

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДНІПРОВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ОЛЕСЯ ГОНЧАРА**

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДНІПРОВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ОЛЕСЯ ГОНЧАРА**

Кваліфікаційна наукова праця
на правах рукопису

ОЛІЙНИК АРТЕМ АНДРІЙОВИЧ

УДК 343.9.02:004 (477)(043.3)

**ДИСЕРТАЦІЯ
КРИМІНОЛОГІЧНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ
БЕЗПЕКИ: МІЖНАРОДНИЙ, НАЦІОНАЛЬНИЙ
ТА ЗАРУБІЖНИЙ ВИМІРИ**

Спеціальність 081 Право

Галузь знань 081 Право

Подається на здобуття ступеня доктора філософії

Подані до захисту наукові досягнення є напрацюванням автора, а всі запозичені ідеї, наукові результати, цитати супроводжуються належними посиланнями на їх авторів та джерела опублікування

А.А. Олійник

Науковий керівник – доктор юридичних наук, професор Наталія Семенівна Юзікова

Дніпро – 2026

АНОТАЦІЯ

Олійник А.А. Кримінологічні засади забезпечення інформаційної безпеки: міжнародний, національний та зарубіжний виміри. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття ступеня доктора філософії з галузі знань 08 «Право» за спеціальністю 081 «Право». Дніпровський національний університет імені Олеся Гончара, Дніпро, 2026.

Дослідження присвячене формуванню та реалізації кримінологічних засад інформаційної безпеки, а також закономірностям детермінації кіберзлочинності та когнітивних впливів в умовах глобалізації, воєнного стану, цифрової трансформації суспільства та активного розвитку технологій штучного інтелекту.

У роботі вперше на системному рівні розкрито зміст інформаційної безпеки через призму трирівневої моделі (міжнародний, національний та зарубіжний виміри), що дозволило обґрунтувати перехід до центричної моделі безпеки та суверенної кіберстійкості держави. Особлива увага приділена аналізу феномену когнітивного впливу та розробці механізмів формування «інтелектуального імунітету» особистості як пріоритетного напрямку кримінологічної превенції. Глобальна цифровізація суспільних відносин, трансформація злочинності та інтенсифікація інструментів міждержавного протистояння у кіберпросторі актуалізують необхідність фундаментального переосмислення наявних превентивних стратегій у сфері інформаційної безпеки. Запропоновано нову систему кримінологічного захисту національного інформаційного простору, яка зміщує акцент з реактивного технічного захисту об'єктів інфраструктури на проактивне формування комплексної кіберстійкості держави та когнітивного імунітету суспільства і особи.

Наукове осмислення сутності, змісту та рівнів інформаційної безпеки як об'єкта кримінологічного захисту та правової превенції полягає у розробці відповідної моделі. Ця модель базується на розширеній міжнародній матриці безпеки - Тріаді СІА (конфіденційність, цілісність, доступність), яку доповнено

процесуальними елементами автентичності й неспростовності. Структурно об'єкт розподілено на три фундаментальні рівні: інфраструктурний, правовий і соціально-психологічний (когнітивний). Доведено, що такий підхід дозволяє виявити характер сучасних кіберзагроз, які вражають апаратне забезпечення, нормативні режими та людську свідомість. На основі цього визначено напрями проактивної превенції для кожного з рівнів та обґрунтовано антропоцентричний пріоритет захисту суспільної свідомості, процесу формування волі й цифрових прав і свобод людини від протиправних маніпулятивних впливів, дезінформації та деструктивних технологічних впливів.

В межах історико-правового та доктринального аналізу розкрито генезис вітчизняної наукової думки, яка пройшла складний шлях від вузького розуміння безпеки як технічного захисту даних (I етап: 1991–1996 рр.), через правову основу базових інститутів (II етап: 1997–2000 рр.) та міжнародну гармонізацію вітчизняних нормативних стандартів (III етап: 2001–2013 рр.) до обґрунтованого нами IV етапу (з 2014 року до сьогодні). З'ясовано, що IV етап зумовлений воєнними викликами і кардинально відрізняється від попередніх періодів своєю онтологічною природою, оскільки характеризується переходом від реактивного технічного захисту локальних інформаційних систем до формування цілісної державної функції та стратегічної кіберстійкості всієї нації. У межах IV етапу в роботі уточнено понятійно-категоріальний апарат через чітке розмежування загального широкого поняття «інформаційна безпека» (орієнтованого на захист свідомості та нецифрових даних) і вузьких технологічних категорій «кібербезпека» та «цифрова безпека», що дозволило конкретизувати межі предмета кримінологічного захисту.

Проаналізовано досвід зарубіжних стратегій забезпечення інформаційної безпеки та специфіку зарубіжної доктрини. На основі узагальнення зарубіжної наукової думки з'ясовано, що на відміну від вітчизняних досліджень, орієнтованих на правову кодифікацію та стратегічне планування, західна доктрина відзначається високим рівнем математизації та техноцентризму,

активно використовуючи інструменти Байєсівських мереж, теорії ігор та марковських моделей для прогнозування векторів потенційних атак. Доведено, що ключовим недоліком зарубіжних моделей є ігнорування динамічної поведінки правопорушника та людського фактора, що суттєво обмежує їхню ефективність для достатньої кримінологічної превенції й актуалізує потребу впровадження антропоцентричного підходу.

Досліджуючи міжнародний сектор безпекових відносин, з'ясовано, що принципи та механізми міжнародно-правового забезпечення інформаційної безпеки у протидії транснаціональним кіберзагрозам потребують негайної адаптації до умов глобальної кризи доведення джерела атак. Обґрунтовано науковий підхід до розуміння сутності інформаційної безпеки держави, що ґрунтується на інтеграції правових, соціальних та етичних аспектів у єдину систему захисту й гармонізації міжнародних стандартів (зокрема, Будапештської конвенції та GDPR) із національними правовими традиціями. Визначено, що засади реалізації принципу невідворотності кримінальної відповідальності у цифровому середовищі вимагають інтеграції техніко-юридичного елемента «неспростовності» до системи доказування, що дозволяє юридично нейтралізувати використання злочинцями систем анонімізації та транскордонної маршрутизації трафіку.

У роботі обґрунтовано чотирирівневий механізм, який через поєднання процесуальних можливостей Будапештської конвенції та матеріальних норм міжнародного гуманітарного права забезпечує чіткий алгоритм притягнення агресора до юридичної відповідальності за вчинені кібератаки на рівнях: процесуальної атрибуції атак; легітимізації цифрових доказів для міжнародних трибуналів; доведення транснаціонального злочинного умислу; техніко-юридичної кваліфікації кібератак як воєнних злочинів. Поряд із цим визначено, що міжнародні стандарти модернізуються: прийняття у 2025 році під егідою УНП ООН Конвенції про запобігання, припинення та боротьбу з кіберзлочинністю, закладає основу для криміналізації нових протиправних діянь

та оперативного обміну даними. Доведено, що гармонізація законодавства України з принципами FISMA, Директивою NIS2 та Конвенцією ООН 2025 року дозволяє трансформувати унікальний вітчизняний бойовий досвід у системний правовий механізм захисту національних інтересів і цифрового суверенітету держави.

Оцінюючи внутрішній правовий простір, доведено, що функціонування системи забезпечення інформаційної безпеки в умовах правового режиму воєнного стану вимагає стратегічного переходу сектору безпеки від реактивної моделі до проактивного реагування. Сформульовано кримінологічну характеристику кіберзлочинності в умовах воєнного стану, до якої включено новітні фактори криміногенного ризику штучного інтелекту та Інтернету речей. На основі цього обґрунтовано доцільність криміналізації нових цифрових загроз, зумовлених воєнним станом та технологічним прогресом, зокрема, створення та поширення згенерованого за допомогою ШІ синтетичного контенту експлуатації дітей, шантажу та дипфейків.

Розкрито сучасні законодавчі та інституційні засади забезпечення інформаційної безпеки в Україні. Ліквідація наявних правових прогалин має базуватися на впровадженні випереджальних превентивних механізмів, які враховують поведінкові ризики та соціальні фактори протиправності. З метою нейтралізації системних кіберзагроз обґрунтовано дворівневий розподіл поняття «кіберстійкість» на державний (публічно-правовий) та особистісний (людиноцентричний) рівні. Представлено авторське визначення понять: «кіберстійкість держави» визначено як стратегічну спроможність підтримувати критичні функції, адаптуватися до гібридних загроз та відновлювати цифрову інфраструктуру на основі інституційної координації сектору безпеки (МВС, Нацполіція, ЦПД), управління ризиками ланцюгів постачання та впровадження засад кіберзрілості; «кіберстійкість особи» дефініційовано як сукупність когнітивних навичок, правової обізнаності та кібергігієни особи.

Визначено, що формування балансу між свободою та безпекою є ключовим викликом сучасної інформаційної політики. Надмірний контроль загрожує порушенням прав людини, тоді як його відсутність створює умови для кіберзлочинності та інформаційних атак. Оптимальне рішення полягає у поєднанні глобальних принципів із національною правовою традицією, що забезпечує ефективність кримінологічного захисту та збереження демократичних цінностей. Такий підхід дозволяє створити правову систему, здатну реагувати на сучасні загрози, не порушуючи основних прав і свобод.

Представлено специфіку та багаторівневу структуру кримінологічної превенції крізь призму забезпечення справедливої рівноваги між свободою слова, захистом державного суверенітету та цифровими правами людини. Обґрунтовано концепцію «когнітивного імунітету» нації як невід’ємного виміру інформаційної безпеки, що базується на зарубіжному досвіді розбудови потенціалу та передбачає перехід від захисту виключно технічного периметра до формування стійкості людського капіталу. Тому пропонується визначення «когнітивного імунітету суспільства» як самостійної кримінологічної та віктимологічної категорії, що визначає здатність громадян виступати внутрішнім самозахисним бар’єром проти ІПСО та цифрового шахрайства.

Узагальнюючи моделі безпеки, запропоновано підхід до класифікації моделей забезпечення кіберстійкості через виокремлення чотирьох взаємозалежних вимірів: стратегічного, нормативного, інституційного та екосистемного, що дозволяє комплексно оцінювати рівень кіберзрілості держави і суспільства за міжнародними стандартами та визначати конкретні шляхи модернізації українського законодавства. Представлено віктимологічний підхід до запобігання кіберзлочинності через обґрунтування змісту «техногенної віктимності» організацій (на основі аналізу міжнародного досвіду використання хмарних сервісів), де чинником посягань визначено організаційну недбалість у налаштуваннях конфігурацій та договірній підзвітності.

На основі міжнародного аналізу обґрунтовано загальний та спеціальний рівні міжнародного співробітництва у сфері протидії транснаціональній кіберзлочинності, що дозволило визначити зміну міжнародно-правового статусу України в системі європейської кібербезпеки. Доведено, що завдяки успішній інтеграції правоохоронних органів України у спільні транскордонні поліцейські операції та системи обміну розвідувальними даними (Європол, мережа SIENA), відбувся остаточний перехід України від ролі пасивного реципієнта (об'єкта захисту) до статусу активного, стратегічно важливого учасника колективної європейської безпеки.

Для практичної реалізації європейських безпекових стандартів розроблено підхід щодо приєднання до європейської системи кібербезпеки та інтеграції авторської пропозиції стосовно заснування національного Інституту безпеки ШІ (за прикладом Інституту безпеки ШІ Великобританії). Він має виступати координаційним хабом для впровадження міжнародних стандартів у вітчизняну практику запобігання, виявлення і розслідування високо-технологічних кіберзлочинів.

Для практичного впровадження результатів дослідження в освітній процес Дніпровського національного університету імені Олеся Гончара, запропоновано міждисциплінарний спецкурс «Правові засади кіберстійкості та цифрова держава». Навчальна дисципліна спрямована на підготовку фахівців (правників, політологів, соціологів, психологів, журналістів), які володітимуть крос-функціональними компетентностями для ефективної протидії гібридним загрозам, захисту критичної інфраструктури та формування когнітивного імунітету суспільства в умовах сталого повоєнного розвитку України.

Ключові слова: права і свободи людини і громадянина, національна безпека, інформаційна безпека, воєнний стан, кібероборона, кіберстійкість, мережа Інтернет, кіберзлочинність, кримінальні правопорушення, кримінальна відповідальність, покарання, справедлива рівновага, запобігання злочинності, Національна поліція України, міжнародне співробітництво.

ABSTRACT

Oliinyk, A.A. Criminological Foundations of Information Security: International, National and Foreign Dimensions. – Qualification scientific work as a manuscript.

Dissertation for the degree of Doctor of Philosophy in the speciality 081 «Law». Oles Honchar Dnipro National University, Dnipro, 2026.

This study focuses on the development and implementation of criminological principles of information security, as well as the patterns governing cybercrime and cognitive influences in the context of globalisation, martial law, the digital transformation of society, and the rapid advancement of artificial intelligence technologies.

For the first time, the work systematically examines the concept of information security through the prism of a three-level model (international, national and foreign dimensions), which has enabled the justification of a transition to a centric security model and the sovereign cyber resilience of the state. Particular attention is paid to the analysis of the phenomenon of cognitive influence and the development of mechanisms for forming an individual's 'intellectual immunity' as a priority area of criminological prevention. The global digitalisation of social relations, the transformation of crime and the intensification of instruments of interstate confrontation in cyberspace highlight the need for a fundamental rethinking of existing preventive strategies in the field of information security. A new system of criminological protection for the national information space is proposed, which shifts the focus from reactive technical protection of infrastructure objects to the proactive development of the state's comprehensive cyber resilience and the cognitive immunity of society and the individual.

The academic analysis of the nature, content and levels of information security as an object of criminological protection and legal prevention involves the development of an appropriate model. This model is based on the expanded international security matrix – the CIA Triad (confidentiality, integrity, availability) – which is supplemented by the procedural elements of authenticity and irrefutability.

Structurally, the object is divided into three fundamental levels: infrastructural, legal and socio-psychological (cognitive). It has been demonstrated that this approach allows for the identification of the nature of modern cyber threats, which affect hardware, regulatory regimes and human consciousness. On this basis, directions for proactive prevention have been identified for each of the levels, and the anthropocentric priority of protecting public consciousness, the process of will-formation, and human digital rights and freedoms from unlawful manipulative influences, disinformation and destructive technological influences has been substantiated.

Within the framework of historical-legal and doctrinal analysis, the genesis of domestic scientific thought is revealed, which has undergone a complex evolution from a narrow understanding of security as technical data protection (Stage I: 1991–1996), through the legal framework of basic institutions (Stage II: 1997–2000) and the international harmonisation of domestic regulatory standards (Stage III: 2001–2013), to the Stage IV we have identified (from 2014 to the present). It has been established that Stage IV is driven by military challenges and differs radically from previous periods in its ontological nature, as it is characterised by a transition from reactive technical protection of local information systems to the formation of a comprehensive state function and strategic cyber resilience for the entire nation. Within the framework of Stage IV, the conceptual and categorical apparatus has been refined through a clear distinction between the general, broad concept of ‘information security’ (focused on the protection of consciousness and non-digital data) and the narrower technological categories of ‘cybersecurity’ and ‘digital security’, which has made it possible to specify the boundaries of the subject of criminological protection.

The article analyses the experience of foreign information security strategies and the specific features of foreign doctrine. Based on a review of foreign academic literature, it has been established that, unlike domestic research, which focuses on legal codification and strategic planning, Western doctrine is characterised by a high degree of mathematisation and techno centrism, actively utilising Bayesian networks, game theory and Markov models to predict the vectors of potential attacks. It has been

demonstrated that a key shortcoming of foreign models is their disregard for the dynamic behaviour of offenders and the human factor, which significantly limits their effectiveness for adequate criminological prevention and highlights the need to adopt an anthropocentric approach.

In examining the international security sector, it has been established that the principles and mechanisms of international legal safeguards for information security in countering transnational cyber threats require immediate adaptation to the conditions of the global crisis of proving the source of attacks. A scientific approach to understanding the essence of a state's information security has been substantiated, based on the integration of legal, social and ethical aspects into a unified system of protection and the harmonisation of international standards (in particular, the Budapest Convention and the GDPR) with national legal traditions. It has been determined that the foundations for implementing the principle of the inevitability of criminal liability in the digital environment require the integration of the technical-legal element of 'irrefutability' into the system of evidence, which makes it possible to legally neutralise the use by criminals of anonymisation systems and cross-border traffic routing.

This paper sets out a four-tier mechanism which, by combining the procedural provisions of the Budapest Convention with the substantive rules of international humanitarian law, provides a clear framework for holding the aggressor legally accountable for cyberattacks committed at the following levels: procedural attribution of attacks; the admissibility of digital evidence before international tribunals; the establishment of transnational criminal intent; and the technical and legal classification of cyberattacks as war crimes. Alongside this, it has been established that international standards are being modernised: the adoption in 2025, under the auspices of the UN, of the Convention on the Prevention, Suppression and Punishment of Cybercrime lays the foundation for the criminalisation of new unlawful acts and the operational exchange of data. It has been demonstrated that harmonising Ukrainian legislation with the principles of FISMA, the NIS2 Directive and the 2025 UN Convention enables the transformation of Ukraine's unique combat experience into a systematic legal

mechanism for the protection of national interests and the state's digital sovereignty.

An assessment of the domestic legal framework has demonstrated that the functioning of the information security system under a legal regime of martial law requires a strategic shift in the security sector from a reactive model to a proactive response. A criminological profile of cybercrime under martial law has been formulated, incorporating the latest criminogenic risk factors associated with artificial intelligence and the Internet of Things. On this basis, the feasibility of criminalising new digital threats caused by martial law and technological progress is substantiated, in particular the creation and dissemination of AI-generated synthetic content involving child exploitation, blackmail and deepfakes.

On this basis, the paper justifies the need to criminalise new digital threats arising from the state of war and technological progress, in particular the creation and dissemination of AI-generated synthetic content involving child exploitation, blackmail and deepfakes.

The current legislative and institutional foundations for ensuring information security in Ukraine are examined. The elimination of existing legal loopholes must be based on the implementation of proactive preventive mechanisms that take into account behavioural risks and social factors of illegality. With the aim of neutralising systemic cyber threats, a two-tier division of the concept of 'cyber resilience' into the state (public-law) and personal (human-centred) levels is justified. The author's definitions of the concepts are presented: 'state cyber resilience' is defined as the strategic capability to maintain critical functions, adapt to hybrid threats and restore digital infrastructure based on institutional coordination within the security sector (Ministry of Internal Affairs, National Police, Central Security Service), supply chain risk management and the implementation of cyber maturity principles; 'individual cyber resilience' is defined as the combination of an individual's cognitive skills, legal awareness and cyber hygiene.

It has been established that striking a balance between freedom and security is a key challenge for modern information policy. Excessive control risks infringing on

human rights, whilst a lack of control creates conditions conducive to cybercrime and cyberattacks. The optimal solution lies in combining global principles with national legal traditions, ensuring the effectiveness of criminological protection and the preservation of democratic values. This approach allows for the creation of a legal system capable of responding to modern threats without infringing upon fundamental rights and freedoms.

The specifics and multi-level structure of criminological prevention are presented through the prism of ensuring a fair balance between freedom of speech, the protection of state sovereignty and digital human rights. The concept of a nation's 'cognitive immunity' is substantiated as an integral dimension of information security, based on international experience in capacity building and involving a shift from the protection of a purely technical perimeter to the development of human capital resilience. It is therefore proposed to define 'societal cognitive immunity' as an independent criminological and victimological category, which determines the ability of citizens to act as an internal self-defence barrier against cyberattacks and digital fraud.

By synthesising security models, an approach to classifying cyber resilience models is proposed through the identification of four interrelated dimensions: strategic, regulatory, institutional and ecosystemic. This enables a comprehensive assessment of the level of cyber maturity of the state and society against international standards, and the identification of specific pathways for modernising Ukrainian legislation. A victimological approach to the prevention of cybercrime is presented by substantiating the concept of 'technogenic victimhood' of organisations (based on an analysis of international experience in the use of cloud services), where organisational negligence in configuration settings and contractual accountability is identified as a factor in attacks.

Based on an international analysis, the general and specific levels of international cooperation in the field of combating transnational cybercrime are substantiated, which has made it possible to identify a change in Ukraine's international

legal status within the European cybersecurity system. It has been demonstrated that, thanks to the successful integration of Ukraine's law enforcement agencies into joint cross-border police operations and intelligence-sharing systems (Europol, the SIENA network), Ukraine has made a definitive transition from the role of a passive recipient (object of protection) to the status of an active, strategically important participant in collective European security.

To put European security standards into practice, an approach has been developed to join the European cybersecurity system and to incorporate a proposal to establish a national AI Security Institute (modelled on the UK's AI Security Institute). It is intended to serve as a coordination hub for the implementation of international standards into domestic practice for the prevention, detection and investigation of high-tech cybercrimes.

To put the research findings into practice within the educational process at the Oles Honchar Dnipro National University, an interdisciplinary specialised course entitled 'Legal Foundations of Cyber Resilience and the Digital State' has been proposed. The course aims to train specialists (lawyers, political scientists, sociologists, psychologists, journalists) who will possess cross-functional competencies to effectively counter hybrid threats, protect critical infrastructure and build society's cognitive immunity in the context of Ukraine's sustainable post-war development.

Keywords: human and civil rights and freedoms, national security, information security, martial law, cyber defence, cyber resilience, the Internet, cybercrime, criminal offences, criminal liability, punishment, fair balance, crime prevention, National Police of Ukraine, international cooperation

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

яких опубліковано основні наукові результати дисертації:

1. Олійник А. А. Сутність інформаційної безпеки як правового явища у національному та міжнародному просторі. *Актуальні проблеми вітчизняної*

юриспруденції № 6. 2023. С.293-299. DOI <https://doi.org/10.32782/2408-9257-2023-6-45>.

2. Олійник А. А. Формування стійкого цифрового суспільства: превентивна роль інформаційної безпеки та кримінально-правової політики у запобіганні злочинності . *Актуальні проблеми вітчизняної юриспруденції* № 2. 2025. С. 177-182. DOI <https://doi.org/10.32782/2408-9257-2025-2-27>
3. Олійник А. А. Запобігання правопорушенням у сфері інформаційної безпеки: від захисту державного суверенітету до гарантування прав людини. *Актуальні проблеми вітчизняної юриспруденції* № 6. 2025. С.129-134.
DOI <https://doi.org/10.32782/2408-9257-2025-6-19>
4. Олійник А.А. Кіберстійкість та права людини: імплементація міжнародних превентивних моделей у цифровий простір в Україні. *Аналітичне порівняльне правознавство* № 6. Ч. 3. 2025. С. 84-90.
DOI <https://doi.org/10.24144/2788-6018.2025.06.3.12>
5. Юзікова Н.С., Олійник А. А. Напрями забезпечення правопорядку на звільнених територіях: інституційні підходи, довіра та практики взаємодії поліції й громади. *Науковий вісник УжНУ. Серія “Право”* № 93. Частина 4. 2026. С.247-255. DOI <https://doi.org/10.24144/2307-3322.2026.93.4.35> (Особистий внесок здобувача: Юзікова Н.С., – методологія, аналіз та узагальнення наукових джерел, напрацювання моделей вирішення питань відновлення та забезпечення правопорядку на деокупованих територіях України, обґрунтування та концептуалізація інклюзивних механізмів залучення громади як базової умови реінституціалізації правопорядку на деокупованих територіях; написання; рецензування та редагування; Олійник А. А. – актуалізація, аналіз та узагальнення зарубіжного законодавства, обґрунтування напрямів забезпечення інформаційної безпеки шляхом інтеграції принципів процедурної справедливості та комунікативного партнерства, розробці пропозицій щодо протидії гібридним загрозам; написання; рецензування та редагування.

які засвідчують апробацію матеріалів дисертації:

6. Олійник А.А. Організація безпеки інформаційного суверенітету для України як об'єкта глобальних інформаційних впливів Збірник тез Всеукраїнського науково-практичного юридичного форуму «Національна парадигма правового розвитку сучасної України» (Дніпровський національний університет імені Олеся Гончара, м. Дніпро, 18 травня 2023 року). Дніпро: Ліра, 2023. С. 334-340. URL:[https://www.dnu.dp.ua/docs/ndc/2023/materiali %20konf/new_NACIONALNA%20PARADIGMA.pdf](https://www.dnu.dp.ua/docs/ndc/2023/materiali%20konf/new_NACIONALNA%20PARADIGMA.pdf)
7. Олійник А.А. Модель забезпечення цифрової безпеки в мережі internet крізь призму досвіду зарубіжних країн. Збірник тез Всеукраїнської науково-практичної конференції «Забезпечення принципів поваги, захисту та реалізації прав дитини у цифровому середовищі». (м. Дніпро 23.листопада 2023) Дніпровський національний університет імені Олеся Гончара, Дніпро, Ліра, 2023. С.349-352 URL: https://www.dnu.dp.ua/docs/ndc/2023/materiali%20konf/new_Zbirnyk_Konf_Zahyst%20prav_dytyny_v_cifrovomu_sviti.pdf
8. Олійник А.А. Окремі форми інформаційної агресії матеріали всеукраїнського науково-практичного круглого столу. Інформаційна агресія в сучасному світі: правовий аналіз та протидія Харків, 21 червня 2024 р. : електрон. наук. вид. / редкол.: В. С. Батиргарєєва та ін. – Харків : Майдан, 2024. С. 56-58. https://ivpz.kh.ua/wp-content/uploads/2024/11/%D0%97%D0%B1%D1%96%D1%80%D0%BD%D0%B8%D0%BA_%D1%96%D0%BD%D1%84%D0%BE%D0%B0%D0%B3%D1%80%D0%B5%D1%81%D1%96%D1%8F_2024-%D0%BD%D0%B0-%D1%81%D0%B0%D0%B9%D1%82.pdf
9. Олійник А. А. Міжнародне запобігання злочинності у сфері цифрових технологій у контексті захисту прав людини. Матеріали міжнародної науково-практичної конференції. Актуальні проблеми прав людини: від універсальних стандартів до національної практики : Київський університет права Національної академії наук України, 11 грудня 2025 р. Львів – Торунь : Liha-Pres, 2025. С. 100-104. DOI <https://doi.org/10.36059/978-966-397-557-3-27>

10. Олійник А.А. Методологічний потенціал генетичного підходу Б. О. Кістяківського у дослідженні генези прав людини. Матеріали Всеукраїнської науково-практичної конференції «Актуальні проблеми правової науки. Запоріжжя. 22.12. 2025. С.79-82. URL: https://www.znu.edu.ua/faculty/law/nauka/2025/_vseukrayins_koyi_naukovo-praktichnoyi_konferents_yi_aktual_n_problemi_pravovoyi_nauki_tapravookhoronnoyi_d_yal_nost_.pdf

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ARPANet - Мережа Агентства перспективних дослідницьких проєктів

CISA - Закон про обмін інформацією про кібербезпеку

DDoS - Розподілена атака на відмову в обслуговуванні

GPC - Глобальна програма з кіберзлочинності (УНП ООН)

NCSC - Національний центр кібербезпеки

NHTCU - Національний підрозділ боротьби зі злочинністю у сфері високих технологій

OSINT - Розвідка на основі відкритих джерел та інформаційна безпека

UNODC – Управління ООН з наркотиків і злочинності

ЄС – Європейський Союз

ЄСПЛ – Європейський суд з прав людини

ЗМІ – засоби масової інформації

ІКТ - інформаційно-комунікаційні технології

ІМІ - Інститут масової інформації

ІПСО - інформаційно-психологічні операції

КК – Кримінальний кодекс

КПК – Кримінальний процесуальний кодекс

МВС – Міністерство внутрішніх справ

МІБ – міжнародна інформаційна безпека

МКС – Міжнародний кримінальний суд

ООН – Організація Об'єднаних Націй

США – Сполучені Штати Америки

ФБР - Федеральне бюро розслідувань

УНП ООН - Управління ООН з питань наркотиків та злочинності

ЦПД - Центр протидії дезінформації

ЗМІСТ

ВСТУП	19
РОЗДІЛ I. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ОСНОВИ КРИМІНОЛОГІЧНОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ	34
1.1. Інформаційна безпека як об'єкт кримінологічного захисту та превенції: зміст, рівні та сучасні виклики	34
1.2. Генезис наукової думки та етапи становлення правових засад забезпечення інформаційної безпеки в контексті вітчизняного і зарубіжного досвіду	50
1.3. Принципи та механізми міжнародно-правового забезпечення інформаційної безпеки	70
Висновки до першого розділу	90
Розділ 2. Національний вимір кримінологічного запобігання загрозам інформаційній безпеці України	93
2.1 Особливості та тенденції забезпечення інформаційної безпеки в умовах воєнного стану	93
2.2. Законодавчі та інституційні засади забезпечення інформаційної безпеки України	108
2.3. Кримінологічна превенція у сфері інформаційної безпеки від державного суверенітету до захисту прав людини	132
Висновки до другого розділу	149
Розділ 3. Зарубіжний досвід та вдосконалення національної системи кримінологічного реагування	152
3.1 Порівняльно-правовий аналіз передового зарубіжного досвіду забезпечення інформаційної безпеки та формування кіберстійкості	152
3.2. Роль міжнародного співробітництва та уніфікації у протидії кіберзагрозам транснаціонального характеру загальний та спеціальний рівні	169
3.3. Основні напрями вдосконалення кримінологічного забезпечення інформаційної безпеки та формування національної кіберстійкості в Україні	188
Висновки до третього розділу	205
ВИСНОВКИ	208
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	214
ДОДАТКИ	259

ВСТУП

Обґрунтування вибору теми дослідження. Сучасний світ переживає зміни, зумовлені переходом від індустріального до інформаційного суспільства, що реально чи потенційно несе нові загрози національній безпеці держави. Динамічна діджиталізація та стрімке поширення комунікаційних платформ (зокрема, соціальних мереж) створили не лише нові можливості для реформування публічного управління, а й стали потужним інструментом для реалізації злочинних намірів та ведення масштабних інформаційних війн. Усвідомлення цього безпекового виклику на міждержавному рівні прийшло наприкінці ХХ століття, що актуалізувало необхідність спільного міжнародного реагування на загрози локального і глобального характеру.

Актуальність теми дослідження зумовлена тим, що сучасна кіберзлочинність вийшла за межі класичних ізольованих фактів несанкціонованого доступу. Сьогодні вона становить собою системну індустрію правопорушень, що охоплює цифрові шахрайства нового покоління, поширення деструктивного програмного забезпечення та скоординовані атаки на критичну інфраструктуру. Особливу суспільну небезпеку становлять цілеспрямовані кібердиверсії проти державних баз даних, енергетичних мереж та систем управління, що здатні паралізувати інституційну спроможність цілих галузей економіки і створити плацдарм для масштабних інформаційно-психологічних операцій.

