КРИМІНАЛІСТИКА МАЙБУТНЬОГО: ЦИФРОВІ ІННОВАЦІЇ, ШТУЧНИЙ ІНТЕЛЕКТ, ГЛОБАЛЬНІ ВИКЛИКИ ТА ЗАГРОЗИ

Матеріали Міжнародної науково-практичної конференції

5 червня 2026 р.

Одеса
2026

УДК 343.98:004.8(062)

К823

Рекомендовано до друку рішенням кафедри криміналістики, судових експертиз та поліграфології НУ»ОЮА» (протокол № 20 від 12 червня 2026 року)
Рекомендовано до друку рішенням Вченої ради ОНДІСЕ (протокол №4 від 22 червня 2026 року)

Криміналістика майбутнього: цифрові інновації, штучний інтелект, глобальні виклики та загрози: збірник матеріалів міжнар. наук.–практ. конф. (м. Одеса, 5 черв. 2026 р.) / [орг. комітет: С. Ківалов, М. Аракелян, , О. Катарага, Д. Кішко, В. Шепітько, Д. Колодін, А. Колодіна Л. Аркуша, та ін.]; Нац. ун–т «Одеська юридична академія», кафедра криміналістики, судових експертиз та поліграфології; Національний центр судових експертиз при Міністерстві юстиції Республіки Молдова; Одеський науково–дослідний інститут судових експертиз Міністерства юстиції України, Міжнародна громадська організація «Конгрес криміналістів». Одеса: НУ «ОЮА», 2026. 564 с.

У збірнику викладено матеріали Міжнародної науково–практичної конференції «Криміналістика майбутнього: цифрові інновації, штучний інтелект, глобальні виклики та загрози», проведеної 5 червня 2026 року Національним університетом «Одеська юридична академія» за участю українських та іноземних науковців, судових експертів, представників правоохоронних органів, практиків, приватних експертів і здобувачів наукових ступенів. Матеріали присвячено криміналістичним інноваціям, цифровим технологіям, штучному інтелекту, розслідуванню злочинів у кіберпросторі, кримінально–правовим і кримінологічним викликам цифровізації, а також кримінально–процесуальним, оперативно–розшуковим та криміналістичним аспектам документування злочинів у цифровий час.

Висловлюємо вдячність усім авторам за активну участь, якісний науковий матеріал та дотримання принципів академічної доброчесності.

Матеріали викладені в авторській редакції.

Відповідальність за зміст, наукову новизну, коректність цитування та достовірність фактичного матеріалу несуть автори.

UDC 343.98:004.8(062)

К823

Recommended for publication by the decision of the Department of Criminalistics, Forensic Examinations and Polygraphology NU «OLA» (Pr. 20, June, 12, 2026)
Recommended for publication by the decision of the Academic Council of ONDISE (Pr. 4, June, 22, 2026)

Criminalistics of the Future: Digital Innovations, Artificial Intelligence, Global Challenges and Threats: Proceedings of the International Scientific and Practical Conference (Odesa, 5 June 2026) / [Organizing Committee: S. Kivalov, M. Arakelyan, O. Cataraga, D. Kishko, V. Shepitko, A. Kolodina, D. Kolodin, L. Arkusha, et al.]; National University «Odesa Law Academy», Department of Criminalistics, Forensic Examinations and Polygraphology; National Centre of Judicial Expertise of the Ministry of Justice of the Republic of Moldova; Odesa Scientific Research Institute of Forensic Examinations of the Ministry of Justice of Ukraine; International Public Organization «Congress of Criminalists». Odesa: NU «OLA», 2026. 564 p.

The Proceedings contain papers presented at the International Scientific and Practical Conference «Criminalistics of the Future: Digital Innovations, Artificial Intelligence, Global Challenges and Threats», held on 5 June 2026 by the National University «Odesa Law Academy». The conference brought together Ukrainian and foreign scholars, forensic experts, representatives of law enforcement agencies, practitioners, private experts and postgraduate researchers. The materials cover criminalistics innovations, digital technologies, artificial intelligence, expert support for justice, investigation of crimes in cyberspace, criminal law and criminological challenges of digitalization, as well as criminal procedure, operational–search and criminalistics aspects of documenting crimes in the digital age.

