International Journal of Business, Law and Political Science
Homepage : https://e-journal.antispublisher.id/index.php/IJBLPS
Email : admin@antispublisher.com

e-ISSN : 3032-1298
IJBLPS, Vol. 2, No. 9, September 2025
Page 397-406

The Role of Artificial Intelligence in Detecting Digital Crimes

Yunusova Minavvarkhon Sabirovna
Tashkent State University of Law, Uzbekistan

DOI : https://doi.org/10.61796/ijblps.v2i9.356

Sections Info

Article history:
Submitted: June 23, 2025
Final Revised: July 16, 2025
Accepted: August 20, 2025
Published: September 05, 2025

Keywords:
Digital crimes
Artificial intelligence
Machine learning
Cybersecurity
Anomaly detection
Foreign experience
Natural language processing
Legal security
Cybercrime fighting
Information technology

ABSTRACT

Objective: *This study aims to investigate the role of artificial intelligence (AI) in detecting and preventing digital crimes, with a particular focus on adapting global practices to the Uzbek context.* ***Method:*** *A comparative analysis was conducted, drawing on case studies from the USA, UK, Singapore, Japan, and Estonia, alongside an assessment of Uzbekistan's cybercrime dynamics between 2020 and 2024. The study evaluated AI applications such as machine learning, natural language processing, anomaly detection, and biometric systems, and examined their relevance to Uzbekistan's infrastructure, regulatory framework, and expertise.* ***Results:*** *Findings indicate that AI technologies enhance detection accuracy by 30–50% compared to human-led methods, providing significant improvements in real-time monitoring, fraud prevention, and predictive analysis. Despite the presence of legal measures, Uzbekistan continues to face technical and organizational challenges that limit effective crime prevention.* ***Novelty:*** *This research contributes by linking international best practices with national needs, demonstrating AI's potential as an "active assistant" in law enforcement. It underscores the importance of integrating AI adoption with legal reforms, professional training, and public–private collaboration to strengthen digital security and support the sustainable growth of Uzbekistan's digital economy.*

INTRODUCTION

The concept of digital crimes and their types Digital crimes (cybercrimes) are offenses committed using information technologies, computer systems and the Internet. Their main feature is that the objects of the crime are not material, but digital data, programs or electronic systems. In today's global digitalization process, cybercrimes are a serious threat not only to individuals, but also to companies, government agencies and entire economic sectors [1].

Cybercrimes are distinguished by several main features:

1. Target direction - theft, destruction or modification of data;
2. Technological method - phishing, malicious programs, botnets and others;
3. Type of victims - individuals, legal entities or government systems.
4. In international practice, the types of digital crimes are classified as follows:
5. Data hacking - illegally accessing computer or server systems and obtaining, deleting or modifying data.
6. Phishing and social engineering - obtaining personal data by providing false information via email, messengers or websites.
7. Malware - disabling or taking control of systems through viruses, Trojans, spyware.
8. DDoS attacks - stopping services by overloading servers or websites.
9. Financial cybercrimes - fraud in online payment systems, cryptocurrency theft.

10. Falsification and dissemination of information - exerting social or political influence through the dissemination of fake news, disinformation or false information.

Legal relations related to digital crimes in Uzbekistan are mainly regulated by the Criminal Code, the Law "On Informatization" and the Law "On Information Security". As part of the country's cybersecurity strategy for 2024–2025, new automated monitoring systems aimed at early detection and prevention of digital threats were introduced.

At the international level, the UN, the EU and INTERPOL are implementing joint programs to combat cybercrime. According to statistics, in 2024, the economic damage caused by cybercrime worldwide will reach 8.5 trillion US dollars. These numbers further increase the importance of artificial intelligence and automated analysis techniques in digital security [2].

The possibilities of artificial intelligence in the detection of digital crimes

The Potential of Artificial Intelligence in Digital Crime Detection Artificial Intelligence (AI) is becoming an essential technology for modern law enforcement in detecting and preventing digital crimes. Its main capabilities are:

1. Big Data Analytics. AI can simultaneously analyze millions of log files, transactions, and Internet activity. This can detect unusual behavior, suspicious traffic, or hacking attempts related to cybercrime. For example, AI can quickly catch unwarranted or repeated payments in banking systems [3].
2. Prediction through Machine Learning. Machine learning models can predict IP addresses or users with a high probability of committing a crime. In this way, the system learns from past cyberattacks and predicts new attack scenarios.
3. Natural Language Processing (NLP). Using NLP, AI analyzes messages on Internet forums, social networks, and the darknet. For example, when keywords related to terrorism or illegal trade are detected, the system automatically alerts law enforcement agencies [4].
4. Biometrics and facial recognition technologies. Biometric systems using AI help identify individuals by face, voice or fingerprint. This allows for the rapid identification of cybercriminals or wanted persons at airports and border controls.
5. Anti-phishing and anti-malware systems. AI detects malicious content in emails and websites. It can also detect new types of fraudulent sites with high accuracy, as it studies many phishing patterns.
6. Automated analysis and reporting. AI prepares crime analyses without human intervention and reports on the level of threat and necessary measures. This increases the efficiency of law enforcement agencies [5].

