INNOVATIONS IN TECHNOLOGY AND SCIENCE EDUCATION
ISSN 2181-371X
https://sr-journals.org/index.php/ITSE

FORMATION OF CYBER COMPETENCIES OF FUTURE EMPLOYEES OF THE MINISTRY OF INTERNAL AFFAIRS IN THE CONTEXT OF DIGITALIZATION OF LAW ENFORCEMENT ACTIVITIES AND THE GROWTH OF CYBER THREATS

Umarov Muxiddin Musinovich,
Head of Department, Doctor of Philosophy in Military Sciences (PhD), Professor

Abstract. The accelerating digitalization of public administration, together with the global expansion of cybercrime, has fundamentally redefined the professional profile required of contemporary law enforcement personnel. This study examines the formation of cyber competencies among future employees of the Ministry of Internal Affairs (MIA) of the Republic of Uzbekistan within the framework of national digital transformation strategies and the international standards on cybersecurity and cybercrime prevention. The aim of the research is to develop a scientifically grounded pedagogical model for the systematic formation of legal, technical, ethical, analytical, and practical cyber competencies in future MIA employees. The methodology combines a literature review of academic and policy sources, a systematic and content analysis of normative-legal documents, comparative analysis of international training frameworks (UNODC, INTERPOL, ITU, OSCE, Council of Europe, OECD), pedagogical modelling, and logical generalization. The principal results include a structured pedagogical model containing six interconnected components (target, content, methodological, practical, diagnostic, and outcome), a competency framework comprising twelve cyber competencies, and a set of measurable assessment indicators. The scientific novelty lies in integrating the requirements of national digital and cybersecurity legislation, the international best practices in capacity-building, and modern pedagogical methods into a coherent training architecture aimed at lawful, ethical, and effective professional performance in digital law enforcement environments. The practical significance of the study is reflected in its applicability to professional education programs, in-service training, and continuing professional development of MIA personnel.

Keywords: cyber competencies, law enforcement education, digital policing, cyber threats, Ministry of Internal Affairs, cybersecurity, digital evidence, professional training, cybercrime prevention, digital literacy.

Annotatsiya. Davlat boshqaruvining jadal raqamlashtirilishi kiberjinoyatchilikning global kengayishi bilan birga zamonaviy huquqni muhofaza qiluvchi organlar xodimlari uchun talab qilinadigan kasbiy qiyofani tubdan qayta belgilab berdi. Ushbu tadqiqotda O‘zbekiston Respublikasi Ichki ishlar vazirligi (IIV) bo‘lajak xodimlarining kiberkompetensiyalarini shakllantirish masalasi milliy raqamli transformatsiya strategiyalari hamda kiberxavfsizlik va kiberjinoyatchilikning oldini olish bo‘yicha xalqaro standartlar doirasida ko‘rib chiqiladi. Tadqiqotning maqsadi - IIV bo‘lajak xodimlarida huquqiy, texnik, etik, tahliliy va amaliy kiberkompetensiyalarni tizimli shakllantirish uchun ilmiy asoslangan pedagogik modelni ishlab chiqishdan iborat. Metodologiya akademik va siyosiy manbalarni o‘rganish, normativ-huquqiy hujjatlarning tizimli va mazmuniy tahlili, xalqaro o‘qitish tizimlarini (BMTning Giyohvand moddalar va jinoyatchilik bo‘yicha boshqarmasi, INTERPOL, ITU, YeXHT, Yevropa Kengashi, IHTT) qiyosiy tahlil qilish, pedagogik modellashtirish va mantiqiy umumlashtirishni o‘z ichiga oladi. Asosiy natijalar sifatida oltita o‘zaro bog‘liq komponentni (maqsadli, mazmunli, metodologik, amaliy, diagnostik va natijaviy) o‘z ichiga olgan

tarkibiy pedagogik model, o‘n ikkita kiberkompetensiyadan iborat kompetensiyalar doirasi va o‘lchanadigan baholash ko‘rsatkichlari to‘plami taqdim etilgan. Ilmiy yangilik - milliy raqamli va kiberxavfsizlik qonunchiligi talablarini, salohiyatni oshirish bo‘yicha xalqaro ilg‘or tajribalarni va zamonaviy pedagogik metodlarni raqamli huquqni muhofaza qilish muhitida qonuniy, etik va samarali kasbiy faoliyatni ta’minlashga qaratilgan yaxlit o‘quv arxitekturasiga birlashtirishdan iborat. Tadqiqotning amaliy ahamiyati uning kasbiy ta’lim dasturlarida, malaka oshirish kurslarida va IIV xodimlarining uzluksiz kasbiy rivojlanishida qo‘llanilishi bilan belgilanadi.