Для України ця проблема набуває важливого значення, тому що в умовах повномасштабної збройної та гібридної агресії кіберпростір перетворився на повноцінний простір воєнних дій. За таких умов формування новітніх правових механізмів протидії кіберзагрозам перестає бути суто галузевим юридичним завданням і стає ключовим фактором збереження державного суверенітету, забезпечення національної безпеки та захисту демократичного розвитку України.

Сьогодні важливим пріоритетом національної політики у галузі інформаційної безпеки та запобіганні злочинності у сфері цифрових технологій

є захист важливих інтересів, прав і свобод людини і громадянина. Спільні заходи сил безпеки, інших органів влади, місцевого самоврядування та громадськості забезпечують захист національних інтересів від реальних і потенційних загроз, що виникають у глобалізаційному світі. Тому, надзвичайно актуальною в умовах глобалізації та стрімкого розвитку цифрових технологій є проблема забезпечення інформаційної безпеки у державі.

У цьому вимірі кібербезпека остаточно трансформується із суто технічної проблеми ІТ-сектору в засадничий національний пріоритет, від якого безпосередньо залежить економічна стабільність держави, рівень суспільної довіри та загальна цифрова безпека громадян. Як обґрунтовано зазначає Ніколь Квінн (віцепрезидентка Palo Alto Networks), сучасний етап технологічного поступу маркує появу штучного інтелекту як своєрідного «двосічного меча» [78, с. 10]. Якщо суб'єкти транснаціональної кіберзлочинності використовують його для масштабування фішингу та розповсюдження шкідливого програмного забезпечення зі «швидкістю машини», то система національного захисту вимагає симетричного впровадження інтелектуальних систем. Це зумовлює необхідність переходу до проактивних моделей оборони, де системи на базі ШІ здатні автономно аналізувати критичні потоки даних, залучаючи людину як стратегічного суб'єкта прийняття рішень лише у випадках, що потребують високорівневого експертного втручання.

Розвиток глобальної мережі Інтернет та цифрова революція трансформували суспільство, принісши безпрецедентні переваги у сфері комунікацій, економіки та державного управління. Проте, поряд із позитивними аспектами, це призвело до зростання кількості та складності кримінальних правопорушень у кіберсфері. Вони охоплюють широкий спектр діянь: від фінансового шахрайства з використанням безготівкових активів та порушення авторських прав до розповсюдження шкідливого контенту та неправомірного доступу до конфіденційної інформації.

Впровадження інноваційних технологій у сферу безпеки є показником рівня розвитку країни і фактором її високого економічного та політичного рівня, спрямованим на забезпечення національних інтересів. Проте технологічний прогрес має й негативні аспекти, що визначають залежність держави і особи від системи комунікативних, енергетичних, біотехнологічних, хімічних, транспортних та фінансових послуг.

Відповідно до щорічного звіту компанії McAfee про загрози, глобальні збитки від кіберзлочинності перевищують 1 трильйон доларів. У 2023 році, кількість кібератак у всьому світі зростає на 38% у порівнянні з 2022 роком. Серед опитаних організацій 56 % відзначили відсутність плану запобігання та реагування на кіберінциденти. З 951 організацій, які справді мали план реагування, лише 32 % сказали, що їх план був ефективним [143].

Особливої небезпеки кіберзлочинність набуває в умовах воєнного стану в Україні. Окрім активних бойових дій, країна зіткнулася з повномасштабною інформаційною війною. Кіберзлочинці активно вчиняють злами урядових серверів, поширюють дезінформацію серед населення, здійснюють цільове кібершахрайство, що завдає суспільству не менших збитків, ніж збройний конфлікт на полі бою. Таким чином, війна виявила необхідність посилення національної кіберстійкості.

На сьогодні, кримінологічні засади запобігання злочинності у цифровому середовищі залишаються на недостатньому рівні. Це пояснюється тим, що кіберзлочинці постійно вдосконалюють методи вчинення правопорушень. Нові виклики, зокрема Генеративний ШІ, створюють можливості для масового виробництва високореалістичного дезінформаційного контенту та синтетичних матеріалів експлуатації, що вимагає негайного правового реагування.

Крім того, однією з проблем є транскордонний характер кіберзлочинів, що значно ускладнює процес їх виявлення, розслідування та притягнення винних до відповідальності. Це підкреслює імператив міжнародного співробітництва та гармонізації національного законодавства з європейськими стандартами та

прецедентною практикою ЄСПЛ. Дослідження має на меті розробити кримінологічні механізми, які сприятимуть формуванню національної кіберстійкості як здатності держави та суспільства ефективно запобігати цифровим загрозам і швидко відновлюватися після них.

Все це підкреслює важливість обраної теми і необхідність ґрунтовного кримінологічного дослідження чинного законодавства, правозастосовної практики і зарубіжного досвіду для розробки ефективних превентивних механізмів та забезпечення інформаційної безпеки як ключового елемента національної безпеки.

Актуальність дослідження також підтверджується офіційними статистичними даними Офісу Генерального прокурора, які свідчать про довгострокового зростання кількості кримінальних правопорушень у сфері інформаційних технологій. Якщо на початковому етапі гібридної агресії у 2014 році було обліковано лише 443 злочини, то в період 2018–2020 років відбулося накопичення латентного потенціалу (з 2 301 до 2 498 правопорушень). Повномасштабне вторгнення спровокувало різку інтенсифікацію криміналізації кіберпростору: у 2021 році обліковано 3 310 кримінальних правопорушень, у 2022 році - 3 415, у 2023 році - 3 841, а у 2024 році показник злочинності досяг історичного піка і становив - 4 055 облікованих кримінальних правопорушень. Порівняно з 2020 р. приріст склав 38,4%, а порівняно з 2023 р. - 5,3% [168].

Проблемам забезпечення інформаційної безпеки, формування кримінально-правової політики, присвячені роботи багатьох учених. Це наукові праці вітчизняних учених, як Д. С. Азаров, А.М. Бабенко, О.М. Бодунова, Я. Берзиньш, І. Р. Березовська, О. І. Бугера, М. В. Гуцалюк, Б. М. Головкін, Г. В. Дідківська, В. М. Дрьомін, М. В. Карчевський, Т.В. Корнякова, О. Г. Колб, А. М. Коломієць, О. В. Климчук, В. А. Ліпкан, В. В. Марков, Л.М. Мудриєвська, Г. Г. Почепцов, М. М. Присяжнюк, О. В. Таволжанський, Ш. Шольберг, С. Хантінгтон, О. Е. Радутний, Д.О. Ричка, О.В. Сачко, В. В. Топчій, Т. Л. Тропіна,

А. В. Тунік, Д. М. Цехан В. М. Шевчук, В. Ю. Шепітько, Н. С. Юзікова, О. М. Яхно та інших.

Проблемам міжнародно-правового регулювання кіберпростору, технічного та когнітивного захисту, моделювання кібератак, протидії транснаціональній кіберзлочинності та використанню OSINT присвячені роботи багатьох провідних зарубіжних і вітчизняних учених. Це наукові праці таких дослідників, як Дж. С. Албанезе, Дж. Андресс, М. Баезнер, Е. Балажанов, Я. Берзінш, К. Бронк, М. Брюс, Р. Вальцман, З. В. Валіулліна, Б. Ван, Х. Дж. Вільямс, М. Глассман, С. Джаджодія, Ю. Діогенес, С. Євсєєв, М. А. Кутайшат, В. Лі, О. Мілов, С. Москаль, П. Павляк, Г. Рзаєва, А. Фатема, Л. Фрімен, С. Цінь, М. Н. Шмітт та інших.

Визнаючи вагомий внесок зазначених науковців у теорію і практику забезпечення інформаційної безпеки та формування кримінально-правової політики, слід констатувати, що динаміка сучасних викликів випереджає існуючі напрацювання. Зокрема, питання розбудови стійкого цифрового суспільства та заходи запобігання кіберзлочинності в умовах воєнного стану залишаються недостатньо вивченими. Попри наявність ґрунтовних праць у сфері протидії цифровим загрозам, сьогодні спостерігається дефіцит досліджень, присвячених аналізу практики ЄСПЛ щодо дотримання прав людини при застосуванні превентивних та санкційних заходів проти суб'єктів, причетних до посягань на інформаційний суверенітет держави.

Зв'язок роботи з науковими програмами, планами, темами, грантами. Дисертаційне дослідження співвідноситься з Переліком пріоритетних тематичних напрямів наукових досліджень і науково-технічних розробок на період до 31 грудня року, наступного після припинення або скасування воєнного стану в Україні, затверджених постановою Кабміну України № 476 від 30 квітня 2024 року; Пріоритетними напрямами розвитку науки і техніки та інноваційної діяльності (відповідно до Закону України від 12 січня 2023 року №2859-IX зі змінами). Положення дисертації корелюють із Цілями сталого розвитку України

на період до 2030 року, затвердженими Указом Президента України від 30 вересня 2019 року № 722/2019; Стратегією національної безпеки України; Стратегією кібербезпеки України; Комплексним стратегічним планом реформування органів правопорядку як частини сектору безпеки і оборони України на 2023 - 2027 роки, затвердженого Указом Президента України від 11 травня 2023 року № 273/2023; Рішенням Ради національної безпеки і оборони України «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації», затвердженому Указом Президента України від 13 лютого 2017 року № 32/2017.

Дисертація відповідає дослідницькій темі кафедри адміністративного і кримінального права Дніпровського національного університету імені Олеся Гончара «Забезпечення реалізації та захист основних свобод, прав людини, національних інтересів держави в умовах гібридних загроз і безпекових викликів» (затвердженої рішенням ради юридичного факультету, протокол № 7 від 08.01.25 р., номер держреєстрації 0125U002352)..

Тему дисертації затверджено рішенням Вченої ради Дніпровського національного університету імені Олеся Гончара від 1 грудня 2022 року (протокол № 4).

Мета і завдання дослідження Метою дослідження є комплексне кримінологічне обґрунтування та розроблення науково-практичних засад забезпечення інформаційної безпеки в Україні, включаючи вдосконалення превентивних механізмів, гармонізацію національного законодавства з європейськими стандартами верховенства права та формування національної кіберстійкості в умовах локальних і глобальних викликів, воєнного стану та повоєнного відновлення держави. Досягнення визначеної мети обумовило вирішення таких *завдань*:

- охарактеризувати сутність, зміст та рівні інформаційної безпеки як об'єкта кримінологічного захисту та правової превенції в сучасних умовах;

- проаналізувати генезис наукової думки та етапи становлення правових засад забезпечення інформаційної безпеки, виявивши ключові тенденції у вітчизняному та зарубіжному досвіді;
- дослідити принципи, механізми та роль міжнародно-правового забезпечення інформаційної безпеки у протидії кіберзагрозам транснаціонального характеру;
- визначити особливості, закономірності та провідні тенденції функціонування системи забезпечення інформаційної безпеки в умовах правового режиму воєнного стану з метою виявлення системних прогалин функціонування державних органів та обґрунтування стратегічного переходу сектору безпеки до проактивної моделі реагування на комплексні кіберзагрози;
- розкрити сучасні законодавчі та інституційні засади забезпечення інформаційної безпеки в Україні як систему правового захисту національного простору, визначити їхнє значення для нейтралізації системних кіберзагроз та ліквідації наявних правових прогалин;
- розкрити специфіку та багаторівневу структуру кримінологічної превенції у сфері інформаційної безпеки в контексті балансу між захистом державного суверенітету та прав і свобод людини;
- здійснити порівняльно-правовий аналіз зарубіжних стратегій забезпечення інформаційної безпеки для обґрунтування шляхів гармонізації національного законодавства та модернізації механізмів правозастосування в Україні відповідно до міжнародних стандартів кіберстійкості;
- обґрунтувати загальний та спеціальний рівні міжнародного співробітництва й уніфікації законодавства у сфері протидії транснаціональній кіберзлочинності і визначити стратегічну роль України в сучасній системі європейської кібербезпеки;
- розробити та сформулювати перспективні напрями вдосконалення кримінологічного забезпечення інформаційної безпеки шляхом формування

національної кіберстійкості на макро- та мікрорівнях, а також рекомендації щодо формування національної кіберстійкості в Україні.

Об'єктом дослідження є суспільні відносини, що виникають у сфері функціонування системи забезпечення інформаційної безпеки України в контексті запобігання кіберзлочинності, гармонізації із міжнародними стандартами та формування національної кіберстійкості.

Предметом дослідження є кримінологічні засади забезпечення інформаційної безпеки: міжнародний, національний та зарубіжний виміри.

Методи дослідження. Методологічною основою дослідження є система філософських, загальнонаукових та спеціально-наукових методів, а також міждисциплінарний підхід, що забезпечує всебічне та об'єктивне вивчення кримінологічних засад інформаційної безпеки. Зокрема, використання діалектичного методу дозволило простежити взаємозв'язок між розвитком інформаційних технологій та появою нових форм високотехнологічної протиправної поведінки (підрозділи 1.1, 1.3, 3.1); системно-структурний метод застосовано для моделювання трирівневої структури інформаційної безпеки та аналізу інституційного механізму її забезпечення (підрозділи 1.1, 2.2, 3.3); порівняльно-правовий метод став основою для аналізу зарубіжних стратегій кібербезпеки та виявлення шляхів їх імплементації в національне законодавство (підрозділи 1.2, 3.1, 3.2); статистичний та віктимологічний методи дозволили дослідити емпіричний масив судової та правоохоронної практики, а також обґрунтувати концепцію техногенної віктимності організацій в умовах воєнного стану (підрозділи 2.1, 2.3); праксеологічний метод застосовувався для оцінки ефективності та раціональності наявних заходів запобігання кіберзлочинності, що дало змогу розробити практичні рекомендації щодо вдосконалення функціональних механізмів забезпечення інформаційної безпеки (підрозділи 1.3, 2.2, 3.3); аксіологічний метод використовувався для дослідження ціннісних пріоритетів у сфері інформаційної безпеки та кримінально-правової політики, що дозволило обґрунтувати необхідність гармонізації національного законодавства

з європейськими стандартами верховенства права та захисту прав людини як ключовими цінностями у цифровому середовищі (підрозділи 1.3, 2.3, 3.3); метод факторного аналізу застосовувався для ідентифікації та систематизації нових криміногенних чинників, зокрема впливу Інтернету речей та використання технологій Big Data у діяльності кіберзлочинців, а також для оцінки їхнього внеску у латентність та динаміку кіберзлочинності (підрозділи 2.1, 2.2). Збір та аналіз інформації базувалися на репрезентативній базі вітчизняних та іноземних джерел, аналітичних матеріалах міжнародних безпекових інституцій та практичному досвіді протидії гібридній агресії.

Нормативно-правову базу дослідження становлять Конституція України, КК України, КПК України, Закони України «Про основні засади забезпечення кібербезпеки України», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про національну безпеку України», а також міжнародні договори України, зокрема Конвенція Ради Європи про кіберзлочинність (Будапештська конвенція), Регламент (ЄС) № 2024/2847 Європейського Парламенту та Ради від 23 жовтня 2024 р. про горизонтальні вимоги до кібербезпеки продуктів із цифровими елементами та ін. Також досліджувалися резолюції та акти ЄС, підзаконні акти та відомчі інструкції, що регламентують правові засади запобігання кіберзлочинності та забезпечення інформаційної безпеки в умовах євроінтеграції.

Теоретичну основу дослідження становлять результати наукових праць вітчизняних і зарубіжних учених у галузі кримінології, кримінального та кримінального процесуального права, міжнародного гуманітарного права, права Європейського Союзу, теорії інформаційної безпеки, кібербезпеки, адміністративного права, соціології, а також філософії права та інформаційних технологій. Додатково вивчалися праці, що мають безпосереднє відношення до тематики верховенства права, прав людини у цифровому середовищі та формування національної кіберстійкості.

Емпіричну базу дослідження становлять: дані кримінально-правової та відомчої статистики Офісу Генерального прокурора, Національної поліції України та Департаменту кіберполіції про стан, структуру, динаміку та латентність комп'ютерних злочинів за період 2014–2026 рр.; аналітичні огляди та узагальнення судової практики Верховного Суду й рішення національних судів різних інстанцій; прецедентна практика Європейського суду з прав людини (ЄСПЛ) у контексті дотримання балансу верховенства права та невтручання у приватне життя; нормативні стандарти Загального регламенту про захист даних Європейського Союзу (GDPR) та безпекові директиви Агентства національної безпеки США (NSA). Документальну основу роботи також складають аналітичні доповіді й рекомендації Спеціальної моніторингової місії (СММ), Центрів передового досвіду з кібероборони НАТО (NATO CCDCOE), Європолу, ООН та Ради Європи.

Наукова новизна отриманих результатів полягає в тому, що дисертація є першим в Україні комплексним монографічним дослідженням, в якому реалізовано кримінологічно-інтегративний підхід до формування засад забезпечення інформаційної безпеки, гармонізованих із європейськими стандартами верховенства права, з визначенням шляхів розв'язання низки фундаментальних і прикладних проблем національної кіберстійкості.

Найсуттєвішими вважаються такі положення:

Вперше:

- обґрунтовано комплексну трирівневу модель інформаційної безпеки як об'єкта кримінологічного захисту, який базується на розширеній міжнародній матриці безпеки (Тріада СІА (конфіденційність, цілісність, доступність) доповнена процесуальними елементами автентичності, неспростовності) та структурно розподіляється на інфраструктурний, правовий режим та підзвітність (інформаційно-регуляторний) і соціально-психологічний (когнітивний) рівні. Такий підхід дозволив виділити наскрізний характер сучасних кіберзагроз та визначити специфічні вектори проактивної превенції для кожного з рівнів;

- обґрунтовано дворівневий розподіл поняття «кіберстійкість» у контексті забезпечення інформаційної безпеки на державний (публічно-правовий) та особистісний (людиноцентричний) рівні. Зокрема, «кіберстійкість держави» визначено як стратегічну спроможність національної системи інформаційної безпеки підтримувати критичні функції, адаптуватися до гібридних загроз та відновлювати цифрову інфраструктуру на основі інституційної координації сектору безпеки (МВС, Нацполіція, ЦПД), ефективному управлінні ризиками ланцюгів постачання та впровадженні метрик «кіберзрілості» за міжнародними стандартами; «кіберстійкість особи» визначено як сукупність когнітивних навичок, правової обізнаності та кібергігієни індивіда, що формують його когнітивний імунітет до дезінформації та здатність захищати приватність у цифровому середовищі;
- обґрунтовано концепцію «когнітивного імунітету» нації як невід'ємного елемента виміру інформаційної безпеки, що базується на зарубіжному досвіді розбудови потенціалу (capacity building) та передбачає перехід від захисту технічного периметра до формування стійкості людського капіталу;
- підхід до забезпечення інформаційної безпеки України в умовах розвитку технологій штучного інтелекту шляхом приєднання до європейської системи кібербезпеки та інтеграції авторської пропозиції заснування національного Інституту безпеки ШІ (за прикладом Інституту безпеки штучного інтелекту Великобританії) як координаційного хабу для впровадження міжнародних стандартів у практику запобігання, виявлення і розслідування високотехнологічних кіберзлочинів;
- запропоновано визначення «когнітивного імунітету суспільства» як самостійної кримінологічної та віктимологічної категорії, що становить мікрорівень національної кіберстійкості і визначає здатність суспільства виступати самозахисним бар'єром проти транснаціональних інформаційно-психологічних операцій та шахрайства у цифровому середовищі.

вдосконалено:

- віктимологічний підхід до запобігання кіберзлочинності через обґрунтування змісту «техногенної віктимності» організацій, на основі аналізу міжнародного досвіду використання хмарних сервісів. Так, в умовах розмиття меж цифрової інфраструктури провідним чинником злочинних посягань є організаційна недбалість, яка виявляється у помилках налаштування конфігурації, поширенні неконтрольованого програмного забезпечення та відсутності чіткої договірної підзвітності, саме ці вразливості нівелюють систему захисту об'єкта та перетворюють легітимних працівників на носіїв кіберзагроз;
- періодизацію розвитку системи забезпечення інформаційної безпеки України шляхом виокремлення IV (з 2014 року до сьогодні), який зумовлений воєнними викликами і характеризується переходом від технічного захисту до формування стратегічної кіберстійкості держави;
- визначення засад реалізації принципу невідворотності кримінальної відповідальності у цифровому середовищі, шляхом інтеграції техніко-юридичного елемента «неспростовності» до системи доказування, що дозволяє нейтралізувати наслідки використання злочинцями систем анонімізації та транскордонної маршрутизації трафіку в умовах глобальної кризи доведення джерела кібератак та причетності конкретної особи до кіберзлочинів;
- кримінологічну характеристику кіберзлочинності в умовах воєнного стану, шляхом включення до неї нових факторів криміногенного ризику штучного інтелекту та Інтернету речей та обґрунтовано доцільність криміналізації нових цифрових загроз, зокрема, створення та поширення згенерованого за допомогою ШІ синтетичного контенту експлуатації дітей;
- підхід до класифікації моделей забезпечення кіберстійкості шляхом виокремлення чотирьох взаємозалежних вимірів (стратегічного, нормативного, інституційного та екосистемного), що дозволяє комплексно оцінювати рівень «кіберзрілості» держави і суспільства;

набуло подальшого розвитку:

- науковий підхід до розуміння сутності інформаційної безпеки держави, що ґрунтується на інтеграції правових, соціальних та етичних аспектів у єдину систему захисту; забезпеченні справедливої рівноваги між свободою слова та межами державного контролю задля превенції кіберзлочинності; гармонізації міжнародних стандартів (зокрема, Будапештської конвенції та GDPR) із національними правовими традиціями, а також на впровадженні випереджальних превентивних механізмів, які враховують поведінкові ризики та соціальні фактори протиправності у цифровому середовищі;
- антропоцентричний підхід до забезпечення інформаційної безпеки, де найвищим пріоритетом (соціально-психологічним рівнем) визнається захист суспільної свідомості, процесу формування волі та цифрових прав людини;
- положення щодо зміни міжнародно-правового статусу України в системі європейської кібербезпеки шляхом успішної інтеграції правоохоронних органів України у спільні транскордонні поліцейські операції та системи обміну розвідувальними даними, для остаточного національного переходу від ролі об'єкта захисту до статусу активного учасника колективної безпеки.

Практичне значення отриманих результатів полягає в тому, що викладені у дослідженні висновки і пропозиції можуть бути використані у:

- *науково-дослідній діяльності* – як основа для подальших наукових досліджень кримінологічних, кримінально-правових та процесуальних аспектів запобігання кіберзлочинності в Україні, зокрема у сфері впливу Генеративного ІІІ та міжнародної співпраці (акт впровадження в наукову діяльність Дніпровського національного університету імені Олеся Гончара від 9 вересня 2025 р.);
- *правотворчій діяльності* – під час розробки змін і доповнень до чинного законодавства, що регулює питання кібербезпеки, захисту персональних даних та протидії дезінформації, а також гармонізації національного законодавства з актами ЄС та стандартами верховенства права;

- *правозастосовній сфері* – як науково обґрунтовані заходи щодо підвищення ефективності діяльності правоохоронних органів (Національної поліції, Кіберполіції, Прокуратури) із виявлення, розслідування та запобігання транскордонним кіберзлочинам, а також для забезпечення дотримання гарантій прав людини відповідно до прецедентної практики ЄСПЛ під час цифрових розслідувань;
- *навчальному процесі* під час підготовки відповідних наукових, навчально-методичних видань та проведенні занять із навчальних дисциплін «Кримінологія», «Запобігання злочинності у контексті глобалізації», «Кримінальне право України» (акт впровадження у навчальний процес Дніпровського національного університету імені Олеся Гончара від 07.10. жовтня 2025 р.).

Особистий внесок здобувача. Дисертація є самостійною, завершеною науковою працею. Сформульовані в ній положення, узагальнення, висновки, рекомендації та пропозиції обґрунтовано на підставі самостійно проведених досліджень.

Автором запропоновано комплексні інституційні та функціональні зміни до системи заходів забезпечення інформаційної безпеки України, що ґрунтуються на всебічному аналізі доктринальних джерел, вітчизняної практики забезпечення кіберстійкості, міжнародно-правових стандартів, а також передового досвіду іноземних держав у сфері протидії гібридним загрозам. Усі наукові положення, висновки, рекомендації та пропозиції, викладені у дисертації, є результатом особистої наукової роботи здобувача. Ідеї, положення та гіпотези інших науковців використані з дотриманням академічної доброчесності та належного цитування з метою аргументації власних наукових підходів до розбудови національної системи інформаційної безпеки.

Апробація результатів дисертації. Основні положення та висновки дисертації оприлюднено у виступах на міжнародних та всеукраїнських науково-практичних конференціях, форумах, круглих столах: всеукраїнському науково-

практичному юридичному форуму «Національна парадигма правового розвитку сучасної України» (м. Дніпро 18.05. 2023 р.); всеукраїнській науково-практичній конференції «Забезпечення принципів поваги, захисту та реалізації прав дитини у цифровому середовищі» (м. Дніпро 23.11.2023 р.); всеукраїнському науково-практичному круглому столі «Інформаційна агресія в сучасному світі: правовий аналіз та протидія» (м. Харків, 21.06. 2024 р.); міжнародній науково-практичній конференції «Актуальні проблеми прав людини: від універсальних стандартів до національної практики» (м. Львів – Торунь 10.12.2025 р.); всеукраїнській науково-практичній конференції «Актуальні проблеми правової науки (м. Запоріжжя 22.12. 2025 р.).

Публікації. Основні положення дисертаційної роботи опубліковано в 10 наукових працях, з яких: 5 – статті в наукових фахових виданнях України, 5 у тезах матеріалів конференцій.

Структура та обсяг дисертації. Дисертація складається з анотації, вступу, трьох розділів, що включають 9 підрозділів, висновків, списку використаних джерел, що включає 347 найменувань, 2 додатки. Повний обсяг дисертації становить 263 сторінок, з яких: основний текст – 194 сторінок, список використаних джерел – 44 сторінки.

РОЗДІЛ I

ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ОСНОВИ КРИМІНОЛОГІЧНОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1. Інформаційна безпека як об'єкт кримінологічного захисту та превенції: зміст, рівні та сучасні виклики

Інформаційна безпека охоплює широкий аспект захисту незалежно від форми, в якій зберігається чи обробляється інформація. Вона включає захист даних, процесів, інформаційних систем і мереж від незаконного доступу, використання, розкриття, розголошення, модифікації чи знищення. Принципи інформаційної безпеки забезпечують конфіденційність, цілісність і доступність всієї значимої інформації - будь то друкована, усна або електронна.

У сучасну епоху гібридних загроз інформаційна безпека поступово трансформувалась зі сфери технічного захисту на ключовий об'єкт кримінологічного захисту національного та транснаціонального рівня. З огляду на те, що кіберпростір став новою сферою впливу, а суспільна свідомість основною ціллю інформаційно-психологічних операцій (ІПСО), традиційні підходи до превенції вимагають радикального переосмислення. Кримінологічна наука має визначити стратегічні межі захисту та сформувати комплекс заходів, спрямованих не лише на боротьбу з кіберзлочинністю, а й на забезпечення правової та соціальної стійкості держави і суспільства. Тому, враховуючи зростання загроз у кіберпросторі наукового значення набуває визначення інформаційної безпеки як об'єкта кримінологічного захисту. Поняття інформаційної безпеки має бути структуровано не лише через технічний захист, а й через призму соціально-правової стійкості держави та суспільства. Проте, аналіз сучасного наукового доробку виявляє значну неповноту та дискусійність у визначенні ключових категорій, що безпосередньо ускладнює формування ефективних превентивних стратегій.

Як слушно зазначається у науковій літературі, ступінь наукової розробки теоретичних засад інформаційних правовідносин, попри їх інтеграцію у всі

сфери людської діяльності, залишається дискусійним та незавершеним, що вимагає однозначного розуміння фундаментальних категорій та усунення відсутності єдності категоріальних понять [201, с. 126-133; 12; 17, с. 187-195; 216]. Саме ця неповнота основних понять в інформаційному праві прямо впливає на визначення об'єкта кримінологічного захисту.

Інформаційна безпека це стан і політика захисту інформації незалежно від форми її існування, каналів передачі (усні комунікації, медіа, документи), а також захист інформаційної свідомості суспільства від маніпулятивного контенту, дезінформації та інших інформаційно-психологічних впливів. Зміст інформаційної безпеки включає правові, організаційні, освітні, етичні та комунікаційні інструменти, спрямовані на забезпечення конфіденційності, цілісності, доступності й законності обробки даних, а також на підтримку державної інформаційної політики та стратегічних комунікацій. Такий підхід узгоджується з сучасними правовими та науковими оглядами, що розглядають інформаційну безпеку як рамкову категорію національної безпеки [35; 97; 216, с. 203-228; 227, с. 97-101; 194; 196; 296, с. 63-70].

Крім того питання інформаційної безпеки можна розглядати у історичному (генетичному) контексті. Так, методологія Б.О. Кістяківського дозволяє розглядати інформаційну безпеку не лише як технічну проблему, а як комплексне соціально-правове явище [127, с. 131-135]. Генетичний підхід допомагає зрозуміти еволюцію загроз і формувати кримінологічні стратегії, що поєднують превентивні заходи, правові гарантії та баланс між свободою і безпекою. Історичний метод дає змогу виявити закономірності, що визначають розвиток правової системи, та уникнути повторення помилок минулого. У сфері інформаційної безпеки ці закономірності проявляються у поступовому розширенні кола прав: від класичних громадянських і політичних прав до сучасних цифрових прав, таких як право на доступ до інформації, захист персональних даних та кібербезпеку. Інша закономірність полягає у залежності пріоритетів від соціально-економічних умов: глобалізація та цифровізація

обумовили появу нових прав, пов'язаних із захистом інформаційного простору та приватності. Помилки, яких слід уникати, включають формальний підхід до регулювання кіберзагроз без створення дієвих механізмів їх запобігання (аналогія з декларативними конституціями XIX століття) та ігнорування потреб суспільства у безпечному цифровому середовищі, що може призвести до кризових явищ, а саме: масових витоків даних, кібертероризму, інформаційних атак. Історичний аналіз показує, що відсутність балансу між свободою слова та інформаційною безпекою або між правами користувачів і їхніми обов'язками створює ризики для стабільності держави.

Аналіз теорії інформаційних відносин вимагає комплексного залучення філософських, соціологічних та правових знань, оскільки відсутність повноти основних понять прямо впливає на ефективність правового регулювання та, як наслідок, на кримінологічну превенцію [201, с.126-133].

