УДК 342.9:351.74:004.056
DOI https://doi.org/10.32782/klj/2026.3.35

Співак М. В.,
доктор політичних наук, професор,
професор кафедри адміністративного права та процесу
Національної академії внутрішніх справ
ORCID: 0000-0002-9471-7154

Дубіна О. М.,
доктор філософії (PhD) у галузі знань право,
начальник відділу Департаменту кіберполіції
Національної поліції України
ORCID: 0000-0002-3654-1920

ТРАНСФОРМАЦІЯ АДМІНІСТРАТИВНО-ПРАВОВОГО МЕХАНІЗМУ ПРОТИДІЇ КІБЕРЗАГРОЗАМ В УМОВАХ ЄВРОІНТЕГРАЦІЇ: ОНОВЛЕННЯ ПОВНОВАЖЕНЬ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Анотація. Актуальність теми пов'язана з критичним зростанням кіберзагроз та домінуванням технологічних методів злочинної діяльності, які виходять за межі ефективності існуючих адміністративно-правових механізмів впливу. У статті показано, що технічні засоби захисту стають недостатніми без належного адміністративно-правового супроводу. Мета дослідження полягає у визначенні шляхів трансформації адміністративно-правового механізму протидії кіберзагрозам в умовах євроінтеграції та оновленні повноважень Національної поліції України. Статистика кіберзагроз і інцидентів дозволила виявити тривожну концентрацію атак на урядовий сектор, що вимагає негайного переходу до проактивної моделі стійкості. Встановлено, що ШІ став фактором подвійного призначення, де стрімке зростання кількості атак на 89% вимагає автоматизації оборонних процесів та жорсткого регулювання. У статті порівнюються вітчизняні підходи до регулювання, закладені в Концепції 2020 року, з вимогами європейського Регламенту (ЄС) 2024/1689. Аналіз дозволяє стверджувати, що чинна національна Концепція є недостатньою для протидії сучасним викликам через відсутність дієвих механізмів відповідальності за використання небезпечних технологій. Зроблені висновки і пропозиції спрямовані на перехід від формального нагляду до ризикоорієнтованої моделі, що передбачає класифікацію систем ШІ, впровадження принципу «ШІ, орієнтованого на людину» та наділення Національної поліції функціями активного суб'єкта превентивної кібергігієни. Авторами доведено, що лише гармонізація вітчизняного законодавства з європейськими стандартами забезпечить захист критичної інфраструктури. Дослідження підкреслює потребу переосмислення адміністративно-правових інструментів задля ефективного запобігання, виявлення та розкриття кіберзлочинів, що є запорукою національної безпеки України у цифровому вимірі.

Ключові слова: *євроінтеграція, правове регулювання, правове забезпечення, адміністративно-правовий механізм, штучний інтелект, кібербезпека, кіберінцидент, кібератака, державна політика, сектор безпеки і оборони*

Spivak M. V., Dubina O. M. Transformation of the administrative and legal mechanism for countering cyber threats in the context of European integration: updating the powers of the National Police of Ukraine

Abstract. The relevance of the topic is related to the critical growth of cyber threats and the dominance of technological methods of criminal activity that exceed the effectiveness of existing administrative and legal mechanisms of influence. The article demonstrates that technical security measures are becoming insufficient without proper administrative and legal support. The purpose of the study is to identify ways to transform the administrative and legal mechanism for countering cyber threats in the context of European integration and to update the powers of the National Police of Ukraine. Statistics on cyber threats and incidents have revealed

© Співак М. В., Дубіна О. М., 2026
Стаття поширюється на умовах ліцензії відкритого доступу CC BY 4.0

an alarming concentration of attacks on the government sector, requiring an immediate transition to a proactive resilience model. It has been established that AI has become a dual-use factor, where the rapid 89% increase in the number of AI-driven attacks necessitates the automation of defense processes and strict regulation. The article compares domestic approaches to regulation, laid down in the 2020 Concept, with the requirements of the European Regulation (EU) 2024/1689. The analysis suggests that the current national Concept is insufficient to counter modern challenges due to the lack of effective accountability mechanisms for the use of hazardous technologies. The conclusions and proposals are aimed at transitioning from formal supervision to a risk-based model, which involves classifying AI systems, implementing the principle of «human-centric AI», and empowering the National Police as an active subject of preventive cyber hygiene. The authors prove that only the harmonization of domestic legislation with European standards will ensure the protection of critical infrastructure. The study emphasizes the need to rethink administrative and legal tools for the effective prevention, detection, and investigation of cybercrimes, which is a guarantee of Ukraine's national security in the digital dimension.

