CADERNOS DE DEREITO ACTUAL
www.cadernosdedereitoactual.es

© ***Cadernos de Dereito Actual*** Nº 31. Núm. Ordinario (2026), pp. 1-22
·ISSN 2340-860X - ·ISSNe 2386-5229

Strategies for modernizing administrative law to strengthen the fight against cybercrime

Inna Pidbereznykh[1,*]
Petro Mohyla Black Sea State University
Yevheniia Mykhailovska[2]
Sumy State University
Dmytro Kuzmin[3]
National University of Life and Environmental Sciences of Ukraine "Nizhyn Agrotechnical Institute"
Ruslan Ovcharenko[4]
Interregional Academy of Personnel Management
Stanislav Zlyvko[5]
Penitentiary Academy of Ukraine

[1] Doctor of Legal Sciences, Professor of the Department of History, Faculty of Political Sciences. ORCID: https://orcid.org/0000-0001-9906-4327; E-mail: innaevgenievna2017@gmail.com (corresponding author).
[2] PhD, Deputy Head of the Department of Administrative, Economic Law and Financial and Economic Security. ORCID: https://orcid.org/0000-0001-6814-8843; E-mail: ye.mykhailovska@yur.sumdu.edu.ua.
[3] PhD in Law, Department of Social and Humanitarian Disciplines. ORCID: https://orcid.org/0000-0003-3756-2480; E-mail: kuzmind03@gmail.com.
[4] Doctor in Science in Public Administration, Professor of the Department of Public Administration Interregional Academy of Personnel Management. ORCID: https://orcid.org/0000-0002-4540-0521; E-mail: dnevnoi_dozor@ukr.net.
[5] Doctor of Sciences Law, Professor, Vice-Rector, Penitentiary Academy of Ukraine. ORCID: https://orcid.org/0000-0003-2732-3144. E-mail: zlsl@ukr.net.

Abstract: This article aims to evaluate and synthesize contemporary scholarly approaches to modernizing administrative law to prevent cybercrime, identify effective tactics, and clarify the pedagogical value of those tactics within legal education. The PRISMA framework guided the selection of pertinent literature, yielding 53 records screened on thematic, chronological, and methodological grounds. Sources span 2019 to 2025 and represent scholarships from North America, Europe, and the Asia Pacific region. Each record was assessed for relevance, methodological rigor, and contribution to the evolving discourse on cyber-legal governance, and appraisal followed accepted evidence-grading protocols. Thematic analysis then structured the evidence. The findings show a pressing need to reform state institutions by establishing specialized cyber units capable of responding rapidly to digital threats. The study further indicates that the effectiveness of cybercrime countermeasures depends on the adaptability and currency of legal norms, underscoring the need to align domestic legislation with international standards. Incorporating emerging technologies, especially artificial intelligence, appears promising for enhancing law enforcement performance and enriching legal curricula. Overall, the research concludes that an effective response to cybercrime requires an integrated strategy that unites legal modernization, technological innovation, and cross-sector collaboration. Such synergy safeguards citizens and key infrastructure worldwide.

Keywords: Administrative Law, Artificial Intelligence, Cybersecurity, Digital Space, Legal Modernization

Resumo: Este artigo visa avaliar e sintetizar abordagens acadêmicas contemporâneas para a modernização do direito administrativo na prevenção do cibercrime, identificar táticas eficazes e esclarecer o valor pedagógico dessas táticas no ensino jurídico. A estrutura PRISMA orientou a seleção da literatura pertinente, resultando em 53 registros analisados com base em critérios temáticos, cronológicos e metodológicos. As fontes abrangem o período de 2019 a 2025 e representam trabalhos acadêmicos da América do Norte, Europa e região Ásia-Pacífico. Cada registro foi avaliado quanto à relevância, rigor metodológico e contribuição para o debate em evolução sobre a governança cibernética jurídica, e a avaliação seguiu protocolos aceitos de classificação de evidências. A análise temática estruturou as evidências. Os resultados demonstram uma necessidade premente de reformar as instituições estatais por meio da criação de unidades cibernéticas especializadas, capazes de responder rapidamente às ameaças digitais. A incorporação de tecnologias emergentes, especialmente a inteligência artificial, mostra-se promissora para aprimorar o desempenho das forças policiais e enriquecer os currículos jurídicos. A pesquisa conclui que uma resposta eficaz ao cibercrime exige uma estratégia integrada que una a modernização jurídica, a inovação tecnológica e a colaboração intersetorial. Essa sinergia protege os cidadãos e as infraestruturas essenciais em todo o mundo.

Palavras-chave: Direito Administrativo, Inteligência Artificial, Cibersegurança, Espaço Digital, Modernização Jurídica

1. Introduction

1.1. Problem statement

Rapid digitalization has rendered cybercrime a truly global phenomenon, posing serious risks to economic stability, public administration, and national security. Concurrent advances in networking, cloud computing, and mobile services have fostered an environment in which innovative forms of wrongdoing frequently elude timely administrative or legal control. In scholarly discourse, cybercrime is defined

as illegal activity perpetrated through or directed against computer systems and telecommunications networks with the intent to disrupt, damage, or unlawfully exploit them. Over the past decade, quantitative indicators have contributed to the accelerating computerization of society. GlobalLogic, for instance, reports that 60% of Ukraine's population maintains at least one social network account, a figure that exemplifies widespread digital engagement. High levels of online connectivity, while beneficial, also expand the attack surface for offenders and enable cyber incidents that inflict substantial harm on individuals, businesses, and government institutions.

Recent studies, therefore, conclude that pre-digital administrative and legal mechanisms lack the agility, scalability, and technological awareness necessary to counter the dynamic threats emerging in cyberspace.[6] Consequently, comprehensive regulatory reform and sustained cross-sector collaboration are urgently required to mitigate future threats. Furthermore, the United Nations Office on Drugs and Crime notes that more than 70 percent of national legal systems lack explicit administrative provisions for handling cross-border cyberincidents, a gap that causes delays and jurisdictional disputes.[7] These conditions call for a systemic upgrade and modernization of administrative law, understood here as the adaptation of legal mechanisms to emerging technologies and global challenges.[8] The primary scientific problem is the conceptual and functional inadequacy of existing administrative instruments to address the distinctive nature of cybercrime. First, current regulations frequently omit precise definitions and classifications of cyberoffenses, which leads to uneven enforcement across jurisdictions. Second, administrative procedures remain inflexible and do not match the speed or complexity of cyberincidents, producing noticeable delays and ineffective responses.

These shortcomings underscore the urgent need to revise the legal framework and to design adaptive, technology-oriented administrative strategies that enable timely, proportionate responses to evolving cyberthreats. Consequently, the theoretical and practical significance of this topic lies in formulating a new paradigm of administrative law that reflects digital realities and safeguards the information space. From a scholarly standpoint, the present study expands interdisciplinary dialogue among law, information technology, and education. From a practical perspective, this study seeks to enhance the effectiveness of administrative measures, optimize the current legal education system, and foster digital legal awareness in society. It offers the first systematic evaluation of contemporary scholarly approaches to modernizing administrative law to counter cybercrime, and considers legal, institutional, technological, and educational dimensions. The analysis also addresses the existing gap in consolidating the factors that determine the success of modernization initiatives aimed at combating cybercrime. In addition, the study provides a structured synthesis of recent reform proposals and evaluates their feasibility across different governance contexts, while maintaining an interdisciplinary outlook. This assessment draws on empirical research published between 2019 and 2025, compares implementation outcomes across civil-law and common-law traditions, and distills best practices adaptable to emerging economies. By mapping these elements, the paper supplies policymakers, academics, and practitioners with an evidence-based roadmap for adaptive cybergovernance.

---

[6] RAAIJMAKERS, Stephan. Artificial Intelligence for Law Enforcement: Challenges and Opportunities. IEEE Security & Privacy. 2019, 17(5), 74–77. DOI: 10.1109/msec.2019.2925649.

[7] United Nations: Office on Drugs and Crime, World Drug Report. Www.unodc.org. 2021. Available at: https://www.unodc.org/unodc/en/data-and-analysis/wdr2021.html (accessed on 09 August 2025).

[8] SERGEYEV, Yuriy. Ukrainian Supreme Court Judicial Practice in Cases Arising from Disputes between Foreign Shipowners or Protection and Indemnity Clubs, and Seafarers or Seafarers' Next of Kin. Lex Portus. 2024, 10(3). DOI: 10.62821/lp10303.

1.2. Aim and research questions

The primary goal is to examine and synthesize advanced methods for the modernization of administrative law in combating cybercrime. The research questions are: (1) Which administrative and legal mechanisms are employed in various jurisdictions to counter cybercrime, and how effective are these mechanisms when confronted with digital threats? (2) In what ways do educational, organizational, and technological factors shape the effectiveness of administrative-law modernization in the cybersecurity arena? (3) Which approaches and practical recommendations can secure a more efficient administrative and legal response to cybercrime within an increasingly digital environment?