Kalit so‘zlar: kiberkompetensiyalar, huquqni muhofaza qilish ta’limi, raqamli politsiya faoliyati, kibertahdidlar, Ichki ishlar vazirligi, kiberxavfsizlik, raqamli dalillar, kasbiy tayyorgarlik, kiberjinoyatchilikning oldini olish, raqamli savodxonlik.

Аннотация. Ускоренная цифровизация государственного управления в сочетании с глобальным расширением киберпреступности коренным образом переопределила профессиональный профиль, необходимый современным сотрудникам правоохранительных органов. В данном исследовании рассматривается формирование киберкомпетенций у будущих сотрудников Министерства внутренних дел (МВД) Республики Узбекистан в рамках национальных стратегий цифровой трансформации и международных стандартов по кибербезопасности и профилактике киберпреступности. Цель исследования заключается в разработке научно обоснованной педагогической модели систематического формирования правовых, технических, этических, аналитических и практических киберкомпетенций у будущих сотрудников МВД. Методология включает обзор академических и политических источников, системный и содержательный анализ нормативно-правовых актов, сравнительный анализ международных структур обучения (УНП ООН, ИНТЕРПОЛ, МСЭ, ОБСЕ, Совет Европы, ОЭСР), педагогическое моделирование и логическое обобщение. Основные результаты включают структурированную педагогическую модель, содержащую шесть взаимосвязанных компонентов (целевой, содержательный, методологический, практический, диагностический и результативный), структуру компетенций, состоящую из двенадцати киберкомпетенций, и набор измеримых показателей оценки. Научная новизна заключается в интеграции требований национального законодательства в области цифровизации и кибербезопасности, передового международного опыта по наращиванию потенциала и современных педагогических методов в целостную архитектуру обучения, направленную на законное, этичное и эффективное профессиональное исполнение обязанностей в цифровой правоохранительной среде. Практическая значимость исследования отражена в его применимости к программам профессионального образования, курсам повышения квалификации и непрерывному профессиональному развитию персонала МВД.

Ключевые слова: киберкомпетенции, правоохранительное образование, цифровая полиция, киберугрозы, Министерство внутренних дел, кибербезопасность, цифровые доказательства, профессиональная подготовка, профилактика киберпреступности, цифровая грамотность.

1. Introduction

The digital transformation of public administration and the dynamic expansion of cyberspace have produced structural changes in the conditions under which internal affairs bodies operate. The expansion of digital public services, the proliferation of online communication channels between citizens and the state, the digitization of operational records and documentation, and the growth of cyber-dependent and cyber-enabled offences require a corresponding evolution of the professional preparation of law enforcement personnel. In the Republic of Uzbekistan, this transformation is anchored in the “Digital Uzbekistan 2030” strategy approved by the Decree of the President of the Republic of Uzbekistan No. UP-6079 of 5 October 2020, which establishes the digitalization of public administration, infrastructure, and human capital as a priority direction of state policy [1]. The adoption of the Law of the Republic of Uzbekistan No. ZRU-764 “On Cybersecurity” of 15 April 2022

reinforced this trajectory by formalizing the legal framework for the protection of national information infrastructure and the prevention of cyber threats [2].

The research problem stems from a discernible gap between the professional functions that future employees of the Ministry of Internal Affairs are expected to perform in a digitalized environment and the level of cyber competencies systematically developed within their professional education. Although digital instruments have become integral to law enforcement workflows-from communication with citizens and the handling of digital evidence to interagency information exchange-pedagogical models that integrate legal, technical, ethical, and analytical preparation in a coherent framework remain underdeveloped in many national contexts. The challenge is amplified by the rapid evolution of cyber threats, which compels educational programs to maintain continuous adaptation rather than rely on static curricula.

The degree of scientific development of the issue is uneven. The conceptual literature on community policing, professional ethics in law enforcement, and digital forensics is well established. International organizations, including the United Nations Office on Drugs and Crime (UNODC), the International Telecommunication Union (ITU), the Organization for Security and Co-operation in Europe (OSCE), INTERPOL, the Council of Europe, and the Organisation for Economic Co-operation and Development (OECD), have developed substantive policy and capacity-building instruments that address the training of law enforcement officers in the digital domain [3; 4; 5; 6; 7]. National legal frameworks in Uzbekistan, particularly those concerning cybersecurity and the protection of personal data, are increasingly aligned with international standards [2; 8]. Nevertheless, integrative pedagogical models that translate these external frameworks into the educational reality of the MIA system require further elaboration.

