacy rights. To resolve this issue, investigators must have appropriate legal grounds and comply with confidentiality rules in the process of data collection and analysis[20].

In the European Union, laws such as the GDPR impose additional requirements for data collection and analysis using AI. These laws regulate the collection, storage, and processing of personal data and protect citizens' privacy rights.

In the Republic of Uzbekistan, the Law "On Personal Data" regulates the protection of personal data and confidentiality. This law regulates the processes of collection, storage, and processing of personal data and protects the privacy rights of citizens.[21].

**Prospects and future trends**

---

[15] AccessData. (2023). “Forensic Toolkit (FTK).” https://www.exterro.com/forensic-toolkit
[16] Magnet Forensics. (2023). “AXIOM.” https://www.magnetforensics.com/products/magnet-axiom/
[17] Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993).
[18] European Union. (2016). “General Data Protection Regulation (GDPR).” https://gdpr-info.eu/
[19] Republic of Uzbekistan. (2022). Law "On Cybersecurity." https://lex.uz/docs/6997403
[20] Solove, D. J. (2011). “Nothing to hide: The false tradeoff between privacy and security.” Yale University Press. https://teachprivacy.com/nothing-to-hide-the-false-tradeoff-between-privacy-and-security/
[21] Republic of Uzbekistan. (2019). Law "On Personal Data." https://lex.uz/docs/4831939

ORIGINAL ARTICLE

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE

ISSN: 2692-5206, Impact Factor: 12,23
**American Academic publishers, volume 05, issue 04,2025**

Journal: https://www.academicpublishers.org/journals/index.php/ijai

**Future development of AI technologies**

Neuromorphic computing also opens up new possibilities in the field of cybercrime investigation. Neuromorphic chips can work more efficiently than traditional chips by simulating the operating principles of the human brain. This technology can increase the energy efficiency of AI algorithms and provide investigators with even more powerful analytical tools[22].

The technology of federated learning is also expected to be widely used in the future. This technology allows training AI models based on data from various devices without sending data to the central server. This, in addition to solving issues of confidentiality and data security, allows for the exchange of information between various law enforcement agencies[23].

Conversational AI systems are also expected to play an important role in cyber investigations. These systems allow investigators to search for, analyze, and prepare reports by communicating in natural language. Chatbots and virtual assistants created on such platforms as IBM Watson Assistant, Google Dialogflow, and Microsoft Bot Framework can help investigators.[24].

**International cooperation and standardization**

Since cybercrimes are a global problem, international cooperation and standardization are crucial in their investigation.

Strengthening international cooperation is crucial for the effective use of AI technologies in the investigation of cybercrimes. Platforms such as Interpol's I-24/7 global police communication system and the Cybersecurity Initiative facilitate data exchange and cooperation between law enforcement agencies in different countries. These platforms can become more efficient by integrating AI algorithms[25].

Standardization of AI technologies is also an important task. International standardization organizations, such as ISO and IEC, are developing international standards for AI technologies. These standards help ensure the quality, security, and transparency of AI algorithms. In particular, the ISO/IEC JTC 1/SC 42 Artificial Intelligence standards are important in establishing international standards for AI technologies[26].

Harmonization of the legal framework for cybercrimes is also an important task. Differences in the legal framework in different countries can create problems in the investigation of cybercrimes. International treaties such as the Budapest Convention (Cybercrime Convention) are important for harmonizing legislation on cybercrime and strengthening international cooperation[27].

---

[22] Davies, M., Srinivasa, N., Lin, T. H., Chinya, G., Cao, Y., Choday, S. H., ... & Wang, H. (2018). "Loihi: A neuromorphic manycore processor with on-chip learning." https://www.wired.com/story/intels-new-chip-design-takes-pointers-from-your-brain/

[23] https://proceedings.mlr.press/v54/mcmahan17a.html

[24] Følstad, A., & Brandtzæg, P. B. (2020). "Users' experiences with chatbots: findings from a questionnaire study."

[25] INTERPOL. (2023). "Global Cybercrime Strategy." https://www.interpol.int/Crimes/Cybercrime

[26] ISO/IEC JTC 1/SC 42. (2023). "Artificial Intelligence." https://www.iso.org/committee/6794475.html

[27] Council of Europe. (2001). "Convention on Cybercrime." https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

ISSN: 2692-5206, Impact Factor: 12,23
**American Academic publishers, volume 05, issue 04,2025**
Journal: https://www.academicpublishers.org/journals/index.php/ijai

**Conclusion**

Artificial intelligence technologies are revolutionizing the investigation of cybercrimes. AI algorithms are of great help to investigators in areas such as processing large amounts of data, detecting anomalies, restoring digital evidence, and identifying criminals.

As discussed in the main part, AI technologies are used in the investigation of cybercrimes in four main areas: data processing and analysis, detection of anomalies and threat forecasting, digital forensics and evidence recovery, and identification and profiling of criminals. In these fields, many AI-based systems and tools are used, such as IBM Watson, Palantir Gotham, Darktrace Enterprise Immune System, FTK, and AXIOM.