Інформаційна безпека в правовому контексті охороняє також основоположні права людини, зокрема право на приватність та конфіденційність, які є важливою частиною прав людини. Тому правові аспекти інформаційної безпеки є значущим компонентом в структурі сучасного права і державної політики. Це положення підтверджується міжнародними актами: Міжнародний пакт про громадянські і політичні права (1966) у ст. 17 гарантує право на недоторканність приватного життя [128]; Європейська конвенція з прав людини (1950) у ст. 8 закріплює право на повагу до приватного і сімейного життя [91]; Будапештська конвенція про кіберзлочинність (2001) встановлює стандарти боротьби з кіберзлочинами, що загрожують конфіденційності даних [252]; а GDPR (2016) визначає принципи обробки персональних даних і права суб'єктів даних [275].

Як зазначають Шишко В.В. та Горошко В.В., право на інформаційну безпеку є гарантією недоторканності приватного життя та правового захисту особи у цифровому середовищі, що узгоджується з цими міжнародними правовими актами [226, с. 275-281]. Барабаш О.О. підкреслює важливість захисту

конфіденційності персональних даних як ключового елементу прав людини [8, с. 560-563]. Добкіна К.Р. акцентує увагу на необхідності оновлення правових підходів для забезпечення балансу між правом на безпеку та правом на приватність у цифрову епоху [47, с.516-522].

Інформаційна безпека як об'єкт кримінологічного захисту – це стан захищеності життєво важливих інтересів особистості, суспільства та держави в інформаційній сфері (або інформаційному просторі), який забезпечується системою проактивних превентивних заходів, спрямованих на запобігання, виявлення, припинення та мінімізацію негативних наслідків криміногенних загроз та інформаційно-психологічних операцій (ІПСО), що мають на меті:

- порушення цілісності, конфіденційності та доступності інформації на будь-яких носіях (цифрових, паперових, усних);
- деструктивний вплив на суспільну свідомість (маніпуляції, дезінформація, вербування).
- дезорганізацію функціонування органів державної влади та об'єктів критичної інфраструктури.

Реалізація такої системи проактивних заходів та досягнення зазначеного стану захищеності вимагають чіткої ідентифікації того, на що саме спрямовані злочинні посягання. Отже, виникає потреба у детальній характеристиці внутрішнього змісту інформаційної безпеки.

Фундаментом змісту інформаційної безпеки, що визначає межі та спрямованість кримінологічної охорони, виступає концепція основних властивостей інформації, відома у міжнародній практиці як Тріада СІА (конфіденційність, цілісність, доступність). Ця тріада формує базову модель для аналізу безпекових концептів, зосереджуючись насамперед на захисті даних від спектра криміногенних загроз та технічних вразливостей. [237, с.4-7; 327]. Так, інформаційна безпека - збереження конфіденційності, цілісності та доступності інформації [283]. Цей стандарт має глибоку техніко-юридичну природу та імплементований у ключові міжнародні і національні нормативні акти. Тріада

CIA формує фундамент для аналізу безпекових концептів, зосереджуючись насамперед на захисті даних від спектра криміногенних загроз та технічних вразливостей. Будь-яка кібератака чи інформаційно-психологічна операція (ІПСО) зрештою має на меті порушити один або декілька елементів цієї тріади.

Конфіденційність полягає у гарантуванні та забезпеченні доступу до інформації виключно авторизованим суб'єктам. Прикладом може слугувати шифрування персональних даних. З кримінологічної точки зору, компрометація конфіденційності (що в індустрії безпеки визначається як витік даних або може статися не лише через складне проникнення зловмисників у систему. Нормативно-правове забезпечення цього елемента має глибоку ретроспективу, починаючи з Закону США про конфіденційність (The Privacy Act of 1974) та Директиви 95/46/ЄС [335; 265]. На сучасному етапі цей елемент змісту гарантується положеннями Конвенції Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних, Додатковим протоколом до Конвенції стосовно органів нагляду та транскордонних потоків даних, Загальним регламентом про захист даних ЄС (GDPR) та Законом України «Про захист персональних даних» [89; 49; 57; 170]. З позиції кримінології, забезпечення конфіденційності є базовою умовою запобігання несанкціонованим витокам інформації та порушенню права на недоторканність приватного життя.

Цілісність передбачає захист від несанкціонованої модифікації, спотворення або знищення даних, що гарантує їх достовірність, тобто здатність запобігати зміні або видаленню даних у несанкціонований чи небажаний спосіб. Прикладом може слугувати використання хешування та цифрових підписів. Для підтримання цілісності важливо не лише блокувати протиправні модифікації (шляхом розмежування прав доступу на рівні операційних систем), а й мати механізми «відкату» до попереднього легітимного стану у разі небажаних змін. У контексті ІПСО саме порушення цілісності (підробка фактів, створення дипфейків) є головним інструментом маніпуляції. Кримінологічна значущість цілісності як об'єкта захисту ілюструється на прикладі баз даних закладів

охорони здоров'я. Якщо правопорушник несанкціоновано змінить електронні результати медичних аналізів пацієнта, це детермінує призначення хибного лікування та може призвести до летальних наслідків для життя людини. Цей елемент, як об'єкт захисту від кіберпосягань, концептуалізовано у Федеральному законі США про модернізацію інформаційної безпеки (FISMA 2014), який встановлює жорсткі вимоги до збереження автентичності інформаційних систем [337]. На глобальному міжнародно-правовому рівні цілісність охороняється нормами Будапештської конвенції про кіберзлочинність (2001 р.), а також відображена у «Принципах, що стосуються міжнародної інформаційної безпеки» (погоджених Групою урядових експертів ООН), які наголошують на неприпустимості протиправного втручання в інформаційні ресурси державзмісту та закріплені у стандартах Національного інституту стандартів і технологій США (NIST SP 800-53) [252; 312; 326; 306; 307; 333], є важливим для збереження цілісності електронних доказів у кримінальному провадженні та протидії цифровим маніпуляціям (зокрема, підробці даних з використанням алгоритмів штучного інтелекту).

Доступність-заключний елемент змісту, означає гарантування своєчасного та безперебійного доступу до інформаційних систем і ресурсів легітимним користувачам. Прикладом може слугувати захист від DDoS-атак та резервне копіювання систем. В умовах тотальної цифровізації цей критерій стає питанням виживання нації, функціонування критичної інфраструктури та основою національної безпеки. Втрата доступності може бути наслідком широкого спектра інцидентів: від перебоїв з електроживленням та збоїв програмного забезпечення до цілеспрямованих мережевих атак. Тому на європейському рівні пріоритет доступності та стійкості систем до атак було нещодавно закріплено у Директиві (ЄС) 2022/2555 [263]. В Україні ж безперебійність і доступність є ключовими об'єктами захисту відповідно до Законів «Про основні засади забезпечення кібербезпеки України» та «Про критичну інфраструктуру» [173; 177]. Порушення доступності (наприклад, через DDoS-атаки або програми-

вимагачі) детермінує паралізацію життєво важливих суспільних функцій. Водночас, стрімкий розвиток цифрових технологій, розширення сфери електронної комерції та ускладнення механізмів кіберзлочинності зумовили еволюцію класичної моделі безпеки. У сучасних кримінологічних концепціях та розширених стандартах інформаційного забезпечення фундаментальний базис Тріади СІА доповнюється ще двома критично важливими елементами, що мають особливе процесуальне та доказове значення [314].

Автентичність полягає у встановленні та верифікації справжності джерела інформації, транзакції або особи користувача (гарантія того, що суб'єкт чи об'єкт є тим, за кого себе видає). У кримінологічному вимірі цей елемент є ключовим для вирішення проблеми атрибуції кіберзлочину, тобто беззаперечної ідентифікації правопорушника в анонімному цифровому середовищі. Захист автентичності (нормативно врегульований, зокрема, законодавством про електронні довірчі послуги) мінімізує ризики шахрайства, крадіжки цифрової особистості та генерації фейкового контенту за допомогою систем ШІ.

Неспростовність - гарантія того, що суб'єкт не зможе успішно заперечити факт здійснення ним певної дії, відправки повідомлення чи ініціювання транзакції. Цей елемент має фундаментальне значення для кримінального процесу та розслідування економічних кіберзлочинів, особливо у сфері фінансового моніторингу та використання блокчейн-технологій. Забезпечення неспростовності (шляхом криптографічного захисту, цифрових підписів та логування) формує надійну доказову базу, позбавляючи правопорушника можливості уникнути юридичної відповідальності шляхом відмови від авторства деструктивних дій. Таким чином, розширення об'єкта захисту від базової технічної стійкості (СІА) до включення автентичності та неспростовності дозволяє правоохоронним і судовим органам констатувати факт атаки та юридично закріпити провину конкретної особи, забезпечуючи принцип невідворотності покарання. Комплексна реалізація цих п'яти елементів вимагає

просторової та функціональної декомпозиції об'єкта захисту на взаємопов'язані ієрархічні рівні, що обумовлюють її якісний зміст.

Перший рівень - об'єктно-функціональний (цілісність інфраструктури), що становить інфраструктурну основу безпеки та обумовлює забезпечення безперебійного та захищеного функціонування критичних інформаційних систем, мереж та баз даних. Об'єктом захисту цього рівня виступає фізична та логічна стійкість цифрового простору до несанкціонованого втручання.

Кримінологічний контекст полягає у забезпеченні цієї стійкості шляхом впровадження жорстких технічних стандартів (наприклад, NIST). Так, як свідчить міжнародний досвід, зокрема результати аудиту Служби генерального інспектора NASA (2016), навіть у високотехнологічних структурах цей базис стає вразливим через так звану «техногенну віктимність», а саме, використання неавторизованих хмарних сервісів (Shadow IT) або помилки в налаштуваннях, що відкривають шлях до порушення цілісності систем [327]. У контексті кримінологічної превенції цей кейс доводить, що об'єктом захисту сьогодні є не лише фізична інфраструктура, а й складний комплекс управлінських відносин та договірних зобов'язань із приватними провайдерами. Відтак, ефективна стратегія превенції має включати не тільки технічний моніторинг, а й механізм «превентивної підзвітності» та посилення наглядових повноважень регуляторів (зокрема, Офісу головного інформаційного офіцера - ОСІО) для мінімізації ризиків використання «тіньових» ІТ-ресурсів та забезпечення цілісності цифрового суверенітету організації.

Другий - системно-ресурсний рівень (захищеність даних), що фокусується на захищеності даних та інформаційному контенті, полягає у забезпеченні правового режиму доступу до інформації (конфіденційність) та гарантування її достовірності. Об'єктом захисту на цьому рівні є право власності на інформацію та право особи на контроль за власними персональними даними (запобігання витокам та незаконному обігу даних). Згідно з положеннями FISMA 2022, цей рівень охоплює інтерфейси взаємодії із зовнішніми суб'єктами (хмарними

провайдерами), що додає до об'єкта захисту управлінські відносини [271]. На цьому рівні, превенція зміщується від суто технічних бар'єрів до механізмів договірної підзвітності та управлінських відносин. Наприклад, ефективна превенція кіберзлочинності потребує включення до контрактів із постачальниками послуг специфічних положень про безпеку. Як свідчить досвід США, відсутність таких застережень у договорах NASA була визнана Генеральним інспектором як серйозний ризик, що потребує впровадження механізму превентивної підзвітності [327].

На системно-ресурсному рівні ключовим вектором проактивного стримування кіберзлочинності та забезпечення фундаментального принципу конфіденційності виступає імплементація міжнародних стандартів, насамперед Загального регламенту про захист даних (GDPR) [275]. Цей акт, що набрав чинності у 2018 році, стандартизує та безпрецедентно посилює правовий режим захисту персональних даних не лише у Європейському Союзі (ЄС), а й екстериторіально, формуючи глобальний еталон інформаційної безпеки.

Особливе процесуальне та превентивне значення мають імперативні вимоги GDPR щодо корпоративної підзвітності. Організації, які операційно займаються обробкою даних, зобов'язані не лише забезпечувати технічну безпеку (шифрування, псевдонімізацію), але й проводити регулярні аудити та впроваджувати процедуру обов'язкового повідомлення наглядових органів про витоки інформації. Це ліквідує латентність інцидентів інформаційної безпеки та забезпечує невідворотність відповідальності.

Для України імплементація основних положень GDPR до національної правової платформи є стратегічним кроком, що сприятиме підвищенню відповідальності онлайн-сервісів та цифрових платформ, зміцнюючи системну основу для боротьби з кіберзлочинністю. Крім того, синхронізація з європейськими вимогами захисту даних важлива для міжнародної взаємодії.

Третій - соціально-психологічний рівень (соціально-ціннісний), що визначає когнітивну безпеку. Це найвищий рівень, де об'єктом захисту виступає

суспільна свідомість. На третьому рівні відбувається захист людини та суспільства від деструктивних інформаційних операцій, маніпуляцій, мови ворожнечі та пропаганди протиправного (злочинного) способу життя. Тут безпека розглядається як стан захищеності процесу формування волі особи від зовнішнього протиправного впливу.

Пріоритетним напрямом охорони постають цифрові права людини (зокрема, права дитини в цифровому середовищі). Головним інструментом захисту на цьому етапі є віктимологічна профілактика: підвищення медіаграмотності, цифрової гігієни та розробка етичних запобіжників проти використання систем штучного інтелекту (ШІ) для генерації дипфейків чи маніпулятивних алгоритмів [111, с. 221-227; 132].

Запропонована кримінологічна модель узгоджується з вектором стратегічного розвитку України, де інформаційна безпека виступає не лише технічним регламентом, а ключовим елементом національної безпеки та відображується у засадах державної політики. Це підтверджується положеннями Стратегії інформаційної безпеки до 2025 року, яка визначає інформаційну безпеку через захищеність інтересів людини, суспільства і держави. Відповідно до Стратегії - це невід'ємна частина загальної національної безпеки, яка визначається захищеністю державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших ключових інтересів людини, суспільства і держави. Забезпечується ефективна система захисту від негативних інформаційних впливів, таких як координоване поширення недостовірної інформації, деструктивна пропаганда та інші інформаційні операції [180]. Інтегритет обмеженої інформації виступає гарантією того, що навіть якщо інформація доступна не всім або доступ обмежений, вона залишається достовірною й захищеною від спотворення.

Правову основу інформаційної безпеки становлять норми що стосуються цифрового середовища, які вказують на форми і методи захисту даних, управління цифровою інформацією та комунікаційними системами. Так, у ст. 17

Конституції України проголошено, що забезпечення інформаційної безпеки України є однією з найважливіших функцій держави справою всього Українського народу[94]. Далі визначено поточні та прогнозовані загрози національній безпеці та національним інтересам України з урахуванням зовнішньополітичних та внутрішніх умов, у Стратегії національної безпеки України [178]. Детально питання основ національної безпеки України було розглянуто у дослідженні професора О.Г. Колба [87, с. 82-87]

Наступним кроком нормативного закріплення сутності, мети, завдань, загроз заходів захисту інформаційної безпеки було Рішення Ради національної безпеки і оборони України від 29 грудня 2016 року, де було схвалено Доктрину інформаційної безпеки України (далі - Доктрина), яка стала стратегічним документом щодо окреслення концептуальних засад державної політики у сфері інформаційної безпеки [181].

Основні положення Доктрини включали: головну мету та стратегічні завдання державної інформаційної політики; основні принципи інформаційної безпеки, серед яких цілісність, автономія, суверенітет у інформаційному просторі, врахування демократичних цінностей і прав людини; характеристику внутрішніх та зовнішніх загроз національній інформаційній безпеці, включаючи дезінформацію, кібератаки та втручання в інформаційний простір.

Після втрати чинності Доктрини, рішенням Ради національної безпеки і оборони України від 15 жовтня 2021 року приймається Стратегія інформаційної безпеки до 2025 року (далі - Стратегія). Стратегія містить визначення загроз, засобів захисту, механізмів виявлення та запобігання злочинам у сфері інформаційної безпеки [180]. Основними напрямками реалізації Стратегії є протидія дезінформації, розвиток медіакультури. Важливими аспектами також є захист особистих даних та культури вільного вираження поглядів, підтримка зв'язку з громадянами на тимчасово окупованих територіях та розвиток стратегічних комунікацій. Також, вона охоплює положення про кібербезпеку, захист від дезінформації, захист критичної інфраструктури та інші аспекти,

спрямовані на міцний захист національних інтересів України. Як і в Доктрині, у Стратегії визначено сутність, засади, механізми інформаційної безпеки, наголошено на доцільності міжнародної співпраці та імплементації міжнародних угод та директив, таких як Конвенція про кіберзлочинність [92] GDPR [275], що формують міжнародно-правову основу інформаційної безпеки. Поряд з цим, у Стратегії більш чітко ніж у Доктрині визначені глобальні та національні виклики та загрози, з урахуванням яких сформовані напрями забезпечення інформаційної безпеки України у стійкості та взаємодії, для досягнення яких необхідним є виконання семи стратегічних цілей та завдань.

З'ясування змісту, рівнів та правової основи інформаційної безпеки створює необхідний теоретичний фундамент для аналізу сучасних криміногенних викликів. Специфіка новітньої кіберзлочинності полягає в її наскрізному характері. Аналіз актуальної криміногенної обстановки дозволяє виокремити три ключові групи викликів, що детермінують необхідність перегляду традиційних превентивних стратегій.

Перша група, інфраструктурні вразливості та «техногенна віктимність» організацій (виклик I та II рівня інформаційної безпеки). В епоху масової міграції даних до хмарних середовищ класичний фізичний периметр організації зникає. Головним криміногенним фактором на об'єктно-функціональному та системно-ресурсному рівнях стає не злам систем ззовні (хакінг у класичному розумінні), а експлуатація внутрішніх організаційних прогалин. Використання неавторизованих сервісів (Shadow IT) та помилки у налаштуваннях баз даних призводять до катастрофічних витоків конфіденційної інформації. Ситуація ускладнюється інтеграцією кіберзлочинності з тіньовим фінансовим сектором: атаки програм-вимагачів, спрямовані на блокування доступу до критичної інфраструктури, супроводжуються вимогою викупу у криптоактивах.

Характеризуючи неправильне налаштування конфігурації, варто зазначити, що у сучасній кримінологічній та технічній літературі цей феномен розглядається не як програмна вразливість (дефект коду), а як наслідок

організаційної недбалості та порушення вимог безпеки. Це охоплює широкий спектр помилок: використання стандартних (заводських) паролів, надання надлишкових прав доступу, відсутність шифрування на рівні баз даних або публічне відкриття хмарних сховищ (наприклад, AWS S3 buckets) без належної автентифікації користувачів [262].

З позиції кримінології, поширення таких інцидентів якісно змінює механізм вчинення кіберзлочину. Правопорушнику більше не потрібні складні інструменти для злому криптографічного захисту. Він використовує автоматизовані сканери для пошуку «відкритих дверей», залишених легітимними адміністраторами. Як зазначається у щорічних аналітичних звітах Verizon Data Breach Investigations Report (DBIR), які є фундаментальною емпіричною базою для світової кримінології, саме помилки конфігурації стабільно входять до трійки головних причин масштабних витоків інформації, формуючи стійку форму «техногенної віктимності» організацій [340].

Високий ступінь суспільної небезпеки цього явища підтверджується також офіційною позицією Агентства національної безпеки США (NSA), яке у своєму керівництві з безпеки хмарних середовищ класифікує misconfiguration як найбільш поширену та масштабну вразливість, що експлуатується кіберзлочинцями для компрометації систем критичної інфраструктури [302]. Зокрема, ключовою загрозою виступає неправильне налаштування конфігурації хмарних сховищ, що у 2016 році призвело до несанкціонованого доступу до масивів сенситивної інформації в межах усєї структури Агентства [327, с. 11-12]. Такий інцидент ілюструє трансформацію внутрішніх користувачів на «мимовільних суб'єктів загрози», коли технічна помилка або ігнорування протоколів безпеки фактично нівелює захисний потенціал об'єкта.

Додатковим викликом є децентралізація закупівель ІТ-послуг (так звані «тіньові ІТ»), коли окремі підрозділи самостійно набувають ліцензії на хмарні сервіси поза межами встановлених стандартів. У віктимологічному контексті це свідчить про «необачність власника інформації», яка полегшує реалізацію

злочинного умислу або призводить до незворотної втрати доказової бази. Останнє підтверджується випадком 2015 року, коли через відсутність у контрактах з провайдером вимог щодо обов'язкового логування мережевої активності, стало неможливим проведення ретроспективного аналізу компрометації облікових записів. Статус «невирішених» рекомендацій у звіті NASA свідчить про складність імплементації стандартів кібербезпеки в умовах децентралізації закупівель [327]. Це підтверджує необхідність жорсткої нормативної регламентації «спільної відповідальності» між державними замовниками та приватними хмарними провайдерами.

Одним із викликів для інформаційної безпеки як об'єкту кримінологічного захисту є суперечність між вимогами безпеки та операційною ефективністю. Приклад NASA ілюструє цю проблему: обмежена кількість сертифікованих за стандартом FedRAMP продуктів (лише 0,5% ринку) змушує суб'єктів управління приймати ризиковані рішення на користь неперевіраних сервісів, що створює лакуни в системі захисту національних інформаційних ресурсів [327, с. 14-15].

На соціально-психологічному рівні актуальні глобалізаційні ризики обумовлюють необхідність всебічного захисту цифрового середовища від посягань, мішенню яких стає сама людина. Серед актуальних ризиків у цій сфері можна виокремити класичні кібератаки, які включають фішинг, віруси, програми-вимагачі та інші загрози, що порушують інформаційну безпеку. Окрему небезпеку становить шпигунське програмне забезпечення, що збирає інформацію без відома користувача, детермінуючи масові витoki даних несанкціоновану публікацію або розкриття конфіденційної інформації.

Водночас, фундаментальним викликом сьогодні є масштабування цих інструментів та їх використання для глобальної дестабілізації суспільства. Як слушно зазначає професор Н.С. Юзікова, незадовільний стан інформаційної безпеки, розміщення у цифровому середовищі спотвореної, провокаційної інформації або дезінформації про політичні, економічні, соціальні процеси, що

відбуваються в Україні, негативно впливає на суспільну свідомість громадян України; детермінує зміни у поведінці та комунікації особистості[228, 346].

Друга група, вплив генеративного ШІ та загрози когнітивній безпеці. Масштабним викликом для соціально-психологічного (антропоцентричного) рівня інформаційної безпеки є милітаризація та криміналізація технологій штучного інтелекту. Використання нейромереж для створення реалістичних аудіо- та відеоматеріалів (діпфейків), автоматизованої генерації фішингових повідомлень та алгоритмічного поширення дезінформації завдає прямого удару по базових принципах «цілісності» та «автентичності». Окремим, вкрай гострим вектором цієї загрози є алгоритмічна віктимізація неповнолітніх: архітектура багатьох цифрових платформ використовує мікротаргетинг, що робить цифрове середовище агресивним та створює прямі загрози цифровим правам і психологічному благополуччю дитини.

Третя група, проблеми ідентифікації суб'єкта кіберзлочинів та межі кримінальної юрисдикції (юрисдикційний виклик інформаційної безпеки). Універсальним викликом, що паралізує ефективність кримінологічної превенції на всіх рівнях, є проблема атрибуції (ідентифікації) та процесуального доведення вини реального суб'єкта кіберзлочину. Злочинці використовують багаторівневі системи анонімізації (Tor, VPN-мережі, транскордонну маршрутизацію трафіку), що дозволяє їм приховувати свою діяльність за межами дії національного законодавства. Правоохоронні органи стикаються з критичними труднощами у процесі збирання, закріплення та легалізації електронних доказів, оскільки злочинець може легко відмовитися від авторства цифрових слідів. Розрив між глобальною, транскордонною природою кіберзлочинності та національними межами кримінальної юрисдикції вимагає переходу до уніфікованих міжнародних стандартів співробітництва та доказування.

Водночас, фундаментальним викликом сьогодення є масштабування цих інструментів до рівня глобальних інформаційно-психологічних операцій. Як слушно зазначає у науковій роботі «Стратегічні засади забезпечення

інформаційної безпеки в сучасних умовах» В.Я. Новицький, досліджуючи інформаційну сферу, до актуальних загроз безпеці України належать: повноформатна експансивна інформаційна політика РФ; низький рівень медійної грамотності населення; збільшення кількості глобальних дезінформаційних кампаній; інформаційне домінування РФ на тимчасово окупованих територіях; використання технологій маніпулювання свідомістю пересічних громадян (зокрема, щодо наслідків вступу України в НАТО та ЄС тощо) [144,с.112]. Характеризуючи нацбезпеку України М.Т. Гаврильців представила характеристику факторів, які обумовлюють загрози у сфері інформаційної безпеки, що мають системний характер, впливають на сфери суспільного життя людини і нормальний розвиток держави [28, с. 200].

Проаналізувавши різні аспекти змісту, рівнів, загроз інформаційної безпеки, можна сформувати прозору картину того, як правове регулювання інформаційної безпеки впливає на запобігання злочинності у сфері цифрових технологій, та визначити, які правові інструменти є найбільш ефективними в цьому контексті та окреслити очікувані результати у цій сфері. Серед них можна визначити:

- захищений інформаційний простір України, що включає в себе запобігання кіберзагрозам, захист критичної інфраструктури та ефективну боротьбу з кіберзлочинністю;
- ефективне функціонування системи стратегічних комунікацій, спрямоване на підвищення рівня інформованості громадян, підтримку позитивного іміджу держави у світі та забезпечення внутрішньої стабільності;
- ефективну протидію поширенню незаконного контенту, включаючи механізми фільтрації та контролю електронних медіа;
- забезпечення сталого процесу інформаційної реінтеграції громадян України на тимчасово окупованих територіях, включаючи розширення доступу до українського телерадіомовлення та інформаційних ресурсів.

- підвищення рівня медіакультури та медіаграмотності населення, сприяючи критичному осмисленню інформації та уникненню впливу дезінформації;
- дотримання конституційних прав особи на вільне вираження своїх поглядів і переконань, а також захист приватного життя, що сприятиме збереженню свободи слова та приватності.
- захист прав журналістів та створення умов для незалежної журналістики, що відіграє ключову роль у підтримці інформаційної свободи та прозорості;
- формування української громадянської ідентичності, що сприятиме утвердженню загальнонаціональної єдності та патріотизму.

1.2. Генезис наукової думки та етапи становлення правових засад забезпечення інформаційної безпеки в контексті вітчизняного і зарубіжного досвіду

Дослідження генезису наукової думки у сфері інформаційної безпеки дозволяє простежити складну еволюцію поглядів від суто технічного захисту даних до формування концепції комплексного когнітивного суверенітету. Становлення правової практики забезпечення інформаційної безпеки в Україні відбувалося паралельно з глобальними цифровими трансформаціями, що зумовило необхідність постійної адаптації національних безпекових стандартів до локальних та глобальних кіберзагроз. Аналіз вітчизняного та зарубіжного досвіду свідчить, що кожна історична епоха пропонувала власну парадигму захисту інформаційного простору, виходячи з наявного рівня технологічного розвитку, наукового доробку та актуальних викликів.

Актуальність обраного міждисциплінарного підходу підтверджується тим, що аналіз теорії інформаційних відносин вимагає комплексного залучення філософських, соціологічних та правових знань, оскільки відсутність повноти основних понять прямо впливає на ефективність правового регулювання та, як наслідок, на кримінологічну превенцію [201]. Усвідомлення проблеми зумовлює

необхідність виходу за межі вузькоправових інтерпретацій та звернення до історико-доктринальних витоків формування безпекової парадигми.

У межах підрозділу буде здійснено комплексний аналіз генезису наукової думки та правової практики, що дозволяє не лише доповнити існуючу періодизацію сучасним етапом (з 2014 року до сьогодні), зумовленим гібридною агресією та воєнними викликами, а й провести необхідний дифінітивний аналіз задля розмежування понять «інформаційна безпека» як стратегічної цілі, що охоплює захист свідомості та нецифрових даних, і більш вузьких технологічних категорій «кібербезпека» та «цифрова безпека», що є фундаментальною умовою для визначення предмета кримінологічного захисту та обґрунтування ефективних і сучасних заходів формування національної кіберстійкості.

Доцільність здійснення періодизації, як інструменту наукового пізнання правової природи інформаційної безпеки, обумовлена необхідністю системного осмислення динаміки трансформації цієї категорії від суто технічного концепту до елемента національного суверенітету. Періодизація дозволяє розв'язати кілька фундаментальних наукових завдань. По-перше, кожен етап становлення правової думки є віддзеркаленням конкретних викликів часу (від початкового формування правових інститутів незалежної держави до реагування на сучасні прояви гібридної агресії). По-друге, періодизація сприяє вивченню еволюції змістовного наповнення категорій «інформаційна безпека», «кібербезпека» та «цифрова безпека», фіксуючи моменти їхньої диференціації та інституціоналізації в науковому дискурсі. Третє, розмежування етапів становлення дозволяє критично оцінити досвід минулих років, виокремити сталі тенденції та, що є найбільш цінним для кримінологічної прогностики, сформулювати підґрунтя для розробки перспективних моделей запобігання кримінальним правопорушенням у сфері інформаційної безпеки.

У науковій літературі щодо становлення засад та правової практики забезпечення інформаційної безпеки України виокремлено три етапи [339, с. 34-

43; 2, с. 95-96; 202, с. 90-99; 139, с. 23-25]. У нашому дослідженні обґрунтовано сучасний, 4-й етап.

Перший етап (1991–1996 рр.) характеризується відсутністю спеціалізованих досліджень інформаційної безпеки як окремого сегмента національної безпеки. Науковий інтерес у цей період був фрагментарним: питання захисту інформації розглядалися лише в контексті загальних проблем національної безпеки, а саме поняття «інформаційна безпека» здебільшого ототожнювалося із захищеністю даних. Основні загрози, ідентифіковані авторами того періоду, мали внутрішню природу і, переважно, зумовлювалися політичною нестабільністю та дефіцитом професійних кадрів.

Другий етап (1996–2000 рр.) характеризується переходом інформаційної безпеки до рангу державних пріоритетів, що було закріплено на конституційному рівні. У наукових працях почали з'являтися перші ґрунтовні роботи, в яких фокус цих робіт зміщувався переважно на державну безпеку, залишаючи поза увагою потреби суспільства та права особи. Характерною ознакою цього періоду стало ототожнення інформаційної безпеки з комп'ютерною, що стимулювало розвиток кримінологічного та кримінально-правового напрямів. Науковці розпочали дискусію щодо появи нових загроз, таких як інформаційний тероризм, кіберзлочинність та методи маніпулювання масовою свідомістю [96; 118; 98, с. 3-6; 99, с.74-77; 141].