The aim of the research is to develop a scientifically grounded pedagogical model for the formation of cyber competencies of future employees of the Ministry of Internal Affairs in the context of digitalization and the growth of cyber threats. The objectives are to analyze the legal, policy, and academic foundations of cyber-related training in law enforcement; to identify cyber competencies essential for future MIA officers; to formulate a structured pedagogical model with target, content, methodological, practical, diagnostic, and outcome components; to propose assessment criteria and indicators; and to outline the conditions for integrating the model into MIA professional education.

The object of the study is the professional preparation of future employees of the Ministry of Internal Affairs. The subject of the study is the pedagogical conditions, content, and methods for forming cyber competencies under conditions of digitalization and increasing cyber threats. The scientific novelty lies in the integration of national legislative requirements, international training principles, and pedagogical modelling into a single, internally consistent framework that addresses lawful, ethical, and analytically informed performance in digital law enforcement environments. The practical significance is reflected in the applicability of the model to professional education curricula, specialized training, in-service development, and interagency cooperation programs.

2. Literature Review and Policy Background

The formation of cyber competencies in law enforcement is positioned at the intersection of three principal bodies of literature: legal-policy frameworks on cybersecurity and cybercrime, academic and institutional studies on professional training of police, and empirical research on the digital transformation of public administration.

National policy in the Republic of Uzbekistan provides a clear normative anchor. The Decree of the President No. UP-6079 of 5 October 2020 approving the “Digital Uzbekistan 2030” strategy operationalizes a long-term vision for the digital economy, e-government, digital education, and digital infrastructure [1]. The Law No. ZRU-764 “On Cybersecurity” of 15 April 2022 introduced unified legal categories-cyberspace, cyber threat, cyberattack, cybersecurity incident, and critical information infrastructure-and assigned authorized state functions in this field [2]. The Law No. ZRU-547 “On Personal Data” of 2 July 2019 (with subsequent amendments) defines the legal regime for the processing and protection of personal data, including data localization requirements introduced by later amendments [8]. The Strategy for the Development of Artificial Intelligence Technologies until 2030,

approved by the Decree of the President No. PQ-358 of 14 October 2024, complements this framework by addressing the regulatory and capacity dimensions of artificial intelligence [9]. Taken together, these acts form a coherent national context within which the cyber competencies of MIA personnel must be conceptualized.

The international legal-policy environment offers consolidated reference points. The Council of Europe Convention on Cybercrime (CETS No. 185), opened for signature in Budapest on 23 November 2001 and entered into force on 1 July 2004, remains the principal binding international instrument harmonizing substantive criminal offences, procedural powers for digital investigations, and international cooperation in cybercrime cases [10]. The UNODC Global Programme on Cybercrime systematically supports states in the strengthening of legal frameworks, capacity-building of law enforcement personnel, the management of digital evidence, and prevention activities, providing training catalogues and operational guidance [4]. The ITU Global Cybersecurity Index 2024 establishes a five-pillar measurement framework-legal, technical, organizational, capacity development, and cooperation-and treats human capacity-building as an indispensable dimension of national cybersecurity [3]. INTERPOL's Cybercrime Capacity Building activities provide structured training in digital forensics, open-source intelligence, and operational cooperation, frequently delivered in partnership with academic institutions [11]. OECD analyses of digital skills, including the report on Uzbekistan, emphasize that the development of digital competencies must be aligned with sectoral demand and institutional reform [7].

The academic literature on professional training in policing and digital forensics demonstrates that effective preparation in cyber-related domains depends on the integration of legal knowledge, technical skills, ethical reasoning, and contextual judgment. The classical conceptualization of community policing by R. Trojanowicz and B. Bucqueroux underscores the relational dimension of policing, which has been extended in later scholarship to include trust-building in digital environments [12]. Reviews in digital forensics emphasize the cross-cutting nature of digital evidence and the necessity of standardized, lawful, and forensically sound procedures throughout the investigative chain [13]. Specialized training programs offered by national institutions, such as the Federal Law Enforcement Training Centers, illustrate how targeted educational design can systematically align competencies with operational requirements while respecting legal limits [14]. The OSCE/UNODC guidebook on police-public partnerships further indicates that the credibility of law enforcement in digital environments depends both on technical competence and on legitimate, transparent engagement with the public [6].

A critical reading of these sources shows convergence around several propositions: cyber competencies must be conceived as a system of interrelated capabilities rather than isolated skills; legal and ethical limits are not subordinate components but constitutive of professional cyber readiness; and capacity-building requires continuous updating in response to technological change. These propositions provide the conceptual foundation for the model proposed in the present study.

3. Research Methodology

The research employs a complementary set of methods consistent with the analytical and design-oriented character of the study.