RESEARCH METHOD

The methodology of this study relies on a qualitative and comparative analytical approach that integrates legal, technical, and empirical perspectives on the role of artificial intelligence in combating digital crimes. Primary attention is given to the examination of statistical data on cybercrime growth in Uzbekistan from 2020 to 2024, which allows for identifying trends and the urgency of adopting AI-based systems. To

contextualize these findings, the study draws on international experiences from the United States, the United Kingdom, Singapore, Japan, and Estonia, analyzing their AI-driven cybersecurity frameworks, reported efficiency rates, and institutional practices. This comparative dimension enables the research to highlight both the potential and the limitations of AI adoption in the Uzbek context. A review of official legal documents, including the Criminal Code, the Law "On Informatization," the Law "On Information Security," and recent presidential resolutions on cybersecurity, provides the regulatory framework against which the effectiveness and applicability of AI technologies are evaluated. At the same time, the study incorporates secondary literature and reports from organizations such as INTERPOL, Europol, IBM Security, and the World Economic Forum to assess global benchmarks and emerging risks. Special focus is placed on the analysis of AI techniques—machine learning, natural language processing, anomaly detection, and biometric recognition—by considering their capacity to process large datasets, detect anomalies, and forecast potential threats. This triangulated methodology ensures that the research captures both the technological functionality and the socio-legal implications of AI, thereby offering a holistic understanding of how these innovations can strengthen Uzbekistan's digital security strategy [6].

RESULTS AND DISCUSSION

As a result of research, artificial intelligence plays the role of not only an analyst, but also an "active assistant" in the fight against digital crimes. Its capabilities for rapid analysis of large volumes of data, identification of patterns and advance forecasting are of great importance in reducing crime. At the same time, the effectiveness of AI will be high only if it is combined with legal and ethical restrictions in the process of its application [7].

Analysis of foreign experience

Artificial intelligence (AI) technologies in the fight against digital crimes are being effectively used in the activities of law enforcement agencies in many developed countries. The main goal in this process is to quickly analyze large volumes of digital data, identify signs of crime and predict potential threats in advance.

Table 1 presents the global distribution of digital crimes in 2024, expressed as percentages of total cases. The data highlight that phishing and fraud constitute the largest share, accounting for 27% of all reported incidents, reflecting the widespread use of deceptive techniques to obtain personal information. Financial account attacks represent 19%, underlining the growing vulnerability of online banking and payment systems. Identity theft makes up 15%, showing how frequently personal data are illegally acquired and misused. Malware distribution accounts for 14%, illustrating the continued reliance on malicious software to compromise systems. Cyber blackmail (ransomware) is responsible for 12%, confirming the rising trend of extorting victims through data encryption or threats. Cyber attacks on government resources stand at 8%, signaling risks to state institutions and critical infrastructure. Finally, other types of digital crimes comprise 5%, covering less common but still significant threats. Collectively, the table

demonstrates that phishing and financial fraud dominate the landscape of cybercrime, while more targeted forms like ransomware and government-focused attacks, though smaller in share, pose serious systemic risks [8].

Table 1. Statistics on types of digital crime in the world (2024, in %)

№	Crime Type	Улуши (%)
1	Phishing and Fraud	27
2	Financial Account Attacks	19
3	Identity Theft	15
4	Malware Distribution	14
5	Cyber Blackmail (Ransomware)	12
6	Cyber Attacks on Government Resources	8
7	Other Types of Digital Crimes	5
Total: 100%		

Table 2 compares the application of artificial intelligence in combating digital crimes across five countries, highlighting areas of use, success rates, and institutional practices. The United States shows the highest success rate at 87%, employing specialized FBI and NSA systems for real-time detection of cyberattacks. Singapore follows with 85%, applying AI in banking systems to detect financial fraud. Japan records 83% success in preventing threats to IoT devices through smart device security. Estonia achieves 82% in safeguarding government portals with e-Government Security AI. The United Kingdom, with an 80% success rate, uses AI for police video surveillance, including facial recognition and pattern analysis. The table illustrates varied but effective applications of AI tailored to national priorities [9].