Третій етап (2001–2013 рр.) відзначається інтернаціоналізацією наукових розвідок у тому числі на рівні дисертаційних досліджень [154 ; 115; 120; 121; 122; 214]. Транснаціональний характер інформаційних загроз та стратегічний курс України на євроінтеграцію зумовили потребу в адаптації вітчизняного законодавства до стандартів ЄС [119; 209, с. 252-259]. У цей час відбувається інтенсивна деталізація наукового апарату: з'являються фахові словники та глосарії [70; 120], а дослідження зосереджуються на конкретизації повноважень органів державної влади та розробці механізмів управління інформаційним простором [121; 157, с. 49-52 ; 39, с. 9-18; 102].

Спираючись на аналіз попередніх етапів, нами запропоновано виокремлення четвертого етапу становлення практики забезпечення інформаційної безпеки України (з 2014 року до сьогодні), який суттєво відрізняється від попередніх періодів своєю онтологічною та функціональною природою. Якщо III етап (2001–2013 рр.) був зосереджений на гармонізації законодавства та інтенсифікації міжнародної співпраці, то IV етап обумовлений кардинальною зміною безпекового середовища під впливом безперервної гібридної агресії та повномасштабного вторгнення РФ.

Основою для виділення цього етапу є перехід від реактивної моделі захисту окремих державних інформаційних систем до формування національної кіберстійкості. У цей період інформаційна безпека перестає бути виключно технічним інструментом і трансформується у стратегічний імператив державного суверенітету, що охоплює захист критичної інфраструктури, протидію дезінформації та забезпечення когнітивної свободи громадян [33; 216, с. 221-223; 147, с. 177-182; 14с. 83-87].

Ключовою ознакою цього етапу є синтез правових та кримінологічних підходів, де кіберзлочинність стає складовою загальної стратегії дестабілізації держави, а превентивні заходи набувають інтерактивного характеру. Таким чином, період з 2014 року характеризується новим підходом, в якому безпека інформаційного простору виступає фундаментом національного виживання, що вимагає відмови від вузького розуміння інформаційної безпеки як захисту лише «цифрових даних» на користь комплексного захисту свідомості та нецифрових інформаційних масивів.

В умовах, коли інформаційний простір став ключовим фактором воєнних дій, класичне розуміння безпеки потребує якісного переосмислення, що й зумовлює необхідність проведення подальшого дифінітивного аналізу та чіткого розмежування понять «інформаційна безпека», «кібербезпека» та «цифрова безпека».

Розмежування понять «інформаційної безпеки» як стратегічної рамки та її технологічних сегментів «кібербезпеки» і «цифрової безпеки» дозволяє окреслити предмет кримінологічного захисту, відмежувати когнітивно-комунікаційні впливи від суто технічних кібератак і визначити релевантні методи доказування та превенції. З огляду на встановлену ієрархію понять і враховуючи воєнний контекст із посиленими ризиками генеративного ШІ, важливо виокремити специфіку правопорушень у цифровому середовищі як окремому об'єкті кримінологічного аналізу [13, с. 7-10; 80; 189, с. 35-41]. Так, кримінальні правопорушення у сфері інформаційних технологій мають унікальну специфіку, що суттєво відрізняє їх від традиційних кримінальних правопорушень: вони транскордонні, високотехнологічні, мають підвищену латентність і часто використовують людський фактор (соціальну інженерію). Ця специфіка ускладнює їх кримінологічний аналіз, прогнозування та наукове дослідження. Для визначення стану наукової розробленості та виявлення теоретичних прогалів, які має заповнити наше дослідження, розглянемо основні наукові праці вчених із зазначеного питання.

З огляду на відсутність у сучасній науці консенсусу щодо трактування терміна «інформаційна безпека», необхідно інтерпретувати його як багаторівневу категорію, що охоплює як об'єктивні умови функціонування суб'єктів інформаційних відносин (особи, суспільства, держави), так і суб'єктивні можливості їхнього свідомого контролю над інформаційним простором [141, с. 253; 21].

Такий підхід дозволяє виокремити два взаємопов'язані аспекти інформаційної безпеки: об'єктивний аспект, як сукупність зовнішніх умов, які забезпечують сталий розвиток інформаційної сфери та виступають еталоном для встановлення безпекових стандартів; суб'єктивний аспект, як здатність суб'єктів до критичного сприйняття, аналізу та контролю інформаційного середовища, що безпосередньо корелює з рівнем інтелектуального розвитку, освіченості та ментальної стійкості громадян.

Сучасний стан наукових розвідок характеризується консенсусом щодо того, що інформаційна безпека не може обмежуватися виключно технічними заходами кіберзахисту. Навпаки, вона потребує комплексної інтеграції прогностичної аналітики, стратегічного планування та глибокого осмислення соціально-цифрових трансформацій. Цей міждисциплінарний підхід стає сполучною ланкою між загальнотеоретичними концепціями безпеки та прикладними напрямками сучасних юридичних наук. Впровадження цифрових технологій у кримінологічні дослідження дозволяє перейти від фіксації злочинності до її прогнозування (predictive policing), що відповідає тезі про необхідність аналізу нових трендів розвитку суспільства [140, с.421-425; 40, с. 141-143; 41; 65, с. 118-121; 217].

Розвиток цього підходу фундаментально обґрунтовано у вітчизняній науковій доктрині, зокрема у підручнику «Інформаційна безпека (соціально-правові аспекти)». Автори видання пропонують комплексну візію інформаційної безпеки як стану захищеності інтересів особи, суспільства та держави, за якого сторонні впливи не завдають суттєвої шкоди національним інтересам [69]. Вчені пропонують комплексний підхід до інформаційної безпеки як трирівневу модель, що охоплює інтереси особи, суспільства та держави. На рівні особи безпека трактується як захист психіки та здоров'я людини від деструктивних впливів, що викривляють сприйняття реальності, тоді як безпека суспільства фокусується на забезпеченні конституційних прав на вільний обіг інформації та розвитку критичного мислення населення. Державний елемент передбачає захищеність національних інтересів від інформаційної агресії, тероризму та розвідувально-підривної діяльності. Важливим аспектом концепції, викладеної у підручнику, є обґрунтування переходу від технічного до гібридного захисту, оскільки в сучасних реаліях військово-технічних засобів недостатньо, і національна стійкість вимагає синергії політичних, економічних та інформаційно-психологічних заходів.

Фундаментальною особливістю цього підходу є крос-секторальна взаємодія. Вона передбачає синергію кіберзахисту, прогновної аналітики, адаптації новітніх технологій та системного підвищення рівня цифрової грамотності населення. Відтак, сучасна форма безпеки має бути адаптивною та орієнтованою на випередження, що є важливим в умовах стрімкої еволюції глобальних викликів та гібридних загроз, обумовлених війною [14, с. 83-87].

Ця концепція детально обґрунтована у праці «Інформаційна безпека України в умовах євроінтеграції» [119, с. 150]. Автори посібника фокусують увагу на соціогуманітарному вимірі безпеки, розкриваючи механізми маніпулювання масовою свідомістю, методику проведення спеціальних інформаційних операцій та стратегії ведення інформаційних війн. Окреме місце в дослідженні посідає генеза інформаційно-психологічного протистояння, а також специфіка деструктивного впливу в межах економічної конкуренції та терористичної діяльності.

Нашинець-Наумова А.Ю у монографії «Інформаційна безпека: питання правового регулювання» визначає інформаційну безпеку як фундаментальне правове поняття, що детермінує стан захищеності національних інтересів через баланс прагнень особи, суспільства та держави. Особливу увагу приділено динамічній природі поняття: інформаційна безпека трактується як система, здатна до постійного саморозвитку, що вимагає безперервного оновлення наукового знання. Дефінітивний аналіз у роботі тісно пов'язаний із практикою державотворення, де інформаційна безпека постає консолідуючим чинником, здатним перетворити державну владу на політико-вольовий центр, забезпечуючи цілісність та незалежність України в умовах сучасних суспільно-політичних викликів [139, с. 8-9].

У контексті нашого дослідження заслуговує на увагу монографія О.М. Бодунової «Теоретико-прикладні основи запобігання злочинності у сфері інформаційних технологій», яка є фундаментальним кримінологічним дослідженням, що закладає теоретичний базис для вивчення проблем

інформаційної безпеки. Авторка детально розкриває кримінологічну характеристику цієї злочинності, аналізуючи її причини, умови та особливості, зокрема латентність та транскордонний характер. Важливою складовою є систематизація суб'єктів запобігання та пропозиції щодо вдосконалення їхніх організаційних і правових функцій [15]. У монографії простежується еволюція української кримінологічної думки та надано систематизований понятійний апарат. Водночас, вона, не охоплює найновіші локальні та глобальні виклики щодо інформаційної безпеки, а також питання необхідності гармонізації національної політики з практикою ЄСПЛ та стратегію національної кіберстійкості в контексті Генеративного ШІ та воєнного стану.

За визначенням В. Петрика, інформаційна безпека являє собою такий стан захищеності інтересів особи, суспільства та держави, за якого забезпечується стабільний інформаційний розвиток, інтелектуальний, технічний, соціально-політичний та морально-етичний, що убезпечений від негативного деструктивного впливу ззовні, здатного завдати суттєвої шкоди національним інтересам [157, с. 49-52].

Еволюція наукових поглядів на природу інформаційної безпеки дозволяє виокремити ключові детермінанти, що зумовлюють необхідність її гарантування як фундаментальної складової національного суверенітету [3, с. 142; 31; 39; 227].

По-перше, у науковому дискурсі утвердилося розуміння інформаційної безпеки не як ізольованого явища, а як невід'ємного елемента загальної системи національної безпеки України. По-друге, акцентується увага на характері загроз інформаційній сфері, здатних завдати незворотної шкоди стратегічним національним інтересам. По-третє, сучасна доктрина визнає пріоритетність захисту когнітивної сфери, враховуючи потенціал інформаційного впливу на трансформацію суспільної свідомості та поведінкових моделей особи.

Відповідно до генезису безпекових завдань, пріоритетом постає розбудова комплексної системи протидії, що охоплює захист національного інформаційного простору, критичної інфраструктури та державних

інформаційних ресурсів. Наукова думка констатує, що в умовах ескалації конфліктів інформаційне протиборство закономірно трансформується в інформаційну війну, де застосування інформаційної зброї характеризується цілеспрямованістю, масштабністю та системністю дій [19; 9, с. 80; 13, с. 8; 221, с. 78]. Таким чином, сучасний етап становлення правових засад безпеки маркується переходом від пасивного захисту даних до проактивного управління ризиками в умовах глобального інформаційного протистояння.

Центральним об'єктом такого управління у сучасній архітектурі безпеки виступає критична інформаційна інфраструктура, що охоплює системи управління енергетикою, транспортом, обороною, охороною здоров'я, фінансами та зв'язком. Будь-яке деструктивне втручання в її функціонування здатне спричинити «каскадний ефект», призводячи до паралічу стратегічних секторів економіки та державного управління.

До структури критичної інформаційної інфраструктури, Білаш О. В., Сорокати М.І. відносять не лише інформаційно-телекомунікаційні комплекси, а й державні реєстри, бази даних та системи, що оперують конфіденційною інформацією. В умовах повномасштабної війни захист цих активів стає складовою національної оборони, оскільки кібератаки на них синхронізуються з військовими операціями і кампаніями саботажу [11, с. 36].

Сьогодні Україна стикається з комплексом гібридних загроз, де критична інфраструктура розглядається ворогом як технічна система та пріоритетна ціль військової стратегії. Ключовий спектр небезпек охоплює як прямі кіберударі по енергомережах, так і використання шкідливого програмного забезпечення для знищення даних, що часто супроводжується фішинговими кампаніями та фізичним пошкодженням інфраструктури. Окремим ризиком постає інституційний дефіцит нестача кваліфікованих кадрів та потреба в уніфікації протоколів реагування [11, с. 36].

Реалізація стратегії захисту критичної інфраструктури забезпечується через скоординовану взаємодію ключових суб'єктів: Держспецзв'язку, що

здійснює загальну координацію кіберзахисту; НкЦК при РНБО, який забезпечує стратегічне управління; Кіберкомандування ЗСУ, відповідального за оборону; а також Мінцифри, СБУ та Кіберполіції, які формують політику стійкості та здійснюють контррозвідальний супровід. Такий багаторівневий підхід дозволяє перетворити теоретичну модель інформаційної безпеки на практичний механізм відсічі гібридній агресії [11, с. 36].

Правове регулювання інформаційної безпеки впливає на запобігання злочинності у сфері цифрових технологій шляхом встановлення правил, вимог та відповідальності за порушення цих правил. Ефективні правові інструменти можуть включати в себе чіткі норми щодо захисту особистих даних, визначення кіберзлочинності та визначення відповідальності за її скоєння, удосконалення процедур електронного підпису та надання повноважень уповноваженим структурам для боротьби з кіберзлочинністю та забезпечення інформаційної безпеки. Ці інструменти становлять основу для регулювання сфери цифрових технологій та сприяють запобіганню злочинності в цьому контексті.

Виходячи з розуміння інформаційної безпеки як стратегічної категорії, стає очевидним, що вона охоплює як захист когнітивного простору, так і нормативно-правовий режим функціонування суспільства. Саме тому, у межах проведеного дифінітивного аналізу, ми виокремлюємо кібербезпеку як функціонально спеціалізований інструментарій захисту. На відміну від інформаційної безпеки, що оперує поняттями «сенсів» та «інтересів». Кібербезпека фокусується на захисті інформації, процесів і послуг саме у кіберпросторі в мережах, інформаційних системах, хмарних платформах, телекомунікаціях, державних реєстрах і системах критичної інфраструктури від кібератак, несанкціонованого доступу, порушення функціонування, ураження шкідливим програмним забезпеченням тощо.

Зазначена інституційна розгалуженість та складність процедур координації суб'єктів кібербезпеки вимагають надійної правової верифікації, що забезпечується через чітку законодавчу дефініцію. Логічним завершенням

формування управлінської моделі стало нормативне закріплення змісту поняття «кібербезпека» у законі України «Про основні засади забезпечення кібербезпеки України» [177].

Відповідно до положень закону, кібербезпека трактується як стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якого забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [177].

Таке нормативне визначення не лише детермінує межі повноважень згаданих раніше суб'єктів, а й остаточно виокремлює кібербезпеку як самостійний, технологічно зумовлений об'єкт правового регулювання та кримінологічної охорони в загальній системі інформаційної безпеки. Використання законодавцем конструкції «життєво важливі інтереси людини і громадянина» прямо корелює з тезою про необхідність переходу від технічного захисту систем до гарантування фундаментальних прав особи у цифровому середовищі. Проте, незважаючи на технологічну природу кібербезпеки, правопорушення у цій сфері виходять далеко за межі технічних збоїв.

Основні особливості, які впливають на стан наукової розробленості, включають: по-перше, еволюційну новизну, адже історія кіберзлочинності є відносною новою, порівняно з іншими видами злочинності. Такий новий феномен, як Генеративний штучний інтелект, постійно створює нові інструменти та методи вчинення злочинів, випереджаючи реакцію законодавства. Це вимагає від безперервного перегляду класичних дефініцій. По-друге, транскордонний характер, коли кримінальні правопорушення у сфері ІТ не обмежені конкретним географічним кордоном, оскільки вони відбуваються у віртуальному (онлайн) середовищі. Ця абстрактність ускладнює визначення часу, місця вчинення злочину та юрисдикції, що є фундаментальною проблемою як для кримінального процесу, так і для міжнародного співробітництва.

У цьому контексті, слушно зазначає Д.О. Ричка, що більшість держав і надалі застосовують до «кіберзлочинів» класичні принципи кримінальної юрисдикції, сформовані на концепції територіального суверенітету. Проте технології глобальних комп'ютерних мереж функціонують поза межами будь-яких національних кордонів і мають виразний позатериторіальний характер, що істотно знижує ефективність традиційних юрисдикційних підходів та породжує широкий спектр правових колізій [190, с. 61]. Водночас у науковій дискусії дедалі більше утверджується альтернативний підхід до правового регулювання відносин у мережі Інтернет. Він полягає в тому, щоб визначати місцем учинення кіберзлочину не територію конкретної держави чи фізичну локацію, а власне кіберпростір як самостійну, особливу сферу суспільних відносин

Трете, висока технологічність, яка проявляється у використанні інформаційних ресурсів, спеціалізованих технічних прийомів, алгоритмів і програмного забезпечення при вчиненні кіберзлочинів. Злочинці використовують ці засоби для неправомірного доступу, крадіжки інформації, шифрування даних (вимагання) та порушення цілісності систем. Четверте, анонімність та дистанційний вплив на потерпілих, тому що кіберзлочинці можуть впливати на третіх осіб через Інтернет, що робить кримінальне правопорушення високо анонімним і дистанційним. І, п'яте, що безпосередньо пов'язане із попереднім положенням, це латентність та ускладнення доказової бази. Велика кількість кіберзлочинів залишається незареєстрованою (латентною) через відсутність фізичних доказів, складність їх фіксації та низьку віктимологічну обізнаність потерпілих [7, с. 105; 101; 74].

Аналіз наявних дисертаційних робіт щодо забезпечення інформаційної безпеки свідчить, що більшість із них зосереджені на адміністративно-правовому регулюванні або на техніко-правових аспектах, спрямованих переважно на захист інфраструктури [2; 122; 214; 190].

Розвиток ідеї комплексного управління безпековими ризиками знаходить своє відображення у дослідженні Ю. Є. Максименко «Теоретико-правові засади

забезпечення інформаційної безпеки України» де, проаналізовано загрози національним інтересам, у контексті інформаційної безпеки як системи, що поєднує інформаційно-технічний, інформаційно-психологічний та гуманітарний аспекти (захист прав і свобод людини) [125].

Важливим внеском науковця є уточнення ролі кібербезпеки як невід'ємної складової загальної системи інформаційної безпеки. Водночас Ю. Є. Максименко звертає увагу на певну асиметрію в сучасному законодавстві: попри те, що основні регуляторні зусилля наразі зосереджені на техніко-технологічному складнику кіберзахисту, поза належною увагою часто залишається захист прав людини в цифровому просторі [125, с. 164-165].

Теоретико-методологічні засади використання кримінального аналізу оперативними підрозділами (зокрема з використанням відеоаналізу та розпізнавання обличчя) є практичним втіленням ідеї інтегрованого аналізу великих масивів даних (Big Data) для забезпечення національної безпеки. [59; 130, с. 90-103; 131, с. С.141-147;256]. Сучасна парадигма профілактики злочинності неможлива без використання новітніх інструментів кримінологічного прогнозування. Аналітика великих даних (Big Data) трансформує підхід до безпеки, дозволяючи переходити від реагування на події до моделювання кримінальної активності. Виявлення стійких закономірностей у цифрових слідах злочинності дає змогу правоохоронним органам стратегічно планувати заходи захисту інформаційного та фізичного простору. Крім того, сучасна парадигма цифрових слідів переосмислює їх не просто як дані, а як динамічні докази, що вимагають нових стратегій захисту від кібератак безпосередньо в процесі кримінального провадження [73, с. 224-232; 290]. Так, Нестерова І.А. зазначає, що сучасна безпекова парадигма базується на інтелектуалізації відеоспостереження: поєднання розпізнавання обличчя із алгоритмами поведінкового аналізу дозволяє ідентифікувати суб'єкта та завчасно виявляти потенційні загрози. Проте масовий збір біометричної інформації породжує ризики для приватності громадян [132, с. 87-89; 148, с. 84-90].

Міжнародний досвід свідчить, що головною перешкодою для легітимізації цих технологій є відсутність чітких стандартів, які б гарантували відсутність дискримінації з боку штучного інтелекту та прозорість роботи правоохоронних алгоритмів [140, с.424].

У своєму дослідженні М. Сироватченко слушно зазначає, що у різних державах поняття «кібербезпека» формулюється по-своєму, проте спільним елементом лишається захист інформаційних систем від загроз кіберпростору та потреба у превентивних і компенсаційних заходах для мінімізації ризиків і наслідків некоректного використання чи атак. Дефіцит кваліфікованих кадрів у сфері кібербезпеки посилює вразливість систем, однак стимулює запровадження дано-орієнтованих стратегій захисту, які використовують аналітику, штучний інтелект та автоматизацію для швидшого виявлення інцидентів, адаптивної відповіді та зниження шкоди і ризиків [196, с. 314-320].

Цифрова безпека охоплює практики й засоби безпеки на рівні користувача та організації: політики приватності й захисту персональних даних, цифрову гігієну, безпечні налаштування облікових записів і пристроїв, протидію фішингу та соціальній інженерії, безпечні канали комунікації (месенджери, соцмережі). В умовах воєнного стану цифрова безпека охоплює спеціальні інструкції для військових і службовців (операційна безпека, контроль витоків, базові налаштування безпеки тощо) [4, с. 28; 10, с. 34-35].

Актуальні виклики сьогодення та глобалізаційні ризики обумовлюють необхідність всебічного захисту цифрового середовища від протиправних, злочинних посягань. Слушно зазначає професор Н.С. Юзікова, що незадовільний стан інформаційної безпеки, розміщення у цифровому середовищі спотвореної, провокаційної інформації або дезінформації про політичні, економічні, соціальні процеси, що відбуваються в Україні, негативно впливає на суспільну свідомість громадян України; детермінує зміни у поведінці та комунікації особистості; сприяє формуванню деформованих моральних установок, девіантної поведінки та асоціального способу життя; продукує віктимну, суїцидальну поведінку [228,

с. 508;346]. А враховуючи швидкі темпи цифровізації та постійну трансформацію глобальний ризиків, питання розробки ефективних заходів у протидії злочинності і забезпеченні інформаційної безпеки є доцільними і актуальними.

Розуміння важливості цього рівня захисту підтверджує той факт, що дослідження проблематики інформаційної безпеки та кіберзлочинності сьогодні має мультидисциплінарний характер. Це засвідчує аналіз вітчизняного наукового доробку, який охоплює кримінально-правовий, адміністративно-правовий та кримінологічний напрями. Сучасні виклики гібридної війни обумовили необхідність розширення цих наукових рамок.

Саме в цьому контексті особливої уваги заслуговує колективна монографія кафедри цивільного права Національного університету «Одеська юридична академія», присвячена результатам досліджень цивілістичних шкіл. Ця праця є яскравим прикладом міждисциплінарного осмислення проблематики ІТ-відносин, демонструючи, що питання інформаційної безпеки виходять далеко за межі публічного права [71].

Автори зосереджують увагу на критичних аспектах кіберстійкості в контексті цивілістичної доктрини, що є цінним для кримінології. Зокрема, у монографії аналізуються: правові рамки для цифрових активів та перспективи цифрової власності, що є об'єктом кіберзлочинних посягань; проблеми визначення концепту «ІТ-право» та цивільно-правової відповідальності за шкоду, завдану кібератаками, що має прямі наслідки для віктимології та превенції. Особливо актуальним для кримінологічного дослідження є аналіз протидії кіберзагрозам у гібридній кібервійні, а також загрози вербування неповнолітніх через соцмережі та месенджери та обґрунтування юридичних заходів запобігання цим загрозам.

Окремі дослідження виходять з важливої тези, що інформаційна безпека не обмежується лише заходами кіберзахисту, і необхідно інтегрувати прогнозування, аналіз нових трендів та осмислення розвитку цифрового суспільства [72, с. 17-22; 123, с.258-264; 66; 36, с. 98-104; 345]. Поряд з цим, частина робіт характеризує ретроспективний (застарілий) підхід: спочатку

аналізуються вже існуючі загрози, а потім формуються напрями їх запобігання [22; 67, с. 27-32; 28, с. 200-203; 85, с. 57-61; 88, с. 313-314]. Такий реактивний підхід є недостатнім в умовах технологічної еволюції (зокрема, поширення Генеративного ШІ) та гібридної війни. Ретроспективний аналіз дійсно має обмежений внесок у вирішення сучасних та майбутніх інформаційних викликів.

Важливою частиною цього орієнтованого на майбутнє підходу є міжсекторальна взаємодія з іншими сферами, такими як: кіберзахист, кіберпрогнозування, розвиток нових технологій, заходи з підвищення кіберсвідомості та віктимологічної безпеки серед громадян. Отже, підхід до інформаційної безпеки повинен бути гнучким, комплексним і системно інтегрованим з європейськими стандартами, щоб ефективно відповідати сучасним цифровим реаліям та глобальним кримінологічним викликам.

Висока швидкість еволюції кібер- та інформаційної безпеки нівелює ефективність канонічних дефініцій, які нерідко втрачають актуальність ще на етапі формалізації. У сучасних умовах постійних технологічних та безпекових трансформацій доцільно спиратися на інтегральні та рухливі концепції, що здатні охопити весь спектр новітніх викликів. Отже, науковий дискурс у цій сфері має бути максимально динамічним, відкритим до генерації інноваційних підходів та постійної ревізії усталених понять. Тільки такий адаптивний інтелектуальний режим дозволяє своєчасно реагувати на появу асиметричних загроз та забезпечувати надійний захист інформаційних активів у глобальному цифровому просторі.

Результати досліджень до повномасштабного вторгнення РФ заклали теоретичне підґрунтя для розуміння загальних підходів до інформаційної безпеки. Водночас запровадження воєнного стану радикально змінило загрозовий ландшафт і управлінські пріоритети, що зумовило появу нової хвилі праць, орієнтованих на оперативну кіберстійкість, протидію дезінформації та правове регулювання в умовах війни (з урахуванням нових технологічних чинників, зокрема генеративного ШІ) [1; 5, с. 271-281; 196; 30; 84; 152; 194; 195;

196]. Далі зосередимося саме на цих дослідженнях, їхніх методологічних новаціях і практичних висновках для державної політики.

Важливим внеском у розробку правових засад забезпечення інформаційної безпеки є дослідження О. Г. Колба та Н. Г. Бендовського в якому фокусується увага на практичному, інституційному та законодавчому вимірах забезпечення національної безпеки, підкреслюючи необхідність посилення суверенітету та координації між силовими структурами для протидії зовнішнім гібридним загрозам [88, с. 82-87]. Автори, аналізуючи діяльність державних органів, виявляють законодавчі прогалини та доводять, що ефективна кіберстійкість залежить від чіткої правової основи та безперервної адаптації інституційно-організаційного механізму до нових викликів.

У науковій роботі «Стратегічні засади забезпечення інформаційної безпеки в сучасних умовах» В.Я. Новицький при дослідженні інформаційної сфери виділив сучасні загрози безпеки України. Вчений до актуальних загроз інформаційній безпеці України відносить: повноформатну експансивну інформаційну політику РФ; низький рівень медійної грамотності населення; збільшення кількості глобальних дезінформаційних кампаній; інформаційне домінування РФ на тимчасово окупованих територіях; використання технологій маніпулювання свідомістю пересічних громадян щодо наслідків вступу України в НАТО та ЄС тощо [144, с. 112]. Характеризуючи національну безпеку України М.Т. Гаврильців представила характеристику факторів, які обумовлюють загрози у сфері інформаційної безпеки, що мають системний характер, і впливають на різні сфери суспільного життя людини і нормальний розвиток держави [28, с. 200]. Ці праці становлять наукове підґрунтя для захисту інформаційної безпеки як правового явища.

Вітчизняна наукова думка, значною мірою сформована в умовах воєнної агресії та посилення інформаційно-психологічних операцій, акцентує увагу на правових та організаційних механізмах забезпечення національної кіберстійкості. Зокрема, досліджуються проблеми кримінальної

відповідальності за кіберзлочини, гармонізації національного законодавства з міжнародними стандартами (насамперед, Будапештською конвенцією) та розробки стратегій протидії дезінформації як інструменту впливу на національну безпеку.

Зарубіжний досвід концентрується переважно на техніко-математичному моделюванні кібератак (зокрема, використання графіків атак, теорії ігор та Байєсівських мереж для прогнозування мережевих вразливостей), а також на концептуальному розвитку захисних механізмів, таких як Загальний регламент про захист даних (GDPR) та Когнітивна безпека (COGSEC) [330; 278, с. 1325–1326; 296; 297; 345]. Ці напрями демонструють перехід від захисту інфраструктури до захисту прав людини та її свідомості.

В останні роки зарубіжні науковці проводять дослідження динаміки та реалізації кібератак з метою більш глибокого аналізу впливу зловмисників, а саме, щодо використання вразливостей мережі для виявлення можливих і реалістичних способів атаки. Так, у дослідженні Райлі М., Елгін Б., Лоуренс Д., Матлак К. наведено конкретні приклади масштабних кібератак [316]. Тенденція використання сторонніх постачальників послуг для отримання доступу до організацій-жертв аналізується у звіті компанії FireEye [299]. Окремо, Джаджодія, С., Ноель С., досліджують нову парадигму аналізу графіків атак, яка доповнює традиційне графічне представлення на основі матриць суміжності графіків [284]. Робота Цінь, С., Лі, В. присвячена проблемі прогнозування потенційних атак на основі спостережуваних атак [313]. Се П., Лі Дж. Х., Оу С., Лю П., Леві Р. наводять приклад байєсівської мережі, заснованої на поточній моделі графа безпеки [344]. У роботі Фава Д. С., Байерса С. Р., Яна С. Дж. аналізується марковська модель змінної довжини, яка фіксує особливості траєкторій атак, що дозволяє прогнозувати ймовірні подальші дії в поточних атаках [270]. Проте, ключовим недоліком цих зарубіжних наукових робіт є те, що зазначені методи враховують лише вразливості мережі, але не виявляють реальних відмінностей між типами зловмисників та їхньою індивідуальною

поведінкою. В роботах Стоц, А. та Судіт, М. це питання розглядалося шляхом моделювання можливостей супротивників [330] або застосування методології теорії ігор для моделювання взаємодії зловмисника та захисника у роботах Вана Б., Цай Ц., Чжан, С. та Лі Ц. [341].

Цей підхід є недостатнім, оскільки, як зазначається у дослідженні, найбільш мінливим (непередбачуваним) аспектом кібератаки є самі атакуючі. Кожна людина є індивідуальною, а отже, процес, за яким зловмисник атакуватиме мережу, буде різним для кожного. Людський фактор, що лежить в основі кібербезпеки, робить кіберпростір складною, адаптивною системою. Це обумовлює необхідність переходу від статичного аналізу мережевих вразливостей до комплексного, міждисциплінарного підходу, що поєднує технічні та поведінкові елементи для раннього виявлення, прогнозування та кримінологічної превенції кіберзлочинів, що є найбільш актуальним напрямом для подальшої наукової розробки

Жоден із зазначених методів не моделює зловмисника на основі інформації, яку він отримує безпосередньо під час атаки, хоча ця інформація відіграє вирішальну роль у прийнятті рішень. Ця концепція вже частково реалізована в методах агентного моделювання (як-от NeSSi2 [278, с. 1325–1326] та MASS [297]), однак навіть ці техніки не надають структури, в якій зловмисник отримує конкретні деталі про цілі та може динамічно змінювати їх та стратегії під час атаки.