2. Literature review

2.1. Cybersecurity and trends in the development of administrative and legal regulatory mechanisms

Recent scholarship addresses multiple dimensions of administrative law's evolution in the digital age. Administrative and legal regulation of cybersecurity has become a central focus, with particular attention to the statutory framework governing the establishment and operation of national cybersecurity systems. Current studies examine the role of executive agencies in safeguarding cyberspace[9] and analyze how hybrid threats shape cybersecurity policy.[10] Comparative research highlights international practice, emphasizing the institutional architecture of cybersecurity in the European Union and the capacity of administrative law to create preventive response mechanisms.[11,12] Empirical evidence shows that many jurisdictions have developed cooperative networks motivated by the need for cross-border information exchange.[13] Scholars also note that the United States and most EU member states treat the fight against cybercrime as a strategic priority, illustrated by the Network and Information Security Directive and its revision, NIS2, which impose obligations on operators of critical infrastructure. Consequently,[14] underscore the urgency of aligning domestic legislation with European standards, including public-law instruments for regulating actors in cyberspace. Additional studies call for enhanced administrative liability for cyberoffenses and for robust state-level response mechanisms to cyberattacks.[15,16]

---

[9] AL-AMAIREH, Monther Abed-Alrazzaq Musleh. The Role of Cybersecurity in Enhancing the Effectiveness of Law Against Cybercrimes. Revista de Gestão Social e Ambiental. 2024, 18(8), e06508. DOI: 10.24857/rgsa.v18n8-124.

[10] OLIINYK, Olena, et al. Criminal legal and administrative methods of ensuring the economic security of the state in the context of globalization and modernization of the economy. International Journal of Agricultural Extension. 2022, 10(2), 91–103. DOI: 10.33687/ijae.010.00.3867.

[11] BRODOWSKI, Dominik. The Role of Criminal Law in Regulating Cybercrime and IT Security. In: Law and Technology in a Global Digital Society. Cham: Springer International Publishing, 2022, pp. 233–255. DOI: 10.1007/978-3-030-90513-2_12.

[12] CHERNIAVSKYI, Serhii, et al. Measures to combat cybercrime: analysis of international and Ukrainian experience. Cuestiones Políticas. 2021, 39(69), 115–132. DOI: 10.46398/cuestpol.3969.06.

[13] NGET, Makara, et al. Cybercrime's Global and National Dimensions: Policy Frameworks, Challenges, and Future Solutions. Law and Humanities Quarterly Reviews. 2024, 3(4). DOI: 10.31014/aior.1996.03.04.132

[14] KAVYN, Sviatoslav, Ivan BRATSUK, and Anatoliy LYTVYNENKO. Regulatory and Legal Enforcement of Cyber Security in Countries of the European Union: The Experience of Germany and France. Teisė. 2021, 121, 135–147. DOI: 10.15388/teise.2021.121.8.

[15] ALLAH RAKHA, Naeem. Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations. Mexican Law Review. 2024, 23–54. DOI: 10.22201/iij.24485306e.2024.2.18892.

2.2. Digital governance strategies

In recent years, the current trend has been the development of digital governance, which plays the role of a multi-level process that affects the infrastructure, regulatory, and social components. Thus, given the digitalization trends, the issue of effective strategic management of cyberspace within the framework of digital governance plays an important role.[17] Modern scientific literature indicates that the successful implementation of digital services of the state directly depends on the level of cybersecurity, data protection, and user trust. According to the results of[18], cyberspace plays the role of not just an infrastructure resource of digital governance but also a critical vulnerability. Accordingly, this requires systematic and effective risk management. In addition, as proven in the works of [19] and[20], digital governance should not be limited to the implementation of electronic services; this system should consist of institutional cybersecurity, control over digital platforms. For this reason, the current literature emphasizes the issues of proper regulation and monitoring of citizens' digital identities.[21] The E-Government Development Index Report showed that those countries with a high level of digital transformation implement various national mechanisms or comprehensive cybersecurity strategies. In these countries, these issues play an integral part of digital government. These methods allow for the establishment of national cyberincident response centers and legal control.[22] Other scholars have also indicated that the cyberresilience of digital government services is an important factor in the system of trust in government platforms.[23]

2.3. The significance of educational policy and legal culture

A vital area actively discussed in modern papers is the need to raise legal culture and digital literacy. Scientists emphasize the importance of integrating innovative educational technologies into specialist training. In addition, it is recommended that significant attention be paid to improving competencies in cyberhygiene among pupils, students, civil servants, and the public. Therefore, the issue of effective specialist training is particularly relevant. Scientific studies have shown that it is necessary to engage students with various digital resources to

---

[16] NGET, Makara, et al. Cybercrime's Global and National Dimensions: Policy Frameworks, Challenges, and Future Solutions. 2024. Ibid.

[17] DANYLENKO-NEHARA, Yuliia, et al. The ethical aspect of public administration under special regime and sustainable development. Salud, Ciencia y Tecnología-Serie de Conferencias. 2024, 3. DOI: 10.56294/sctconf2024.755.

[18] BUÇAJ, Enver, and Kenan IDRIZAJ. The need for cybercrime regulation on a global scale by the international law and cyber convention. Multidisciplinary Reviews. 2024, 8(1), 2025024. DOI: 10.31893/multirev.2025024.

[19] CHRISTOU, George. The challenges of cybercrime governance in the European Union. European Politics and Society. 2018, 19(3), 355–375. DOI: 10.1080/23745118.2018.1430722.

[20] GUMZEJ, Nina, and Nikola PROTRKA. Evaluation of Digital Evidence in Criminal Proceedings in Croatia with a Focus on Preservation Requirements and Role of Standard Operative Procedures. In: 2021 44th International Convention on Information, Communication, and Electronic Technology (MIPRO). 2021. DOI: 10.23919/mipro52101.2021.9597136.

[21] ERIKHA, Annisa, and Ade SAPTOMO. Dilemma of Legal Policy to Address Cybercrime in the Digital Era. Asian Journal of Social and Humanities. 2024, 3(3), 499–507. DOI: 10.59888/ajosh.v3i3.452.

[22] BREWER, Russell, et al. Universal Communication Strategies. Cybercrime Prevention. Cham: Springer International Publishing, 2019, pp. 35–48. DOI: 10.1007/978-3-030-31069-1_3.

[23] SIAGIAN, Erwin Sondang. Public-private partnerships in Indonesia: a comprehensive legal framework of significance to action and analysis. Asia Pacific Journal of Public Administration. 2017, 39(1), 72–78. DOI: 10.1080/0142159x.2017.1294395.

develop a high level of digital literacy and media culture. At the same time, other works have shown that the preventive role of education is an underestimated component of the cybersecurity system. The probability of successful phishing attempts, data leaks, and online fraud can be reduced through awareness among Internet users and across different platforms, according to modern experts. Furthermore, other publications highlight the challenge of implementing digital security education programs at the high school and college levels. However, this area is not sufficiently covered in modern scientific literature and requires more detailed empirical research on the use of innovative methods and their effectiveness. However, despite the significant volume of scientific publications on cybersecurity, several gaps remain that complicate a holistic picture of effective regulatory mechanisms. As the review of individual publications shows, digital governance is a tool for modernizing public services, whereas cybersecurity is often analyzed in isolation. This requires systematic, holistic research. There is also a pressing need to highlight the experiences of different countries in regulating administrative law in light of modern cyber challenges. All these aspects indicate the need for a systematic analysis of the definition of relevant mechanisms for the development of administrative law to strengthen the fight against cybercrime. This study will attempt to describe not only different models of combating cybercrime but also certain shortcomings in their implementation.

3. Methodology

3.1. Research design

Given the lack of comprehensive reviews in the current scientific discourse, the study used a systematic literature review. This type will allow us to summarize existing scientific approaches and identify gaps in knowledge of the implementation of instruments to combat cybercrime. In addition, this review will aim to build an important evidence base for further empirical and theoretical research. The main advantages of systematic reviews are their clarity, generalizability, reproducibility, and validity of source selection. This approach was also chosen from an interdisciplinary perspective, combining aspects of administrative law, digital governance, and cybersecurity.

3.2. Sampling

The study used a criterion-based sampling to include scientific sources. This sampling involved including sources based on relevance to the topic, time range, full-text availability, and language criteria. At the same time, the exclusion criteria concerned the language of writing and thematic inconsistency. Those studies written before 2017 were also rejected.

So, the inclusion criteria are: (1) Sources published from 2017 to 2025. (2) Various types of materials were subject to inclusion: peer-reviewed scientific articles, analytical reports, chapters from monographs, and conference proceedings. (3) Materials must cover at least 1 of the following aspects: analysis of the administrative and legal regulation in the field of cybersecurity; examination of digital governance and digital changes; explanation of legal culture; analysis of legal education in the field of cybersecurity; study different mechanisms for combating cybercrime. (4) All materials must be published in peer-reviewed collections. (5) Full text accessibility. (6) Language of writing: English, sometimes Ukrainian in the case of an English-language abstract.

Exclusion criteria are: (1) Publications written before 2017. (2) The following types of materials were excluded: posts from social networks, blogs, journalistic articles, and sources without reviews. (3) Duplicates without scientific novelty were

excluded. (4) Lack of thematic relevance. (5) Sources that do not have full text for qualitative analysis. (6) Sources written in languages other than English.