We express our sincere gratitude to all authors for their active participation, high–quality academic contributions and adherence to academic integrity.

The materials are published in the authors' original versions.

Authors bear responsibility for the content, scientific novelty, accuracy of citations and reliability of factual information.

Шанигін Антон
доктор філософії з медицини, доцент,
кафедри гігієни, медичної екології та громадського здоров'я
Одеського національного медичного університету,
м. Одеса, Україна
ORCID: https://orcid.org/0000–0003–2644–4542
e–mail: anton.shanyhin@onmedu.edu.ua

Волошина Владлена
кандидат юридичних наук, доцент, доцент кафедри кримінального процесу
Національного університету «Одеська юридична академія»,
м. Одеса, Україна
ORCID: https://orcid.org/0000–0001–8772–4172
e–mail:vkvoloshyna@gmail.com

Аль–Файюми Халед
доктор філософії з кібербезпеки
Державний університет інтелектуальних технологій і зв'язку,
м. Одеса, Україна
ORCID: https://orcid.org/0000–0003–4624–2569
e–mail:khaled@alfaiomi.com

ЦИФРОВІ ТЕХНОЛОГІЇ У СФЕРІ ГРОМАДСЬКОГО ЗДОРОВ'Я: ВИКЛИКИ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ МЕДИЧНИХ ДАНИХ

У тезах розглянуто сучасні виклики цифровізації системи громадського здоров'я, пов'язані із кібербезпекою та захистом медичних даних. Проаналізовано ризики використання цифрових медичних систем і штучного інтелекту, а також правові механізми захисту персональної інформації.

Ключові слова: цифровізація, громадське здоров'я, кібербезпека, медичні дані, штучний інтелект.

Shanyhin Anton
PhD in Medicine, Associate Professor, of the
Department of Hygiene, Medical Ecology and Public Health,
Odesa National Medical University,
Odesa, Ukraine

Voloshyna Vladlena
Candidate of Law, Associate Professor, Associate Professor of the
Department of Criminal Procedure,
National University «Odesa Law Academy»,
Odesa, Ukraine

Al–Faiyomi Khaled
PhD in Cybersecurity, State University of Intelligent Technologies and Telecommunications, Odesa, Ukraine

DIGITAL TECHNOLOGIES IN PUBLIC HEALTH: CHALLENGES OF CYBERSECURITY AND PROTECTION OF MEDICAL DATA

The theses examine current challenges of digitalization in the public health system related to cybersecurity and protection of medical data. The risks associated with digital medical systems and artificial intelligence, as well as legal mechanisms for personal data protection, are analyzed.

Key words: digitalization, public health, cybersecurity, medical data, artificial intelligence.

The modern public health system is characterized by the active implementation of digital technologies, including artificial intelligence, Big Data, telemedicine, cloud services, and the Internet of Medical Things (IoMT) [1, p. 36; 2, p. 258]. Digitalization contributes to the automation of medical processes, improvement of epidemiological monitoring, and increased accessibility of healthcare services, particularly under the conditions of the COVID–19 pandemic and martial law [2, p. 256; 3, p. 215].

In Ukraine, healthcare digitalization is being implemented through the development of the national eHealth system, electronic prescriptions, medical information systems, and telemedicine services [2, p. 258]. At the same time, the expansion of digital infrastructure is accompanied by increasing cybersecurity risks, since healthcare systems accumulate large volumes of confidential information, including personal identifiers, clinical records, laboratory results, genetic, and financial data [2, p. 259; 4, p. 64].

Medical information belongs to the category of highly sensitive data, and its compromise may lead to discrimination, insurance fraud, blackmail, and violations of patients' rights [5, p. 42]. A particularly dangerous threat is the modification of clinical information, which may result in diagnostic and treatment errors. In recent years, additional risks have emerged due to the use of artificial intelligence technologies. Among the most significant threats are deepfake technologies and Prompt Injection attacks aimed at manipulating AI algorithms and obtaining unauthorized access to confidential information through medical chatbots or digital assistants.