Аналіз зарубіжного наукового доробку дозволяє констатувати зміну парадигми: від суто технічного захисту інфраструктури до комплексного гарантування прав людини та її свідомості (концепції GDPR та COGSEC). Отже, зарубіжний досвід демонструє високий рівень технічного інструментарію, проте водночас обґрунтовує гостру необхідність переходу до міждисциплінарного, заснованого на знаннях підходу. Це вимагає інтеграції технічного аналізу з поведінковими та кримінологічними елементами, що дозволить моделювати

кіберзлочинність не як послідовність машинних команд, а як динамічний інтелектуальний конфлікт.

У межах нашого дослідження інформаційна безпека розглядається як стратегічна категорія, що інтегрує питання інформаційного забезпечення держави та суспільства, орієнтуючись на захист інформаційних ресурсів та реалізацію законних інтересів суб'єктів. На відміну від технологічних категорій, таких як «кібербезпека» чи «цифрова безпека», зміст інформаційної безпеки у нашому трактуванні є значно ширшим, адже він включає когнітивну складову, що полягає у захисті свідомості та нецифрових інформаційних масивів, що є критично важливим для забезпечення національного суверенітету в умовах сучасних гібридних загроз.

Водночас, детальне розмежування понятійного апарату вимагає чіткого визначення змісту суміжних категорій, які часто помилково ототожнюються з інформаційною безпекою.

Кібербезпека у нашому дослідженні постає як технологічно-орієнтований сегмент, що фокусується на забезпеченні стійкості та захищеності саме кіберпростору. Її зміст полягає у захисті інформаційних систем, мереж, хмарних платформ та об'єктів критичної інфраструктури від деструктивних технічних впливів: кібератак, шкідливого програмного забезпечення та несанкціонованого доступу. Якщо інформаційна безпека оперує категоріями «сенсів» та «національних інтересів», то кібербезпека зосереджена на «цілісності», «доступності» та «конфіденційності» цифрових даних і функціонуванні апаратно-програмних комплексів.

Натомість цифрова безпека виокремлюється як категорія, що має виражений людиноцентричний та приватно-правовий характер. Вона охоплює сукупність умов і засобів, які гарантують захищеність прав та інтересів окремого суб'єкта (фізичної або юридичної особи) у процесі його віртуальної життєдіяльності. Цифрова безпека інтегрує захист персональних даних, безпеку цифрових правочинів та приватність комунікацій, мінімізуючи ризики

протиправних посягань на майнові та немайнові права особи в цифровому середовищі.

Таким чином, якщо кібербезпека забезпечує технічну надійність інфраструктури, то цифрова безпека гарантує правомірність та захищеність взаємодії «суб'єктів» всередині цього середовища. Таке багаторівневе розуміння безпекової системи дозволяє констатувати, що інформаційна безпека як стратегічна категорія інтегрує в собі технологічну стійкість кібербезпеки та правову захищеність цифрової безпеки, створюючи комплексний механізм протидії сучасним загрозам локального і глобального характеру.

1.3. Принципи та механізми міжнародно-правового забезпечення інформаційної безпеки

Проблематика міжнародно-правового забезпечення інформаційної безпеки у цифровому просторі є наскрізною та міждисциплінарною, охоплюючи значний масив наукових досліджень як в Україні, так і на міжнародній арені [155, с. 269–272; 148, с. 84-90; 345]. Широта розробки зумовлена необхідністю комплексної відповіді на гібридні та транснаціональні загрози. Фахівці у сфері міжнародного права та політології висвітлювали проблему через призму суверенітету держав у кіберпросторі та норм відповідальної поведінки, тоді як представники кримінології та інформаційного права акцентували на особливостях транскордонної кіберзлочинності та необхідності уніфікації правових механізмів [58, с. 112-120; 219; 27; 18, с. 74-79; 55; 56; 244; 266; 323; 342]. Завдяки такому комплексному підходу, було детально проаналізовано принципи та механізми міжнародно-правового забезпечення інформаційної безпеки, крізь призму конвенцій, декларацій, директив та міжнародних норм, що містять концептуальні засади протидії інформаційним війнам та загрозам, пов'язаним із несанкціонованим втручанням у критичну інфраструктуру.

Зловживання інформаційними технологіями з боку окремих держав становить значну загрозу для міжнародної безпеки та стабільності, економічного

і соціального розвитку. Це вимагає від міжнародної спільноти невідкладного та глибокого осмислення не лише технічної, а й правової природи інформаційної агресії. Загрози, що виходять від кіберзлочинів та інформаційно-психологічних операцій, мають транскордонний характер, унеможливаючи ефективну протидію виключно на національному рівні.

Глобальні зміни, пов'язані з переходом до інформаційного суспільства, висувають перед людством безпрецедентні виклики безпеці, які потребують наукового осмислення кримінологічної складової діджиталізації. Широке розповсюдження соціальних мереж, окрім їхньої функції як засобу комунікації, створило ідеальне середовище для реалізації злочинних намірів та безперешкодного ведення інформаційних війн. У цьому процесі формування глобальних стандартів і механізмів колективної протидії одну з провідних ролей справедливо відведено ООН.

Основні засади міжнародної інформаційної безпеки закладені в Статуті ООН, серед цілей якого чітко виділяються підтримка міжнародного миру та безпеки, а також повага до прав людини. Водночас, з часу затвердження Статуту, світ зазнав істотних трансформацій, зумовлених процесами економічної, технологічної та політичної глобалізації. Ці зміни, зокрема, стрімкий розвиток системи інформаційних технологій, призвели до того, що практична діяльність ООН була вимушена розширитися, охопивши всі сфери міжнародної безпеки, включаючи інформаційну. Таким чином, задачі та принципи діяльності ООН сформували регуляторну основу для міждержавних відносин у сфері інформаційної безпеки. На цій основі відбувається розробка відповідних міжнародних угод та рекомендацій, спрямованих на протидію новим транскордонним загрозам.

Формування принципів міжнародної інформаційної безпеки на рівні ООН було ініційовано у 1998 році прийняттям резолюції A/RES/53/70 «Досягнення у сфері інформатизації та телекомунікацій в контексті міжнародної безпеки» [51]. Резолюція стала першим значним кроком, який закликав держави-члени

продовжити діалог щодо питань інформаційної безпеки, надати конкретні визначення можливих загроз та розробити міжнародні принципи забезпечення безпеки глобальних інформаційних систем. На виконання її рекомендацій, у серпні 1999 року в Женеві було проведено міжнародний семінар з питань міжнародної інформаційної безпеки за участю представників понад 50 технологічно розвинених країн [199]. Представники цих держав, одногосно підтвердили актуальність проблеми міжнародної інформаційної безпеки та своєчасність ініціативи ООН. Наступним важливим кроком стало прийняття Генеральною Асамблеєю ООН резолюції A/RES/54/49 «Досягнення у сфері інформатизації та телекомунікацій в контексті міжнародної безпеки» [51]. Ця резолюція вперше розширила фокус міжнародної уваги, прямо вказавши, що загрози міжнародній інформаційній безпеці стосуються не лише цивільної (соціальної та економічної), а й військової сфери.

Вказані резолюції A/RES/53/70, A/RES/54/49 та A/RES/55/28 «Досягнення у сфері інформатизації та телекомунікацій в контексті міжнародної безпеки» заклали фундаментальні основи міжнародно-правового осмислення загроз в інформаційному просторі [51; 52; 319].

На виконання цих резолюцій, у 2000 році в Секретаріаті ООН були представлені «Принципи, що стосуються міжнародної інформаційної безпеки» [312]. Ці принципи визначають норми поведінки держав в інформаційному просторі, створюючи для них відповідні моральні зобов'язання та закладаючи основу для подальших міжнародних переговорів. Вперше було уніфіковано понятійний апарат, введено такі ключові дефініції, як: інформаційна війна, інформаційна зброя, міжнародна інформаційна безпека, інформаційна безпека, інформаційний простір, загроза інформаційної безпеки, інформаційний ресурс, неправомірне використання інформаційно-телекомунікаційних систем, несанкціоноване втручання в інформаційно-телекомунікаційні системи і інформаційні ресурси, критично важливі структури, міжнародний інформаційний тероризм. Під інформаційною безпекою відповідно до Принципів

розуміється стан захищеності основних інтересів особистості, суспільства і держави в інформаційному просторі, включаючи критичну інфраструктуру і власне інформацію щодо таких її властивостей, як цілісність, об'єктивність, доступність і конфіденційність [312].

Міжнародно-правове регулювання відносин у сфері забезпечення інформаційної безпеки та протидії кіберзагрозам транснаціонального характеру визначається широкою системою міжнародних норм, угод, конвенцій, директив та резолюцій. Ці документи стосуються питань боротьби з кіберзлочинністю, організованою злочинністю, тероризмом та іншими протиправними діями, які використовують інформаційні технології.

Це регулювання охоплює правила щодо взаємодії міжнародних структур, урядів та правоохоронних органів у сфері виявлення, розслідування та притягнення до відповідальності за кіберзлочини. Також воно містить механізми співробітництва, обміну інформацією та взаємодії у сфері забезпечення кіберстійкості та обміну технічними даними про загрози. Загалом, міжнародно-правове регулювання встановлює міжнародні стандарти та процедури, спрямовані на забезпечення ефективної боротьби з кіберзлочинністю та захист національної інформаційної інфраструктури.

В умовах повномасштабної гібридної агресії РФ ці міжнародно-правові положення набувають нового значення. Встановлення дефініцій «інформаційна війна» та «інформаційна зброя» дозволяє Україні на міжнародній арені кваліфікувати дії агресора не лише як військову, а й як інформаційну агресію, що є підґрунтям для правового переслідування та фіксації збитків. Більше того, включення «критично важливих структур» до понятійного апарату підтверджує, що кібератаки на українську енергетичну чи фінансову інфраструктуру є порушенням міжнародних принципів інформаційної безпеки. Принципи акцентують на об'єктивності та цілісності інформації, вони слугують нормативною основою для кримінологічного захисту суспільної свідомості від ПСО та дезінформації, що є ключовим компонентом національної стійкості.

Доповідь Генерального секретаря ООН від 3 жовтня 2001 року «Про досягнення в сфері інформатизації та телекомунікацій в контексті міжнародної безпеки» є ключовим документом, оскільки вона вперше систематизувала одинадцять основних факторів, що створюють небезпеку для інтересів особистості, суспільства і держави в інформаційному просторі [51]. Ці фактори охоплюють як технічні, так і політико-психологічні загрози, і є надзвичайно актуальними в умовах гібридної агресії. Серед них виділяється розробка та використання засобів несанкціонованого втручання в роботу і неправомірного використання інформаційних ресурсів іншої держави, а також завдання їм шкоди за допомогою, зокрема, вірусних програм. Особливий акцент зроблено на загрозах критично важливим структурам, включаючи несанкціоноване втручання в їхні інформаційно телекомунікаційні системи та використання недокументованих можливостей існуючих систем з метою неправомірного впливу. До загроз також віднесені дії, спрямовані на домінування в інформаційному просторі, ведення інформаційних війн та використання інформаційної зброї. Нарешті, документ акцентує на зв'язку з міжнародною злочинністю, вказуючи на небезпеку заохочення та використання інформаційного тероризму та неправомірне використання інформаційних ресурсів іншої держави, що призводить до завдання шкоди її основним інтересам.

Міжнародна інформаційна безпека, як сучасний об'єкт правового регулювання, є прямим продовженням та адаптацією класичних принципів міжнародного права до реалій цифрової епохи, що є визначальним для формування ефективних механізмів колективної протидії локальним та глобальним загрозам сучасності.

Водночас практична імплементація задекларованих Статутом ООН засад миру та безпеки у цифровому середовищі вимагає переходу від загальних політичних конвенцій до конкретних нормативних стандартів.

Фундаментом такого переходу є уніфіковане розуміння самої сутності безпеки. Сучасна міжнародна практика визначає інформаційну безпеку через тріаду принципів: доступності, цілісності та конфіденційності, які знайшли своє нормативне закріплення у таких засадничих актах, як FISMA [337], Privacy Act та історичній Директиві 95/46/ЄС, які заклали основу для захисту персональних даних та інформаційних систем [335; 265; 263].

Закон про модернізацію федеральної інформаційної безпеки (Federal Information Security Modernization Act (FISMA)) є одним із ключових нормативних актів США, що регулює захист інформаційних систем федеральних органів влади. Він був ухвалений у 2002 році та модернізований у 2014 році для врахування сучасних кіберзагроз. FISMA заклав світовий стандарт переходу від «паперової безпеки» до безперервного моніторингу, що дає можливість встановити вимоги до створення комплексних програм інформаційної безпеки, які охоплюють оцінку ризиків, впровадження контролів та безперервний моніторинг. Цей нормативний акт встановлює принципи управління ризиками, контролю доступу та моніторингу безпеки, які узгоджуються з глобальними підходами до захисту даних. FISMA демонструє, як національні моделі можуть інтегруватися в систему міжнародних стандартів, забезпечуючи цілісність, конфіденційність та доступність інформації в умовах зростаючих кіберзагроз.

Для України, яка перебуває під постійними кіберударами, підхід, закладений у FISMA, є питанням виживання державних інституцій. Трансформація національної системи інформаційної безпеки України вимагає переходу від застарілих моделей статичного захисту до динамічної стійкості, де концептуальним орієнтиром виступає досвід імплементації FISMA. Адаптація принципів FISMA до вітчизняних реалій дозволяє розв'язати ключову суперечність між тривалими процедурами сертифікації та необхідністю миттєвого реагування на кіберзагрози в умовах воєнного стану. Головним вектором такої адаптації є впровадження механізму безперервного моніторингу,

що перетворює безпеку з разового акту отримання атестата на циклічний процес автоматизованого сканування вразливостей у режимі 24/7.

Основою для реалізації вимог FISMA є стандарти Національного інституту стандартів і технологій (NIST), зокрема NIST SP 800-53 та FIPS 199, що визначають категорії ризиків і рівні захисту [306]. Розробка Control Overlays for Securing AI Systems (COSAIS) на основі NIST SP 800-53 спрямована на адаптацію існуючих контролів безпеки до специфіки штучного інтелекту. AI-системи, хоча й базуються на програмному забезпеченні, створюють нові ризики, пов'язані з цілісністю моделей, захистом навчальних даних та протидією атакам типу adversarial (деструктивним маніпуляціям із вхідними даними). COSAIS доповнює вимоги FISMA, що реалізуються через стандарти NIST SP 800-53 та FIPS 199, які визначають категорії ризиків і рівні захисту [326; 306]. Цей підхід узгоджується з міжнародними стандартами, такими як ISO/IEC 27001 та ISO/IEC 23894, забезпечуючи комплексне управління ризиками AI [281; 282]. Основні контролі охоплюють автентифікацію доступу до моделей, моніторинг аномалій, захист конфіденційності даних та управління життєвим циклом AI. Таким чином, COSAIS створює практичний міст між рамкою управління ризиками AI (AI RMF) та традиційними вимогами кібербезпеки [307]. Закон поширюється не лише на державні установи, а й на приватні компанії, які працюють з федеральними даними, що робить його важливим елементом міжнародної практики кіберзахисту. FISMA орієнтований на забезпечення конфіденційності, цілісності та доступності інформації, що відповідає загальним принципам інформаційної безпеки. Його впровадження сприяє підвищенню стійкості цифрового середовища до атак і зменшенню ризиків витоку даних.

Важливим аспектом адаптації FISMA є впровадження ризик-орієнтованого підходу, що передбачає жорстку класифікацію об'єктів за рівнем їхнього впливу на національну безпеку. Такий підхід нерозривно пов'язаний з обов'язковою інвентаризацією та повною «видимістю» цифрових активів, що мінімізує ризики

використання неперевіреного програмного забезпечення або виникнення «тіньових» ІТ-систем у державному секторі.

Шлях впровадження цих стандартів в Україні передбачає двоетапну стратегію. На етапі воєнного стану пріоритетом є законодавче закріплення «гнучкого периметра» та персональної відповідальності керівників за дотримання протоколів безпеки. У період же повоєнної відбудови акцент має зміститися на глибоку інституціоналізацію, де основою буде створення національних центрів сертифікації, які проводитимуть регулярні тести на проникнення за методиками NIST, та інтеграцію вимог безпечного життєвого циклу у кожен державну закупівлю.

Таким чином, гармонізація українського законодавства з принципами FISMA та європейськими директивами NIS2 формує комплексну систему безпеки, де технічна захищеність гармонізується з антропоцентричним захистом приватності. Це дозволяє Україні адаптуватися до міжнародних стандартів та трансформувати унікальний бойовий досвід у системний механізм легітимізації національних інтересів у глобальному цифровому просторі, забезпечуючи сталий розвиток і цифрову суверенність держави.

Закон про захист особистих даних (Privacy Act 1974р.) є одним з перших у світі масштабних законів, що обмежив всевладдя державних органів у зборі інформації про громадян [335]. Це відповідь на розвиток комп'ютерних баз даних у 70-х роках. Відповідно до Privacy Act було реалізовано наступні засади: принцип мінімізації втручання, коли державні установи мали право збирати лише ту інформацію, яка є «необхідною та релевантною» для виконання їхніх законних функцій; право на доступ та корекцію, коли громадянин отримав законне право знати, які дані про нього зберігаються, та вимагати виправлення помилок; заборона таємних систем, що полягала у публічній фіксації баз персональних даних та визнання незаконним існування «секретних дос'є» на громадян поза межами спецслужб.

В умовах воєнного стану, коли держава збирає величезні масиви даних (через додаток «Дія», реєстри «Оберіг» тощо), принципи, закріплені у Privacy Act нагадують про необхідність цифрової гігієни державних інституцій. Після перемоги це має трансформуватися у жорсткий аудит: видалення надлишкових даних, які збиралися суто для цілей оборони, щоб запобігти створенню «цифрового тоталітаризму».

Транснаціональний характер кіберзлочинності унеможливорює ефективну протидію виключно на локальному рівні, оскільки цифрові атаки не обмежені географічними кордонами. У зв'язку з цим уніфікація кримінального законодавства трансформуються з допоміжних інструментів у фундаментальні елементи системи глобальної інформаційної безпеки. Ключовим суб'єктом у цьому процесі виступає Європейський Союз, який через гармонізацію правових механізмів забезпечує рішучу відповідь на транснаціональні кіберзагрози.

Засади міжнародно-правового забезпечення інформаційної безпеки знаходять своє практичне втілення через механізми уніфікації, закладені в Директиві 2013/40/EU, яка встановила єдині стандарти криміналізації посягань на інформаційні системи [264]. Директива забезпечує ідентичність правової оцінки кіберзлочинів у ЄС, що усуває прогалини, які злочинці використовують для уникнення кримінальної відповідальності. Вона зобов'язує держави-учасниці криміналізувати наступні правопорушення: а) незаконний доступ (Ст. 3), що полягає в умисному неправомірному доступі до всієї інформаційної системи або її частини, вчиненому із порушенням заходів безпеки; б) незаконне втручання в систему (Ст. 4), що полягає у перешкоджанні або перериванні функціонування інформаційної системи шляхом введення комп'ютерних даних, передачі, пошкодження, видалення, погіршення, зміни або приховування таких даних, або шляхом навмисного та безпідставного надання доступу до таких даних; в) незаконне втручання в дані (Ст. 5), що полягає у видаленні, пошкодженні, погіршенні стану, зміни або приховуванні комп'ютерних даних в інформаційній системі, або навмисному та безпідставному наданні доступу до

таких даних. Необхідно звернути увагу, що у Директиві розмежовано втручання у функціонування системи (перешкоджання або переривання роботи) та дії безпосередньо з комп'ютерними даними (видалення, пошкодження, зміна). Важливою є вимога карати також за навмисне та безпідставне надання доступу до таких даних; г) незаконне перехоплення (Ст. 6), що охоплює перехоплення технічними засобами неpubлічних передач даних, включно з електромагнітним випромінюванням; д) використання знарядь для скоєння злочинів (Ст. 7).

Низка положень Директиви знайшли відображення у кримінальному законодавстві України. Положення Ст. 3 Директиви (Незаконний доступ до інформаційних систем) в українському правовому полі імплементовані через ст. 361 КК України, де криміналізовано несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж [81]. Важливо зауважити, що під час повномасштабної агресії вітчизняний законодавець доповнив цю норму посиленням, на вчинення цих дій під час дії воєнного стану, що свідчить про адаптивність системи до сучасних викликів.

Втручання в систему та дані, регламентовані статтями 4 та 5 Директиви, знайшли своє відображення у ст. 361 та ст. 362 КК України відповідно [81]. Якщо європейський стандарт фокусується на забезпеченні цілісності та доступності даних, то українська модель додатково акцентує увагу на суб'єктному складі правопорушень (зокрема, щодо осіб, які мають право доступу), що посилює внутрішню інституційну стійкість організацій. Питання незаконного перехоплення даних (Стаття 6 Директиви) в кримінальному законодавстві України криміналізовано через комплексну дію ст. 163 КК України, що захищає конституційну таємницю спілкування, та ст. 361 КК України, у частині, що стосується витоку інформації [81].

Така гармонізація перетворює КК України з суто карального інструмента на елемент розвитку потенціалу. Синхронізація дефініцій дозволяє Україні повноцінно використовувати інфраструктуру Європолу та Євроюсту, оскільки

ідентичність правового сприйняття кіберзагроз знімає процесуальні бар'єри при транскордонному зборі цифрових доказів. Таким чином, національний кримінальний закон стає «юридичним щитом», який не лише копіює європейські норми, а й доповнює їх унікальним досвідом протидії державним кібератакам, забезпечуючи перехід України до статусу активного суб'єкта формування колективної кібербезпеки Європи.

Фундаментом європейської цифрової етики стала Директива 95/46/ЄС [265], як умовна «конституція» приватного життя в Європі на понад 20 років, поки її не було замінено на GDPR (OJ L 119, 04.05.2016; cor. OJ L 127, 23.5.2018) у 2016 році з поправками 2018 року [317]. Саме вона ввела поняття «контролер даних» та «процесор». Ключові положення Директиви 95/46/ЄС полягали у наступному: інформація має бути точною, актуальною та зберігатися не довше, ніж це необхідно для визначеної мети; вперше було виокремлено спеціальну категорію даних (расове походження, політичні погляди, стан здоров'я, релігійні переконання), захист яких має бути посиленим; було встановлено заборону передавати дані в країни, які не забезпечують належного рівня захисту цих даних.

Україна наразі перебуває у процесі повної гармонізації законодавства з наступником цієї Директиви 95/46/ЄС - GDPR (OJ L 119, 04.05.2016; cor. OJ L 127, 23.5.2018) [317]. Проте саме історичні засади Директиви 95/46/ЄС є важливими для розуміння того, як збалансувати безпеку та приватність. Так, по-перше, принципи Директиви 95/46/ЄС дозволяють обґрунтувати обмеження доступу до даних у зонах бойових дій задля безпеки самих громадян (наприклад, приховування адрес чи місць роботи у відкритих реєстрах); по-друге, дотримання цих стандартів є перепусткою для іноземних інвестицій. Західні ІТ-гіганти та інвестори не зайдуть у країну, де правове поле не гарантує захисту комерційної та персональної таємниці за європейським зразком.

Сучасна система інформаційної безпеки ЄС та НАТО базується на концепції «операційної стійкості», де головним є не лише захист, а здатність

системи функціонувати безпосередньо під час атаки. Таким чином, розвиток нормативного підґрунтя призвів до формування сучасної екосистеми правового регулювання.

Директива EU NIS2 (2022/2555) (далі – Директива 2022/2555) є логічним завершенням аналізу еволюції європейського законодавства, оскільки цей документ знаменує перехід від «захисту даних» (GDPR) до «захисту систем та інфраструктури» (кіберстійкості). Вона запроваджує високий спільний рівень кібербезпеки в межах Європейського Союзу, встановлюючи жорсткі вимоги до стійкості критичних секторів [263].

Синтез цих нормативних документів формує цілісну правову рамку, де технічна захищеність інфраструктури (згідно з директивами NIS) невід’ємно пов’язана з антропоцентричним захистом прав особи на приватність (згідно з GDPR та Privacy Act). Для України адаптація цих положень у національне законодавство є не лише вимогою євроінтеграції, а й критичною умовою побудови сучасної системи інформаційної безпеки, здатної функціонувати в єдиному правовому полі з провідними державами світу.

Прийнята у грудні 2022 року, Директива NIS2 (Directive (EU) 2022/2555) замінила першу Директиву NIS 2016 року, суттєво посиливши вимоги до безпеки в умовах гібридних загроз. До новацій та механізмів, закріплених у Директиві 2022/2555, можна віднести: а) розширення сфери застосування, що проявляється у регулюванні, окрім енергетики та банківської сфери, таких сфер як охорона здоров’я, виробництво критичних товарів, публічна адміністрація та поштові послуги; б) персональну відповідальність керівництва, яке має затверджувати заходи з управління кіберризиками та нести персональну відповідальність за їх виконання (Ст. 20); в) безпеку ланцюгів постачання шляхом оцінки організатором кібербезпеки своїх постачальників (наприклад, розробників софту), що є прямою відповіддю на атаки типу SolarWinds; г) двоступеневу звітність про інциденти [263].

В умовах війни, принципи Директиви 2022/2555, дозволяють Україні побудувати систему, де кожне критичне підприємство стає цифровою фортецею. Для України це означає перехід від добровільних рекомендацій до жорстких стандартів аудиту, які будуть обов'язковими для отримання міжнародних контрактів та інвестицій.

Міжнародно-правове забезпечення інформаційної безпеки є наріжним каменем у протидії транскордонній кіберзлочинності та гібридній агресії, що набуває критичного значення для України. Фундаментальним принципом у цій сфері є суверенна рівність держав у кіберпросторі та принцип ненападу, які формують основу для міжнародної співпраці. Аналіз ключових принципів міжнародної інформаційної безпеки дозволяє виокремити дієві механізми співпраці, необхідні для формування національної кіберстійкості.

Водночас, саме застосування цих принципів у сучасних геополітичних умовах породжує складні правові колізії. Зокрема, принцип рівної та неподільної безпеки має складну та амбівалентну кореляцію з українською позицією у сфері інформаційної безпеки та євроінтеграційним курсом, оскільки його тлумачення прямо залежить від геополітичного контексту. Важливо проаналізувати його справжній зміст та адаптувати до стратегічних інтересів України. Так, Росія історично використовує принцип рівної та неподільної безпеки (особливо в контексті безпеки НАТО) для ствердження, що безпека однієї держави (РФ) є порушеною розширенням оборонних союзів або суверенітету інших держав. У контексті інформаційної безпеки це проявляється у вимогах до «інформаційної нейтральності» та неприпустимості «інформаційного домінування» Європейських країн заходу.

Українська позиція щодо інформаційної безпеки надає пріоритет неподільності суверенітету та територіальної цілісності в кіберпросторі. Безпека України не може бути предметом торгу або залежною від інтересів агресора. Таким чином, будь-яке тлумачення принципу рівної та неподільної безпеки, що обмежує право України на захист, міжнародну співпрацю (наприклад, з НАТО

або ЄС) чи формування власної кіберполітики, є неприйнятним. У сучасному взаємозалежному світі реалізація цього права на захист суверенітету вимагає виходу за межі виключно національного правопорядку та інтеграції у глобальні безпекові механізми. Тому стратегічним інструментом утвердження українського «цифрового суверенітету» та правової стійкості виступає Конвенція про кіберзлочинність підписана у Будапешті 23.11.2001 р. (далі - Будапештська конвенція) [92].

Будапештська конвенція розглядається не лише як юридичний документ, а як фундамент міжнародно-правового забезпечення інформаційної безпеки, що дозволяє державі захищати свої інтереси у глобальному масштабі. Її роль як універсального механізму проявляється у трьох важливих аспектах. По-перше, вона забезпечує уніфікацію матеріального права, класифікуючи злочини проти конфіденційності, цілісності та доступності даних. По-друге, Будапештська конвенція запроваджує спеціальний процесуальний інструментарій, адаптований до специфіки кіберпростору, зокрема механізм термінового збереження комп'ютерних даних, які зберігаються (ст. 16). По-третє, завдяки Другому додатковому протоколу (2022р.), Конвенція радикально трансформує швидкість взаємодії, дозволяючи українським правоохоронцям звертатися безпосередньо до приватних сервіс-провайдерів.

Другий додатковий протокол до Будапештської конвенції є відповіддю міжнародної спільноти на динамічну трансформацію кіберзлочинності, що забезпечує модернізацію глобальної системи безпеки відповідно до сучасних технологічних викликів [53]. Ключова новація документа полягає у переході від громіздких бюрократичних процедур до механізмів прямої транскордонної взаємодії правоохоронних органів із приватними постачальниками послуг та реєстраторами доменних імен для оперативного отримання електронних доказів (даних про абонентів та трафік). Важливою ознакою цього інструментарію є суворе дотримання принципів верховенства права та прав людини, де розширення повноважень органів влади збалансоване жорсткими міжнародними

гарантіями захисту персональних даних [53]. Протокол формує нову парадигму ефективної міждержавної та державно-приватної співпраці, спрямовану на захист критичної інфраструктури та забезпечення невідворотності покарання у глобальному кіберпросторі.

Будапештська конвенція виступає тим глобальним механізмом, який наповнює декларативний принцип суверенітету реальним змістом. Для України це означає можливість використовувати колективний інтелектуальний та технічний ресурс міжнародної спільноти для захисту власного інформаційного простору, перетворюючи міжнародне право на активний елемент національної оборони.

В умовах сучасної гібридної війни кібератаки на критичну цивільну інфраструктуру (енергомережі, медичні установи, транспортні комунікації, системи водопостачання тощо) можуть розглядатися як воєнні злочини, якщо вони спричиняють наслідки, аналогічні до кінетичних ударів. Будапештська конвенція виступає техніко-юридичним містком, який дозволяє кваліфікувати ці дії для майбутніх міжнародних трибуналів через відповідні механізми.

Будапештська конвенція перетворює цифрові сліди на юридичні аргументи. Для України це означає, що кожна зафіксована за міжнародними стандартами кібератака стає не просто епізодом у розумінні диспозицій КК України, а потенційним пунктом обвинувального акту в Гаазі. Це остаточно закріплює статус України як держави, що захищає свій суверенітет у правовому полі, де міжнародно-правове забезпечення інформаційної безпеки стає інструментом глобальної справедливості.