3.3. Tools and procedure

Scientific sources were collected and identified using the PRISMA methodological framework, an approach widely recognized as effective for systematic reviews covering the period 2019–2025. We first selected the scientometric databases to be searched: Scopus, Web of Science, Google Scholar, and HeinOnline. The following keywords and their derivatives were entered in the queries: "administrative law," "cybersecurity policy," "cybercrime," "mechanisms of counteraction," "protection models," "strategies," "digital governance," "legal awareness," "cyberhygiene," "e-government," "modernization," "public administration and cybersecurity," "digital transformation," and "rule of law in cyberspace." The initial search retrieved 2,894 records. After duplicate removal (–956), 1,938 records remained; duplicates were identified algorithmically and then confirmed manually. Title and abstract screening for topical relevance excluded a further 689 items, leaving 1,249. Additional 251 records were discarded because they did not meet the subject criteria. The remaining materials were then assessed against the predefined exclusion parameters.

After that, the codes were combined into broader themes: (1) The main administrative and legal mechanisms that affect the fight against cybercrime in different countries. (2) Institutional vulnerability. (3) National approaches. (4) The need for international coordination. (5) Technological strengthening of administrative forms of control. (6) Strategic priorities for modernization.

The process of identification, screening, assessment of suitability, and final inclusion of sources in the study was carried out in accordance with the PRISMA methodology and summarized in the form of a diagram (Figure 1).

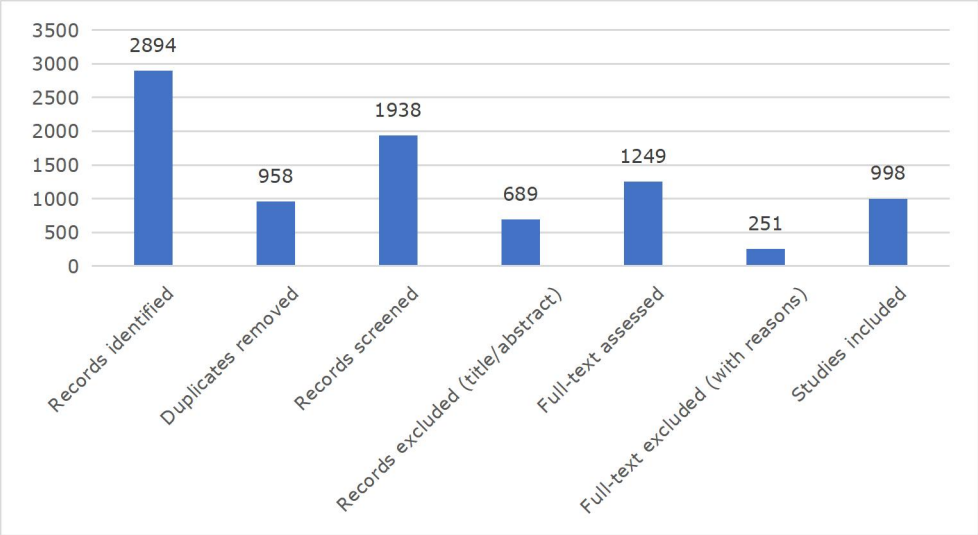

Figure 1. PRISMA flow diagram of the study selection process.

The data obtained was compared with the conclusions of other researchers using comparative analysis. The search for scientific sources was conducted across the databases Scopus, Web of Science Core Collection, Google Scholar, and HeinOnline. The search covered the period from January 2017 to March 2025. The final search was carried out on March 15, 2025.

The search was limited to publication titles, abstracts, and keywords (where the database's technical capabilities allowed). The sample included only peer-reviewed scientific materials with full-text access.

The following logical combinations of keywords were used for the search (adapted to the syntax of each database): ("administrative law" OR "public administration") AND ("cybercrime" OR "cybersecurity policy" OR "cyberspace security") AND ("digital governance" OR "e-government" OR "digital transformation") AND ("mechanisms" OR "models" OR "strategies" OR "legal culture" OR "legal awareness").

3.4. Research quality assessment

To ensure methodological transparency and robustness of the results, the quality of the included sources was assessed using standardized critical appraisal tools.

Empirical and mixed studies were assessed using CASP (Critical Appraisal Skills Programme) checklists, while analytical legal studies, policy documents, and public administration works were analyzed using the JBI (Joanna Briggs Institute) approach, adapted to research in the field of law and digital governance.

The assessment was carried out according to the following criteria: clarity of research objectives, soundness of methodology, logicality of legal analysis, relevance to cybersecurity issues, and coherence of conclusions.

Sources with lower methodological quality were not automatically excluded from the analysis, but they were given less analytical weight in the thematic synthesis. A comparative analysis of thematic findings with and without such sources was conducted, which did not reveal a significant impact on the overall results of the study.

Thematic coding of the materials was carried out qualitatively using a previously developed codebook. Given the interdisciplinary nature of the study and the predominantly qualitative design of the review, quantitative percentages were not used. Instead, descriptive wording (e.g., "most studies," "a significant portion," "a limited number") was used to reflect the relative prevalence of the themes identified.

4. Results

Within the framework of this study, the modernization of administrative law is interpreted through the prism of the theory of regulatory governance, in particular the approaches of risk-based regulation and responsive regulation. In this context, administrative law is considered not only as a tool of coercion but also as a flexible risk management system that combines preventive, sanctioning, and coordination mechanisms in response to dynamic threats in the digital environment. This approach allows us to assess the effectiveness of administrative and legal instruments in countering cybercrime, taking into account the level of risk, institutional capacity, and the interaction between state and non-state actors.

As a result of the review of the selected 53 scientific sources published between 2017 and 2024, the main thematic clusters related to the modernization of administrative law in the framework of countering cybercrime were identified. Many studies (n = 38; 73%) focused on reforming institutional structures, including the creation of specialized cyber units, cyber police, and cybersecurity centers within public authorities.[24] Accordingly, these works indicate that the process of optimizing such systems is determined not only by technical support but also by administrative autonomy. The importance of prompt response is also mentioned. The research cases of Sweden, the United States, and Estonia highlight the importance of

[24] COLLIER, Ben, et al. Influence, infrastructure, and recentering cybercrime policing: evaluating emerging approaches to online law enforcement through a market for cybercrime services. Policing and Society. 2021, 1–22. DOI: 10.1080/10439463.2021.1883608.

integrating administrative units with digital threat monitoring systems.[25,26] However, within this thematic cluster, a prominent role is played by the problem of the formation and development of regional and interstate cyberincident information exchange centers that are actively operating in the EU, NATO, and other international structures.[27] Thus, institutional modernization is interpreted as an important foundation for the formation of future strategies. Besides, the second most frequently mentioned cluster (n = 34; 65%) is the perfection of administrative and legal mechanisms for authorizing violations in cyberspace.[28,29] Modern works point to the problem of expanding the powers of administrative bodies in the system of responding to cybercrime. This is done without the need to initiate criminal proceedings in cases of minor or repeated offenses.[30] In general, there is a consensus in the scientific literature on the need for institutional autonomy for specialized cyberunits, but discussions remain about the cost of maintaining them and the risks of fragmentation of powers, especially in countries with limited administrative resources.

The results from the selected scientific literature indicate that a combination of administrative fines, access restrictions, and sanctions against digital service providers is an important promising alternative. However, the need for unification of administrative legislation within regional associations is also notable.[31] At the same time, about 42% of sources (n = 22) described the introduction of digital platforms as an effective tool for recording and responding to cyberincidents.[32,33] In particular, scientific literature presents an analysis of web interfaces for filing complaints, mobile applications, and automated systems for processing citizens' appeals. Practices where digital platforms operate within public administration are important, as they interact with law enforcement databases.[34] Another important area is international coordination, in particular, n = 28 (54%) of the papers pointed to the importance of transnational cooperation in the field of cybersecurity.[35,36] The scientific literature also emphasizes the importance of the Budapest Convention on

[25] DUPONT, Benoît. Enhancing the effectiveness of cybercrime prevention through policy monitoring. Journal of Crime and Justice. 2019, 42(5), 500–515. DOI: 10.1080/0735648x.2019.1691855.
[26] BRODOWSKI, Dominik. The Role of Criminal Law in Regulating Cybercrime and IT Security. 2022. Ibid.
[27] CHRISTOU, George. The challenges of cybercrime governance in the European Union. 2018. Ibid.
[28] ALLAH RAKHA, Naeem. Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations. 2024. Ibid.
[29] DEWI SURYANDARI, Wieke. Efforts to Reform Law Enforcement in Tackling Cybercrime. International Journal of Law Social Sciences and Management. 2024, 1(2). DOI: 10.69726/ijlssm.v1i2.27.
[30] ELEGBE, Ifeoluwa. Cybercrime legislation: a comparative analysis of legal frameworks, policy responses and recommendations. 2024. Ibid.
[31] BUÇAJ, Enver, and Kenan IDRIZAJ. The need for cybercrime regulation on a global scale by the international law and cyber convention. 2024. Ibid.
[32] BATRACHENKO, Tetiana, et al. Cybercrime in the context of the digital age: analysis of threats, legal challenges and strategies. Multidisciplinary Science Journal. 2024, 6, 2024ss0212. DOI: 10.31893/multiscience.2024ss0212.
[33] AL-AMAIREH, Monther Abed-Alrazzaq Musleh. The Role of Cybersecurity in Enhancing the Effectiveness of Law Against Cybercrimes. Revista de Gestão Social e Ambiental. 2024. Ibid.
[34] CHERNIAVSKYI, Serhii, et al. Measures to combat cybercrime: analysis of international and Ukrainian experience. 2021. Ibid.
[35] BUSSER, Els De. EU-US Digital Data Exchange to Combat Financial Crime: Fast is the New Slow. German Law Journal. 2018, 19(5), 1251–1267. DOI: 10.1017/s2071832200023026.
[36] BOUSTA, Rhita, and Yseult MARIQUE. Taking Comparative Administrative Law (Almost) Seriously? Comparative Administrative Law in French & Belgium Legal Education. SSRN Electronic Journal. 2016. DOI: 10.2139/ssrn.2711289.