The literature review supports the systematic identification of academic and institutional contributions on cyber competencies, digital policing, cybercrime prevention, and law enforcement education. The content analysis of normative-legal documents addresses the legislative and policy frameworks of the Republic of Uzbekistan and selected international instruments, with attention to the legal categories that determine the lawful conduct of digital law enforcement work. The comparative analysis examines international training frameworks-UNODC, INTERPOL, ITU, OSCE, Council of Europe, and OECD-in order to identify transferable principles rather than to advocate mechanical replication. The systematic analysis treats the educational preparation of MIA personnel as an integrated system in which legal, technical, ethical, and practical components interact. Pedagogical modelling provides the design vocabulary for the proposed framework, organizing it into target, content, methodological, practical, diagnostic, and outcome components. Generalization and logical

analysis ensure internal coherence between the literature, the legal framework, the proposed model, and the assessment indicators.

Each method is selected for a defined function. The literature review and the content analysis establish the empirical and normative bases of the study; the comparative method ensures that the model engages with international best practices; pedagogical modelling translates these inputs into an applied training architecture; and logical analysis guarantees that the resulting framework is internally consistent and verifiable.

4. Main Body

4.1. The concept of cyber competencies in law enforcement education

In the present study, cyber competencies are understood as a structured system of legal, technical, ethical, analytical, communicative, and practical capabilities that enable a future law enforcement officer to perform professional duties lawfully and effectively in digital environments. This understanding extends beyond general digital literacy, which refers to the basic ability to use digital tools, by integrating professional responsibilities such as the lawful handling of digital information, the recognition and prevention of cybercrime, the management of digital evidence within procedural limits, and the ability to engage with citizens through digital channels in a manner consistent with public service ethics.

Cyber competencies thus combine four interrelated dimensions. The legal dimension includes knowledge of the constitutional, criminal, administrative, and sectoral norms governing digital activity; it ensures that professional action remains within lawful boundaries. The technical dimension comprises the operational understanding of information systems, digital evidence, and cyber-hygiene practices necessary for investigative and preventive tasks. The ethical dimension encompasses the standards governing privacy, proportionality, and the responsible exercise of digital powers. The analytical dimension entails critical reasoning, source verification, and risk assessment in digital contexts. Together, these dimensions distinguish professional cyber competencies of a law enforcement officer from the digital literacy expected of an ordinary citizen.

4.2. The impact of digitalization on the activities of internal affairs bodies

Digitalization reshapes internal affairs activity along several lines. Communication with citizens increasingly takes place through digital channels, which requires officers to apply procedural and ethical standards to interactions that previously occurred face-to-face. The digitization of documentation creates an information environment in which procedural compliance, secure storage, and authenticity of records become central professional concerns. Online crime reporting and the digital intake of complaints alter the early stages of investigation, requiring officers to recognize digital signals and route information appropriately.

Digital evidence has become a routine element across virtually all categories of crime, not only cyber-dependent offences [4; 13]. Data-driven decision-making, supported by interoperable information systems, requires officers to interpret and contextualize digital information rather than rely solely on field observation. Cooperation between institutions-both intra-state and cross-border-is increasingly mediated through digital platforms, which implicates legal regimes for personal data protection [8] and international cooperation [10]. New risks accompany these changes: misuse of personal data, harmful online content, identity-related fraud, and threats to critical information infrastructure. The evolving environment requires that professional preparation move from peripheral coverage of digital topics to a structured, integrated treatment.

4.3. Main cyber threats relevant to law enforcement training

A number of cyber threats are particularly pertinent to law enforcement education from a legal, preventive, and defensive perspective. These include cyber fraud, identity theft, illegal access to digital systems, online harassment and exploitation, the misuse of personal data, social engineering as a category of risk, threats against public institutions, and the dissemination of digital misinformation and harmful online content. The Council of Europe Convention on Cybercrime provides authoritative categories for substantive offences, including offences against the confidentiality, integrity, and availability of computer data and systems, computer-related fraud, and content-related offences [10].

UNODC training materials and reports systematically address these categories in the context of investigation, prosecution, and prevention [4].

The educational treatment of these threats must remain strictly preventive, defensive, and academic. The objective is to equip future officers with the conceptual, legal, and procedural understanding necessary to recognize, investigate, and prevent harm; not to provide operational knowledge that could be misused. Educational programs must also address contemporary phenomena such as digital misinformation, which can affect public order and trust in institutions, while preserving freedom of expression and information rights.