Українські правоохоронні органи, судова система та профільні міністерства вже впроваджують практичні заходи з адаптації процесуальних механізмів, передбачених Будапештською конвенцією. Зокрема, йдеться про вдосконалення процедур збору електронних доказів, реагування на кіберінциденти та налагодження ефективної взаємодії з міжнародними контактними пунктами. Важливим напрямом залишається також розвиток

національної експертизи у сфері цифрової криміналістики, оновлення нормативно-правової бази та запровадження спеціалізованих освітніх програм для слідчих, прокурорів і суддів. Паралельно Україна активно долучається до глобальних ініціатив у сфері протидії кіберзлочинності, обміну досвідом, підготовки фахівців і вироблення спільних стандартів кіберзахисту. Співпраця з Європолем, INTERPOL, ENISA та іншими міжнародними інституціями сприяє інтеграції до європейського простору цифрової безпеки та забезпечує оперативне реагування на транснаціональні загрози [151, с.259].

Таким чином, імплементація положень Директив [263; 264; 265] та Будапештської конвенції у національне законодавство формує надійний нормативний фундамент. Проте в умовах системної міждержавної агресії правова стійкість держави не обмежується лише внутрішньою криміналізацією діянь. Вона вимагає створення дієвого механізму трансляції технічних даних про кібератаки у площину міжнародного кримінального права.

Фундаментальний підхід до розуміння технічної та правової природи таких діянь було закладено у спеціальному Робочому документі, підготовленому Комітету II для семінару-практикуму в рамках Десятого Конгресу ООН щодо запобігання злочинності та поводження з правопорушниками (Відень, 2000 р.). Цей акт визначив дихотомію кіберделіктів, розмежувавши їх на дві базові категорії. Перша охоплює кіберзлочини у вузькому розумінні (так звані «комп'ютерні злочини») прямі електронні атаки, спрямовані на подолання захисту комп'ютерних систем та оброблюваних баз даних. Друга категорія визначає кіберзлочини у широкому розумінні, де комп'ютерні мережі виступають не ціллю, а інструментом вчинення інших протиправних діянь, зокрема для незаконного зберігання чи трансляції інформації (п. 14 документа ООН A/CONF.187/10) [255, с. 5].

В умовах збройного конфлікту ідентифікація приналежності атаки до однієї з цих категорій є лише першим кроком. Належна правова оцінка таких дій вимагає виходу за межі загально-кримінальної площини. Цей виконавчий

(процесуальний) механізм безпосередньо реалізує фундаментальні принципи міжнародного гуманітарного права в цифрову епоху. Він є ключовим елементом міжнародно-правового забезпечення інформаційної безпеки, оскільки дозволяє перевести первинні технічні факти в юридично значущі та беззаперечні докази для міжнародних трибуналів. Він реалізується через чотири рівні.

Перший рівень стосується процесуальної атрибуції та ідентифікації комбатантів. Так, головна проблема міжнародних судів полягає у доведенні зв'язку між цифровим кодом та конкретним державним органом агресора. Конвенція через свої процесуальні норми (ст. 18 Запит комп'ютерних даних, ст. 19 Обшук та вилучення даних) дозволяє відстежити ланцюжок команд. Це допомагає довести, що хакерська група діяла не як «приватна ініціатива», а як підрозділ збройних сил, що є обов'язковою умовою для кваліфікації дій за Римським статутом.

Другий рівень торкається легітимізації цифрових доказів для Міжнародного кримінального суду (МКС). МКС має суворі вимоги до допустимості доказів. Оскільки Будапештська конвенція визнана більшістю демократичних країн, докази, зібрані згідно з її протоколами (наприклад, через термінове збереження даних за ст. 16), автоматично вважаються «процесуально чистими». Це дозволяє перетворити лог-файли, IP-адреси та фрагменти шкідливого коду на неспростовні докази навмисного спрямування атаки проти цивільного населення.

Третій рівень стосується доведення злочинного умислу через транскордонну співпрацю. Для кваліфікації воєнного злочину необхідно підтвердити суб'єктивну сторону діяння. Другий додатковий протокол до Конвенції дозволяє отримувати дані безпосередньо від глобальних сервіс-провайдерів про зміст комунікацій. Це дає змогу виявити конкретні накази про «цифрові удари» по об'єктах, що мають життєво важливе значення для цивільних осіб (лікарні, водоканали), що прямо заборонено Додатковим протоколом I до Женевських конвенцій.

Четвертий рівень стосується техніко-правової кваліфікації кібер-інциденту як воєнного злочину. Завдяки уніфікації дефініцій «втручання в систему» та «втручання в дані», міжнародні трибунали можуть застосовувати до кібератак принципи пропорційності та розрізнення. Якщо втручання в систему керування енергомережею призвело до тяжких наслідків для населення, Конвенція надає технічну характеристику діяння, а міжнародне гуманітарне право його кінцеву правову кваліфікацію як воєнного злочину.

Розвиток цього процесуального підходу відображено і на глобальному рівні. Логічним продовженням зусиль щодо інституціоналізації протидії цифровим загрозам стало відкриття до підписання у жовтні 2025 року в Ханой (В'єтнам) першої міжнародної Конвенції про запобігання, припинення та боротьбу з кіберзлочинністю (Конвенція відкрита для підписання до 31 грудня 2026 року) [336]. Це відбулось під час Конференції високого рівня на тему «Боротьба з кіберзлочинністю - Спільна відповідальність - Забезпечення нашого майбутнього», яка була організована урядом В'єтнаму у співпраці з Управлінням ООН з наркотиків і злочинності (УНП ООН).

Конвенція є першим всеохоплюючим глобальним договором з цього питання, який надає державам низку заходів, що мають бути вжиті для запобігання кіберзлочинності та боротьби з нею. Вона також спрямована на зміцнення міжнародної співпраці в обміні електронними доказами щодо тяжких злочинів. Послідовно підтримуючи переговорний процес, УНП ООН тепер виконує функції секретаріату Конференції держав-учасниць Конвенції та відіграватиме центральну роль у сприянні імплементації та швидкому набранню чинності Конвенції.

Фундаментальною метою Конвенції є закладення міжнародно-правового базису для превенції та нейтралізації кіберзагроз. Це передбачає не лише гармонізацію національних законодавств у частині криміналізації правопорушень у цифровій сфері, а й якісну трансформацію інститутів міжнародної правової допомоги. Особливий акцент зроблено на створенні

протоколів оперативного обміну даними між компетентними органами, що дозволяє нівелювати перевагу правопорушників у швидкості та анонімності.

Запровадження таких уніфікованих стандартів є необхідною відповіддю на виклики глобальної цифровізації. Оскільки сучасна кіберзлочинність остаточно набула транскордонного та мережевого характеру, ефективна протидія їй неможлива в межах окремих юрисдикцій. Це підкреслює, що формування стійкого міжнародного правопорядку в кіберпросторі є тривалим процесом, який вимагає політичного консенсусу та адаптації внутрішніх правових систем до нових універсальних норм.

Додатково варто зауважити, що імплементація положень Конвенції повинна базуватися на дотриманні балансу між інтересами національної безпеки та захистом основоположних прав людини. Очікується, що цей документ не лише підвищить розкриваність транскордонних злочинів, а й стане інструментом стримування для державних акторів, які використовують прогалини у міжнародному праві для ведення гібридної агресії.

Попри те, що реальна дієздатність цього нового правового режиму буде залежати від темпів національної ратифікації, він створює глобальну рамку, в яку органічно вписується український кейс. Важливо зазначити, що сучасний вітчизняний досвід протидії системній державній кіберагресії, поєднаний із правовими механізмами ЄС, Ради Європи та положеннями нової Конвенції ООН, дозволяє Україні претендувати на роль лідера у розробці нових норм відповідальної поведінки держав у кіберпросторі.

Для України в умовах воєнного стану та майбутньої повоєнної відбудови імплементація цих міжнародних принципів і механізмів набуває характеру стратегічного безпекового пріоритету. В умовах першої у світі повномасштабної кібервійни, що супроводжує збройну агресію, використання уніфікованої моделі CIA (конфіденційність, цілісність, доступність) та стандартів NIS2 дозволяє українській цифровій інфраструктурі функціонувати як «розподілена фортеця», здатна витримувати масовані атаки на державні реєстри та системи

життєзабезпечення. Водночас дотримання європейських стандартів GDPR та принципів виступає надійним запобіжником від ризиків формування цифрового тоталітаризму, гарантуючи, що надзвичайні заходи контролю в умовах війни не призведуть до незворотної деградації прав людини та приватного життя.

У контексті євроінтеграційних прагнень та підготовки до Конвенції ООН 2025 року, Україна має унікальну можливість не лише гармонізувати національне законодавство з міжнародним, а й стати активним суб'єктом формування нових глобальних стандартів кіберстійкості. Створення прозорих механізмів превентивної підзвітності та безперервного аудиту стане основою для залучення міжнародних інвестицій у цифрову економіку та технологічну відбудову.

Висновки до першого розділу

1. Обґрунтовано перехід від вузькотехнологічного розуміння кібербезпеки до комплексної тривірневої моделі інформаційної безпеки як об'єкта кримінологічної охорони й правової превенції. Встановлено, що сутність цього об'єкта базується на міжнародній Тріаді CIA (конфіденційність, цілісність, доступність), яку було доповнено важливими для процесуального доказування елементами автентичності та неспростовності.

Комплексний захист цих елементів вимагає розподілу об'єкта охорони на такі рівні: а) техніко-технологічний (інфраструктурний рівень) щодо забезпечення фізичної та логічної цілісності цифрового простору, мереж, хмарних сховищ та об'єктів критичної інфраструктури за міжнародними стандартами; б) інформаційно-регуляторний рівень, який спрямований на захист правового режиму обігу даних (персональних даних, таємниць) та договірну підзвітність провайдерів; в) соціально-психологічний (антропоцентричний вимір) виступає найвищим стратегічним пріоритетом, що передбачає проактивний захист суспільної свідомості, процесу формування волі та цифрових прав людини від транснаціональних інформаційних атак, ІПСО та неетичного використання штучного інтелекту.

2. Визначено транскордонну природу сучасних кіберзагроз, які послідовно «прошивають» усі рівні інформаційної безпеки, що генерує нові виклики і вимагає перегляду превентивних стратегій. Виокремлено наступні виклики: техногенна віктимність організацій щодо інфраструктурної вразливості, яка зумовлена складністю управління хмарними ресурсами та поширенням неавторизованих сервісів, що перетворює легітимний персонал на джерело внутрішніх ризиків; експансія когнітивних загроз, яка полягає у деформації суспільної свідомості через масштабування інструментів соціальної інженерії до рівня глобальних дезінформаційних кампаній, спрямованих на штучне продукування віктимної та девіантної поведінки; криза процесуальної атрибуції суб'єкта кримінального правопорушення коли використання багаторівневих

систем анонізації та транскордонної маршрутизації трафіку долає національні кордони, нівелює принцип неспростовності доказування та обмежує кримінальну юрисдикцію.

Ефективна превенція можлива лише за умови інтеграції технічного аудиту з механізмами превентивної підзвітності та постійною віктимологічною профілактикою відповідно до стратегії інформаційної безпеки України.

3. На основі ретроспективного та дефінітивного аналізу становлення правових засад інформаційної безпеки удосконалено періодизацію вітчизняної наукової думки та здійснено термінологічне розмежування безпекових категорій. Доведено, що вітчизняна доктрина пройшла шлях від технічного захисту даних (1991–1996 рр.) до формування цілісної державної функції безпеки. Обґрунтовано виокремлення четвертого етапу (з 2014 року - дотепер), який зумовлений воєнними викликами і характеризується переходом від реактивного апаратного захисту до формування стратегічної кіберстійкості держави та захисту когнітивної сфери нації в умовах гібридної агресії РФ.

Здійснено розмежування понятійно-категоріального апарату: «інформаційна безпека» - стратегічна категорія, що поєднує умови функціонування держави та здатність особи до контролю інформаційних впливів, охоплюючи когнітивну складову та національний суверенітет; «кібербезпека» - прикладний технологічний рівень, покликаний забезпечити техніко-технологічну стійкість систем критичної інфраструктури, мереж і цифрових даних; «цифрова безпека» - людиноцентрична категорія приватно-правового характеру, зосереджена на захищеності прав, інтересів та персональних даних особи у віртуальному просторі.

4. Виявлено специфічні особливості та обмеження зарубіжної доктрини інформаційної безпеки, та обґрунтовано мультидисциплінарний характер кримінологічної превенції. На відміну від вітчизняних досліджень, орієнтованих на правову кодифікацію та стратегічне планування, зарубіжна доктрина

відзначається високим рівнем математизації та техноцентризму (моделювання атак через теорію ігор, Байєсівські та марковські мережі).

Доведено, що провідним недоліком західних математичних моделей є ігнорування динамічної поведінки правопорушника та «людського фактора», що обмежує їхню ефективність для повної кримінологічної превенції. А новітні зарубіжні концепції (GDPR, COGSEC) відображають позитивний глобальний тренд переходу до захисту індивідуальної свідомості та прав людини.

5. Систематизовано принципи та механізми міжнародно-правового забезпечення інформаційної безпеки, та запропоновано авторську дефініцію міжнародної інформаційної безпеки як динамічного стану захищеності глобального цифрового простору, суверенних інформаційних екосистем держав, їхньої критичної інфраструктури, фундаментальних цифрових прав та когнітивної свободи людини від транснаціональних кіберзагроз, що забезпечується системою уніфікованих міжнародних правових норм та інституційних механізмів взаємної процесуальної допомоги.

6. Обґрунтовано стратегічне значення міжнародно-правових орієнтирів інформаційної безпеки для України в умовах воєнного стану та повоєнної відбудови. Гармонізація вітчизняного законодавства з принципами FISMA, Директиви NIS2 та нової Конвенції ООН (2025 року) дозволяє трансформувати унікальний національний бойовий досвід у системний правовий механізм захисту цифрового суверенітету держави.

Дотримання європейських стандартів приватності (Стаття 8 Конвенції), свободи вираження поглядів (Стаття 10) та права на власність (Стаття 1 Першого протоколу) виступає надійним запобіжником від деградації прав особи в умовах впровадження надзвичайних заходів контролю та проведення стабілізаційних заходів на деокупованих територіях. У контексті євроінтеграції Україна трансформує свій статус, остаточно переходячи від ролі пасивного реципієнта міжнародної допомоги до статусу активного і важливого суб'єкта формування глобальних стандартів кіберстійкості та колективної безпеки.

РОЗДІЛ 2. НАЦІОНАЛЬНИЙ ВИМІР КРИМІНОЛОГІЧНОГО ЗАПОБІГАННЯ ЗАГРОЗАМ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ УКРАЇНИ

2.1 Особливості та тенденції забезпечення інформаційної безпеки в умовах воєнного стану

У сучасних умовах повномасштабної агресії з боку Російської Федерації забезпечення інформаційної безпеки набуло статусу стратегічної військово-кримінологічної проблеми. Воєнний стан формує безпрецедентний «стан винятку», який визначає нову реальність функціонування правової системи України. У цій реальності кримінальні правопорушення у сфері інформаційних технологій набувають основні загрози, оскільки паралельно з кінетичними бойовими діями розгортається масштабна інформаційна агресія, спрямована на виснаження державних інституцій та дестабілізацію суспільства.

Парадигма інформаційної безпеки, в умовах воєнного стану вимагає концептуального розширення. Вона має трансформуватися з пасивної моделі стримування загроз у проактивну стратегію формування національної наративи. Це передбачає не лише реактивне спростування фейків, а й створення цілісного, правового обґрунтованого та ціннісного орієнтованого інформаційного порядку денного, який виконує функцію соціального «імунітету» проти зовнішніх маніпуляцій. Доцільним є впровадження механізмів стратегічного прогнозування, що дозволяють ідентифікувати потенційні вектори атак ще на етапі їхнього планування, а також розбудову системи цифрової стійкості.

Нормативно-правовим втіленням такої проактивної розбудови цифрової стійкості стала постанова Кабінету Міністрів України від 12.03.2022 № 263 «Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану» [43]. У постанові кардинально змінено підхід до захисту критичної інфраструктури, дозволивши міграцію державних баз даних та реєстрів до захищених хмарних середовищ (зокрема поза межами країни). Це

рішення стало класичним прикладом стратегічного прогнозування, яке замість пасивного захисту фізичних серверів, дало нормативне право державі превентивно вивести інформаційні ресурси з-під удару ворожих кіне-кібер атак. Це забезпечило не лише технологічну виживаність державного апарату, а й безперервний доступ громадян до життєво важливої інформації, гарантуючи тим самим інституційну та когнітивну стійкість держави.

Кіберзлочинці активно використовуються ворожими спецслужбами для зламу державних інформаційних систем, поширення дезінформації серед населення та створення мереж фальшивих акаунтів (ботоферм) у соціальних мережах, що є проявом гібридної війни. Значного поширення набуло й кібершахрайство, коли зловмисники, видаючи себе за представників офіційних структур, намагаються незаконно отримати доступ до банківських даних громадян для заволодіння їхніми грошовими коштами.

Характеризуючи Російську агресію проти України, необхідно відзначити широкомасштабні і постійні кібератаки та інші методи інформаційної агресії, щоб дестабілізувати Україну, підірвати довіру до країну серед західних партнерів, підірвати довіру до органів державної влади і місцевого самоврядування, до військових, волонтерів. Кібератаки, які спонсоруються державою, переслідують три цілі – використання слабкості інфраструктури; збір інформації; отримання грошей для компенсації втрат від санкцій. Такі атаки політично мотивовані, а цілі з часом можуть змінюватися [150, с. 57]. Таким прикладом, може бути виступ Прем'єр-міністра Дональда Туска, який назвав хакерську атаку (стосувалась інформації що поляки будуть мобілізовані воювати в Україні) частиною спроб Росії дестабілізувати ЄС напередодні виборів до Європейського парламенту, які відбудуться у червні 2024 року [311].

Небезпечною формою інформаційної агресії виступає кібершпionaж. Таємне отримання інформації з комп'ютерних систем, мереж або веб-сайтів. Ця форма інформаційної агресії використовується для крадіжки промислових

секретів, військової інформації або особистих даних із подальшим їх використанням з протиправною метою та небезпечними наслідками [150, с. 58].

Комплексний наліз сучасних викликів дозволяє стверджувати, що в умовах воєнного стану спектр актуальних ризиків суттєво розширився: від класичних кібератак (фішинг, віруси-вимагачі, шпигунське програмне забезпечення) до масштабних операцій із несанкціонованого розкриття конфіденційних даних, що мають на меті підрив обороноздатності. Наприклад, технологічна перевага в обробці даних стає вирішальним чинником у протидії цим загрозам, перетворюючи інформацію на стратегічний актив. Так, практичне застосування інтелектуальних систем засвідчило свою ефективність ще під час оборони Київщини у 2022 році, де аналітичні групи використовували алгоритми штучного інтелекту для дешифрування супутникових знімків та прогнозування логістики ворожих підрозділів. Цей досвід успішного моделювання загроз був під час Харківського контрнаступу, де застосування ШІ для автоматизованого аналізу розвідданих дозволило ідентифікувати вразливі сектори оборони противника та забезпечити високу точність маневрів українських сил [10, с. 34].

Окрім безпосередньої підтримки воєнних операцій, зазначають Бібік А. В., Городиський Р. О., Ваврічен О. А., штучний інтелект став ключовим інструментом у сфері кібернетичного та когнітивного протиборства. Сучасні алгоритми забезпечують: миттєве виявлення та нейтралізацію бот-мереж, що поширюють деструктивний контент; розпізнавання патернів пропаганди та блокування фішингових кампаній ще на етапі їхнього планування; оперативну нейтралізацію спроб ворога вплинути на систему прийняття управлінських рішень через вкиди дезінформації [10, с. 35].

Інтеграція таких інструментів дозволяє не лише нівелювати наслідки ворожих кібератак, а й перехопити ініціативу в інформаційному просторі. Це доводить, що розвиток «інтелектуальної» оборони є шляхом для підвищення інформаційної стійкості України в умовах тривалої гібридної агресії, де швидкість обробки даних часто стає вагомішою за будь-який інший ресурс.

Водночас, концептуалізація такої «інтелектуальної» оборони не може обмежуватися виключно технологічним виміром. Для того, щоб інформаційна стійкість набула системного характеру і забезпечила не лише відбиття атак, а й невідворотність покарання агресора, вона має бути глибоко імплементована в правову та інституційну площину.

Відтак, специфіку забезпечення інформаційної безпеки в умовах воєнного стану доцільно деталізувати за трьома основними напрямками. Ця просторова характеристика ґрунтується на нормах міжнародного гуманітарного права та враховує релевантний досвід держав, які успішно подолали наслідки збройних конфліктів та масштабних гібридних посягань (наприклад, постконфліктний досвід збирання доказової бази в Хорватії та практика інституціоналізації кіберзахисту в країнах Балтії). Слушно зазначає професор Юзікова Н.С., з огляду на геополітичне положення, країни Балтії, постійно знаходяться під загрозою кібератак. Атаки спрямовуються на енергетичний сектор і банківську систему тощо та призводять до тимчасового блокування веб-сайтів, витоку важливих даних [227, с. 37].

Перший, міжнародно-правовий та доказовий напрям (криміналізація кібервоєнних злочинів) передбачає необхідність чіткої документації та фіксації кібератак, що мають ознаки воєнних злочинів (напади на цивільну критичну інфраструктуру, медичні заклади). Це важливо для міжнародного правосуддя та використання у позовах проти держави-агресора (як того вимагає прецедентна практика щодо фіксації збитків у збройних конфліктах). Досвід Балканських війн продемонстрував важливість фіксації воєнних злочинів для подальшого розгляду в міжнародних трибуналах. Як показує практика роботи Міжнародного кримінального трибуналу щодо колишньої Югославії (зокрема, у контексті подій у Хорватії), своєчасне збирання та легалізація доказової бази є критичною умовою забезпечення правосуддя [272, с. 165]. У сучасних реаліях агресії РФ проти України цей напрям трансформується у необхідність належного збирання та легалізації електронних доказів атак на критичну інформаційну

інфраструктуру України. Відповідно до положень Талліннського керівництва 2.0 щодо застосування міжнародного права до кібероперацій, цілеспрямовані кібератаки на цивільні об'єкти (енергетику, медичні реєстри, системи зв'язку) повинні кваліфікуватися як воєнні злочини [324]. Це вимагає від українських правоохоронних органів розробки нових процесуальних механізмів фіксації цифрових слідів для Міжнародного кримінального суду. Центральне місце у цьому процесі має посісти імплементація положень Протоколу Берклі з ведення розслідувань з використанням відкритих цифрових даних, який на сьогодні є єдиним уніфікованим міжнародним стандартом у цій сфері.

Протокол Берклі з ведення розслідувань з використанням відкритих цифрових даних (Berkeley Protocol on Digital Open Source Investigations), спільно розроблений Центром з прав людини Каліфорнійського університету в Берклі та Управлінням Верховного комісара ООН з прав людини, є першим глобальним рамковим документом, покликаним стандартизувати збір та аналіз інформації з відкритих джерел (OSINT) для потреб національного та міжнародного кримінального судочинства [243].

Зокрема, застосування Протоколу дозволяє забезпечити безперервність «цифрового ланцюжка збереження доказів» при документуванні кібератак на цивільну критичну інфраструктуру та медичні заклади. Що важливо для міжнародного правосуддя, оскільки стандарти Берклі встановлюють чіткі алгоритми верифікації та автентифікації даних із відкритих джерел (OSINT), супутникових знімків та відеоматеріалів, що фіксують наслідки кібердиверсій.

Впровадження цих стандартів дозволить українським слідчим не лише ідентифікувати цифрові сліди зловмисників, а й забезпечити їхню доказову силу через фіксацію метаданих та криптографічне хешування. Такий підхід мінімізує ризики маніпуляцій чи оскарження доказів стороною захисту в міжнародних інстанціях, гарантуючи, що цифрова інформація про кібератаки перетвориться на процесуально бездоганну базу для притягнення держави-агресора до відповідальності за воєнні злочини в кіберпросторі.

Доречною є думка професора Бабенка А.М., що проста фіксація інформації про воєнні злочини є лише початковою стадією розслідування. Фундаментальною метою є процесуальне доведення вини, що досягається шляхом ретельного формування доказового масиву. Стратегія розслідування має спрямовуватися не просто на підтвердження самої події злочину, а на персоніфікацію відповідальності: чітку прив'язку діяння до конкретних осіб для забезпечення невідворотності покарання. Досягнення такого високого стандарту доказування безальтернативно вимагає інтеграції різногалузевого експертного інструментарію, що поєднує передові досягнення науки, техніки та кримінального процесуального права [5, с. 274].

Практична реалізація такого комплексного підходу об'єктивно потребує застосування уніфікованої, міжнародно визнаної методології. У цьому контексті слушною є позиція Ю. О. Виходця та Г.К.Тетерятника, які аргументують доцільність імплементації Протоколу Берклі як базового стандарту для проведення інтернет-розслідувань воєнних злочинів. На переконання дослідника, інкорпорація передбачених Протоколом методів та процедур дозволяє здійснювати збір, аналіз і збереження цифрової інформації із суворим дотриманням професійних, правових та етичних імперативів [25, с. 70].

Деталізуючи модель цього процесу, науковці структурують його за такими послідовними етапами: виявлення інформації, шляхом здійснення цілеспрямованих онлайн-запитів та системного моніторингу цифрового середовища; попередня оцінка, первинний аналіз релевантності та значущості виявлених даних; надійна фіксація та вилучення цифрових слідів із мережі Інтернет у спосіб, що гарантує їхню доказову автономність. Це забезпечує можливість підтвердження фактів навіть у разі знищення першоджерела інформації (через резервне копіювання, архівацію контенту, криміналістичну фіксацію знімків екрана тощо); верифікація даних, а саме, глибока перевірка автентичності (правдивості) змісту та встановлення надійності джерел його походження; аналітична інтерпретація масивів даних, формулювання

обґрунтованих висновків, виявлення доказових прогалин та остаточне з'ясування процесуальної ваги отриманої інформації для цілей кримінального провадження [25, с. 72–73].

Враховуючи вищевикладене, можна констатувати, що в умовах повномасштабної збройної агресії РФ проти України розвідка на основі відкритих джерел (OSINT) довела свою безальтернативну ефективність як інструмент документування правопорушень. Проте, незважаючи на успішну практичну апробацію новітнього програмного забезпечення та аналітичних алгоритмів, у вітчизняній та зарубіжній кримінально-правовій доктрині досі тривають дискусії [1; 25; 54; 145; 232; 279; 295]. Вони стосуються насамперед догматичного розуміння меж «відкритості» джерел інформації та механізмів гарантування легітимності отримання масивів даних із соціальних мереж чи месенджерів (зокрема, з огляду на захист права на приватність).

Водночас, ключовим критерієм результативності застосування OSINT-інструментарію є не сам факт виявлення цифрових слідів, а їхня судова перспектива - здатність набувати статусу належних і допустимих доказів як у національних юрисдикціях, так і в (МКС). І хоча завдяки синергії міжнародних стандартів та набутого досвіду вітчизняних фахівців уже сформовано певний концептуальний фундамент, стратегічним і найбільш проблемним напрямом реформування залишається нормативна процесуалізація такої інформації. Саме розробка чітких, адаптованих до вимог сучасності механізмів Кримінального процесуального кодексу України щодо збирання, криміналістичної верифікації та правової оцінки OSINT-даних дозволить подолати наявний законодавчий вакуум і забезпечити невідворотність покарання воєнних злочинців.

Ефективна реалізація міжнародно-правових механізмів неможлива без адаптації національного законодавства. Інформаційна війна завдає суспільству не меншої шкоди, ніж кінетичні бойові дії, посягаючи на суспільну свідомість та фінансову стійкість громадян. З огляду на це, в Україні розпочато реформування

кримінального та кримінального процесуального законодавства з метою підвищення ефективності протидії таким правопорушенням.

Проте, нині рівень запобігання кіберзлочинам залишається недостатнім, зважаючи на постійне вдосконалення злочинцями методів здійснення атак. Йдеться, зокрема, про використання інструментів штучного інтелекту для автоматизації соціальної інженерії, застосування дипфейків у шахрайських схемах та використання децентралізованих фінансових мереж (криптовалют) для відмивання злочинних доходів і фінансування підривної діяльності.

Це вимагає кримінологічного аналізу та обґрунтування проактивних заходів для формування національної кіберстійкості. У процесуальному вимірі така проактивність передбачає необхідність глибокої імплементації стандартів цифрової криміналістики, нормативного вдосконалення процедур збирання, перевірки та оцінки електронних доказів, а також імплементації положень Другого додаткового протоколу до Будапештської конвенції, що дозволить українським правоохоронцям оперативно отримувати електронну інформацію від іноземних технологічних корпорацій [50; 252]. Трансформація правосуддя має перейти від реактивного розслідування одиничних епізодів до системної протидії транскордонним кіберугрупованням

Другий, інституційно-оборонний напрям (мілітаризація кіберпростору та національний спротив) Цей напрям відображає перехід від цивільного адміністрування мереж до побудови диференційованої системи військового кіберзахисту. В умовах воєнного стану інформаційна безпека полягає у кардинальному зміщенні пріоритетів та масштабуванні загроз, що вимагає негайної та радикальної адаптації правових, інституційних та операційних механізмів.

Слушно зауважують Д. Смотрич та Л. Браїлко, з 2014 року Україна перебуває в стані перманентної відсічі інформаційній агресії, яка після повномасштабного вторгнення 2022 року трансформувалася у тотальну когнітивну війну. Російські операції інформаційно-психологічного впливу

(ШПО) мають чітко виражений деструктивний характер: вони спрямовані на штучну фрагментацію суспільства, делегітимізацію інститутів державної влади та підрив морально-психологічної стійкості Сил оборони України [198].

За таких обставин парадигма інформаційної безпеки вимагає розширення. Вона має трансформуватися з пасивної моделі стримування загроз у проактивну стратегію формування національного наративу. Це передбачає не лише спростування фейків, а й створення цілісного, правово обґрунтованого та ціннісно орієнтованого інформаційного порядку денного, який виконує функцію «імунітету» проти зовнішніх маніпуляцій. Доцільно впровадження механізмів стратегічного прогнозування, що дозволяють ідентифікувати потенційні вектори атак ще на етапі їхнього планування, а також розбудову системи цифрової стійкості, де кожне повідомлення в офіційному полі працює на зміцнення когнітивного суверенітету держави та захист фундаментальних прав громадян на достовірну інформацію.