Key words: *European integration, legal regulation, legal support, administrative and legal mechanism, artificial intelligence, cybersecurity, cyber incident, cyber attack, state policy, security and defense sector.*

Постановка проблеми. Сучасна геополітична турбулентність та тотальна цифровізація зумовлюють виникнення нових, технологічно досконалих кіберзагроз, які вимагають перегляду парадигми захисту інформаційних систем. Динаміка злочинної діяльності в кіберпросторі засвідчує недостатню ефективність технічних засобів безпеки без належного адміністративно-правового супроводу. Нині постає нагальна потреба в трансформації механізмів державного управління кібербезпекою – від пасивного нагляду до моделей проактивної стійкості та превентивної протидії. В умовах євроінтеграції ключовим викликом стає переосмислення повноважень Національної поліції України (далі – НПУ), яка має трансформуватися з реактивного суб'єкта в активного гаранта захисту критичної інфраструктури. Отже, наукова проблема полягає у необхідності модернізації адміністративно-правового інструментарію відповідно до сучасних викликів, зумовлених стрімким впровадженням штучного інтелекту.

Аналіз останніх досліджень і публікацій. Питання кібербезпеки та протидії протиправним посяганням у кіберпросторі активно досліджуються вітчизняними науковцями. Зокрема, М. Гуцалюк вивчає імплементацію європейських стандартів правового регулювання, а В. Кальченко з колегами порівнюють вітчизняні вимоги щодо захисту даних із міжнародними аналогами. Питання трансформації парадигми безпеки розглядає Н. Фесьоха, тоді як технологічні аспекти застосування штучного інтелекту для виявлення та прогнозування атак детально аналізують В. Бандура, І. Стоцький та їхні співавтори. Роль міжнародної співпраці у цій сфері висвітлює Н. Ларіончева. Незважаючи на ґрунтовність теоретичних напрацювань, автори цієї статті фокусуються на вивченні практичного аспекту функціонування системи кіберзахисту. Для цього було залучено та систематизовано актуальні дані Державної служби спеціального зв'язку та захисту інформації України, Ради національної безпеки і оборони України, а також Національного інституту стратегічних досліджень. Такий емпіричний базис у поєднанні з детальним аналізом чинних нормативних актів, що регулюють діяльність НПУ, та їх критичним порівнянням із новітніми європейськими стандартами, дозволяє виявити суттєві прогалини у вітчизняному законодавстві. Вказаний підхід надає дослідженню вираженого прикладного характеру, обґрунтовуючи необхідність трансформації адміністративно-правового механізму протидії кіберзагрозам в умовах євроінтеграції.

Метою статті є обґрунтування концептуальних напрямів трансформації адміністративно-правового механізму протидії кіберзагрозам в умовах євроінтеграції та розширення повноважень НПУ як активного суб'єкта превентивної кібергігієни. Для досягнення поставленої мети передбачено розв'язання таких завдань: за допомогою статистичного методу – показати інтерпретацію даних про стан кіберзагроз і ідентифікувати динаміку протиправних посягань у кіберпросторі; за допомогою порівняльно-правового методу провести порівняння національних адміністративних підходів із відповідними нормами та регламентами Європейського Союзу (далі – ЄС); системний метод, використати для цілісного дослідження функціонального навантаження НПУ як ключового

суб'єкта системи кібербезпеки, а також для обґрунтування концептуальних напрямів еволюції адміністративно-правових механізмів в умовах цифровізації.