4.4. The role of cybersecurity, digital literacy, and digital evidence awareness in professional training

Future MIA employees require a baseline level of cybersecurity literacy that includes safe authentication practices, awareness of social engineering risks, and the secure handling of work-related digital information. They require an operational understanding of digital evidence: its potential sources, the legal limits on its acquisition, and the principles of preservation, integrity, and chain of custody. They require an explicit grounding in the legal and ethical limits of digital work, including the requirements arising from the legislation on personal data and cybersecurity [2; 8]. They require communicative competencies adapted to digital environments, where tone, accuracy, and professional restraint shape the perception of police legitimacy. Finally, they require the ability to cooperate with specialized cybercrime units and with non-police institutions-prosecution authorities, courts, the State Security Service as the authorized cybersecurity body [2], and where relevant, the State Personalization Centre under the Cabinet of Ministers as the authorized body for personal data [8].

4.5. Problems in preparing future employees of the Ministry of Internal Affairs for digital law enforcement activities

The literature and policy analysis suggest several recurring challenges. First, cyber-related content is often integrated into curricula in a fragmentary manner rather than as a coherent, sequenced strand. Second, scenario-based and simulation-based training, although recognized in international programs as essential to skill consolidation [4; 11], remains underused in many national systems. Third, digital ethics and personal data protection are sometimes treated as supplementary topics, despite their constitutive role in lawful digital practice [8]. Fourth, interdisciplinary teaching that combines legal, technical, psychological, and communicative perspectives is uncommon, although the operational reality of digital law enforcement requires precisely this combination. Fifth, structured cooperation between educational institutions and specialized cybersecurity bodies is often informal rather than institutionalized. Sixth, the rapid evolution of cyber threats requires regular curriculum updating, which is difficult to achieve through standard academic revision cycles. The present study treats these as design problems to be addressed through the proposed model rather than as reasons for criticism alone.

4.6. International experience in cyber training for police and law enforcement agencies

The international experience offers transferable principles. The UNODC Global Programme on Cybercrime emphasizes the integration of legal frameworks, capacity-building, international cooperation, and prevention as four mutually reinforcing pillars; its training programs combine legal, technical, and procedural elements with attention to digital evidence and ethical standards [4]. The ITU Global Cybersecurity Index 2024 highlights capacity development as one of five constitutive pillars of national cybersecurity and provides a comparative benchmark for national performance [3]. INTERPOL's Cybercrime Capacity Building initiatives demonstrate the value of sustained training-encompassing digital forensics, open-source intelligence, and operational cooperation-delivered in partnership with academic institutions [11]. The OSCE/UNODC guidebook on police-public partnerships, while not exclusively focused on cyber matters, offers principles of legitimate engagement that are directly applicable to digital interactions between police and the public [6]. The Council of Europe Convention on Cybercrime serves as a normative reference that aligns substantive offences and procedural powers across jurisdictions [10].

For Uzbekistan, the relevance of these instruments lies less in formal accession or membership and more in the principles they articulate: integration of legal and technical knowledge, scenario-based

training, ethical anchoring, interdisciplinary structure, and continuous adaptation. UNODC training activities for Central Asian law enforcement and prosecutorial practitioners have already demonstrated the operational feasibility of such adaptation [15].

4.7. The need to integrate cyber competencies into professional education programs

The integration of cyber competencies into professional education is not a question of adding new modules to existing curricula but of redesigning the architecture of training. Basic professional training should include a foundational strand on legal frameworks, cybersecurity literacy, and digital evidence awareness. Specialized training should address advanced topics-digital forensics, cybercrime investigation, work with personal data-within strict legal and ethical limits. Continuing professional development should ensure that practicing officers regularly update their knowledge as threats evolve [3; 4]. Scenario-based exercises should bridge the gap between theoretical knowledge and operational performance, reflecting the design principles used in international capacity-building [11]. Interdisciplinary modules should combine legal, technical, psychological, and communicative elements. Practical cooperation with cybersecurity bodies should be structurally embedded rather than left to ad hoc arrangements.

5. Proposed Model for Developing Cyber Competencies

The proposed pedagogical model organizes the formation of cyber competencies into six interconnected components.

5.1. Target component

The target component defines the principal goal of the model: to form, in future employees of the Ministry of Internal Affairs, a coherent system of legal, digital, cybersecurity, ethical, analytical, and practical competencies necessary for the lawful and effective performance of professional duties in conditions of digitalization and increasing cyber threats. This goal subordinates all subsequent components and ensures that the formation of competencies is framed by the principles of legality, respect for human rights, and professional ethics.

