https://cyberpolice.gov.ua/

6. Times of India. CBI dismantles transnational cybercrime networks. URL: https://timesofindia.indiatimes.com/city/delhi/cbi-dismantles- transnationalcybercrime-networks-targeting-minors-

7. World Economic Forum. Cybersecurity and digital resilience, 2024. URL: https://www.weforum.org/storiescybercrime-systemsafety/

Шевчук А.,
здобувач ступеня вищої освіти бакалавра
Національної академії внутрішніх справ
Консультант з мови: **Зубенко В.**

THE USE OF MODERN TECHNOLOGIES IN COMBATING CRIME: INTERNATIONAL EXPERIENCE

The use of modern technologies in combating crime has become a defining element of contemporary law enforcement strategy, shaping both operational practice and policy frameworks. Rapid advances in digital forensics, biometric systems, artificial intelligence (AI), predictive analytics and cyber-investigation tools have expanded investigative capabilities far beyond traditional policing methods. These technologies enable law enforcement agencies to process large volumes of digital evidence, uncover complex criminal networks, and respond more quickly to cyber-dependent and cyber-enabled threats. Recent strategic assessments emphasise that the integration of technological instruments into policing is not merely a matter of acquiring equipment, but requires coherent institutional adaptation, interoperability between agencies, and legal-ethical calibration to preserve democratic oversight and civil liberties [1].

The relevance of studying international experience in technological applications for crime control is underscored by the transnational nature of many contemporary offences. Cybercrime markets, digital fraud schemes and organised online exploitation routinely cross national borders, thereby demanding international cooperation and shared technical standards. Analyses conducted at the European level reveal persistent trends: growth in the scale and

sophistication of online criminal activity, increasing misuse of commodified cyber tools, and the emergence of new operational challenges for evidence preservation and attribution [1]. Parallel research from the United States documents how analytical methods such as crime-forecasting and data-driven deployment strategies have been trialled across multiple jurisdictions, producing mixed evidence on effectiveness and fairness that calls for careful empirical evaluation before wide application [2].

A critical dimension of modern technology use in policing concerns predictive and analytical tools which aim to anticipate criminal activity and guide resource allocation. Predictive policing systems apply statistical models to historical incident data, environmental variables and human mobility patterns to produce risk maps and patrol suggestions. Proponents argue that these tools can improve the efficiency of patrol deployment, reduce response times and enable proactive interventions targeted at high-risk locations or behaviours. However, empirical studies and implementation reviews caution that predictive methods are highly sensitive to data quality, reporting biases and model assumptions; without robust validation, they risk amplifying existing policing disparities and generating unjustified surveillance of marginalised communities [2]. Thus, responsible application requires transparency of algorithms, continuous performance monitoring, and mechanisms for independent oversight.

Biometric technologies and automated identification systems represent another major area of deployment. Fingerprint databases, facial recognition, and DNA analysis have demonstrably improved identification speed and accuracy in many investigations. At the same time, the diffusion of face recognition in public-facing settings raises profound policy questions about consent, proportionality and error rates, particularly when algorithms are trained on non-representative datasets. Internationally, regulatory responses vary: some jurisdictions emphasise strict procedural safeguards and limited operational use, whereas others prioritise capability expansion for counterterrorism and serious crime detection. Comparative evidence indicates that effective governance frameworks — combining legal limits, audit trails, and redress mechanisms — are essential to maintain public trust and to ensure that technological benefits do not come at the expense of fundamental rights [1][3].

Cyber-investigation and digital forensics have become indispensable as criminal activity migrates online. Law enforcement agencies deploy specialized tools for malware analysis, network tracing, and the extraction of evidence from encrypted devices. Cross-border cooperation and information sharing platforms enable coordinated takedowns and the tracing of criminal proceeds through complex financial and cryptocurrency channels. Yet these operations confront technical obstacles (such as widespread encryption and anonymisation services), legal fragmentation among states, and the need to reconcile investigative imperatives with data protection regimes. Strategic reviews recommend enhancing capabilities in cyber-forensics, investing in specialised personnel, and fostering cooperative frameworks that balance investigatory reach with due process safeguards [1].