Виклад основного матеріалу. Статистичні дані за 2024 рік демонструють кризову концентрацію загроз саме в урядовому секторі, на який припадає понад 90% усіх опрацьованих кіберінцидентів. Це вказує на цілеспрямований характер атак, що потребує відповідної трансформації адміністративного контролю та процесуального забезпечення діяльності правоохоронних органів. Структура виявлених подій інформаційної безпеки у 2024 році підтверджує домінування технологічних методів злочинної діяльності. 58,8% усіх подій пов'язані зі шкідливим програмним кодом (Malicious Code), що свідчить про високу автоматизацію атак. Спроби втручання (Intrusion Attempts) склали 17,6%, а збір інформації зловмисниками (Information Gathering) – 12,1%. Найбільш поширеним типом кіберінцидентів стало «Шкідливе підключення» (спроби з'єднання з ресурсами, пов'язаними з ботмережами та командними центрами C&C), що фактично нівелює традиційні межі адміністративного нагляду за інформаційними мережами. Особливого адміністративно-правового значення набуває той факт, що основним вектором первинної компрометації систем залишається фішинг (за класифікацією MITRE ATT&CK: T1566.001 Phishing: Spearphishing Attachment). Активність окремих злочинних кластерів (зокрема, згідно з класифікацією CERT-UA: UAC-0010, UAC-0006, UAC-0050) вказує на організований характер атак, що вимагає від правоохоронців не просто технічного реагування, а розробки дієвих адміністративних процедур нейтралізації загроз «на випередження» [1]. У 2025 році зафіксовано понад 5900 кіберінцидентів, спрямованих на українську інфраструктуру. Це на 37% більше, ніж у 2024 році [2].

Сучасний стан глобальної індустрії кібербезпеки характеризується наростанням геополітичної турбулентності та стратегічної невизначеності, що на тлі тотальної цифровізації, базованої на новітніх IT-технологіях, зумовлює трансформацію парадигми захисту інформаційних систем. Аналіз ключових кількісних та якісних показників галузі засвідчує, що штучний інтелект (далі – ШІ) став фактор подвійного призначення. Адже зафіксоване зростання ШІ-атак на 89% вимагає від суб'єктів захисту негайної автоматизації оборонних процесів, де конкурентна перевага визначається швидкістю інтеграції ШІ-рішень. Окрім того, актуалізується проблема цілісності самих ШІ-моделей, які потребують надійного захисту від компрометації. Фундаментальною проблемою залишається структурна асиметрія індустрії – за прогнозами, до 2031 року збитки від кіберзлочинності сягнуть 12,2 трлн дол., що майже в 12 разів перевищуватиме обсяги інвестицій у безпеку (1 трлн дол.). В умовах такої диспропорції стратегічною лінією оборони стає ідентифікація, контроль доступу та захист даних – з огляду на те, що понад 70% хмарних зломів зумовлені компрометацією облікових даних, концепція «нульової довіри» (Zero Trust) трансформується з опційної моделі у базовий стандарт корпоративної безпеки. Поряд із цим зростає загроза типу «зберігай зараз, розшифровуй потім» (SNDL-атаки), що ставить перед організаціями завдання щодо негайної міграції на постквантові криптографічні алгоритми (PQC), оскільки нехтування «криптогнучкістю» при проектуванні систем загрожує масовими витоками в наступному десятилітті. Системною вразливістю також стала логістика програмного забезпечення – атаки через ланцюги постачання (Supply Chain Attacks) зросли до 30%, що вимагає включення безпеки третіх сторін до обов'язкового складника корпоративної політики. Попри технологічний прогрес, критичним залишається людський чинник – розвиток дистанційних форм праці за умов недостатнього рівня кібергігієни перетворює кінцеві пристрої на вразливі вектори входу. Нарешті, регуляторний тиск, зумовлений впровадженням стандартів NIS2, CRA, DORA та CIRCIA, перетворює кібербезпеку на пріоритет корпоративного управління та зону юридичної відповідальності. Отже, у 2026 році відбувається остаточне утвердження нової парадигми, де пасивний захист поступається місцем концепції проактивної стійкості, що передбачає збереження функціональності інформаційних систем та мінімізацію витоків даних навіть в умовах успішного здійснення кібератак [3].