5.2. Content component

The content component covers the legal foundations of cybersecurity and cybercrime prevention, including the Law on Cybersecurity, the Law on Personal Data, and relevant provisions of the Criminal Code and the Code of Administrative Liability of the Republic of Uzbekistan; the digitalization of law enforcement activities and its implications for procedural and ethical standards; the typology of cybercrime from a legal and educational perspective, drawing on the conceptual categories of the Council of Europe Convention on Cybercrime; digital evidence awareness, including standards of acquisition, preservation, and integrity; personal data protection and privacy under the national framework and international references; cybersecurity hygiene at a level appropriate to professional duties; ethical limits of digital investigations; the responsible use of artificial intelligence and digital tools, with reference to the national AI strategy [9]; media and information literacy; and interagency cooperation in cybercrime prevention.

5.3. Methodological component

The methodological component justifies a combination of pedagogical methods. Case studies allow students to analyze authentic or realistic situations within a controlled educational environment. Scenario-based training and simulation exercises consolidate knowledge by recreating professional contexts in which legal, technical, and ethical considerations interact. Problem-based learning develops analytical autonomy, encouraging students to formulate solutions in the absence of predefined answers. Digital safety modules build cybersecurity literacy systematically. The analysis of real legal cases-within the bounds of confidentiality and ethics-anchors learning in authentic professional reasoning. Interdisciplinary training combines legal, technical, psychological, and ethical perspectives. Guided discussion and reflective analysis support the consolidation of professional judgment. Cooperation with cybersecurity specialists provides exposure to operational realities and contemporary threat landscapes. The selected methods are consistent with the international standards of capacity-building [4; 11] and with the conceptual literature on professional learning in policing [12].

5.4. Practical training component

The practical training component encompasses learning activities that translate competencies into observable performance: the analysis of digital risk situations; simulated communication with citizens in digital environments, including the formal handling of online complaints; exercises on the safe handling of digital information; legal analysis of cybercrime cases drawn from public sources; practical tasks on the lawful and procedurally correct documentation of digital incidents; and interdisciplinary training that combines legal, technical, psychological, and ethical elements. The practical component is designed to remain strictly within educational and lawful boundaries; it does not include technical instructions on hacking, exploitation, or other harmful operations.

5.5. Diagnostic and assessment component

The diagnostic component combines several assessment instruments: tests on legal and regulatory awareness; situational tasks measuring the application of legal and ethical reasoning to digital scenarios; case analysis assignments; practical scenario assessments observing performance under simulated conditions; reflective reports requiring students to articulate their reasoning; oral defense of solutions; assessment of ethical decision-making, including responses to sensitive scenarios; and evaluation of teamwork and interagency cooperation readiness. Assessment is conducted at entry, intermediate, and final stages to capture progression rather than only end-point performance.

5.6. Expected results

The model is designed to produce identifiable outcomes: improved cybersecurity literacy at a level appropriate to professional duties; an enhanced understanding of cybercrime prevention; increased readiness to operate in digital law enforcement environments; improved awareness of digital evidence and the procedural limits associated with it; stronger legal and ethical responsibility; an improved ability to identify digital risks; and structured readiness to cooperate with specialized cybercrime units and other institutions.

6. Cyber Competency Framework

The framework consolidates twelve cyber competencies that operationalize the model.

Basic cybersecurity literacy denotes the ability to apply elementary cyber-hygiene practices in professional and personal digital activity, including awareness of common risk categories such as social engineering. **Understanding of cybercrime and cyber threats** refers to the conceptual capacity to recognize and classify offences within the legal categories of national legislation and the Council of Europe Convention on Cybercrime [10]. **Digital evidence awareness** covers the principles of acquisition, preservation, and integrity of digital evidence within procedural limits [4; 13]. **Safe handling of digital information** is the routine application of professional standards to the storage, transmission, and protection of work-related digital information.

Knowledge of legal and ethical limits in digital investigations denotes the explicit understanding of constitutional, criminal, administrative, and sectoral norms applicable to digital activities, including those arising from the Law on Personal Data [8] and the Law on Cybersecurity [2]. **Ability to cooperate with cybercrime units and other institutions** comprises procedural knowledge and communicative skills required for effective cooperation with specialized internal and external bodies. **Critical thinking in the digital environment** is the disciplined evaluation of digital sources, signals, and patterns under conditions of uncertainty.

Media and information literacy is the ability to assess the credibility, provenance, and possible distortion of information in digital media. **Protection of personal data and privacy** denotes the routine professional respect for data protection principles in the planning and execution of digital tasks [8]. **Responsible use of artificial intelligence and digital tools** covers awareness of the capabilities, limits, and risks of AI-assisted instruments in law enforcement, in line with the priorities articulated in the national AI strategy [9]. **Communication with citizens in digital environments** is the capacity to maintain professional, lawful, and ethically appropriate interaction with the public via digital channels. **Interagency cooperation skills** complete the framework by integrating legal, procedural, and communicative competencies necessary for joint action.