Відповіддю на ці виклики стала консолідація суспільства. В умовах воєнного стану особливого значення набуло функціонування диференційованої системи захисту, що об'єднала державний сектор та волонтерські спільноти (наприклад, ІТ-армію України). Діяльність цих структур зосереджена на безперервному моніторингу цифрового простору, превенції складних атак на об'єкти критичної інформаційної інфраструктури, а також реалізації заходів активної кібероборони. Виникнення таких інституційних одиниць стало об'єктивною реакцією на еволюцію безпекових викликів, де конвенційні методи правової та технічної охорони виявилися недостатньо адаптивними до умов гібридного протистояння. Це зумовлює необхідність подальшої законодавчої легітимізації статусу кіберволонтерства та розробки чітких протоколів їхньої взаємодії з державними інституціями в межах єдиного безпекового контуру.

Логічним кроком у цьому напрямі та етапом інституціоналізації національної стійкості стало прийняття за основу законопроекту №12349 «Про Кіберсили Збройних Сил України» [172]. Дана ініціатива знаменує перехід від

розпорошених оборонних заходів до формування цілісної військово-технічної структури за стандартами НАТО, що діє під безпосереднім керівництвом Головнокомандувача ЗСУ.

Створення нового органу військового управління - Кіберсил ЗСУ, як окремого роду військ, дозволяє нормативно закріпити спроможності до кіберстримування та проведення активних операцій в електромагнітному спектрі, що є важливим для здобуття військової переваги в сучасному цифровому полі воєнних дій.

Третій, інфраструктурно-відновлювальний напрям (стійкість та модель нульової довіри). Враховуючи досвід постконфліктної відбудови, інфраструктура має відновлюватися не за старими, вразливими лекалами, а за принципом «відбудувати краще, ніж було». Важливою тенденцією забезпечення інформаційної безпеки в умовах воєнного стану є відмова від застарілих моделей «периметра довіри» на користь концепції Zero Trust Architecture (ZTA) [347]. Специфіка воєнного часу - інтенсивне впровадження хмарних технологій для збереження даних, робота фахівців із різних географічних точок та використання персональних пристроїв у межах політики BYOD, робить традиційні методи захисту корпоративних мереж неефективними. Класична модель кібербезпеки будувалася на презумпції безпеки внутрішньої мережі (принцип «замок і рів») коли кожен, хто пройшов автентифікацію та опинився всередині системи, вважався довіреним користувачем. Проте в умовах війни, коли існує ризик фізичного захоплення обладнання на тимчасово окупованих територіях, викрадення облікових даних або залучення інсайдерів, внутрішній периметр більше не гарантує безпеки.

Концепція ZTA, фундаментально закріплена у спеціальній публікації Національного інституту стандартів і технологій США (NIST SP 800-207) [347], базується на zasadі «ніколи не довіряй, завжди перевіряй». Як зазначають у своїх монографічних дослідженнях провідні фахівці з кібербезпеки та концепції ZTA (Дж. Кіндерваг, С. Роуз, О. Борчерта, С. Мітчелл, С. Коннеллі, Дж. Гарбіс та Дж.

В. Чепмен), ZTA вимагає безперервної авторизації кожного запиту на доступ до ресурсів, незалежно від того, звідки він надходить ззовні чи зсередини мережі [289; 347; 274].

Основним принципом ZTA у контексті воєнних викликів, зазначають Солодовник В. І., Шевчук Д. Л., стає теза «ніколи не довіряй, завжди перевіряй». В умовах високого ризику компрометації облікових даних або діяльності внутрішніх суб'єктів впливу, жоден користувач чи пристрій не може вважатися безпечним лише на підставі знаходження у внутрішній мережі. Кожна спроба доступу до стратегічних ресурсів підлягає безперервній верифікації через багаторівневі механізми автентифікації [200, с. 260-261].

З кримінологічної та правової точок зору, впровадження ZTA означає перехід до мікросегментації та гранулярного контролю доступу. Це мінімізує «радіус ураження» у разі успішної кібератаки. Навіть якщо зловмисник отримує доступ до одного сегмента мережі критичної інфраструктури, він позбавлений можливості вільно переміщуватися системою [274]. В умовах постійних атак на енергетичний, фінансовий та державний сектори України, імплементація принципів ZTA стає не просто технічною інновацією, а життєво необхідним стандартом виживання та захисту національних інформаційних ресурсів.

Для успішної імплементації моделі «нульової довіри» в національну державну систему безпеки необхідна реалізація комплексу заходів:

- а) перегляд державних політик безпеки та приведення їх у відповідність до міжнародних стандартів ZTA;
- б) впровадження інноваційних систем ідентифікації та безперервного моніторингу активності в мережах критичної інфраструктури;
- в) підготовка персоналу та зміна організаційної психології в бік постійної пильності;
- г) нормативно-правове закріплення аудиту ланцюгів постачання та жорстка регламентація доступу сторонніх ІТ-підрядників до державних інформаційних

ресурсів (що дозволить мінімізувати ризики «тіньових ІТ» та делегованої віктимності);

д) створення інтегрованої системи обміну даними про кіберзагрози між різними суб'єктами забезпечення національної безпеки, сектором оборони (зокрема Кіберсилами ЗСУ) та операторами критичної інфраструктури для забезпечення безперервного контекстного аналізу запитів на доступ;

є) поступова (поетапна) мікросегментація державних реєстрів і баз даних на основі ризик-орієнтованого підходу, що передбачає першочергову ізоляцію найбільш чутливих масивів інформації від загальнонаціональних мереж;

ж) посилення інституційної та персональної юридичної відповідальності суб'єктів владних повноважень за ігнорування протоколів моделі «нульової довіри» та неналежне управління цифровими ідентифікаторами.

Таким чином, впровадження ZTA дозволяє мінімізувати наслідки у випадку успішної кібератаки на окремі вузли системи, що є важливим для збереження керованості державою в умовах безперервної гібридної агресії. Таким чином, перехід до моделі «нульової довіри» виступає не лише технічним оновленням, а фундаментальним управлінським рішенням, що формує основу інформаційної стійкості України нового покоління.

Четвертий, правозахисний (антропоцентричний) напрям (баланс між імперативами безпеки та гарантіями прав людини). Цей напрям відображає концептуально складну тенденцію забезпечення інформаційної безпеки в умовах воєнного стану збереження демократичного базису держави. Забезпечення національної стійкості об'єктивно вимагає оперативного надання правоохоронним органам та спецслужбам розширених повноважень (зокрема, для превентивного моніторингу мережевої активності, блокування деструктивних ресурсів та проведення негласних слідчих дій у цифровому середовищі). При цьому, складною тенденцією забезпечення інформаційної безпеки в умовах воєнного стану є збереження антропоцентричного підходу та пошук балансу між імперативами національної оборони і дотриманням

фундаментальних прав людини. Як засвідчує практика Європейського суду з прав людини (зокрема, у справі «*K.U. v. Finland*», заява № 2872/02), держава несе позитивне зобов'язання щодо захисту суспільства від кримінальних посягань у кіберпросторі, що робить право на мережеву анонімність неабсолютним у випадках вчинення злочинів [249].

Фундаментальним механізмом балансування у цій площині виступає доктрина легітимізації втручання. В умовах гібридної агресії національне законодавство об'єктивно має дозволяти оперативне та тимчасове обмеження окремих цифрових прав (наприклад, розширений збір телекомунікаційних даних або обмеження доступу до певних інтернет-ресурсів) з метою гарантування національної безпеки. Однак така легітимізація не тотожна свавіллю, вона повинна здійснюватися виключно з дотриманням принципу пропорційності та підлягати дієвому контролю (судовому чи парламентському). Цей імператив прямо впливає з вимог Європейської конвенції з прав людини (зокрема ст. 15 щодо відступу від зобов'язань під час надзвичайної ситуації) та відповідної прецедентної практики ЄСПЛ [91]. Як наголосив Європейський суд з прав людини у своєму фундаментальному рішенні у справі «*Szabó and Vissy v. Hungary*» (заява № 37138/14), посилення держави на необхідність боротьби з тероризмом або загрози національній безпеці не надає владі «карт-бланш» на необмежене втручання у цифрові права громадян. Суд підкреслив, що будь-яке законодавство, яке дозволяє масштабне негласне збирання даних або перехоплення електронних комунікацій, навіть в умовах надзвичайних ситуацій, повинно містити «адекватні та ефективні гарантії проти зловживань». Це вимагає чіткого визначення меж повноважень безпекових органів, встановлення суворого незалежного (переважно судового) контролю за їхніми діями та доведення пропорційності вжитих заходів реальній загрозі [250].

Незважаючи на об'єктивну необхідність запровадження правового режиму «стану винятку», який допускає легітимні та пропорційні обмеження вільного обігу інформації (відповідно до ст. 64 Конституції України) [94], правові

інструменти протидії загрозам не повинні руйнувати демократичний базис держави.

Водночас, імплементація обмежувальних інструментів не повинна руйнувати антропоцентричний підхід. Навіть в умовах правового режиму «стану винятку» застосування розширених повноважень має відбуватися з неухильним збереженням гарантій прав людини, відповідно до принципів Європейської конвенції з прав людини (ЄКПЛ) та вимог Загального регламенту про захист даних (GDPR) [57; 91]. Будь-яке розширення юрисдикційних повноважень щодо ідентифікації користувачів має відповідати критерію пропорційності. Згідно з правовою позицією ЄСПЛ, висловленою у справі «*Benedik v. Slovenia*» (заява № 62357/14), особа має обґрунтоване очікування приватності щодо своєї динамічної IP-адреси та історії мережевої активності, а отже, доступ правоохоронних органів до таких даних вимагає суворого судового контролю та запобіжників проти свавілля [247].

У цьому контексті важливого значення набуває гарантування конституційних прав на недоторканність приватного життя та посилений кримінально-правовий захист законної професійної діяльності журналістів. Як доводить сучасна українська наукова доктрина, в умовах інтенсивних інформаційно-психологічних операцій агресора преса виступає не лише гарантом демократичного цивільного контролю, а й потужним інституційним «фільтром». Захист журналістської діяльності трансформується з вузькопрофесійної проблеми на невіддільний елемент національної інформаційної стійкості, оскільки саме функціонування об'єктивних та незалежних медіа ефективно протидіє поширенню дезінформації та зміцнює когнітивний суверенітет нації. Зважаючи на прецедентну практику ЄСПЛ (зокрема, рішення Великої Палати у справі «*Delfi AS v. Estonia*», заява № 64569/09), блокування ресурсів або притягнення до відповідальності за поширення інформації має ґрунтуватися на справедливому балансі між свободою

вираження поглядів (ст. 10 ЄКПЛ) та необхідністю захисту національної безпеки [248].

Узагальнюючи викладене, варто наголосити, що імплементація зазначених чотирьох напрямів (міжнародно-правового, інституційного, інфраструктурного та правозахисного) дозволяє сформувати комплексну, багаторівневу модель забезпечення інформаційної безпеки України. Відповідно до сучасних тенденцій та викликів воєнного стану, практична реалізація цієї моделі концептуалізується у системі таких пріоритетних стратегічних напрямів:

- Створення захищеного інформаційного суверенітету, що передбачає проактивну превенцію кіберзагроз, жорсткий захист критичної інфраструктури (зокрема через імплементацію моделі нульової довіри) та інституціоналізацію боротьби з високотехнологічною злочинністю.
- Розбудова системи стратегічних комунікацій, спрямованої на забезпечення внутрішньої соціальної стабільності та трансляцію об'єктивного іміджу України як надійного і стійкого цифрового партнера на міжнародній арені.
- Інформаційна реінтеграція тимчасово окупованих територій як беззаперечний пріоритет державної політики, що включає подолання наслідків ворожої пропаганди, розширення доступу до вітчизняного мовлення та відновлення безпечного цифрового зв'язку з громадянами в умовах їхньої тривалої ізоляції.
- Формування «цифрового імунітету» суспільства через системне підвищення медіакультури, цифрової гігієни та критичного мислення населення, що є найефективнішим антропоцентричним запобіжником проти маніпулятивних інформаційно-психологічних операцій.
- Нормативне забезпечення когнітивного захисту шляхом впровадження ефективних механізмів фільтрації деструктивного та незаконного контенту, і протидії дезінформації без порушення крихкого балансу зі свободою слова.
- Гарантування конституційних прав особи на вільне вираження своїх поглядів і переконань, а також захист недоторканності приватного життя, що

перешкоджатиме трансформації правового режиму воєнного стану в інструмент надмірної цензури.

- Захист прав журналістів та створення безпечних умов для їхньої законної діяльності, оскільки саме незалежна журналістика відіграє ключову роль у підтримці інформаційної свободи, прозорості та демократичного цивільного контролю в умовах війни [146, с. 298-299].

Підсумовуючи, можна констатувати, що правовий режим воєнного стану фундаментально трансформував парадигму забезпечення інформаційної безпеки України. Відбувся концептуальний перехід від пасивної моделі захисту технічного «периметра» до проактивної стратегії національної цифрової стійкості, де кіберпростір функціонує як повноцінний спектр воєнних дій.

2.2. Законодавчі та інституційні засади забезпечення інформаційної безпеки України

Забезпечення інформаційної безпеки України на сучасному етапі базується на стрімкій трансформації законодавчих та інституційних засад, що адаптуються до викликів воєнного стану та концепції «стану винятку». Інституційна система зміщується в бік мілітаризації кіберпростору, де ключову роль у протидії гібридним загрозам відіграють не лише правоохоронні органи, Центр протидії дезінформації, а й заплановані до створення Кіберсили ЗСУ.

Локальні ризики, зокрема атаки на критичну інфраструктуру та масштабні психологічні операції, тісно переплітаються з глобальними трендами кібершпигунства та використанням штучного інтелекту для дезінформації. У відповідь на ці виклики національне правове поле еволюціонує в бік імплементації міжнародних стандартів цифрової стійкості та моделі «нульової довіри», що має на меті гарантувати когнітивний суверенітет держави та формування інформаційної стійкості суспільства.

У вітчизняній правовій доктрині системний аналіз законодавчих засад здійснюється крізь призму кількох концептуальних наукових підходів, які відображають багатогранність феномену інформаційної безпеки.

Перший, інформаційно-правовий підхід (широкий). У межах цього підходу (який досліджується у працях А.М. Бабенка, В. Л Гончарука, О. Д. Довганя, В.М. Желіховського, Б. А. Кормича, Т.В. Корнякової, О. М. Литвинов, В. А. Ліпкана, Ю. Є. Максименко, О. Онопрієнко, С. Онопрієнко Т. Ю Ткачука, Н.С. Юзікової) законодавчі засади розглядаються як комплексна система норм, що регулюють суспільні відносини у сфері обігу інформації, реалізації інформаційного суверенітету та захисту національних інтересів в інформаційній сфері [34; 48; 95, 119; 133; 151]. З позиції цього підходу, базовим вектором законодавства є пошук балансу між конституційним правом громадян на вільне збирання, зберігання і поширення інформації (ст. 34 Конституції України) та імперативами державної безпеки [94]. Основу цього масиву становить Закон України «Про інформацію» та Закон України «Про основні засади забезпечення кібербезпеки України» [171; 177]. Відповідно до праць Б. А. Кормича, сучасне законодавство має еволюціонувати від заборонних методів до механізмів стимулювання безпечної інформаційної поведінки [95].

У контексті цього широкого підходу держава несе не лише пасивний обов'язок утримуватися від порушень прав людини, а й виконує позитивний конституційний обов'язок щодо їх активного захисту в умовах стрімкої цифрової трансформації.

Правову основу інформаційної безпеки становлять норми що стосуються цифрового середовища, які вказують на форми і методи захисту даних, управління цифровою інформацією та комунікаційними системами. Так, у ст. 17 Конституції України проголошено, що забезпечення інформаційної безпеки України є однією з найважливіших функцій держави справою всього Українського народу» [94]. Продовженням є визначення поточних та прогнозованих загроз національній безпеці та національним інтересам України з

урахуванням зовнішньополітичних та внутрішніх умов, визначених у Стратегії національної безпеки України [178].

Правове підґрунтя інформаційної безпеки України становить багаторівнева система нормативних актів: Конституція України, Кримінальний та Кримінальний процесуальний кодекси України, спеціалізовані закони (зокрема «Про основні засади забезпечення кібербезпеки України», «Про інформацію», «Про захист інформації в інформаційно-комунікаційних системах», «Про національну безпеку України») [169; 171; 175; 177]. Концептуальний рівень регулювання забезпечується Доктриною інформаційної безпеки України, тоді як міжнародно-правовий вимір спирається на Конвенцію Ради Європи про кіберзлочинність (Будапештську конвенцію) та інші ратифіковані міжнародні договори [92].

Саме в межах інформаційно-правового підходу базовим Законом України «Про основні засади забезпечення кібербезпеки України» нормативно закріплено розмежування ключових понять. Під кібербезпекою розуміють стан захищеності життєво важливих інтересів особи, суспільства та держави у процесі використання кіберпростору. Натомість кіберзахист розглядається як більш прикладна, технологічна категорія, що охоплює комплекс організаційних, нормативно-правових, інженерно-технічних та інших заходів технічного захисту інформації, спрямованих на запобігання кіберінцидентам.

Водночас, застосування норм цього широкого підходу на практиці (особливо в умовах правового режиму воєнного стану) генерує фундаментальну колізію: забезпечення національної та громадської безпеки в кіберпросторі об'єктивно вимагає застосування інструментів, що обмежують приватність (наприклад, превентивний моніторинг електронних комунікацій, збір масивів метаданих, розширений доступ до електронних доказів). Це створює перманентну державно-правову «діалектику» напруги та необхідність пошуку оптимального балансу між захистом індивідуальної недоторканності приватного

життя та імперативом ефективної протидії високотехнологічній злочинності [146, с. 294-295].

У інформаційно-правовому вимірі головним завданням є пошук балансу між свободою інформації та необхідністю захисту держави. Національна стратегія у сфері прав людини виступає фундаментальним запобіжником у всій системі інформаційної безпеки та гарантує, що процеси цифровізації та боротьби з кіберзагрозами не перетворяться на інструмент тотального стеження [138]. Стратегія легітимізує тезу про те, що право на недоторканність приватного життя та свобода вираження поглядів є пріоритетними, а будь-які обмеження цих прав правоохоронними органами мають бути законними, пропорційними та підлягати судовому контролю.

Доктрина інформаційної безпеки України, це перший концептуальний документ після 2014 року, який юридично закріпив визнання російської пропаганди як загрози національній безпеці [181]. У межах першого інформаційно-правового підходу Доктрина заклала нормативні основи для створення механізмів виявлення та блокування деструктивного контенту, зберігаючи при цьому гарантії вільного розвитку вітчизняного медіа-простору.

Відповідно до європейських правових стандартів, будь-які втручання держави у приватне життя мають бути пропорційними до переслідуваної легітимної мети, регламентованими законом та необхідними у демократичному суспільстві. Надання правоохоронним органам надмірних, дискреційних повноважень без належного та ефективного судового контролю неминуче створює ризики порушення фундаментальних прав людини. Важливу роль у підтримці цього балансу відіграє чітко врегульована законодавством взаємодія правоохоронних органів з інтернет-провайдерами щодо оперативного доступу до електронних доказів. Для результативного реагування на кіберзагрози необхідне функціонування комплексної правової основи, яка гарантує проведення слідчих дій із дотриманням балансу між повагою до автономії особи та наданням

достатніх процесуальних інструментів для розслідування, що є ключовим викликом для сучасного інформаційного права України.

Саме прагнення інституційно забезпечити цей складний баланс та не допустити розширення дискреційних повноважень слідства визначає специфіку підходу нашої держави до імплементації міжнародних стандартів. Показовим є досвід приєднання України до Будапештської конвенції про кіберзлочинність (2005 рік). Засвідчивши свою стратегічну відданість глобальній архітектурі цифрової безпеки, держава водночас продемонструвала зважену правову позицію, скориставшись передбаченим правом на застереження щодо застосування статті 6 Конвенції (криміналізація зловживання пристроями) [92].

Ця національна адаптація, як слушно зазначають О. Онопрієнко та С. Онопрієнко, була продиктована гострою необхідністю узгодити міжнародні норми з базовими гарантіями вітчизняного кримінального права, насамперед, щодо забезпечення чіткості конструкції складу кримінального правопорушення та запобігання необґрунтованому притягненню до відповідальності за обіг технічних засобів. Такий гнучкий підхід дозволив Україні уникнути правової невизначеності у внутрішній політиці кібербезпеки, зберігши процесуальну пропорційність. Сьогодні, Україна залишається проактивним суб'єктом глобальної взаємодії, беручи системну участь у роботі Кіберкомітету Ради Європи (Т-СҮ) [151]. Це, доводить, що вітчизняна правова система здатна не лише імплемувати міжнародний досвід, а й безпосередньо впливати на формування сучасної нормативної бази цифрової епохи.

Згідно зі Стратегією інформаційної безпеки України, інформаційна політика РФ визнана прямою загрозою не лише для України, а й для інших демократичних країн. Російські спецслужби цілеспрямовано здійснюють спеціальні інформаційні операції, спрямовані на ключові демократичні процеси, зокрема вибори, та прагнуть посилити внутрішні розбіжності в Україні та за її межами. Технології гібридної війни, які Росія застосовує проти України, швидко адаптуються та поширюються на інші держави. Відповіддю на таку

дезінформаційну агресію є запровадження обмежувальних заходів (санкцій) та створення ефективного механізму моніторингу й притягнення до відповідальності за їх порушення [180].

Наступним кроком нормативного закріплення заходів захисту інформаційної безпеки було Рішення РНБО України від 29 грудня 2016 року, де було схвалено Доктрину інформаційної безпеки України (далі - Доктрина), яка стала стратегічним документом щодо окреслення концептуальних засад державної політики у сфері інформаційної безпеки [181]. Основні положення Доктрини включали головну мету та стратегічні завдання державної інформаційної політики; основні принципи інформаційної безпеки, серед яких цілісність, автономія, суверенітет у інформаційному просторі, врахування демократичних цінностей і прав людини; характеристику потенційних внутрішніх та зовнішніх загроз національній інформаційній безпеці, включаючи дезінформацію, кібератаки та втручання в інформаційний простір; зазначення кроків та механізмів реагування на виклики і загрози інформаційній безпеці, у тому числі, наголос зроблено на необхідності співпраці з іноземними державами та міжнародними організаціями у сфері інформаційної безпеки.

Після втрати чинності Доктрини, рішенням РНБО України від 15 жовтня 2021 року приймається Стратегія інформаційної безпеки до 2025 року (далі - Стратегія). Стратегія містить визначення загроз, засобів захисту, механізмів виявлення та запобігання злочинам у сфері інформаційної безпеки [180]. Основними напрямками реалізації Стратегії є протидія дезінформації, розвиток медіакультури та медіаграмотності. Важливими аспектами також є захист особистих даних та культури вільного вираження поглядів, підтримка зв'язку з громадянами на тимчасово окупованих територіях та розвиток стратегічних комунікацій. Крім цього, стратегія передбачає створення ефективної системи інформаційного суспільства та підвищення рівня культури діалогу. Як і в Доктрині, у Стратегії визначено сутність, засади, механізми інформаційної безпеки, наголошено на доцільності міжнародної співпраці та імплементації

міжнародних угод та директив, таких як Конвенція про кіберзлочинність, GDPR, що формують міжнародно-правову основу інформаційної безпеки. Поряд з цим, у Стратегії більш чітко ніж у Доктрині визначені глобальні та національні виклики та загрози, з урахуванням яких сформовані напрями забезпечення інформаційної безпеки України. Визначено механізми захисту інформаційної безпеки України: координацію діяльності різних органів виконавчої влади, нормативно-правове регулювання, моніторинг і прогнозування загроз, популяризацію та захист інтересів країни.

Другий підхід, спеціально-режимний (контекстуальний). Він набув особливої актуальності з початком збройної агресії РФ і детально розкривається в колективній монографії Інституту держави і права ім. В. М. Корецького НАН України (за ред. О. В. Радченка) [163]. Прихильники цього підходу акцентують увагу на тому, що законодавчі засади в умовах правового режиму воєнного стану (стану винятку) зазнають фундаментальної трансформації. У межах цього підходу законодавчі засади можна розглянути через призму правового режиму воєнного стану [37, с. 79-85; 198, с. 121-127; 114; 201, с. 126-133]. Головна проблема, полягає в тому, що чинна інституційна система, побудована для умов мирного часу, виявилася недостатньо гнучкою для відбиття гібридних воєнних загроз. З позицій спеціально-режимного підходу, ключовим захисним фактором стає мілітаризація ІТ-сектору та інституціоналізація нових суб'єктів національного спротиву (наприклад, інтеграція волонтерських ІТ-спільнот у державну систему). Законодавство тимчасово відходить від класичних демократичних стандартів вільного інформаційного ринку на користь жорсткої централізації, легітимізації цензурних обмежень, блокування ворожих медіа-ресурсів та запровадження кримінальної відповідальності за колабораційну діяльність, глорифікацію в інформаційному просторі.

Впровадження такого спеціально-режимного підходу є об'єктивною необхідністю та симетричною відповіддю на виклики сучасної гібридної війни, яка змістила фокус із конвенційних збройних зіткнень на створення керованого

інформаційного хаосу. Сьогодні мішенню агресора виступає не лише фізична інфраструктура, а й когнітивний простір (масова свідомість суспільства та психологічна стійкість особового складу ЗСУ. Ворожий інструментарій охоплює весь спектр деструктивного впливу, від цілеспрямованих хакерських атак на критичні системи життєзабезпечення до масштабних психологічних операцій. Використання мереж ботів, глибинних фейків та спеціально створених пропагандистських ресурсів перетворилося на ефективну зброю маніпулювання, дезорієнтації та залякування, що експлуатує людську схильність до некритичного, поверхневого сприйняття інформації [114, с. 290].

У цих умовах небезпеки, що кардинально відрізняється від загроз мирного часу, парадигма забезпечення інформаційної безпеки трансформується у фундаментальне питання виживання людини, суспільства та держави. Відповідно, технічна основа інформаційної безпеки, забезпечення цілісності, конфіденційності, доступності та надійності даних, набуває нового ціннісного виміру. В межах спеціального режиму технічні стандарти стають інструментом захисту прав і свобод особи від деструктивного інформаційного програмування, підпорядковуючи індивідуальні інтереси загальнонаціональному завданню збереження державного суверенітету [198, с. 122-123].

Третій, кримінально-правовий та кримінологічний підхід, стосується законодавчих засад інформаційної безпеки. У межах цього підходу, наукова думка стосується системи кримінально-правових заборон та процесуальних механізмів, спрямованих на охорону суспільних відносин від кіберпосягань [1; 25; 144, с. 111-118 ; 201, с. 126-133; 145, с. 144-155].

Інформаційна безпека в правовому контексті охороняє основоположні права людини, зокрема право на приватність та конфіденційність, які є важливою частиною прав людини. Тому правові аспекти інформаційної безпеки є значущим компонентом в структурі сучасного права і державної політики [146, с. 295]. Відповідно до позицій провідних вітчизняних фахівців у сфері кримінальної юстиції, законодавчі засади інформаційної безпеки розглядаються

як система кримінально-правових заборон та кримінально-процесуальних механізмів, спрямованих на охорону суспільних відносин від суспільно небезпечних посягань у кіберпросторі та когнітивній сфері [13; 79; 102].

Основною проблемою у цій площині є стійкий нормативний дисонанс. Темпи еволюції гіберзлочинності (використання ШП, криптоміксерів, дипфейків) випереджають процеси законодавчої модернізації. Причиною низької ефективності протидії є те, що норми матеріального права (Розділ XVI КК України «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин...»), а також норми, що передбачають відповідальність за злочини проти основ національної безпеки (державна зрада, диверсія в кіберпросторі) не повною мірою охоплюють транскордонну специфіку сучасних атак, а норми процесуального права (КПК України) досі не містять деталізованих стандартів обігу цифрових доказів, що ускладнює їх легалізацію для міжнародних судових інстанцій. Водночас, синтез цих наукових підходів дозволяє констатувати наявність стійкого нормативного дисонансу, темпи еволюції гібридних загроз суттєво випереджають процеси законодавчої модернізації механізмів протидії. Незважаючи на наявність Закону «Про основні засади забезпечення кібербезпеки України», законодавча база виявляє низку системних прогалин, насамперед у площині кримінальної юстиції. Вона концептуально сформована переважно для умов мирного часу або конфліктів низької інтенсивності, виявляє низку прогалин у регулюванні суспільних відносин періоду повномасштабної війни.

Формування ефективної системи забезпечення інформаційної безпеки в умовах сучасних глобальних викликів неможливе без гнучкого нормативно-правового фундаменту. Основа цієї системи визначаються Конституцією України, яка гарантує право на інформацію та водночас допускає його легітимне обмеження в інтересах національної безпеки, а також профільним Законом України «Про основні засади забезпечення кібербезпеки України» [94; 177].

У площині матеріального кримінального права проблемою залишається недосконалість понятійно-категоріального апарату. Традиційні склади кримінальних правопорушень (Розділ XVI КК України) не повною мірою охоплюють специфіку сучасних транскордонних кібератак на критичну інфраструктуру, які здійснюються іноземними спецслужбами та афілійованими хакерськими угрупованнями.

Не менш гострою є проблема у сфері кримінального процесуального законодавства. Незважаючи на об'єктивну потребу, КПК України потребує глибокої системної модернізації в частині регламентації обігу електронних доказів. Відсутність деталізованих, міжнародно визнаних стандартів цифрової криміналістики у національному законодавстві ускладнює легалізацію цифрових слідів, їх належну процесуальну фіксацію та передачу до міжнародних судових інстанцій. А в умовах стрімкої мілітаризації кіберпростору та масового використання відкритих цифрових даних (OSINT) для фіксації воєнних злочинів, в умовах збройної агресії РФ, актуалізують проблему, яка полягає у допустимості та верифікації електронних доказів. Процесуальне законодавство досі демонструє інституційну неготовність до повноцінної роботи з цифровими слідами, зібраними з відкритих джерел (соціальних мереж, супутникових знімків, баз даних), що створює ризики їх визнання недопустимими як у національних судах, так і в міжнародних судових інстанціях (зокрема, у Міжнародному кримінальному суді).

Напрямом реформування законодавства, у цьому руслі, є імплементація в українське правове поле стандартів Протоколу Берклі з ведення розслідувань з використанням відкритих цифрових даних. Цей практичний посібник, розроблений Управлінням Верховного комісара ООН з прав людини, формує еталонну методологію ефективного використання цифрової інформації у відкритому доступі для розслідування порушень міжнародного кримінального та гуманітарного права. Протокол Берклі визначає міжнародні стандарти проведення онлайн-розслідувань щодо ймовірних порушень міжнародного

кримінального, гуманітарного права та прав людини. Цей документ надає чіткі методологічні вказівки для професійного, законного та етичного збору, аналізу й збереження цифрової інформації. Окрема увага у ньому приділяється заходам із забезпечення комплексної (цифрової, фізичної та психосоціальної) безпеки розслідувачів, свідків, потерпілих і громадянських активістів, які документують воєнні злочини заради притягнення винних до відповідальності. Протокол Берклі розкривається через три взаємопов'язані виміри: процесуально-доказовий, правозахисний та методологічний [243].