Robotics, unmanned aerial vehicles (UAVs) and sensor networks are being trialled for situational awareness and tactical support. Drones provide dynamic aerial surveillance, while ground robotics can access hazardous environments; Internet of Things (IoT) sensor data can augment incident reconstruction. These platforms increase operational flexibility but also introduce new vectors for misuse and technical failure. It is therefore crucial to integrate resilience planning, standards for evidence admissibility, and clearly articulated deployment protocols that reflect proportionality and necessity principles. Lessons from pilot programmes suggest that multidisciplinary evaluation — combining technical, legal, and community perspectives — is required before scaling deployments.

A growing body of policy research also addresses the governance of AI in criminal justice contexts. AI applications for risk assessment, recidivism prediction, and investigative prioritisation promise resource efficiencies but pose risks related to opacity, bias and accountability. Recent governmental reviews have recommended stronger requirements for model documentation, impact assessments, human-in-the-loop decision architectures and public reporting on outcomes. These recommendations align with field evidence showing that algorithmic systems must be embedded within broader institutional safeguards to prevent unintended harms and to maintain legitimacy [3]. Moreover, capacity building within agencies — including digital literacy for frontline officers, legal training for prosecutors and judges,

and technical expertise for oversight bodies — is necessary to translate technological potential into durable public safety gains.

International cooperation emerges repeatedly as a precondition for effective technological responses to modern crime. Operational partnerships, shared investigative toolkits, and joint training programs enable faster cross-border casework and foster harmonisation of best practices. Nevertheless, cooperative arrangements require mutual legal assistance, interoperable technical standards and agreed safeguards for handling personal data across jurisdictions. The experience of recent multinational operations demonstrates that when states combine technical tools with shared investigative protocols, they can achieve significant disruption of criminal networks; however, success is contingent on trust, capacity parity and legal interoperability [1].

In conclusion, modern technologies offer powerful instruments to detect, deter and investigate crime, but their deployment entails complex trade-offs. Empirical evidence from European and American contexts indicates that technological effectiveness depends as much on governance, transparency and human capital as on the tools themselves. Policy priorities should therefore include: ensuring data quality and model validation for analytic systems; establishing clear legal frameworks and oversight mechanisms for biometric and AI deployments; investing in specialised cyber-forensic capacity; and strengthening international cooperation to address transnational threats. Only through integrated strategies that combine technical innovation with ethical governance and rigorous evaluation can states harness technological advances to enhance public safety while upholding democratic rights and the rule of law [1][2][3].

References:

1. Europol. Internet Organised Crime Threat Assessment (IOCTA). 2024. Europol. The Hague: Europol, 2024. URL: https://www.europol.europa.eu/cms/sites/defaultdocuments/2024.pdf

2. Perry W.L., McInnis B., Price C.C. Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations / RAND Corporation. Santa Monica (CA): RAND Corporation, 2013. URL: https://www.rand.org/content/dam/rand/pubs/research_reports.pdf

3. U.S. Department of Justice. Artificial Intelligence and Criminal Justice. Final Report. Washington (DC): U.S. Department of

Justice, Office of Legal Policy, 2024. URL: https://www.justice.gov/olp/media/1381796/dl

Шляжко К.,
здобувач ступеня вищої освіти бакалавра
Донецького державного
університету внутрішніх справ
Консультант з мови: **Березенко Н.**

PECULIARITIES OF POLICE ACTIVITIES UNDER MARTIAL LAW

The full-scale invasion of Russian troops, which began against Ukraine in February 2022, posed numerous security challenges for the state and its law enforcement agencies, which had to be addressed as quickly as possible and with the most effective use of available forces and resources. The National Police of Ukraine, as part of the Ministry of Internal Affairs of Ukraine, has been defending the sovereignty and territorial integrity of the country since the first days of the war [1].

According to the Minister of Internal Affairs, Ihor Klymenko, before the full-scale invasion began, the total number of police personnel was approximately 98,000. It is important to note that these forces were evenly distributed throughout the country. However, during the legal regime of martial law, the majority of them were moved to the combat zone and transferred to enhanced duty. In particular, according to his data, about 10 % of personnel are currently involved in combat missions on the front lines, while another 25 % of police officers are directly serving in regions where hostilities are ongoing (Zaporizhzhia, Donetsk, Kharkiv, Kherson and Sumy regions). In total, approximately 40–45% of personnel are currently involved in performing functions that are not typical for the police, as some law enforcement officers from rear areas also periodically perform combat tasks on a rotational basis, in particular, demining territories [1, с. 7-8].

Therefore, it should be noted that under the legal regime of martial law, the personnel of the National Police not only perform purely law enforcement functions, but are also involved in protecting state sovereignty, providing assistance to the civilian population during