These competencies are interdependent rather than discrete. A deficit in one area, particularly in legal or ethical foundations, undermines the legitimacy of performance in technical or operational areas.

7. Assessment Criteria and Indicators

The evaluation of cyber competencies is structured around nine criteria, each accompanied by measurable or observable indicators.

Legal and regulatory awareness is evaluated by the accurate identification of applicable norms in given scenarios, the ability to articulate the relationship between national legislation and international instruments, and the recognition of legal limits in digital activities.

Cybersecurity literacy is evaluated by the demonstrated application of cyber-hygiene principles in scenario-based tasks, the recognition of common risk categories, and the appropriate response to simulated incidents within an educational setting.

Ability to identify digital risks is evaluated by the capacity to recognize and prioritize risks within structured scenarios, the use of risk categories grounded in international frameworks [3; 4], and the formulation of preventive recommendations.

Understanding of cybercrime prevention is evaluated by the correct application of legal categories from national and international instruments, the design of preventive measures appropriate to the situation, and the integration of legal and ethical considerations.

Digital evidence awareness is evaluated by the demonstration of correct procedural reasoning in scenarios involving the identification, preservation, and integrity of digital evidence, in line with international guidance [4; 13].

Ethical responsibility is evaluated by the quality of decision-making in scenarios involving conflicts between effectiveness and legality, by reflective justification of choices, and by behaviour consistent with professional ethics.

Practical readiness for digital law enforcement tasks is evaluated by performance in simulation exercises that combine legal, technical, and communicative elements; by the appropriate handling of digital documentation; and by lawful and proportionate response to evolving scenarios.

Ability to work with citizens in the digital environment is evaluated through simulated interactions assessing accuracy, professional tone, ethical handling of personal information, and lawful use of digital communication channels.

Interagency cooperation skills are evaluated by the demonstrated knowledge of partner institutions' functions, the ability to formulate cooperation requests within procedural and legal limits, and the capacity to coordinate with internal and external partners in joint scenarios.

The indicators are designed to be observable, replicable, and aligned with the principles of formative and summative assessment.

8. Discussion

The proposed model rests on a set of explicit scientific foundations. It synthesizes the principles articulated by international frameworks in cybersecurity capacity-building [3; 4; 11] with the legal and policy environment of the Republic of Uzbekistan [1; 2; 8; 9]. It draws on the conceptual literature on policing and digital forensics [12; 13] and on the institutional design of structured law enforcement training [14]. The model is internally coherent: each component logically follows from the previous one, and the assessment criteria correspond to the competencies defined in the framework.

In the educational system of the Ministry of Internal Affairs, the model can be adapted in several ways. It can serve as the conceptual basis for the design of a dedicated cyber-competency strand within bachelor-level programs. It can be integrated into specialized programs for officers entering investigative or preventive units that interact with digital environments. It can structure short-cycle in-service training and continuing professional development programs designed to update competencies in response to evolving threats. It can also support the formalization of cooperation between MIA educational institutions and the authorized state body in cybersecurity [2], the State Personalization Centre [8], and academic institutions specializing in law and information security.

Several limitations should be noted. The model is conceptual and pedagogical; its implementation requires institutional decisions concerning curricula, resources, and teaching staff that are beyond the scope of an academic article. The empirical validation of the model-through pilot implementation, longitudinal evaluation, and comparative testing-remains a task for future research. Statistical claims about the prevalence of specific cyber threats or about the effectiveness of particular training methods in the Uzbek context are not asserted here, since reliable, peer-reviewed empirical data tailored to that context were not identified within the scope of this study. Where comparative claims are made, they refer to general principles documented in the cited international sources rather than to country-specific outcomes. Future research should pursue the empirical validation of the model, the elaboration of methodological standards for scenario-based training in Uzbek MIA institutions, and the development of evidence-based curriculum-update mechanisms responsive to changing cyber threats.

9. Conclusion

The study has examined the formation of cyber competencies of future employees of the Ministry of Internal Affairs of the Republic of Uzbekistan under conditions of digitalization and the growth of cyber threats. The principal findings are threefold. First, the legal and policy environment of Uzbekistan-anchored in the "Digital Uzbekistan 2030" strategy, the Law on Cybersecurity, the Law on Personal Data, and the Strategy for the Development of Artificial Intelligence Technologies until 2030-provides a coherent normative basis for the development of cyber competencies in MIA personnel. Second, international frameworks developed by UNODC, ITU, INTERPOL, OSCE, the Council of Europe, and OECD articulate transferable principles, including the integration of legal and technical knowledge, scenario-based training, ethical anchoring, and continuous adaptation. Third, an internally consistent pedagogical model can be constructed by combining target, content, methodological, practical, diagnostic, and outcome components and by aligning them with a competency framework and observable assessment indicators.