Викладена вище статистична картина демонструє критичний дисбаланс між технологічною озброєністю зловмисників та інертністю існуючих процедур реагування. У цьому контексті постає нагальна потреба в переосмисленні адміністративно-правового механізму управління кібербезпекою – від формального нагляду до активної превенції та проактивної протидії. Поточні виклики вимагають не лише оновлення технічних регламентів, а й суттєвого перегляду повноважень суб'єктів владних повноважень, зокрема НПУ, щодо їх дій в умовах кіберінцидентів. Отже, доцільно здійснити аналіз нормативно-правового забезпечення цієї сфери, приділивши увагу як чинним національним нормативно-правовим актам, так і європейським ініціативам, що формують новий стандарт контролю у віртуальному середовищі.

У 2017 році Закон України «Про основні засади забезпечення кібербезпеки України» визначив правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки. Закон визначив, вже згадані нами терміни. Зокрема, інцидент кібербезпеки розуміється як подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів. А кібератака розглядається, як спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту. Законодавець у ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України» встановлює нормативно закріплений понятійний апарат, який є фундаментальним для забезпечення єдності правового тлумачення в цій сфері. Окрім вище згаданих нами є: індикатори кіберзагроз, інформація про інцидент кібербезпеки, кібербезпека, кіберзагроза, кіберзахист, кібероборона, кіберпростір, кіберрозвідка, кібертероризм, кібершпигунство та ін [4].

Важливим етапом інституційного оформлення системи протидії кіберзлочинності в Україні стала постанова Кабінету Міністрів України від 13 жовтня 2015 року № 831 «Про утворення територіального органу Національної поліції». Відповідно до цього акта, було утворено Департамент кіберполіції як міжрегіональний територіальний орган НПУ зі статусом юридичної особи публічного права. Це рішення забезпечило необхідну організаційно-правову базу для функціонування спеціалізованого підрозділу, наділивши його належною адміністративною правосуб'єктністю для реалізації державної політики у сфері боротьби з кримінальними правопорушеннями у кіберпросторі та формування цілісної інфраструктури спеціалізованої правоохоронної діяльності [5].

Згодом, Закон України «Про Національну поліцію» визначив, що поліція здійснює у визначеному законом порядку протидію злочинним посяганням на об'єкти критичної інфраструктури, які загрожують безпеці громадян і порушують функціонування систем життєзабезпечення; захист об'єктів критичної

інфраструктури, інтересів суспільства і держави від злочинних посягань у кіберпросторі, здійснює заходи із запобігання, виявлення, припинення та розкриття кіберзлочинів проти об'єктів критичної інфраструктури (ст. 23 п. 24-1) [6].

Особливої уваги в контексті еволюції адміністративно-правових механізмів заслуговує ст. 8 Закону України «Про основні засади забезпечення кібербезпеки України», що регламентує функціонування Національної системи кібербезпеки. Протягом останніх років ця норма зазнала суттєвих трансформацій шляхом внесення змін у 2020 та 2025 роках законодавець акцентував роль НПУ як ключового суб'єкта протидії кіберзлочинності. Зокрема, редакція п. 2 ст. 8 чітко закріплює за поліцією повноваження щодо забезпечення захисту прав і свобод людини і громадянина, а також інтересів суспільства та держави від протиправних посягань у кіберпросторі. Визначений законодавцем перелік функцій поліції включає комплекс заходів із запобігання, виявлення, припинення та розкриття кіберзлочинів, а також спеціалізованих правопорушень проти об'єктів критичної інформаційної інфраструктури. Окрім силового та розшукового блоку, нова редакція ст. 8 імперативно виокремлює обов'язок НПУ здійснювати заходи з інформування громадян про безпеку в кіберпросторі, що перетворює інституцію на активний суб'єкт превентивної кібергігієни та правового просвітництва [4].