Cybercrime[37]. This document is a model international treaty that combines administrative and criminal law approaches. However, the authors often criticize the slowness in implementing its provisions in national legal systems.[38] Within this cluster, most studies support the expansion of administrative powers as a flexible alternative to criminal prosecution, while some authors emphasize the risks of excessive discretion and potential conflict with the principles of the rule of law.

At the same time, 33% of the selected sources (n = 17) described the role of education, training, and public awareness. These aspects are important parts of creating modernization strategies.[39] A new thematic cluster (n = 16; 31%) is research on the use of artificial intelligence and data analytics. It is stated that these technologies are important for detecting, recording, and responding to cybercrime. However, some authors have emphasized the need for clear administrative regulations on the use of AI and pointed out the problems of regulatory regulation.[40] At the level of international coordination, there is general agreement on the importance of the Budapest Convention as a basic normative reference point, but the slow implementation of its provisions and the conflict between national sovereignty and supranational cooperation mechanisms remains the main point of tension.

The description of the selected 53 sources showed some geographical and jurisdictional differences in the strategies of legal regulation of cybercrime. The study divided the countries from the selected analytical works by the level of legal regulation of digital security. In particular, 40% of the countries received the status of advanced, 47% – at the developing stage, 13% – at the early stage.

In particular, the European Union countries are dominated by a process of unified policies based on EU directives and the GDPR. In these countries, the transformation of legislation on digital evidence is an active process.[41,42] A notable phenomenon is the analysis of transnational cooperation. At the same time, in Asia, Latin America, and Africa, there is a noticeable lag in the legal framework. This affects legal fragmentation and limited use of administrative law.[43] In these regions, the key challenges relate to the lack of institutional resources. The conflict between sovereignty and international coordination is also prominent.[44] However, in Canada and the United Kingdom, the theme of responsibilities is prevalent. This concept

---

[37] Council of Europe (COE): Convention on Cybercrime. International Legal Materials. 2002, 41(2), 282–302. DOI: 10.1017/s0020782900009918.

[38] DIOP, Serigne Mouhamadane, et al. To Coerce or Not to Coerce? A Quantitative Investigation on Cybersecurity and Cybercrime Legislations Towards Large-Scale Vulnerability Notifications. In: 2019 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW). 2019. DOI: 10.1109/issrew.2019.00085.

[39] CATOTA, Frankie E., M. Granger MORGAN, and Douglas C. SICKER. Cybersecurity education in a developing nation: the Ecuadorian environment. Journal of Cybersecurity. 2019, 5(1). DOI: 10.1093/cybsec/tyz001.

[40] DUPONT, Benoît. Enhancing the effectiveness of cybercrime prevention through policy monitoring. 2019. Ibid.

[41] GOLOVIN, Dmytro. Electronic evidence in proving crimes of drugs and psychotropic substances turnover. Access to Justice in Eastern Europe. 2022, 5(2), 1–13. DOI: 10.33327/ajee-18-5.2-n000217.

[42] GUMZEJ, Nina, and Nikola PROTRKA. Evaluation of Digital Evidence in Criminal Proceedings in Croatia with a Focus on Preservation Requirements and Role of Standard Operative Procedures. 2021. Ibid.

[43] ELEGBE, Ifeoluwa. Cybercrime legislation: a comparative analysis of legal frameworks, policy responses and recommendations. International Journal of Education and Social Science Research. 2024, 07(02), 199–207. DOI: 10.37500/ijessr.2024.7211.

[44] MENSAH, Ebenezer Kojo Gyesi. Investigating International Criminal Law and Sovereignty Issues Surrounding the Prosecution of Heads of State for War Crimes and Genocide. SSRN Electronic Journal. 2024. DOI: 10.2139/ssrn.4813323.

implies that a significant part of the burden of cyberdefense is placed on citizens.[45] Although the introduction of digital platforms is mostly assessed positively as a tool for increasing the speed of response, some authors warn about the high costs of their support and the dependence of the effectiveness of such systems on the level of digital literacy of the population.

To enhance comparative legal analytical value, the results are systematized considering the differences between the civil law and common law legal systems. The analysis reveals both convergence of approaches to the administrative and legal regulation of cybersecurity (in particular, in the field of digital evidence and institutional coordination) and divergences that manifest themselves in the level of discretion of administrative bodies, the role of case law, and mechanisms of responsibilization.

Accordingly, this influences the formation of a different strategic model where administrative law plays the role of establishing framework obligations rather than directly regulating cybercrime (See Table 1).

Table 1. Geographical and jurisdictional differences in strategic priority for the legal regulation of cybercrime.

Region/ country	**Approach**	**Legal modernization status**	**References**
Germany	EU harmonization, GDPR-based digital evidence policies Specialized educational programs for civil servants Courses on digital law	Advanced	Kavyn et al. (2021)[46]; Busser (2018)[47]; Nowacki & Willits (2019)[48]
France	EU harmonization, cybersecurity law integration Active coordination between the Ministry of Justice, the National Gendarmerie, and ANSSI Digital Law Courses	Advanced	Nowacki & Willits (2019)[49]; Kavyn et al. (2021)[50]
Italy	Intersection of data protection and cybersecurity in investigations Strengthening sanctions for cyberattacks and data theft	Developing	Flor & Panattoni (2023)[51]

[45] RENAUD, Karen, et al. Cyber Security Responsibilization: An Evaluation of the Intervention Approaches Adopted by the Five Eyes Countries and China. Public Administration Review. 2020, 80(4), 577–589. DOI: 10.1111/puar.13210.

[46] KAVYN, Sviatoslav, Ivan BRATSUK, and Anatoliy LYTVYNENKO. Regulatory and Legal Enforcement of Cyber Security in Countries of the European Union: The Experience of Germany and France. 2021. Ibid.

[47] BUSSER, Els De. EU-US Digital Data Exchange to Combat Financial Crime: Fast is the New Slow. 2018. Ibid.

[48] NOWACKI, Jeffrey, and Dale WILLITS. An organizational approach to understanding police response to cybercrime. Policing: An International Journal. 2019, 43(1), 63–76. DOI: 10.1108/pijpsm-07-2019-0117.

[49] Ibid.

[50] KAVYN, Sviatoslav, Ivan BRATSUK, and Anatoliy LYTVYNENKO. Regulatory and Legal Enforcement of Cyber Security in Countries of the European Union: The Experience of Germany and France. 2021. Ibid.

[51] FLOR, Roberto, and Beatrice PANATTONI. Digital criminal investigations in Italy. The intersection between data protection and cybersecurity. New Journal of European Criminal Law. 2023. DOI: 10.1177/20322844231212836.

Region/ country	Approach	Legal modernization status	References
Croatia	Standard Operating Procedures for digital evidence National Cybersecurity Center established Significant attention to training digital law specialists	Developing	Gumzej & Protrka (2021)[52]
Lithuania	EU-based administrative legal adaptation Introduction of the Law on Cybersecurity of Lithuania Formation of National Cybersecurity Centers	Developing	Kavyn et al. (2021)[53]
USA	Responsibilization, public-private coordination Digital Law Courses CFAA (Computer Fraud and Abuse Act) Formation of the FBI Cyberdivision International cooperation	Advanced	Renaud et al. (2020)[54]
UK	Responsibilization, intelligence-led policing Introduction of the UK Computer Misuse Act Introduction of a separate Cybersecurity Strategy of the UK	Advanced	Renaud et al. (2020)[55]
Australia	Administrative risk regulation and cyberstrategy Digital recording of incidents Digitalization	Advanced	Renaud et al. (2020)[56]
Canada	Framework-aligned cybersecurity education (NICE) Formation of national cybersecurity centers	Advanced	Newhouse et al. (2017)[57]
Indonesia	Post-COVID legal synthesis, weak enforcement Information and Electronic Act regulating cybercrime	Early-stage	Nugroho & Chandrawulan (2022)[58]
Liberia	Draft legislation, alignment with international norms	Developing	Gilbert & Gilbert (2024)[59]

[52] GUMZEJ, Nina, and Nikola PROTRKA. Evaluation of Digital Evidence in Criminal Proceedings in Croatia with a Focus on Preservation Requirements and Role of Standard Operative Procedures. 2021. Ibid.
[53] KAVYN, Sviatoslav, Ivan BRATSUK, and Anatoliy LYTVYNENKO. Regulatory and Legal Enforcement of Cyber Security in Countries of the European Union: The Experience of Germany and France. 2021. Ibid.
[54] RENAUD, Karen, et al. Cyber Security Responsibilization: An Evaluation of the Intervention Approaches Adopted by the Five Eyes Countries and China. 2020. Ibid.
[55] Ibid.
[56] Ibid.
[57] NEWHOUSE, William, et al. National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. Gaithersburg, MD: National Institute of Standards and Technology, August 2017. DOI: 10.6028/nist.sp.800-181.
[58] NUGROHO, Agus, and An An CHANDRAWULAN. Research synthesis of cybercrime laws and COVID-19 in Indonesia: lessons for developed and developing countries. Security Journal. 2022. DOI: 10.1057/s41284-022-00357-y.
[59] GILBERT, Chris, and Mercy Abiola GILBERT. Bridging the Gap: Evaluating Liberia's Cybercrime Legislation Against International Standards. International Journal of Research