The theoretical significance of the study lies in the conceptualization of cyber competencies as a structured system encompassing legal, technical, ethical, analytical, and practical dimensions. The practical significance is reflected in the applicability of the model to professional education, specialized training, in-service development, and interagency cooperation programs of the Ministry of Internal Affairs. The contribution of the proposed model consists in offering a coherent design that integrates national legislative requirements, international best practices, and pedagogical methods within a unified architecture. Possible implementation areas include MIA higher educational institutions, professional development programs, and joint training initiatives with specialized state bodies.

The principal limitation of the study is its conceptual and design-oriented character; the empirical testing of the model requires further work. Directions for further research include the pilot implementation of the model in MIA educational institutions, the empirical evaluation of its outcomes, the development of context-specific scenario libraries within strict ethical and legal limits, and the elaboration of mechanisms for the continuous updating of curricula in response to evolving cyber threats.

References

1. Decree of the President of the Republic of Uzbekistan No. UP-6079 of 5 October 2020 "On the approval of the 'Digital Uzbekistan 2030' strategy and measures for its effective implementation." National Database of Legislation of the Republic of Uzbekistan. Available at: https://lex.uz/
2. Law of the Republic of Uzbekistan No. ZRU-764 of 15 April 2022 "On Cybersecurity." National Database of Legislation of the Republic of Uzbekistan. Available at: https://lex.uz/en/docs/6997403
3. International Telecommunication Union. (2024). *Global Cybersecurity Index 2024*. Geneva: ITU. Available at: https://www.itu.int/epublications/publication/global-cybersecurity-index-2024
4. United Nations Office on Drugs and Crime. (n.d.). *Global Programme on Cybercrime*. Vienna: UNODC. Available at: https://www.unodc.org/unodc/en/cybercrime/home.html

5. Organisation for Economic Co-operation and Development. (2023). *Digital Skills for Private Sector Competitiveness in Uzbekistan*. Paris: OECD Publishing. Available at: https://www.oecd.org/
6. Murphy, C. (2022). *Good Practices in Building Police-Public Partnerships*. 2nd edition. SPMU Publication Series, Vol. 4. Vienna: OSCE Secretariat, Transnational Threats Department, Strategic Police Matters Unit, in cooperation with UNODC. Available at: https://www.osce.org/files/f/documents/8/4/32547.pdf
7. Organisation for Economic Co-operation and Development. (2024). *Roadmap for Sustainable Investment Policy Reforms in Uzbekistan*. Paris: OECD Publishing. Available at: https://www.oecd.org/
8. Law of the Republic of Uzbekistan No. ZRU-547 of 2 July 2019 "On Personal Data" (with subsequent amendments). National Database of Legislation of the Republic of Uzbekistan. Available at: https://lex.uz/docs/4396428
9. Decree of the President of the Republic of Uzbekistan No. PQ-358 of 14 October 2024 "On the Approval of the Strategy for the Development of Artificial Intelligence Technologies until 2030." Government of the Republic of Uzbekistan. Available at: https://gov.uz/
10. Council of Europe. (2001). *Convention on Cybercrime* (CETS No. 185). Budapest: Council of Europe. Available at: https://www.coe.int/en/web/cybercrime/the-budapest-convention
11. INTERPOL. (n.d.). *Cybercrime Capacity Building*. Lyon: INTERPOL. Available at: https://www.interpol.int/en/Crimes/Cybercrime/Cyber-capabilities-development
12. Trojanowicz, R., & Bucqueroux, B. (1990). *Community Policing: A Contemporary Perspective*. Cincinnati, OH: Anderson Publishing.
13. Arshad, H., Jantan, A. B., & Abiodun, O. I. (2018). Digital forensics: Review of issues in scientific validation of digital evidence. *Journal of Information Processing Systems*, 14(2), 346–376. Available at: https://www.jips-k.org/
14. Federal Law Enforcement Training Centers. (n.d.). *Digital Forensics Investigator and Examiner Programs*. U.S. Department of Homeland Security. Available at: https://www.fletc.gov/
15. United Nations Office on Drugs and Crime, Regional Office for Central Asia. (2024). *Building cybersecurity capacity: UNODC's training initiative for Central Asian prosecutors*. Available at: https://www.unodc.org/roca/en/