Концептуальне бачення стратегічних цілей держави у сфері захисту віртуального середовища знаходить відображення у Стратегії кібербезпеки України, затвердженій Указом Президента України від 26 серпня 2021 року № 447/2021. В основі цього доктринального документа лежить усвідомлення глобального характеру сучасних викликів, зумовлених переходом до шостого технологічного укладу, що супроводжується якісно новими ризиками для стабільності світової цивілізації. У цьому контексті Україна декларує прагнення до формування відкритого, вільного, стабільного та безпечного кіберпростору. Зазначена стратегічна мета розглядається не лише як технічне завдання, а як фундаментальна умова забезпечення прав і свобод людини, що є ключовим передумовою для ефективного соціального, політичного та економічного розвитку держави в умовах глобальної цифровізації. Для подальшої розбудови національної системи кібербезпеки на засадах стримування, кіберстійкості, взаємодії необхідним є:

– посилення спроможності національної системи кібербезпеки для унеможливлення збройної агресії проти України у кіберпросторі або з його використанням, нейтралізації розвідувально-підривної діяльності, мінімізації загроз кіберзлочинності та кібертероризму (стримування);

– набуття здатності швидко адаптуватися до внутрішніх і зовнішніх загроз у кіберпросторі, підтримувати та відновлювати стале функціонування національної інформаційної інфраструктури, насамперед об'єктів критичної інформаційної інфраструктури (кіберстійкість);

– забезпечення розвитку комунікації, координації та партнерства між суб'єктами забезпечення кібербезпеки на національному рівні, розвиток стратегічних відносин у сфері кібербезпеки із ключовими іноземними партнерами, передусім з ЄС, США та іншими державами – членами НАТО, співробітництво у цій сфері з іншими державами та міжнародними організаціями на основі національних інтересів України (взаємодія) [7].

Сучасний етап науково-технологічного розвитку України характеризується інтеграцією ШІ до стратегічних пріоритетів державної політики. Концепція розвитку штучного інтелекту в Україні визначає методологічні засади, принципи та завдання щодо впровадження цих технологій, розглядаючи їх як ключовий інструмент науково-технологічного прогресу. Особливого значення набуває той факт, що ШІ стає невід'ємною складовою вдосконалення управлінських та операційних процесів у сферах загальнодержавного значення. Його імплементація, зокрема в оборонній та правовій діяльності, виступає фундаментом для підвищення ефективності державних інституцій, забезпечуючи технологічну спроможність держави в умовах викликів сьогодення. Ключовим завданням державної політики у сфері ШІ є забезпечення стійкості комунікаційних та технологічних систем, що обслуговують об'єкти критичної інфраструктури. Оскільки безперервність функціонування держави та безпека

громадян безпосередньо залежать від цілісності цих технологій, комплексне розв'язання проблем кібербезпеки передбачає виконання таких завдань:

– удосконалення законодавства і створення сучасної нормативно-правової бази для впровадження кращих світових практик штучного інтелекту у сфері кібербезпеки і кіберзахисту;

– розроблення інноваційних систем кібербезпеки, які широко застосовують технології ШІ для автоматичного аналізу та класифікації загроз і автоматичного вибору стратегії їх стримування і запобігання;

– вивчення питання ліцензування іноземних розробок ШІ у сфері кібербезпеки, особливо у державному секторі;

– створення національних інформаційних систем, платформ і продуктів з метою зменшення частки іноземного програмного забезпечення у сфері кібербезпеки, що використовується органами державного управління;

– оновлення державних стандартів щодо інформаційної безпеки, зокрема державних інформаційних ресурсів, а також розроблення нових національних стандартів у сфері кібербезпеки і кіберзахисту, зокрема організаційних і технічних вимог, що стосуються безпеки додатків, мобільних пристроїв, робочих станцій, серверів і мереж, моделей хмарних обчислень. Оновлення стандартів та розроблення нових необхідно здійснювати з урахуванням європейських та міжнародних стандартів, зокрема стандартів ISO 27001, ISO/IEC 27032 [8].

У Концепції ШІ розглядається як організована сукупність інформаційних технологій, із застосуванням якої можливо виконувати складні комплексні завдання шляхом використання системи наукових методів досліджень і алгоритмів обробки інформації, отриманої або самостійно створеної під час роботи, а також створювати та використовувати власні бази знань, моделі прийняття рішень, алгоритми роботи з інформацією та визначати способи досягнення поставлених завдань. А от у Регламенті (ЄС) 2024/1689 Європейського Парламенту та Ради від 13 червня 2024 року ШІ – це швидкорозвинуте сімейство технологій, що сприяє широкому спектру економічних, екологічних та соціальних переваг у всьому спектрі галузей промисловості та соціальної діяльності [9].