Region/ country	**Approach**	**Legal modernization status**	**References**
Cambodia	Emerging policy frameworks, resource constraints	Early-stage	Nget et al. (2024)[60]
India	Sector-specific e-banking protection Digital recording of incidents Digitalization	Developing	Roy & Dixit (2024)[61]
Ukraine	Adaptation to EU standards Mixed administrative-criminal enforcement for digital security Creation of cyberunits Digital recording of incidents Digitalization Cyberhygiene Digital education of employees	Developing	Oliinyk et al. (2022)[62]; Batrachenko et al. (2024)[63]; Vitvitskiy et al. (2021)[64]; Semenets-Orlova et al. (2023)
Brazil	Global penal law perspective on cybercrime Digital recording of incidents Digitalization	Developing	Fortes & Boff (2017)[65]

Source: Author's development. Note: Jurisdictions were classified according to the following criteria: Advanced—presence of a comprehensive national cybersecurity strategy; specialized administrative or interagency cyberunits; integration of digital evidence into administrative and criminal proceedings; alignment with international standards (including the Budapest Convention). Developing—fragmented regulatory framework; partial institutionalization of cyberunits; limited integration of digital tools; selective implementation of international norms. Early-stage—lack of a systemic strategy; initial or draft regulatory initiatives; limited institutional capacity and resources.

A comparative analysis of jurisdictions shows that countries with developed regulatory governance models tend to gravitate towards risk-based and responsibilization approaches, while states in the early stages of modernization focus on fragmented administrative control. This demonstrates a direct connection between institutional capacity, economic resources, and the choice of administrative and legal strategies in the field of countering cybercrime.

The examples of jurisdictions provided in the table meet the specified classification criteria and illustrate different trajectories of administrative law

and Innovation in Applied Science. 2024, IX(X), 131–147. DOI: 10.51584/ijrias.2024.910013.

[60] NGET, Makara, et al. Cybercrime's Global and National Dimensions: Policy Frameworks, Challenges, and Future Solutions. 2024. Ibid.

ILYINA, Anastasiya. Mechanism of Innovation and Investment Development in Modern Economy. Economic Affairs. 2022, 67(4s). DOI: 10.46852/0424-2513.4s.2022.16.

[61] ROY, Reena, and Anil Kumar DIXIT. Legal Framework of Cybercrimes against E-Banking in India. In: Cybersecurity, Law, and Economics. London: Routledge, 2024, pp. 69–90. DOI: 10.4324/9781003517290-7.

[62] OLIINYK, Olena, et al. Criminal legal and administrative methods of ensuring the economic security of the state in the context of globalization and modernization of the economy. 2022. Ibid.

[63] BATRACHENKO, Tetiana, et al. Cybercrime in the context of the digital age: analysis of threats, legal challenges and strategies. 2024. Ibid.

[64] S. VITVITSKIY, Sergij, et al. Formation of a new paradigm of anti-money laundering: The experience of Ukraine. Problems and Perspectives in Management. 2021, 19(1), 354–363. DOI: 10.21511/ppm.19(1).2021.30.

[65] FORTES, Vinícius Borges, and Salete Oro BOFF. An analysis of cybercrimes from a global perspective on penal law. Revista Brasileira de Direito. 2017, 13(1), 7–24. DOI: 10.18256/2238-0604/revistadedireito.v13n1p7-24.

modernization depending on legal tradition, level of institutional capacity, and economic development.

An important aspect for further improvement of counteraction to cybercrime is updating the practices proposed in the research. Considering the analysis of the most modern scientific works devoted to the issues of compliance with digital security, it is possible to single out some promising recommendations for improving administrative law (See Table 2).

Table 2. Key recommendations for improving the situation in combating cybercrime.

Vector(s)	**Description**	**References**
Legal partnership between the state and the private sector	Improving the legal basis for public-private partnership	Roy & Dixit (2024)[66]
Improving digital methods for combating cybercrime	Using digital solutions for cybersecurity systems	Smailov et al. (2024)[67]
Responsibility of Internet intermediaries for content, use of search algorithms, etc.	Increasing the responsibility of online intermediaries who provide (knowingly and unknowingly) platforms for the spread of cybercrime	Sorbán (2022)[68]
Processing of payment systems	Improving digital electronic evidence analysis systems which will allow for more effective investigation of cybercrime	Sturc et al. (2022)[69]
Providing balanced access to information, including on national security	Development of new legal norms to ensure a balance between access to information and national security	Sviatun et al. (2021)[70]
Economic and legal factors	Economic and legal factors of countering the consequences of cybercrime	Sviatun et al. (2021)[71]; Shevchuk et al.[72]
Countering existing money laundering schemes	Formation and testing in practice of new paradigms of countering money laundering schemes	Vitvitskiy et al. (2021)[73]

[66] ROY, Reena, and Anil Kumar DIXIT. Legal Framework of Cybercrimes against E-Banking in India. In: Cybersecurity, Law, and Economics. 2024. Ibid.

[67] SMAILOV, Nurzhigit, et al. Streamlining Digital Correlation-Interferometric Direction Finding with Spatial Analytical Signal. Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska. 2024, 14(3), 43–48. DOI: 10.35784/iapgos.6177.

[68] SORBÁN, Kinga. The role of Internet intermediaries in combatting cybercrime: Organisation and liabilities. Central and Eastern European edem and egov Days. 2022, 335, 19–31. DOI: 10.24989/ocg.v335.1.

[69] STURC, Boris, Tatyana GUROVA, and Sergei CHERNOV. The Specifics and Patterns of Cybercrime in the Field of Payment Processing. International Journal of Criminology and Sociology. 2022, 9, 2021–2030. DOI: 10.6000/1929-4409.2020.09.237.

[70] SVIATUN, Olena V., et al. Combating cybercrime: economic and legal aspects. WSEAS TRANSACTIONS ON BUSINESS AND ECONOMICS. 2021, 18, 751–762. DOI: 10.37394/23207.2021.18.72.

[71] Ibid.

[72] SHEVCHUK, O., et al. The Rights to access to Information and National Security in the Ukraine in the System of Human Rights. Revista Juridica Portucalense. 2023, 34, 257–282. Available at: https://revistas.rcaap.pt/juridica/article/view/31229 (accessed on 09 August, 2025).

[73] S. VITVITSKIY, Sergij, et al. Formation of a new paradigm of anti-money laundering: The experience of Ukraine. 2021. Ibid.

Vector(s)	**Description**	**References**
Challenges of using artificial intelligence for criminal purposes	Problems of regulating the work of artificial intelligence in the criminal and administrative codes	Vuletić (2021)[74]
Cooperation between law enforcement agencies	Cooperation of law enforcement agencies in combating cybercrime	Wang et al. (2020)[75]
Certain legal issues of regulating cybercrime	Legal issues of combating cybercrime that will need to be resolved	Yerjanov et al. (2018)[76]
Lawyer practice in combating cybercrime	Emphasis on the legal foundations of legal practice	Oderiy et al. (2024)[77]
Countering existing money laundering schemes	Using international experience to counteract international money laundering schemes money	Diop et al. (2019)[78]
Existence of different legal interpretations in the field of combating cybercrime	Overcoming existing inaccuracies in definitions of cybercrimes and their constituent aspects	Gilbert & Gilbert (2024)[79]
Research on cybercrime in a global dimension	An important aspect is the involvement of maximum international experience to overcome the consequences of cybercrimes	Fortes & Boff (2017)[80]

Source: authors' development.

Therefore, based on the analyzed scientific literature, we can summarize certain results. The researchers noted that the main promising recommendations for improving further counteraction to the spread of cybercrime are the use and development of new legal norms that take into account the current problems of the spread of cybercrime, combining the efforts of public and private entities, increasing the level of international coordination in the field of cybersecurity, improving digital systems for collecting and analyzing electronic evidence, raising awareness of ordinary citizens about the threats of digital crime, using the latest technological solutions to improve the administrative law system.

For practical application of the results, it is advisable to use a balanced system for assessing the effectiveness of administrative and legal measures to combat cybercrime. Such a system can include economic indicators (costs for institutional infrastructure), operational indicators (speed of response, number of incidents processed), indicators of trust and ethics (citizen trust, number of appeals of administrative decisions), as well as indicators of compliance with legislation and

[74] VULETIĆ, Igor. Criminal Law and the Challenges of Autonomous Intelligence: Substituting a Theory of Guilt with the Division of Labor. In: The Law and Economics of Patent Damages, Antitrust, and Legal Process. Emerald Publishing Limited, 2021, pp. 111–126. DOI: 10.1108/s0193-589520210000029007.

[75] WANG, Shun-Yung Kevin, et al. Collaboration between Law Enforcement Agencies in Combating Cybercrime: Implications of a Taiwanese Case Study about ATM Hacking. International Journal of Offender Therapy and Comparative Criminology. 2020, 0306624X2095239. DOI: 10.1177/0306624x20952391.