At the same time, the use of AI technologies in the investigation of cybercrimes raises a number of legal and ethical issues. The legal status of evidence collected using AI, issues of personal data protection and confidentiality, as well as transparency and explanation of AI algorithms are the main problems that need to be addressed. To address these issues, technologies such as Explainable AI (XAI) are being developed and the legal framework is being improved.

In the future, further development of AI technologies, especially such as quantum computing, Edge AI, neuromorphic computing, and federated learning, is expected to open up new opportunities in the field of cybercrime investigation. At the same time, both cybercrime is evolving, and criminals are using AI technologies in their activities, which encourages law enforcement agencies to develop more effective AI-based solutions.

International cooperation and standardization are also important for the effective use of AI technologies in the investigation of cybercrimes. Platforms such as Interpol systems and the Cybersecurity Initiative, international standards for AI technologies, and international agreements such as the Budapest Convention are expected to play an even more important role in the future.

In conclusion, artificial intelligence technologies have great potential in the field of investigating cybercrimes, but appropriate legal frameworks, ethical principles, and international cooperation are necessary for their effective application. It is expected that the technological revolutions in this area will continue, and AI-driven systems will play an increasingly important role in detecting, preventing, and investigating cybercrimes.

**Literature:**

1. IBM. (2023). “IBM Watson for Cybersecurity.” https://www.ibm.com/security/artificial-intelligence
2. Blei, D. M., Ng, A. Y., & Jordan, M. I. (2003). “Latent dirichlet allocation.” Journal of Machine Learning Research, 3, 993-1022.
3. Devlin, J., Chang, M. W., Lee, K., & Toutanova, K. (2019). “BERT: Pre-training of deep bidirectional transformers for language understanding.” arXiv preprint arXiv:1810.04805.
4. Koonce, B. (2021). “Convolutional Neural Networks with Swift for Tensorflow: Image Recognition and Dataset Creation for iOS Applications.” Apress.
5. Liu, F. T., Ting, K. M., & Zhou, Z. H. (2008). “Isolation forest.” In 2008 Eighth IEEE International Conference on Data Mining (pp. 413-422). IEEE.
6. [6-11] Hochreiter, S., & Schmidhuber, J. (1997). “Long short-term memory.” Neural computation, 9(8), 1735-1780.
7. Kipf, T. N., & Welling, M. (2016). “Semi-supervised classification with graph convolutional networks.” arXiv preprint arXiv:1609.02907.

ISSN: 2692-5206, Impact Factor: 12,23
**American Academic publishers, volume 05, issue 04,2025**
Journal: https://www.academicpublishers.org/journals/index.php/ijai

8. Chainalysis. (2023). "Chainalysis Crypto Crime Report." https://www.chainalysis.com/
9. Moustafa, N. (2022). "Digital Forensics in the Era of Artificial Intelligence" https://www.routledge.com/Digital-Forensics-in-the-Era-of-Artificial-Intelligence/Moustafa/p/book/9781032244686
10. Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., ... & Bengio, Y. (2014). "Generative adversarial nets." Advances in neural information processing systems, 27.
11. Fridrich, J. (2009). "Steganography in digital media: principles, algorithms, and applications." Cambridge University Press.
12. Darktrace. (2020). " Darktrace Immune System Version 5 Redefines Enterprise Security" https://www.darktrace.com/news/darktrace-immune-system-version-5-redefines-enterprise-security-5
13. FireEye. (2023). "FireEye Helix Security Platform." https://www.fireeye.com/products/helix.html
14. AccessData. (2023). "Forensic Toolkit (FTK)." https://www.exterro.com/forensic-toolkit
15. Magnet Forensics. (2023). "AXIOM." https://www.magnetforensics.com/products/magnet-axiom/
16. Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993).
17. European Union. (2016). "General Data Protection Regulation (GDPR)." https://gdpr-info.eu/
18. O'zbekiston Respublikasi. (2021). "Kiberxavfsizlik to'g'risida"gi qonun. https://lex.uz/docs/5607825
19. Solove, D. J. (2011). "Nothing to hide: The false tradeoff between privacy and security." Yale University Press.
20. O'zbekiston Respublikasi. (2019). "Shaxsga doir ma'lumotlar to'g'risida"gi qonun.
21. Davies, M., Srinivasa, N., Lin, T. H., Chinya, G., Cao, Y., Choday, S. H., ... & Wang, H. (2018). "Loihi: A neuromorphic manycore processor with on-chip learning." https://www.wired.com/story/intels-new-chip-design-takes-pointers-from-your-brain/
22. https://proceedings.mlr.press/v54/mcmahan17a.html
23. Følstad, A., & Brandtzæg, P. B. (2020). "Users' experiences with chatbots: findings from a questionnaire study."
24. INTERPOL. (2023). "Global Cybercrime Strategy." https://www.interpol.int/Crimes/Cybercrime
25. ISO/IEC JTC 1/SC 42. (2023). "Artificial Intelligence." https://www.iso.org/committee/6794475.html
26. Council of Europe. (2001). "Convention on Cybercrime." https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185