Аналіз вітчизняних та європейських підходів до регулювання ШІ виявляє суттєву трансформацію правової парадигми. Якщо Концепція оперує узагальненим поняттям «галузь штучного інтелекту», фокусуючись на стимулюванні діяльності, то Регламент впроваджує жорстку ризикоорієнтовану модель. Європейський законодавець відходить від абстрактного «напряму діяльності» до визначення конкретних об'єктів («система штучного інтелекту») та суб'єктів («розповсюджувач»), що підлягають суворому нагляду. Використання таких категорій, як «біометрична ідентифікація», «розпізнавання емоцій» чи «загальнодоступний простір», свідчить про перехід від стратегії «розвитку» до стратегії «контролю та захисту прав».

Аналіз також засвідчує суттєві відмінності між вітчизняним концептуальним баченням та інтегрованим європейським стандартом. По-перше, Концепція має статус підзаконного нормативно-правового акта, що визначає стратегічні пріоритети, принципи та загальні завдання. Вона спрямована переважно на стимулювання розвитку галузі, інтеграцію ШІ в оборонні та правові структури, проте не встановлює жорстких санкцій чи детальних правил експлуатації систем. Регламент є актом прямої дії, що впроваджує юридично обов'язкові вимоги на всій території ЄС. Це законодавство має імперативний характер і створює комплексну правову базу для контролю за життєвим циклом систем ШІ. По-друге, українська модель базується на «позитивному» підході, де головним акцентом є розвиток технологій, розбудова інфраструктури та підвищення конкурентоспроможності держави. Це декларативний документ, що відображає намір України зайняти нішу у глобальному технологічному просторі. Європейська модель застосовує ризикоорієнтований підхід. Регламент класифікує системи ШІ за рівнем ризику – від систем з «неприйнятним рівнем ризику» (які заборонені) до систем «високого ризику», що підлягають суворим процедурам сертифікації, аудиту та нагляду. По-третє, якщо Концепція фокусується на імплементації ШІ в інтересах держави та безпеки (розвиток, дослідження,

оборонна сфера), то Регламент ЄС спрямований на контроль та безпеку. Головна мета Регламенту – захист фундаментальних прав людини, безпеки та здоров'я громадян від потенційно шкідливого впливу ШІ, при збереженні стимулів для інновацій [8, 9].

Тож національна Концепція 2020 року на сьогодні є недостатньою для комплексного правового регулювання сфери ШІ, оскільки вона не містить дієвих механізмів відповідальності за використання небезпечних технологій. У процесі євроінтеграції Україна постає перед необхідністю імплементації положень Регламенту ЄС 2024/1689 у національне законодавство, що вимагає переходу від загальних концептуальних засад до жорсткого та ризикоорієнтованого адміністративно-правового регулювання. Тому, інтеграція правових норм, що регулюють ШІ, є критично важливою для кібербезпеки, оскільки вона перетворює поліцію з реактивного органу на проактивного суб'єкта, здатного контролювати технологічні ризики та ефективно захищати критичну інфраструктуру. Чітка термінологія та європейські стандарти правового регулювання забезпечують надійну правову основу для правоохоронних органів при використанні новітніх інструментів кримінального аналізу та запобіганні загрозам у кіберпросторі.

Висновки. Слід констатувати, що критичне зростання кількості кіберінцидентів та їхня висока технологічна автоматизація свідчать про глибокий дисбаланс між наступальним потенціалом зловмисників та інертністю існуючих процедур реагування. У таких умовах актуальність дослідження полягає в необхідності термінової трансформації адміністративно-правового механізму, який має перейти від формального нагляду до моделі проактивної стійкості, здатної адекватно відповідати на сучасні загрози із застосуванням ШІ.

Аналіз адміністративного законодавства свідчить про системну трансформацію ролі НПУ, яка нині виходить за межі суто правоохоронних функцій, стаючи гарантом кібербезпеки та стабільності критичної інфраструктури держави. Така еволюція нормативно-правової бази засвідчує перехід від виключно базових методів протидії кіберзлочинності до комплексного забезпечення безпекового середовища через впровадження превентивних механізмів, правового просвітництва та активного захисту прав громадян у цифровому просторі.