[76] YERJANOV, Timur Keldeshevich, et al. Legal Issues Related to Combating Cybercrime: Experience of the Republic of Kazakhstan. Journal of Advanced Research in Law and Economics. 2018, 8(7), 2286. DOI: 10.14505//jarle.v8.7(29).30.

[77] ODERIY, Oleksiy, et al. The Impact of EU Criminal Law Policy on the Prevention of Transnational Environmental Crime. Pakistan Journal of Criminology. 2024, 16(3), 1155–1172. DOI: 10.62271/pjc.16.3.1155.1172.

[78] DIOP, Serigne Mouhamadane, et al. To Coerce or Not to Coerce? A Quantitative Investigation on Cybersecurity and Cybercrime Legislations Towards Large-Scale Vulnerability Notifications. 2019. Ibid.

[79] GILBERT, Chris, and Mercy Abiola GILBERT. Bridging the Gap: Evaluating Liberia's Cybercrime Legislation Against International Standards. 2024. Ibid.

[80] FORTES, Vinícius Borges, and Salete Oro BOFF. An analysis of cybercrimes from a global perspective on penal law. 2017. Ibid.

international standards. This allows avoiding a narrow technocratic approach to assessing the success of reforms.

5. Discussion

Given the main research problem, namely, a holistic analysis of existing strategies for modernizing administrative law with a description of educational, technological, and institutional aspects. The study analyzes 53 items of literature in the period from 2017 to 2024 and identifies the main thematic clusters and international strategic models related to the development and modernization of the administrative law system. The first research question concerned the identification of the main administrative and legal mechanisms for combating cybercrime in different countries. To this end, the author identified the main thematic clusters present in scientific literature relating to the process of modernization of administrative law in the framework of combating cybercrime. In particular, the data showed that most studies (n = 38; 73%) pointed to the importance of reforming institutional structures and creating specialized cyberunits within public authorities. The second most frequently mentioned cluster was the optimization of administrative and legal mechanisms for authorizing violations in cyberspace. These results are in line with other works that point to the importance of expanding the powers of administrative bodies in the cybercrime response system.[81] That issue was also emphasized by other scholars who proposed specific optimized mechanisms. In particular, Buçaj et al.[82] and Zybin et al.[83] pointed out the importance of introducing a synthesis of administrative fines, access restrictions, and sanctions against digital service providers. This study also emphasizes that this direction is an important alternative. Another significant cluster (42% of sources; n = 22) was the introduction of digital resources as important objects for recording and responding to cyberincidents. That aspect was also emphasized by other scholars who described the main opportunities of digitalization for ensuring a secure cyberspace.[84,85] It is also shown that international coordination (54%; n = 28) and an optimized training system (33%; n = 17) have become important thematic clusters. In general, the problem of effective training is not new in the scientific space. Other studies have more comprehensively examined the role of the educational system in ensuring effective counteraction to cybercrime by training professionals capable of operating within the context of digital transformation. Their findings are directly aligned with the present study. Specifically, the recent research highlights that improving digital literacy among law enforcement officers, attorneys, legal practitioners, and civil servants facilitates the more precise application of administrative and legal norms to emerging cyberthreats.

Moreover, within the framework of administrative law modernization, education serves as a foundation for developing an interdisciplinary approach that integrates legal, technical, and ethical dimensions in the fight against cybercrime. Contemporary educational programs may incorporate topics such as international cooperation, personal data protection, and cyberhygiene mechanisms. The study

---

[81] ELEGBE, Ifeoluwa. Cybercrime legislation: a comparative analysis of legal frameworks, policy responses and recommendations. 2024. Ibid.
[82] BUÇAJ, Enver, and Kenan IDRIZAJ. The need for cybercrime regulation on a global scale by the international law and cyber convention. 2024. Ibid.
[83] ZYBIN, Serhii, et al. Blockchain technologies and their application in security software development. Sustainable Engineering and Innovation. 2025, 7(1), 209–224. DOI: 10.37868/sei.v7i1.id499.
[84] BATRACHENKO, Tetiana, et al. Cybercrime in the context of the digital age: analysis of threats, legal challenges and strategies. 2024. Ibid.
[85] AL-AMAIREH, Monther Abed-Alrazzaq Musleh. The Role of Cybersecurity in Enhancing the Effectiveness of Law Against Cybercrimes. Revista de Gestão Social e Ambiental. 2024. Ibid.

also notes the emergence of a relatively new thematic cluster (31%; n = 16), consisting of research focused on the use of artificial intelligence technologies and data analytics. Other publications likewise conclude that modern technological tools play a critical role in detecting, documenting, and responding to cybercrime.[86]

The next question concerned the identification of certain geographical and jurisdictional differences in the strategies of legal regulation of cybercrime. Accordingly, the data obtained showed the existence of significant variability in the strategies of legal regulation of cybercrime. They are determined by the level of economic development and the institutional capacity of countries. Such variability correlates with previous findings in the literature on the unevenness of legal responses to global digital security challenges.[87,88,89] Other studies have confirmed the thesis that unified policies in the European Union, based on pan-European legal acts, including the GDPR and relevant EU directives, are preferable.[90,91,92] As noted by[93], a vital trend is the modernization of the regulatory framework for electronic evidence and the simplification of cross-border interaction procedures. Accordingly, such opinions indicate the strengthening of the role of administrative law as a prominent mechanism in the field of harmonization of interstate approaches. The comparison with the countries of Asia, Latin America, and Africa showed the existence of a gap in both the legal framework and institutional readiness to counter cybercrime. This has been emphasized by other scholars who have pointed out the difficulties in establishing effective enforcement systems.[94] Often, in these circumstances, administrative law serves as a declaratory instrument rather than a practical mechanism. The proposed results indicate that several measures implemented in modern research are promising avenues for the next confrontation with cybercrime. First, it is worth highlighting the importance of further strengthening legal norms, combining the efforts of private and public entities to counter cybercrime, increasing international coordination, improving digital security and evidence collection systems, and raising awareness among ordinary citizens about digital crime. In fact, the findings align with the conclusions of other scholars

---

[86] MEENA, Shiv Ram. Sparseness Controlled Proportionate RLS Algorithm for Sparse and Non-Sparse Systems. International Journal of Advanced Networking and Applications. 2024, 15(05), 6101–6108. DOI: 10.35444/ijana.2024.15504.

[87] YERJANOV, Timur Keldeshevich, et al. Legal Issues Related to Combating Cybercrime: Experience of the Republic of Kazakhstan. 2018. Ibid.

[88] KHALYMON, S., and A. PRYTULA. Problems of implementation of whistleblower institution. Ukraine Juridical Tribune Journal. 2019, 9(2), 436–454. Available at: https://ideas.repec.org/a/asr/journl/v9y2019i2p436-454.html (accessed on 09 August 2025).

[89] WANG, Shun-Yung Kevin, et al. Collaboration between Law Enforcement Agencies in Combating Cybercrime: Implications of a Taiwanese Case Study about ATM Hacking. 2020. Ibid.

[90] VULETIĆ, Igor. Criminal Law and the Challenges of Autonomous Intelligence: Substituting a Theory of Guilt with the Division of Labor. In: The Law and Economics of Patent Damages, Antitrust, and Legal Process. 2021. Ibid.

[91] ZYBIN, Serhii, et al. Approach of the Attack Analysis to Reduce Omissions in the Risk Management. Proceedings of Selected Papers of the Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS 2021), Kyiv, Ukraine, January 28, 2021, 2923, 318–328. Available at: http://ceur-ws.org/Vol-2923/paper35.pdf (accessed on 09 August, 2025).

[92] GOLOVIN, Dmytro. Electronic evidence in proving crimes of drugs and psychotropic substances turnover. 2022. Ibid.

[93] NEWHOUSE, William, et al. National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. 2017. Ibid.

[94] MENSAH, Ebenezer Kojo Gyesi. Investigating International Criminal Law and Sovereignty Issues Surrounding the Prosecution of Heads of State for War Crimes and Genocide. 2024. Ibid.

who merely arrange these perspectives differently.[95,96,97] Obviously, this is due to the experience of scholars and the scientific works used which have an impact on the formation of the overall picture of legal concepts. At the same time, some scholars point out the relevance of strengthening criminal and administrative liability for the use of artificial intelligence systems for criminal purposes.[98,99] In their opinion, artificial intelligence tools are extremely promising, including from the point of view of fraudsters, and therefore responding to such a challenge will require significant efforts.[100,101] Therefore, it is worth agreeing with this point of view, since even a superficial analysis of modern research has also allowed us to identify the threat of artificial intelligence in cybercrime as extremely relevant. The results obtained should be interpreted considering a number of methodological limitations. First, although the use of the PRISMA methodology ensured a transparent and reproducible selection of sources, the focus mainly on English-language publications leads to language bias. This means that some relevant developments in the field of administrative and legal regulation of cybersecurity published in other languages may not have been included in the analysis. Second, the study was based on materials indexed in leading international databases (Scopus, Web of Science, Google Scholar, HeinOnline). Despite their broad representativeness, such databases do not fully cover regional legal studies, policy documents and "gray literature," which especially affects the representation of countries with an early or transitional level of development of cybersecurity systems. Third, the corpus of analyzed sources is mainly descriptive and normative in nature. The number of studies that provide causal or quasi-experimental analyses of the effectiveness of administrative and legal reforms in combating cybercrime remains limited. As a result, the research findings reflect general trends, approaches, and regulatory logics rather than direct causal relationships between individual policy decisions and their consequences.