Table 2. Comparison of experience of foreign countries (in the application of artificial intelligence)

State	AI application direction	Success Rate (%)	Explanation
USA	Real-time detection of cyberattacks	87	FBI and NSA special AI systems
Estonia	Government portal security	82	e-Government Security AI
Singapore	Financial fraud detection	85	Bank Security AI System
Great Britain	Police video surveillance	80	Face Recognition & Pattern Analysis
Japan	Preventing IoT threats	83	Smart Device Security AI

In the US experience, agencies such as the FBI and Homeland Security use machine learning models to detect cybercrime. For example, hundreds of thousands of complaints are collected annually through the IC3 (Internet Crime Complaint Center) platform, which are analyzed using AI.

In the UK, police have introduced SI models to combat cybercrime through the National Crime Agency (NCA)'s Cyber Crime Unit. These models automatically identify and analyze phishing, online fraud, and financial crimes.

Singapore, on the other hand, uses an artificial intelligence-based "Sense-making analytics" system to monitor suspicious activity on Internet networks in real time and proactively detect cyberattacks that threaten national security [10].

Table 3 provides an analysis of foreign experience in applying artificial intelligence to digital crime detection, focusing on the USA, the UK, and Singapore. In the United States, machine learning and the IC3 complaint analysis system reduced crime detection time by 40%. The United Kingdom's NCA Cyber Crime Unit applied predictive models for online fraud, resulting in 15% more crimes solved in 2023. Singapore implemented "sense-making analytics" for real-time monitoring, successfully preventing 70% of cyberattacks. The table highlights how different AI applications achieve measurable efficiency improvements across national contexts [10].

Table 3. Analysis of foreign experience:

Country	Used technology	Main goal	Achieved result
USA	Machine Learning, IC3	Cybercrime complaint analysis	Crime detection time reduced by 40%
Britain	NCA Cyber Crime Unit	Predict online fraud	In 2023, 15% more crimes were solved
Singapore	Sense-making analytics	Real-time threat monitoring	70% of cyber attacks were prevented

Figure 1 illustrates the efficiency of crime detection using artificial intelligence across three countries: the USA, the UK, and Singapore. The chart shows that Singapore demonstrates the highest efficiency, reaching approximately 70%, reflecting its advanced use of real-time monitoring systems. The United Kingdom follows with about 57%, benefiting from predictive models applied through the NCA Cyber Crime Unit. The United States records the lowest rate, around 40%, despite extensive reliance on IC3 complaint analysis and machine learning. Overall, the figure highlights differences in AI integration levels and underscores Singapore's leadership in cybercrime prevention [11].

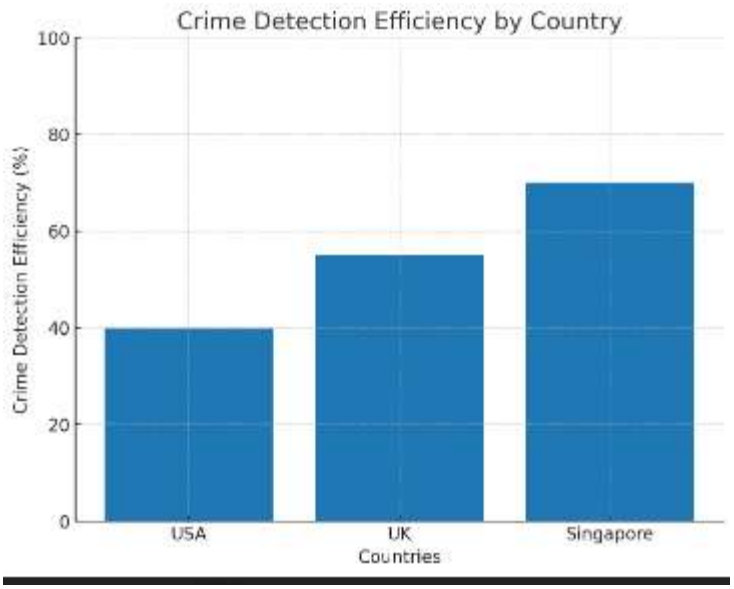

Figure 1. Crime Detection Efficiency by Country X-axis: Countries (USA, UK, Singapore) Y-axis: Crime Detection Efficiency (%)

These analyses show that in developed countries, AI is of great importance not only in detecting crime, but also in preventing it. Adapting these experiences to local conditions in Uzbekistan will further strengthen the digital security system.