The scale of cybersecurity threats in healthcare is confirmed by several global cyber incidents. One of the largest attacks targeted Change Healthcare in the United States in 2024, affecting the data of more than 100 million individuals and temporarily disrupting a significant part of the healthcare system [2, p. 262]. Significant consequences were also caused by cyberattacks on the Ascension hospital network, the

MediSecure data breach in Australia, and the WannaCry attack, which seriously disrupted the operation of hospitals in the United Kingdom [6].

For Ukraine, cybersecurity of medical infrastructure has strategic importance under conditions of war, as cyberattacks are increasingly combined with attacks on critical infrastructure facilities [7, p. 497]. Disruptions of healthcare information systems may result in delays in medical care, reputational losses, and threats to patients' lives [7, p. 496].

Legal regulation of medical data protection in Ukraine is based on the Law of Ukraine «On Personal Data Protection», the Law of Ukraine «On Protection of Information in Information and Communication Systems», and international legal instruments [8; 9]. An important direction of legislative development is harmonization with the requirements of the European Union General Data Protection Regulation (GDPR), which establishes high standards for personal data processing and protection [10].

Particular attention is currently paid to the regulation of artificial intelligence in medicine. The European Union AI Act defines medical AI systems as high–risk technologies and establishes mandatory requirements regarding algorithm transparency, human oversight, and safety assessment [11]. International organizations also emphasize the implementation of the principles of «Security by Design» and «Privacy by Design», according to which cybersecurity mechanisms should be integrated into digital systems from the earliest stages of development.

Therefore, digitalization of public health creates significant opportunities for improving healthcare accessibility and efficiency; however, it is simultaneously associated with substantial cybersecurity risks. Ensuring cyber resilience of healthcare infrastructure, improving legal regulation, and increasing digital literacy among healthcare professionals are essential conditions for the safe development of digital medicine.

List of sources used:

1. Bachuk O. Digital transformation in the health care system. Odesa National University Herald. Economy. 2024. Vol. 29, 3(101). c. 36–41 URL: https://doi.org/10.32782/2304–0920/3–101–6

2. Романенко С. В. Впровадження електронної медицини в управлінні медичними закладами: переваги та виклики. Інвестиції: практика та досвід. 2025. № 4. с. 256–264. URL: https://doi.org/10.32702/2306–6814.2025.4.256

3. Опанасюк М. Світові тенденції цифрової трансформації системи охорони здоров'я як об'єкта публічного управління. Економіка, управління та адміністрування. 2026. № 1(115). с. 212–222. URL: https://doi.org/10.26642/ema–2026–1(115)–212–222

4. Security of medical cyber–physical systems. Bulletin of V.N. Karazin Kharkiv National University, series «Mathematical modeling. Information technology.

Automated control systems». 2025. No. 66. P. 63–72. URL: https://doi.org/10.26565/2304–6201–2025–66–06

5. Bryhinets O. Legal security of protection personal data in the field of health care. Economics. Finances. Law. 2024. Vol. 5/2024, no. –. P. 41–43. URL: https://doi.org/10.37634/efp.2024.5.8

6. A retrospective impact analysis of the WannaCry cyberattack on the NHS / S. Ghafur et al. npj Digital Medicine. 2019. Vol. 2, no. 1. URL: https://doi.org/10.1038/s41746–019–0161–6

7. Tokarieva K. S. The problem of personal data protection in the field of health protection in the conditions of informatization. Juridical scientific and electronic journal. 2022. No. 11. P. 496–499. URL: https://doi.org/10.32782/2524–0374/2022–11/120

8. Про захист персональних даних: Закон України від 01.06.2010 № 2297–VI : станом на 14 черв. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2297–17#Text

9. Про захист інформації в інформаційно–телекомунікаційних системах : Закон України від 05.07.1994 № 80/94–ВР : станом на 20 квіт. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/80/94–%D0%B2%D1%80#Text

10. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union. 2016. URL: https://eur–lex.europa.eu/eli/reg/2016/679/oj

11. Artificial Intelligence Act: deal on comprehensive rules for trustworthy AI News European Parliament. URL: https://www.europarl.europa.eu/news/en/press–room/20231206IPR15699/artificial–intelligence–act–deal–on–comprehensive–rules–for–trustworthy–ai