6. Conclusions

The study shows that the modernization of administrative law in the field of combating cybercrime is a complex, multi-level, and contextually determined process. It is determined by the level of institutional capacity of the state, the type of legal system, and the overall level of economic development. The analysis of scientific literature has shown a gradual transition from purely repressive

---

[95] BOUSTA, Rhita, and Yseult MARIQUE. Taking Comparative Administrative Law (Almost) Seriously? Comparative Administrative Law in French & Belgium Legal Education. 2016. Ibid.
[96] DUPONT, Benoît. Enhancing the effectiveness of cybercrime prevention through policy monitoring. 2019. Ibid.
[97] SANNERHOLM, Richard. Rule of Law and Public Administration in Sweden. Law, Politics, Culture. Scandinavian studies in law. 2023, (2023 69), 231–250. DOI: 10.53292/32f26f7c.5b65be00.
[98] CATOTA, Frankie E., M. Granger MORGAN, and Douglas C. SICKER. Cybersecurity education in a developing nation: the Ecuadorian environment. 2019. Ibid.
[99] SEMENETS-ORLOVA, Inna, et al. Organizational Development and Educational Changes Management in Public Sector (Case of Public Administration During War Time). International Journal of Professional Business Review. 2023, 8(4), e01699. DOI: 10.26668/businessreview/2023.v8i4.1699.
[100] PITTIGLIO, Rosanna, et al. Cybersecurity, Personal Data Protection and Crime Prevention from an Italian Perspective. In: The Palgrave Handbook of Corporate Sustainability in the Digital Era. Cham: Springer International Publishing, 2020, pp. 131–156. DOI: 10.1007/978-3-030-42412-1_7.
[101] HASANOVA, Ilhama Zakir kizi. The Role of the Advocate's Motions and Complaints in a Criminal Trial: A Scoping Review. Futurity Economics&Law. 2024, 4(4), 25–41. DOI: 10.57125/fel.2024.12.25.02.

approaches to models of risk-oriented and adaptive regulatory governance, within which administrative law plays a key coordinating and preventive role.

In the short term, pilot measures aimed at strengthening the institutional capacity of public authorities are a priority. These include the creation or strengthening of specialized cyber units, the expansion of administrative sanctions for minor and repeated cyber offenses, and the introduction of digital platforms for recording incidents and collecting electronic evidence.

In the medium term, the key task is to harmonize administrative and legal regulation and to coordinate across state lines. This involves harmonizing national legislation with international standards, particularly the provisions of the Budapest Convention on Cybercrime, improving mechanisms for cross-border information exchange, and clear separation of powers between administrative and criminal law institutions. In the area of training and institutional development, it is advisable to apply a simplified decision-making framework that combines the definition of key competencies (digital law, e-evidence analysis, cyberhygiene), institutional mechanisms for cooperation (memorandums of understanding between universities, regulators, and law enforcement agencies), and basic indicators for evaluating results (quality of training, practical applicability of knowledge, institutional sustainability). This approach contributes to the systematic and replicable nature of educational reforms.

In the long term, the growing use of artificial intelligence and data analytics in administrative law enforcement requires the formation of minimum management standards. These should include requirements for auditability of algorithms, mandatory human control, transparency of automated decisions, and effective mechanisms for reviewing complaints, which is a necessary condition for adhering to the principles of the rule of law. This is particularly relevant in the context of shaping legal regimes for high-risk AI systems, where administrative law must play a key role in ensuring accountability and protecting human rights.

The practical significance of the study lies in the formation of conceptual approaches to the modernization of administrative law in the field of cybersecurity. The identified comparative patterns can be used to improve legislative initiatives, develop effective administrative policies, create specialized cyberunits, as well as train and improve the skills of civil servants and lawyers in the field of digital law.

Further research should move from descriptive analysis to more explanatory and evaluative approaches. Promising are quasi-experimental studies of the effectiveness of cybersecurity institutional reforms, comparative cross-country studies of policy diffusion between continental and Anglo-Saxon legal systems, and empirical audits of the use of artificial intelligence in administrative law enforcement, particularly in automated selection and response to cyber incidents. Expanding the linguistic and regional coverage of sources will enhance the scientific validity of future research.

7. References

AL-AMAIREH, Monther Abed-Alrazzaq Musleh. The Role of Cybersecurity in Enhancing the Effectiveness of Law Against Cybercrimes. Revista de Gestão Social e Ambiental. 2024, 18(8), e06508. DOI: 10.24857/rgsa.v18n8-124.

ALLAH RAKHA, Naeem. Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations. Mexican Law Review. 2024, 23–54. DOI: 10.22201/iij.24485306e.2024.2.18892.

BATRACHENKO, Tetiana, et al. Cybercrime in the context of the digital age: analysis of threats, legal challenges and strategies. Multidisciplinary Science Journal. 2024, 6, 2024ss0212. DOI: 10.31893/multiscience.2024ss0212.

BOUSTA, Rhita, and Yseult MARIQUE. Taking Comparative Administrative Law (Almost) Seriously? Comparative Administrative Law in French & Belgium Legal Education. SSRN Electronic Journal. 2016. DOI: 10.2139/ssrn.2711289.

BREWER, Russell, et al. Universal Communication Strategies. Cybercrime Prevention. Cham: Springer International Publishing, 2019, pp. 35–48. DOI: 10.1007/978-3-030-31069-1_3.
BRODOWSKI, Dominik. The Role of Criminal Law in Regulating Cybercrime and IT Security. In: Law and Technology in a Global Digital Society. Cham: Springer International Publishing, 2022, pp. 233–255. DOI: 10.1007/978-3-030-90513-2_12.
BUÇAJ, Enver, and Kenan IDRIZAJ. The need for cybercrime regulation on a global scale by the international law and cyber convention. Multidisciplinary Reviews. 2024, 8(1), 2025024. DOI: 10.31893/multirev.2025024.
BUSSER, Els De. EU-US Digital Data Exchange to Combat Financial Crime: Fast is the New Slow. German Law Journal. 2018, 19(5), 1251–1267. DOI: 10.1017/s2071832200023026.
CATOTA, Frankie E., M. Granger MORGAN, and Douglas C. SICKER. Cybersecurity education in a developing nation: the Ecuadorian environment. Journal of Cybersecurity. 2019, 5(1). DOI: 10.1093/cybsec/tyz001.
CHERNIAVSKYI, Serhii, et al. Measures to combat cybercrime: analysis of international and Ukrainian experience. Cuestiones Políticas. 2021, 39(69), 115–132. DOI: 10.46398/cuestpol.3969.06.
CHRISTOU, George. The challenges of cybercrime governance in the European Union. European Politics and Society. 2018, 19(3), 355–375. DOI: 10.1080/23745118.2018.1430722.
COLLIER, Ben, et al. Influence, infrastructure, and recentering cybercrime policing: evaluating emerging approaches to online law enforcement through a market for cybercrime services. Policing and Society. 2021, 1–22. DOI: 10.1080/10439463.2021.1883608.
Council of Europe (COE): Convention on Cybercrime. International Legal Materials. 2002, 41(2), 282–302. DOI: 10.1017/s0020782900009918.
DANYLENKO-NEHARA, Yuliia, et al. The ethical aspect of public administration under special regime and sustainable development. Salud, Ciencia y Tecnología-Serie de Conferencias. 2024, 3. DOI: 10.56294/sctconf2024.755.
DEWI SURYANDARI, Wieke. Efforts to Reform Law Enforcement in Tackling Cybercrime. International Journal of Law Social Sciences and Management. 2024, 1(2). DOI: 10.69726/ijlssm.v1i2.27.
DIOP, Serigne Mouhamadane, et al. To Coerce or Not to Coerce? A Quantitative Investigation on Cybersecurity and Cybercrime Legislations Towards Large-Scale Vulnerability Notifications. In: 2019 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW). 2019. DOI: 10.1109/issrew.2019.00085.
DUPONT, Benoît. Enhancing the effectiveness of cybercrime prevention through policy monitoring. Journal of Crime and Justice. 2019, 42(5), 500–515. DOI: 10.1080/0735648x.2019.1691855.
ELEGBE, Ifeoluwa. Cybercrime legislation: a comparative analysis of legal frameworks, policy responses and recommendations. International Journal of Education and Social Science Research. 2024, 07(02), 199–207. DOI: 10.37500/ijessr.2024.7211.
ERIKHA, Annisa, and Ade SAPTOMO. Dilemma of Legal Policy to Address Cybercrime in the Digital Era. Asian Journal of Social and Humanities. 2024, 3(3), 499–507. DOI: 10.59888/ajosh.v3i3.452.
FLOR, Roberto, and Beatrice PANATTONI. Digital criminal investigations in Italy. The intersection between data protection and cybersecurity. New Journal of European Criminal Law. 2023. DOI: 10.1177/20322844231212836.
FORTES, Vinícius Borges, and Salete Oro BOFF. An analysis of cybercrimes from a global perspective on penal law. Revista Brasileira de Direito. 2017, 13(1), 7–24. DOI: 10.18256/2238-0604/revistadedireito.v13n1p7-24.
GILBERT, Chris, and Mercy Abiola GILBERT. Bridging the Gap: Evaluating Liberia's Cybercrime Legislation Against International Standards. International Journal of Research and Innovation in Applied Science. 2024, IX(X), 131–147. DOI: 10.51584/ijrias.2024.910013.
GOLOVIN, Dmytro. Electronic evidence in proving crimes of drugs and psychotropic substances turnover. Access to Justice in Eastern Europe. 2022, 5(2), 1–13. DOI: 10.33327/ajee-18-5.2-n000217.
GUMZEJ, Nina, and Nikola PROTRKA. Evaluation of Digital Evidence in Criminal Proceedings in Croatia with a Focus on Preservation Requirements and Role of Standard Operative