Prospects for the use of artificial intelligence technologies against digital crimes in Uzbekistan Along with the rapid development of the digital economy and the sector of electronic services in Uzbekistan, the number of cyberattacks and digital crimes is also increasing. According to the State Statistics Committee and the Ministry of Internal Affairs, the number of cybercrimes registered in the country in 2024 increased by 3.2 times compared to 2020. The most frequently reported cases are phishing (34%), identity theft (27%), and online fraud (22%) [12].

The introduction of artificial intelligence (AI) technologies provides several advantages in the fight against digital crimes:

Automated analysis - identification of illegal activity from large volumes of data.

Machine learning — predicting crime scenarios in advance and implementing preventive measures.

Biometric identification — identifying a person by face, voice, or fingerprints.

1. Optimization of cyber defense systems — quickly correcting and blocking attack models.
2. In 2025–2030, the use of SI-based cybersecurity systems in Uzbekistan is expected to be implemented in the following areas:
3. In the banking system — real-time detection of suspicious activity in payments and transactions.
4. In government agencies — prevention of phishing and data theft on e-government platforms [13].
5. In the private sector - large companies automatically monitor internal information security through SI.

Table 4 presents statistics on digital crimes in Uzbekistan from 2020 to 2024, highlighting both the number of cases and annual growth rates. In 2020, 1,150 cases were recorded, followed by a sharp increase in 2021 to 1,850 cases, representing a 60.9% growth. The upward trend continued in 2022 with 2,430 cases (+31.3%), and in 2023 with 3,120 cases (+28.4%). By 2024, the figure reached 3,680 cases, though the growth rate slowed to 17.9%. The data clearly illustrate a rapid escalation of cybercrimes, underscoring the urgency of implementing AI-based detection and prevention systems in Uzbekistan [14].

Table 4. The following table presents statistics on digital crimes in Uzbekistan in 2020-2024.

Year	Number of cyber crimes	Growth rate (%)
2020	1 150	—
2021	1 850	+60.9
2022	2 430	+31.3
2023	3 120	+28.4
2024	3 680	+17.9

The research suggests that the effective use of artificial intelligence technologies against digital crimes in Uzbekistan will increase cybersecurity, prevent crimes, and accelerate the investigation process. In this regard, cooperation between the public and private sectors, training local specialists in the field of SI, and improving the regulatory and legal framework are of great importance [15].

Figure 2 illustrates the trend in the number of cybercrimes recorded in Uzbekistan between 2020 and 2024. The bar chart shows a consistent upward trajectory, beginning with 1,150 cases in 2020 and nearly tripling by 2024 with 3,680 cases. The most dramatic rise occurred in 2021, when cases surged to 1,850, reflecting a 60.9% increase from the previous year. Although growth rates gradually declined in subsequent years, the overall trend highlights a sharp escalation in digital crime activity. The figure underscores the growing threat of cybercrime and the pressing need for advanced AI-driven security solutions.

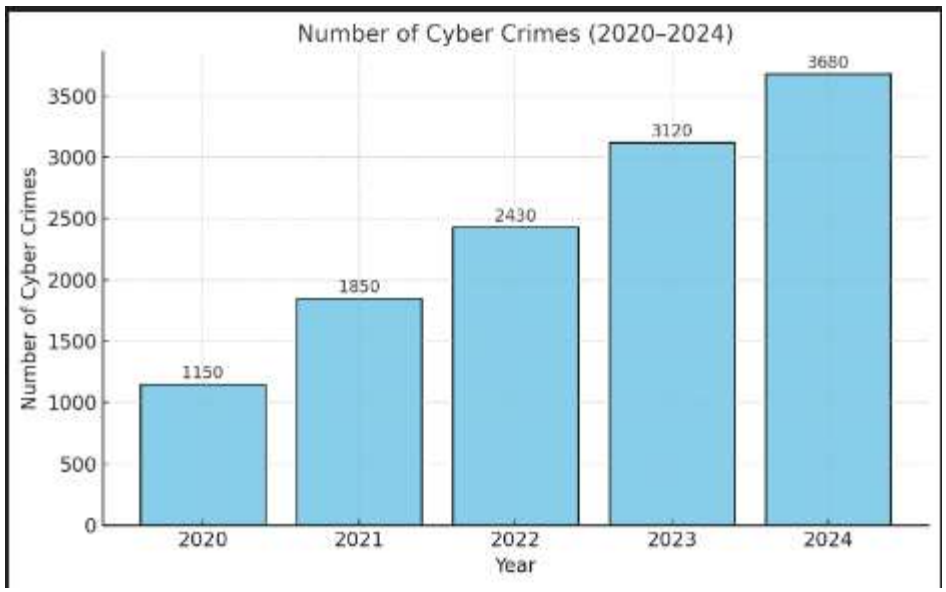

Figure 2. Number of Cyber Crimes in Uzbekistan (2020–2024)")

Challenges and risks

The use of artificial intelligence (AI) technologies in the fight against digital crime, along with great opportunities, also poses a number of challenges and risks. Understanding them correctly and taking preventive measures is crucial for the effective and safe implementation of technologies.