Дослідження показало, що часовий розрив між ухваленням Концепції розвитку штучного інтелекту в Україні (2020 рік) та Регламенту (ЄС) 2024/1689 (2024 рік) становить майже чотири роки. У контексті стрімкого розвитку технологій цей період є критично великим. За ці чотири роки відбулася радикальна еволюція ШІ – від вузькоспеціалізованих систем до поширення генеративного ШІ (наприклад, моделей на кшталт ChatGPT), що докорінно змінило ландшафт ризиків у кіберпросторі. У 2020 році світ перебував на етапі осмислення потенціалу ШІ, тоді як у 2024 році – на етапі жорсткого правового регулювання та введення механізмів відповідальності. З огляду на необхідність модернізації вітчизняного законодавства та його гармонізації з європейськими стандартами, слід запропонувати такі концептуальні зміни та доповнення до Національної концепції розвитку штучного інтелекту: 1. доповнити Концепцію положенням про класифікацію систем ШІ за рівнем ризику. Замість загального сприяння розвитку всіх технологій, пріоритезувати контроль над системами «високого ризику», встановивши для них жорсткі вимоги щодо прозорості та підзвітності; 2. замість абстрактного поняття «галузь ШІ», імплементувати в текст Концепції та подальші законопроєкти чіткі дефініції, що відповідають європейським: «система ШІ», «біометрична ідентифікація», «система розпізнавання емоцій» тощо. Це необхідно для того, щоб органи НПУ мали чіткі межі допустимого використання таких технологій (зокрема, щодо приватності та захисту персональних даних); 3. додати розділ, присвячений принципам «ШІ, орієнтованого на людину». Слід зафіксувати, що будь-яке застосування ШІ органами НПУ має здійснюватися під належним наглядом людини, щоб уникнути помилок алгоритмічного прийняття рішень та дискримінації.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:

1. Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки : звіт за 2024 рік / Державна служба спеціального зв'язку та захисту інформації України. Київ, 2025. URL: https://scpc.gov.ua/api/files/72e13298-4d02-40bf-b436-46d927c88006 (дата звернення: 11.07.2026).

2. Діяльність Національного координаційного центру кібербезпеки : вебсайт / Рада національної безпеки і оборони України. Київ, 2026. URL: https://www.rnbo.gov.ua/ua/Diialnist/7376.html (дата звернення: 11.07.2026).

3. Глобальна індустрія кібербезпеки станом на 2026 рік: основні тренди та виклики : аналітичні матеріали / Національний інститут стратегічних досліджень. Київ, 2026. URL: https://niss.gov.ua/doslidzhennya/natsionalna-bezpeka/hlobalna-industriya-kiberbezpeky-stanom-na-2026-rik-osnovni (дата звернення: 12.07.2026).

4. Про основні засади забезпечення кібербезпеки України : Закон України від 05 жов. 2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 12.07.2026).

5. Про утворення територіального органу Національної поліції : Постанова Кабінету Міністрів України від 13 жов. 2015 № 831. URL: https://zakon.rada.gov.ua/laws/show/831-2015-%D0%BF#Text (дата звернення: 12.07.2026).

6. Про Національну поліцію : Закон України від 02 лип. 2015 № 580-VIII. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text (дата звернення: 19.07.2026).

7. Про Стратегію кібербезпеки України : Указ Президента України від 26 серп. 2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021 (дата звернення: 19.07.2026).

8. Про схвалення Концепції розвитку штучного інтелекту в Україні : розпорядження Кабінету Міністрів України від 02 груд. 2020 № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text (дата звернення: 20.07.2026).

9. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2009/125/EC, (EU) 2015/835 and (EU) 2019/904 (Artificial Intelligence Act). Official Journal of the European Union. L series, 2024/1689. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202401689 (date of access: 20.07.2026).

Дата першого надходження статті до видання: 21.07.2026
Дата прийняття статті до друку після рецензування: 18.08.2026
Дата публікації (оприлюднення) статті: 16.11.2026