Procedures. In: 2021 44th International Convention on Information, Communication, and Electronic Technology (MIPRO). 2021. DOI: 10.23919/mipro52101.2021.9597136.
HASANOVA, Ilhama Zakir kizi. The Role of the Advocate's Motions and Complaints in a Criminal Trial: A Scoping Review. Futurity Economics&Law. 2024, 4(4), 25–41. DOI: 10.57125/fel.2024.12.25.02.
ILYINA, Anastasiya. Mechanism of Innovation and Investment Development in Modern Economy. Economic Affairs. 2022, 67(4s). DOI: 10.46852/0424-2513.4s.2022.16.
KAVYN, Sviatoslav, Ivan BRATSUK, and Anatoliy LYTVYNENKO. Regulatory and Legal Enforcement of Cyber Security in Countries of the European Union: The Experience of Germany and France. Teisė. 2021, 121, 135–147. DOI: 10.15388/teise.2021.121.8.
KHALYMON, S., and A. PRYTULA. Problems of implementation of whistleblower institution. Ukraine Juridical Tribune Journal. 2019, 9(2), 436–454. Available at: https://ideas.repec.org/a/asr/journl/v9y2019i2p436-454.html (accessed on 09 August 2025).
MEENA, Shiv Ram. Sparseness Controlled Proportionate RLS Algorithm for Sparse and Non-Sparse Systems. International Journal of Advanced Networking and Applications. 2024, 15(05), 6101–6108. DOI: 10.35444/ijana.2024.15504.
MENSAH, Ebenezer Kojo Gyesi. Investigating International Criminal Law and Sovereignty Issues Surrounding the Prosecution of Heads of State for War Crimes and Genocide. SSRN Electronic Journal. 2024. DOI: 10.2139/ssrn.4813323.
NEWHOUSE, William, et al. National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. Gaithersburg, MD: National Institute of Standards and Technology, August 2017. DOI: 10.6028/nist.sp.800-181.
NGET, Makara, et al. Cybercrime's Global and National Dimensions: Policy Frameworks, Challenges, and Future Solutions. Law and Humanities Quarterly Reviews. 2024, 3(4). DOI: 10.31014/aior.1996.03.04.132
NOWACKI, Jeffrey, and Dale WILLITS. An organizational approach to understanding police response to cybercrime. Policing: An International Journal. 2019, 43(1), 63–76. DOI: 10.1108/pijpsm-07-2019-0117.
NUGROHO, Agus, and An An CHANDRAWULAN. Research synthesis of cybercrime laws and COVID-19 in Indonesia: lessons for developed and developing countries. Security Journal. 2022. DOI: 10.1057/s41284-022-00357-y.
ODERIY, Oleksiy, et al. The Impact of EU Criminal Law Policy on the Prevention of Transnational Environmental Crime. Pakistan Journal of Criminology. 2024, 16(3), 1155–1172. DOI: 10.62271/pjc.16.3.1155.1172.
OLIINYK, Olena, et al. Criminal legal and administrative methods of ensuring the economic security of the state in the context of globalization and modernization of the economy. International Journal of Agricultural Extension. 2022, 10(2), 91–103. DOI: 10.33687/ijae.010.00.3867.
PITTIGLIO, Rosanna, et al. Cybersecurity, Personal Data Protection and Crime Prevention from an Italian Perspective. In: The Palgrave Handbook of Corporate Sustainability in the Digital Era. Cham: Springer International Publishing, 2020, pp. 131–156. DOI: 10.1007/978-3-030-42412-1_7.
RAAIJMAKERS, Stephan. Artificial Intelligence for Law Enforcement: Challenges and Opportunities. IEEE Security & Privacy. 2019, 17(5), 74–77. DOI: 10.1109/msec.2019.2925649.
RENAUD, Karen, et al. Cyber Security Responsibilization: An Evaluation of the Intervention Approaches Adopted by the Five Eyes Countries and China. Public Administration Review. 2020, 80(4), 577–589. DOI: 10.1111/puar.13210.
ROY, Reena, and Anil Kumar DIXIT. Legal Framework of Cybercrimes against E-Banking in India. In: Cybersecurity, Law, and Economics. London: Routledge, 2024, pp. 69–90. DOI: 10.4324/9781003517290-7.
S. VITVITSKIY, Sergij, et al. Formation of a new paradigm of anti-money laundering: The experience of Ukraine. Problems and Perspectives in Management. 2021, 19(1), 354–363. DOI: 10.21511/ppm.19(1).2021.30.
SANNERHOLM, Richard. Rule of Law and Public Administration in Sweden. Law, Politics, Culture. Scandinavian studies in law. 2023, (2023 69), 231–250. DOI: 10.53292/32f26f7c.5b65be00.
SEMENETS-ORLOVA, Inna, et al. Organizational Development and Educational Changes Management in Public Sector (Case of Public Administration During War Time).

International Journal of Professional Business Review. 2023, 8(4), e01699. DOI: 10.26668/businessreview/2023.v8i4.1699.
SERGEYEV, Yuriy. Ukrainian Supreme Court Judicial Practice in Cases Arising from Disputes between Foreign Shipowners or Protection and Indemnity Clubs, and Seafarers or Seafarers' Next of Kin. Lex Portus. 2024, 10(3). DOI: 10.62821/lp10303.
SHEVCHUK, O., et al. The Rights to access to Information and National Security in the Ukraine in the System of Human Rights. Revista Juridica Portucalense. 2023, 34, 257–282. Available at: https://revistas.rcaap.pt/juridica/article/view/31229 (accessed on 09 August, 2025).
SIAGIAN, Erwin Sondang. Public-private partnerships in Indonesia: a comprehensive legal framework of significance to action and analysis. Asia Pacific Journal of Public Administration. 2017, 39(1), 72–78. DOI: 10.1080/0142159x.2017.1294395.
SMAILOV, Nurzhigit, et al. Streamlining Digital Correlation-Interferometric Direction Finding with Spatial Analytical Signal. Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska. 2024, 14(3), 43–48. DOI: 10.35784/iapgos.6177.
SORBÁN, Kinga. The role of Internet intermediaries in combatting cybercrime: Organisation and liabilities. Central and Eastern European edem and egov Days. 2022, 335, 19–31. DOI: 10.24989/ocg.v335.1.
STURC, Boris, Tatyana GUROVA, and Sergei CHERNOV. The Specifics and Patterns of Cybercrime in the Field of Payment Processing. International Journal of Criminology and Sociology. 2022, 9, 2021–2030. DOI: 10.6000/1929-4409.2020.09.237.
SVIATUN, Olena V., et al. Combating cybercrime: economic and legal aspects. WSEAS TRANSACTIONS ON BUSINESS AND ECONOMICS. 2021, 18, 751–762. DOI: 10.37394/23207.2021.18.72.
United Nations: Office on Drugs and Crime, World Drug Report. Www.unodc.org. 2021. Available at: https://www.unodc.org/unodc/en/data-and-analysis/wdr2021.html (accessed on 09 August 2025).
VULETIĆ, Igor. Criminal Law and the Challenges of Autonomous Intelligence: Substituting a Theory of Guilt with the Division of Labor. In: The Law and Economics of Patent Damages, Antitrust, and Legal Process. Emerald Publishing Limited, 2021, pp. 111–126. DOI: 10.1108/s0193-589520210000029007.
WANG, Shun-Yung Kevin, et al. Collaboration between Law Enforcement Agencies in Combating Cybercrime: Implications of a Taiwanese Case Study about ATM Hacking. International Journal of Offender Therapy and Comparative Criminology. 2020, 0306624X2095239. DOI: 10.1177/0306624x20952391.
YERJANOV, Timur Keldeshevich, et al. Legal Issues Related to Combating Cybercrime: Experience of the Republic of Kazakhstan. Journal of Advanced Research in Law and Economics. 2018, 8(7), 2286. DOI: 10.14505//jarle.v8.7(29).30.
ZYBIN, Serhii, et al. Approach of the Attack Analysis to Reduce Omissions in the Risk Management. Proceedings of Selected Papers of the Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS 2021), Kyiv, Ukraine, January 28, 2021, 2923, 318–328. Available at: http://ceur-ws.org/Vol-2923/paper35.pdf (accessed on 09 August, 2025).
ZYBIN, Serhii, et al. Blockchain technologies and their application in security software development. Sustainable Engineering and Innovation. 2025, 7(1), 209–224. DOI: 10.37868/sei.v7i1.id499.