1. Technical challenges. The implementation of AI systems requires a high-quality database, powerful computing resources, and sophisticated algorithms. In practice, the incompleteness and reliability of data, as well as the complexity of the data cleaning process, reduce the effectiveness of AI. Also, some types of cybercrime (for example, zero-day attacks) are based on scenarios that are not known in advance, which limits the ability of AI to detect them.
2. Legal and regulatory issues. Since AI-based decisions can affect human lives, the issue of their legal liability is of great importance. In many cases, AI decisions are poorly explained, which makes them difficult to use as evidence in court proceedings. In Uzbekistan, special legislation related to the use of AI has not yet been fully developed.
3. Security threats. AI systems themselves can also become targets of attack. Machine learning can lead to incorrect decisions through attacks such as "data poisoning" or "adversarial attacks" on algorithms.
4. Ethical risks. AI can violate privacy when processing personal data. There may also be cases where AI-based surveillance systems monitor a person's movements, online activities, or social connections beyond their limits. This can threaten human rights and freedoms.
5. Staffing and qualification issues. There is a shortage of qualified specialists to combat digital crimes based on AI. In addition, the cooperation of lawyers, cybersecurity specialists, and programmers is necessary to properly direct AI technologies.

Addressing technical, legal, security, and ethical issues in using AI to combat digital crime, while also increasing human resource capacity, is a strategic task.

CONCLUSION

Fundamental Finding : The research confirms that artificial intelligence is a decisive instrument in detecting and preventing digital crimes, significantly improving law enforcement efficiency through real-time monitoring, anomaly detection, predictive analysis, and biometric identification, with stronger performance than traditional methods. **Implication :** The integration of AI into national cybersecurity strategies has the potential to reduce economic losses, safeguard critical infrastructures, and enhance public trust in digital ecosystems, particularly in contexts such as Uzbekistan where cybercrime has sharply increased. **Limitation :** Despite these benefits, challenges remain in terms of technical capacity, insufficient infrastructure, legal and ethical uncertainties, vulnerabilities in AI systems themselves, and a shortage of trained specialists, which constrain large-scale implementation. **Future Research :** Further studies should explore context-specific AI frameworks tailored to developing nations, examine the governance of AI-driven cybersecurity with ethical safeguards, and evaluate long-term socio-economic impacts of widespread AI adoption in combating digital crimes.

REFERENCES

[1] Future of Privacy Forum, «AI and Data Protection in Criminal Justice», 2023. https://fpf.org
[2] IBM Security, «AI in Cybersecurity Report», 2023. https://www.ibm.com/security
[3] Symantec, «AI-based Fraud Detection Systems», 2023. https://www.broadcom.com/company/newsroom/press-releases
[4] Microsoft Security, «AI-driven Threat Detection», 2024. https://www.microsoft.com/security
[5] Ministry for the Development of Information Technologies and Communications of the Republic of Uzbekistan, «Annual Reports». 2023 г.
[6] INTERPOL, «Artificial Intelligence in Policing», 2022. https://www.interpol.int
[7] National University of Uzbekistan, «Artificial Intelligence: Development Prospects and Applications», *Sci. J. Natl. Univ. Uzb.*, 2023.
[8] World Economic Forum, «Cybersecurity Futures 2030», 2024. https://www.weforum.org
[9] OECD, «Ethics of AI in Law Enforcement», 2022. https://www.oecd.org
[10] Europol, «Internet Organised Crime Threat Assessment (IOCTA)», 2023. https://www.europol.europa.eu
[11] Law of the Republic of Uzbekistan, «On Information Security».
[12] Law of the Republic of Uzbekistan, «On Informatization».
[13] President of the Republic of Uzbekistan, «On Measures for the Development of the Cybersecurity Sector». 2022 г.
[14] McAfee, «The Hidden Costs of Cybercrime», 2023. https://www.mcafee.com
[15] Gartner, «Top Trends in AI for Security», 2023. https://www.gartner.com

*** Yunusova Minavvarkhon Sabirovna (Corresponding Author)**
Tashkent State University of Law, Uzbekistan