У цьому контексті, слушно зазначає професор Бабенко А.М., що процес фіксації та процесуального закріплення доказів воєнних злочинів в умовах воєнного стану стикається зі значними викликами. Зокрема, матеріали, які акумулюються через платформу застосунку «Дія», часто генеруються без дотримання належних криміналістичних методів та норм КПК України, що суттєво ускладнює їхню експертну оцінку та знижує доказовість висновків судових експертів. Вирішення цієї проблеми вимагає комплексної модернізації апробованих експертних методик. Крім того, орієнтир на міжнародні стандарти, зокрема Протокол Берклі (як базовий посібник з використання відкритих цифрових даних у розслідуваннях), ставить перед вітчизняним законодавцем безліч невирішених питань щодо необхідності концептуального оновлення КПК України та регламентів проведення судових експертиз [5, с. 272, 274].

З позицій кримінально-процесуального права, впровадження принципів Протоколу Берклі дозволить вирішити одразу кілька стратегічних завдань. По-перше, він пропонує чіткий алгоритм забезпечення «цифрового ланцюжка збереження доказів», що гарантує цілісність, автентичність та незмінність електронних даних з моменту їх виявлення до подання в суді. По-друге, імплементація його етичних та правових стандартів відповідає діалектичному балансу, де Протокол встановлює жорсткі рамки щодо захисту персональних даних, мінімізації шкоди та поваги до права на приватність навіть під час проведення розслідувань у відкритих масивах даних.

Таким чином, інтеграція норм Протоколу Берклі до відомих інструкцій правоохоронних органів України (СБУ, Національної поліції, ЦПД) та відповідна зміна норм КПК України є фундаментальною умовою переходу від хаотичного збору цифрової інформації до процесуально бездоганного механізму доказування. Це не лише посилить спроможність держави притягувати до відповідальності кіберзлочинців та воєнних злочинців, але й стане запобіжником проти порушень конституційних прав людини під час роботи з великими даними (Big Data).

Водночас, довершена система забезпечення інформаційної безпеки не може обмежуватися слідчо-процесуальними механізмами реагування на вже вчинені правопорушення. Створення стійкого цифрового середовища вимагає синергії між покаранням винних та надійним превентивним захистом самих систем. Законодавчі засади захисту інформаційної інфраструктури досі значною мірою спираються на застарілу концепцію «периметральної безпеки». Законодавство потребує імперативного закріплення обов'язку для операторів критичної інфраструктури щодо впровадження стандартів Моделі нульової довіри, що має супроводжуватися відповідними механізмами аудиту та юридичної відповідальності за недотримання протоколів кіберстійкості.

Інформаційна безпека сьогодні розглядається не лише як технічна, а як комплексна соціально-правова проблема, що потребує системного підходу. Її забезпечення вимагає врахування правових, соціальних, етичних та психологічних аспектів, адже загрози інформаційному простору впливають на стабільність держави та права громадян. Ключовим завданням є формування балансу між свободою слова та безпекою, а також між правами і обов'язками користувачів цифрового середовища. Надмірний контроль може призвести до обмеження демократичних свобод, тоді як його відсутність створює умови для кіберзлочинності та інформаційних атак. Таким чином, правовий контекст інформаційної безпеки має ґрунтуватися на принципах гнучкості, балансу та інтеграції міжнародних і національних підходів.

Інформаційна безпека охоплює широкий аспект захисту незалежно від форми, в якій зберігається чи обробляється інформація. Вона включає захист даних, процесів, інформаційних систем і мереж від незаконного доступу, використання, розкриття, розголошення, модифікації чи знищення. Принципи інформаційної безпеки забезпечують конфіденційність, цілісність і доступність всієї значимої інформації (друкованої, усної або електронної). Останні, охоплюють комплекс скоординованих заходів, які здійснюються державними органами, військовими або іншими суб'єктами і спрямовані на вплив на свідомість, емоції, волю та поведінку населення, військовослужбовців або осіб, які приймають рішення. Водночас, чинне інституційне поле зіштовхується з проблемою дублювання функцій та недостатньої гнучкості у співпраці державних та недержавних структур, що робить реформування системи гарантування інформаційної безпеки першочерговим завданням кримінологічного забезпечення.

Далі розглянемо інституційну модель забезпечення інформаційної безпеки. Ефективність нормативно-правового регулювання безпосередньо залежить від дієвості інституційного механізму, системи державних органів, на які покладено завдання щодо протидії кіберзлочинності та забезпечення інформаційної безпеки. Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України», національна інституційна модель має поліцентричний характер. Координацію діяльності суб'єктів сектору безпеки і оборони у цій сфері здійснює РНБО, яка формує стратегічні вектори розвитку через рішення Національного координаційного центру кібербезпеки.

Департамент кіберполіції Національної поліції України, як спеціалізований підрозділ, відіграє ключову роль у протидії традиційній кіберзлочинності [183]. Його діяльність регламентується Законом України «Про Національну поліцію» та відповідними відомчими положеннями [176]. Основний фокус діяльності зосереджений на розслідуванні злочинів у сфері використання електронно-обчислювальних машин (Розділ XVI КК України), протидії кібершахрайству,

поширенню протиправного контенту та порушенню авторських прав у мережі Інтернет. Водночас, в умовах воєнного стану Департамент стикається з викликами, коли розслідування транскордонних фінансових кіберзлочинів, вчинених із використанням криптовалют, вимагає імплементації складних міжнародно-правових механізмів співробітництва.

Поряд із вирішенням завдань кримінального переслідування, реалії гібридного конфлікту зумовили розширення функціоналу Національної поліції у площину забезпечення когнітивної безпеки та організації руху національного спротиву в кіберпросторі. Практичним втіленням такої інституційної трансформації стала реалізація комплексного проєкту «BRAMA», який репрезентує інноваційну модель кіберзахисту та державно-громадського партнерства. Вона зосереджена на двох взаємопов'язаних стратегічних напрямках: проактивній протидії інформаційним загрозам та превентивному підвищенню цифрової грамотності населення [42].

У межах першого напрямку, під егідою правоохоронних органів, відбувається консолідація потенціалу волонтерської спільноти (ІТ-фахівців, медійних осіб, лідерів думок). Головним механізмом їхньої взаємодії є масове алгоритмічне блокування осередків ворожої дезінформації та деструктивного контенту шляхом подання скоординованих, обґрунтованих скарг адміністраторам соціальних мереж і месенджерів. Одночасно із цим розгортається другий, профілактичний контур, спрямований на мінімізацію вразливості суспільства до психологічних маніпуляцій. Через спеціалізовані державні платформи, зокрема вебпортал «Кібер Брама» [76], здійснюється формування навичок критичного мислення, кібергігієни та безпечної поведінки, що фактично перетворює пересічних громадян із пасивних споживачів інформації на активних суб'єктів загальнонаціональної системи кіберстійкості.

Аналіз емпіричних показників діяльності Національної поліції України засвідчує трансформацію підходів до протидії кіберзлочинності, у напрямку комплексно-наступальної стратегії. Динаміка 2025 року демонструє закономірну

оптимізацію кількісних показників: підрозділами кіберполіції зареєстровано понад 2,1 тис. кримінальних правопорушень (порівняно з 2,5 тис. у 2024 році), повідомлено про підозру близько 1,5 тис. особам (у 2024 р. - 1,7 тис.), а до суду з обвинувальним актом скеровано понад 2,7 тис. проваджень (у 2024 р.- 4 тис.). Однак на тлі цього статистичного спаду загального масиву справ фіксується безпрецедентне зростання якісної ефективності слідства, насамперед у його економічному вимірі. Обсяг відшкодованих збитків збільшився більш ніж удвічі, сягнувши 342,6 млн грн, що становить 70,9% від загальної суми завданої шкоди (проти 168,5 млн грн та 42,5% у 2024 році). Одночасно збережено стабільно високий рівень нейтралізації організованої кіберзлочинності - до суду скеровано 58 обвинувальних актів щодо організованих груп та злочинних організацій (у 2024 році – 57) [42].

Служба безпеки України (СБУ), відповідно до Закону України «Про Службу безпеки України», виконує функції контррозвідувального захисту інтересів держави у сфері інформаційної безпеки [182]. Ситуаційний центр забезпечення кібербезпеки СБУ зосереджує увагу на протидії кібертероризму, кібершпигунству та розслідуванні кібератак на державні електронні інформаційні ресурси, що становлять загрозу національній безпеці (зокрема кібероперацій іноземних спецслужб). За офіційними даними Ситуаційного центру забезпечення кібербезпеки СБУ 2022 року виявлено та знешкоджено понад 15 тис. критичних кіберінцидентів та цілеспрямованих кібератак на мережі державних органів та об'єкти критичної інфраструктури України. Професійні дії фахівців Ситуаційного центру кібербезпеки СБУ забезпечили стабільність України під тиском російських хакерів, які підтримували вторгнення окупаційних військ і намагалися зірвати роботу державних служб, банківських установ, систем зв'язку тощо, маючи на меті створити паніку в суспільстві [197].

Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язку), спеціалізований центральний орган виконавчої влади, є головним суб'єктом забезпечення технічного та криптографічного захисту

інформації [165]. У структурі відомства функціонує Урядова команда реагування на комп'ютерні надзвичайні події України (CERT-UA), яка забезпечує цілодобовий моніторинг, фіксацію кіберінцидентів та координацію дій операторів критичної інфраструктури під час атак. Завдання Держспецзв'язку, їх можна звести до чотирьох стратегічних макронапрямів: 1) регуляторно-наглядової функції у сфері захисту інформації; 2) гарантування безпеки об'єктів критичної інформаційної інфраструктури (ОКІІ) та державних баз даних; 3) забезпечення безперебійного функціонування систем урядового спеціального зв'язку; 4) реалізації мілітарно-безпекової складової. Остання передбачає перехід від пасивного захисту до проактивних дій шляхом розбудови Центру активної протидії агресії у кіберпросторі, нейтралізації технічних розвідок противника та координаційної підтримки антитерористичних заходів.

Кримінологічний аналіз діяльності зазначених суб'єктів вказує на наявність системних інституційних проблем. По-перше, спостерігається фрагментація повноважень під час розслідування комплексних гібридних атак (наприклад, коли масована *DDoS*-атака супроводжується інформаційно-психологічною операцією та спробою заволодіння фінансовими ресурсами), що ускладнює визначення підслідності між Кіберполіцією та СБУ. По-друге, цивільний та правоохоронний характер діяльності наявних суб'єктів об'єктивно не дозволяє їм повною мірою реалізовувати проактивні (наступальні) кібероперації проти військових та інфраструктурних об'єктів держави-агресора.

У стратегічному вимірі така структура як Кіберсили у складі Збройних Сил України (передбачено у законопроекті №12349 «Про Кіберсили Збройних Сил України») виступатиме визначальним чинником здобуття стратегічної переваги в умовах сучасних цифрових конфліктів [172]. Формування цього органу військового управління дозволить нормативно закріпити спроможності держави до активного кіберстримування, що є критично важливим для захисту суверенітету в кіберпросторі. Крім того, таке законодавче рішення сформує

правову платформу для реалізації стратегії оборони, забезпечуючи синергію військового потенціалу з цивільними та волонтерськими ініціативами.

Виокремлення когнітивного виміру інформаційної безпеки як самостійного об'єкта захисту зумовило формування спеціалізованого органу, діяльність якого сфокусована на протидії деструктивному контенту. Це Центр протидії дезінформації (ЦПД) при РНБО України, створений відповідно до Указу Президента України (як робочий орган РНБО)[179]. ЦПД відіграє ключову роль у виявленні, аналізі та нейтралізації масованих інформаційно-психологічних операцій (ІПСО) держави-агресора. В умовах воєнного стану діяльність Центру виступає фундаментальним інструментом захисту когнітивного суверенітету нації та формування віктимологічного «цифрового імунітету» суспільства.

Об'єктивна незавершеність юридичних механізмів примусового блокування контенту наразі компенсується потужною дослідницькою спроможністю відомства. У практично-аналітичній площині ефективність інституційної діяльності ЦПД найбільш точно виявляється у впровадженні науково обґрунтованих алгоритмів реагування на складні інформаційні операції. Прикладом успішної апробації методики аналізу «чорних джерел» є кейс із нейтралізації фейкового сюжету, поширеного російськими пропагандистськими ресурсами від імені українського медіа United24. У згаданому сюжеті, що базувався на сфальсифікованих «радіоперехопленнях» про нібито масові отруєння українських військових на Курському напрямку, простежується чітка відповідність розробленому алгоритму ідентифікації загрози за ознакою «автор та актор різні» [222].

Аналіз продемонстрував, що синхронне поширення дезінформації мережею ворожих телеграм-каналів із використанням псевдо-актора (United24) свідчить про керовану операцію з прихованим авторством. Характерно, що повідомлення було побудоване не на емоційній складовій, а на багатоетапних логічних висновках, що характеризує його як раціональну дезінформацію, спрямовану на аудиторію з наявним критичним мисленням.

У даній ситуації фахівці Центру застосували комплексне рішення, що повністю корелює з рекомендаціями наукового алгоритму щодо поєднання прямого спростування з методами імунізації та випередження. Зокрема, публікація спростування безпосередньо Центром (а не лише самим медіа (United24) із закликом довіряти виключно верифікованим джерелам, сформувала у суспільства своєрідний «інформаційний імунітет». Запропонований алгоритм підтримки прийняття рішень не має обов'язкового характеру та не розглядається як чітко регламентований протокол. Як зазначає Кудрявський І. В., що відповідність алгоритму перевіреним практикам професійної діяльності фахівців у сфері протидії деструктивним інформаційно-психологічним впливам свідчить про доцільність подальших досліджень та практичного застосування [110, с. 223-224].

Окремим, віктимологічно значущим вектором інституційної моделі є захист цифрового простору неповнолітніх. В умовах стрімкої цифровізації, зумовленої, зокрема, переходом до дистанційних форм навчання під час правового режиму воєнного стану, діти та підлітки перетворилися на найбільш вразливу соціальну групу. Вони є первинною мішенню для специфічних кримінальних посягань: онлайн-грумінгу, сексторшну, кібербулінгу, а також цілеспрямованого втягнення у деструктивні радикальні спільноти та споживання ворожих маніпулятивних наративів [111, С. 221-227; 133; 142, С. 94–105; 149, С.349-352; 346].

Провідну роль відіграє Управління ювенальної превенції Національної поліції України у тісній міжвідомчій взаємодії з Департаментом кіберполіції [176]. Їхня спільна діяльність сфокусована на ранньому виявленні та превентивному блокуванні контенту, що пропагує насильство або суїцидальну поведінку, а також на розслідуванні злочинів проти статевої свободи та недоторканості дітей у мережі Інтернет.

Кобко Є., зазначає, що у структурі Національної поліції України підрозділи ювенальної превенції відіграють роль у забезпеченні прав та свобод дітей. Проте

в умовах воєнного стану ця функція трансформується, адже до фізичних загроз додається тотальна цифрова незахищеність [84, с. 49]. Руйнування звичного способу життя, масове внутрішнє переміщення та розрив соціальних зв'язків критично підвищують рівень віктимності специфічних категорій неповнолітніх (дітей-переселенців, вихованців інституційних закладів інтернатного типу, спеціалізованих будинків дитини). Позбавлені стабільного офлайн-захисту та переживаючи психологічну травму, вони масово інтегруються у віртуальне середовище, де стають найбільш легкою здобиччю для цифрових хижаків та ворожих інформаційних спецоперацій.

Сьогодні перед співробітниками служби ювенальної превенції постає важке завдання: не лише допомогти дітям адаптуватися до реалій війни, а й гарантувати їхню безпеку в кіберпросторі. Вирішення цієї проблеми вимагає безперервного вивчення новітніх практик протидії онлайн-насильству та формування ефективного механізму міжвідомчого адміністрування. Запорукою мінімізації цифрових правопорушень щодо дітей є плідна взаємодія підрозділів ювенальної превенції з кіберполіцією та широкою мережею цивільних суб'єктів: службами у справах дітей, практикуючими психологами, органами місцевого самоврядування, міжнародними та волонтерськими організаціями [84, с. 50]. Лише комплексне об'єднання цих зусиль на засадах рівноправного партнерства здатне створити надійний захисний контур, який поверне українським дітям відчуття безпеки як у фізичному, так і в цифровому вимірах.

Невід'ємною складовою розбудови такого контуру є інституційна та координаційна підтримка з боку міжнародних гуманітарних організацій (зокрема, UNICEF, Save the Children, Товариства Червоного Хреста та Ukraine Medical Relief Fund). Зважаючи на їхній унікальний досвід роботи в умовах збройних конфліктів, ці інституції виконують роль стратегічних партнерів у модернізації вітчизняних механізмів забезпечення прав неповнолітніх. Їхня участь дозволяє посилити спроможності Нацполіції шляхом проведення спеціалізованих тренінгів та навчання правоохоронців передовим практикам

захисту дітей. Крім того, міжнародні партнери відіграють роль у впровадженні стандартизованих інструментів моніторингу та об'єктивної звітності щодо стану дотримання прав дитини в реаліях воєнного стану [158, с. 127].

З огляду на зазначене, як слушно зазначає К.О. Пісоцька, специфіка адміністративної діяльності підрозділів ювенальної превенції в умовах правового режиму воєнного стану зазнає концептуальної трансформації [159, с. 8]. Її пріоритетним вектором стає формування комплексного безпекового середовища для неповнолітніх, що об'єктивно вимагає реалізації, наступних ключових завдань. Перше, забезпечення фізичної безпеки та міжвідомча координація евакуаційних процесів. Головна мета полягає у своєчасному виявленні сімей із дітьми в зонах активних бойових дій та на прифронтових територіях, сприянні їхній безпечній евакуації (включно із супроводженням процедури примусової евакуації) та запобіганні дитячій бездоглядності під час масового внутрішнього переміщення.

Важливого значення, у контексті нашого дослідження, має друге завдання, протидія цифровим загрозам та захист когнітивного простору неповнолітніх. В умовах гібридної агресії превентивна робота поліції неминуче поширюється на віртуальне середовище. Окремим завданням є формування у неповнолітніх стійких навичок інформаційної гігієни та кіберстійкості з метою захисту їхньої свідомості від деструктивного впливу ворожих інформаційно-психологічних спеціальних операцій, які мають маніпулятивне, залякування, дезінформацію, дистанційне вербування молоді в інтересах держави-агресора.

Тому, важливим напрямом діяльності Департаменту кіберполіції є системна превентивна робота, спрямована на захист цифрового простору неповнолітніх. Протягом 2025 року фахівці Департаменту розгорнули масштабну інформаційно-просвітницьку кампанію на базі закладів освіти. Ключовим фокусом цих заходів стала адаптація дітей до новітніх цифрових викликів та мінімізація їхньої віктимності. Зокрема, значну увагу було зосереджено на нейтралізації кримінальних проявів (кібербулінг, сексторшн) та новітніх загрозах

використанні дитячих онлайн-стрімів як інструменту пошуку потенційних жертв. Окремий акцент робився на специфічних ризиках правового режиму воєнного стану: спробах дистанційного вербування підлітків ворожими спецслужбами через соціальні мережі та поширенні деструктивного контенту (екстремальні «челенджі», пропаганда самокалічення) [42].

Поряд із безпосередньою комунікацією в освітньому середовищі, ДКП імплементавав інноваційні форми підвищення загальної цифрової грамотності шляхом розробки спеціалізованих матеріалів з інтернет-безпеки та проведення національної комунікаційної кампанії. Залучивши інфраструктурні потужності провідних вітчизняних телекомунікаційних операторів (ПрАТ «ВФ Україна», ПрАТ «Київстар» та ТОВ «Лайфселл»), кіберполіція здійснила масову профілактичну SMS-розсилку з верифікованим ідентифікатором «Cyberpolice», що дозволило максимально масштабувати охоплення цільової аудиторії превентивними заходами [42].

Реалізація державної політики щодо захисту дітей у цифровому просторі упродовж 2025 року набула системного характеру завдяки впровадженню цільових інформаційних кампаній. Перший етап (червень-липень 2025 р.) був зосереджений на масштабному просвітництві щодо базових алгоритмів безпеки, тоді як другий етап (листопад 2025 р.), приурочений до Дня захисту дітей, мав виражений превентивний та віктимологічний акцент [42].

Як зазначає К. Ярош, з січня по жовтень 2025 року гаряча лінія ІННОРЕ в Україні опрацювала 3224 звернення, з яких 1195 підтверджено як злочини. Тобто понад тисяча дітей стали жертвами експлуатації, а їхні зображення поширювалися в мережі [46]. Це не лише українська тенденція. За даними Internet Watch Foundation, у 2023 році понад 90 % усіх зображень сексуального характеру з дітьми у світі були «self-generated». Проблема має глобальний масштаб [62]. Ключовим завданням цих заходів стало реагування на новітні вектори онлайн-експлуатації, зокрема через стрімінгові платформи та соціальні мережі. Комунікаційна стратегія була спрямована на деконструкцію хибних

уявлень про безпеку ігрових форматів взаємодії, застерігаючи неповнолітніх від передачі персонального контенту (фото- та відеоматеріалів) третім особам. Використання спеціалізованих верифікованих ресурсів (зокрема платформи (<https://chatovi.online/articles/d1fs65> та <https://chatovi.online/articles/sf134aw>) дозволило забезпечити адресатів валідною інформацією щодо стандартів безпечної поведінки.

Концептуальна мета зазначених ініціатив охоплювала: а) мінімізацію латентності, що охоплювала стимулювання активності населення щодо повідомлень про випадки цифрового насильства та подолання психологічних бар'єрів і страхів перед зверненням до правоохоронних органів; б) інституційну превенцію, яка полягала у розвінчанні міфів про анонімність кіберзлочинів та формування у суспільстві моделі нульової толерантності до онлайн-експлуатації; в) віктимологічну підтримку щодо створення надійного контуру захисту для постраждалих дітей та забезпечення їхньої подальшої соціально-психологічної реабілітації.

У практичній площині ефективність протидії транскордонним злочинам проти статевої свободи та недоторканності дітей забезпечується інтеграцією вітчизняних правоохоронних органів у глобальну модель безпеки. Для ідентифікації зловмисників та верифікації жертв Департамент кіберполіції використовує високотехнологічний міжнародний інструментарій:

1. IsacCops. Спеціалізований програмний продукт, призначений для автоматизованого моніторингу та детекції каналів розповсюдження контенту, що містить ознаки дитячої порнографії. Система дозволяє ідентифікувати джерела дистрибуції матеріалів як у режимі реального часу, так і в архівних мережевих сегментах, незалежно від протоколів передачі даних.
2. NCMEC (National Center for Missing & Exploited Children). Глобальна база даних Національного центру у справах зниклих та експлуатованих дітей (США), що виступає центральним хабом для обміну оперативною інформацією. Через цей інструмент здійснюється координація зусиль із

міжнародними технологічними гігантами та неурядовими організаціями щодо блокування шкідливого контенту.

3. International Child Sexual Exploitation (ICSE). Міжнародна база даних Інтерполу, яка є ключовим механізмом міждержавної поліцейської взаємодії. Вона забезпечує доступ до унікальних алгоритмів візуальної ідентифікації жертв та імплементацію єдиних стандартів криміналістичного аналізу цифрових доказів у межах транскордонних розслідувань [42].

Кримінологічний аналіз діяльності зазначених суб'єктів (Кіберполіції, СБУ, Держспецзв'язку та ЦПД ювенальної превенції) вказує на наявність системних інституційних проблем. По-перше, спостерігається фрагментація повноважень під час реагування на комплексні загрози. Наприклад, коли масована DDoS-атака супроводжується масштабною інформаційно-психологічною операцією, або коли деструктивний вплив на підлітків здійснюється через зашифровані канали транснаціональних злочинних угруповань, виникають об'єктивні складнощі у координації дій між технічними, контррозвідувальними, кримінальними та ювенальними підрозділами. Брак спеціалізованих ювенальних кібер-слідчих суттєво знижує ефективність протидії латентним злочинам у Darknet-середовищі. По-друге, виключно цивільний та правоохоронний характер діяльності вказаних суб'єктів об'єктивно не дозволяє їм повною мірою реалізовувати проактивні (наступальні) кібероперації проти військових та інфраструктурних об'єктів держави-агресора. Цей вакуум в умовах мілітаризації кіберпростору актуалізує необхідність розгортання Кіберсил ЗСУ. Їх створення усуне прогалину в проведенні військових кібероперацій та завершить формування цивільно-правоохоронно-військової моделі національної кіберстійкості.

У межах такої оновленої моделі повноцінна інституціоналізація спеціалізованих підрозділів кібербезпеки в системі сектору оборони виступатиме фундаментальним елементом захисту в умовах багатодоменного гібридного конфлікту. Відповідно, ці структури зможуть правомірно реалізовувати

комплексні завдання з алгоритмічного виявлення та проактивної нейтралізації транскордонних загроз, проведення глибинної кіберрозвідки та здійснення зустрічних інформаційних операцій. Мілітарна діяльність цих структур об'єктивно залишатиметься тісно пов'язаною з положеннями Будапештської конвенції, що вимагатиме дотримання складного балансу між гарантуванням максимальної результативності бойових кібероперацій, забезпечуючи при цьому стандарти прав людини та процесуальну чистоту збору електронних доказів, які в майбутньому стануть основою для притягнення кібертерористів до відповідальності в міжнародних кримінальних трибуналах.

Як свідчить аналіз ювенального виміру, сучасні гібридні загрози (від цілеспрямованого кібергрумінгу до масованих ІІСО) характеризуються безпрецедентною масштабністю та швидкістю поширення. Це робить традиційні («ручні») методи інституційного реагування правоохоронних органів об'єктивно недостатніми.

Дієвою та асиметричною відповіддю на цей виклик виступає впровадження інноваційних алгоритмів підтримки прийняття рішень. Важливою перевагою зазначеного алгоритму, яка зумовлює його високу практичну цінність для інституційного сектору безпеки, є його масштабованість. На відміну від класичних методик, що лежать в основі доктринальних документів НАТО і зазвичай орієнтовані на чисельні ієрархічні структури (військові штаби чи масштабні аналітичні центри) [303; 304], цей підхід є прийнятним. Він може ефективно впроваджуватися не лише великими колективами, а й мобільними робочими групами або навіть окремими фахівцями «на території» (селище, місто, область). Така гнучкість робить алгоритм підтримки прийняття рішень важливим інструментом в умовах сучасної інформаційної війни та ресурсних обмежень, що є характерними для держави, яка протистоїть агресору, який має чисельну перевагу у декілька разів.

2.3. Кримінологічна превенція у сфері інформаційної безпеки від державного суверенітету до захисту прав людини

Сучасна парадигма інформаційної безпеки України потребує радикальної трансформації: від застарілої концепції виключно державного суверенітету до людиноцентричної моделі захисту прав і свобод. Проблема полягає в тому, що кримінологічна превенція, яка традиційно фокусувалася на технічному моніторингу та покаранні за кіберзлочини, сьогодні втрачає свою ефективність, оскільки не враховує транснаціональний та когнітивний характер загроз.

Інформаційна безпека в правовому контексті сприяє охороні основоположних прав людини, зокрема право на приватність та конфіденційність, які є невід'ємною частиною конституційних прав та міжнародних зобов'язань. Тому правові аспекти інформаційної безпеки становлять компонент у структурі сучасного права і державної політики, вимагаючи гармонізації внутрішніх стандартів із зовнішніми вимогами. Ключовим механізмом, що стандартизує та посилює захист персональних даних, є Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви [95/46/ЄС](#) (Загальний регламент про захист даних) (General Data Protection Regulation) (далі - GDPR), має на меті забезпечення більш високого рівня захисту особистих даних громадян ЄС та спрощення регулювання обробки та передачі цих даних [188]. Важливі аспекти Регламенту включають право осіб на доступ до власних даних, право на забуття (вимагати видалення своїх персональних даних), а також жорсткі обов'язки для організацій щодо забезпечення безпеки даних, повідомлення про порушення безпеки та виконання аудитів відповідності. Регламент виходить за межі простої технічної безпеки даних, створюючи правовий бар'єр проти маніпулювання свідомістю (ст. 21, 22 про автоматизоване прийняття рішень та профілювання) [188].

Імплементация GDPR в Україні є не лише необхідною умовою для євроінтеграції, а й стратегічним кроком, оскільки вона підвищить рівень захисту

даних, позитивно вплине на міжнародну торгівлю та довіру до українських компаній. Він сприяє підвищенню міжнародного співробітництва при розслідуванні кіберзлочинів, оскільки вимагає від компаній співпрацювати з наглядовими органами, створюючи системну основу для кримінологічної превенції кіберзлочинності на європейському рівні.

Розглянемо три рівні цієї системи (макрорівень - рівень державного суверенітету, мезорівень - рівень кримінологічної превенції та мікрорівень - рівень когнітивної безпеки), що дозволяють охопити весь спектр викликів: від безпеки держави як політичного інституту до захисту когнітивної свободи кожної особи.

Макрорівень - рівень державного суверенітету. Інформаційна безпека, на цьому рівні, реалізується як складова державного управління. В умовах гібридних загроз держава виступає «центричним вольовим центром», що забезпечує захист критичної інфраструктури та незалежність національного інформаційного простору. Міжнародна координація (зокрема через «Талліннський механізм») [208] розглядається як інструмент посилення власного кіберкордону, а не як відмова від контролю.

Мезорівень - рівень кримінологічної превенції забезпечує перехід від стратегічних рішень до практичного захисту прав людини. Кримінологічна превенція в цифровому просторі стає інструментом запобігання шкоді до її настання.

Мікрорівень - рівень когнітивної безпеки, де об'єктом охорони стає свідомість особи. Метою рівня когнітивної безпеки є формування «інтелектуального імунітету», що дозволяє людині самостійно ідентифікувати деструктивний вплив та протистояти йому.

Розгляд кожного з цих рівнів дозволяє простежити трансформацію інформаційної безпеки від формальних державних протоколів до безпосередніх гарантій прав людини та когнітивної свободи. Відтак, подальший аналіз ми

зосередимо на послідовному вивченні кожного з означених сегментів інформаційної безпеки (безпекового контуру).

Сучасна стратегія захисту персональних даних не повинна обирати між технічними обмеженнями та свободою обміну. Оптимальний шлях полягає у синтезі цих підходів, де реалістична технічна захищеність створює необхідний фундамент для ліберального та відкритого інформаційного простору, гарантуючи при цьому непорушність цифрових прав особи.

Відображення цього підходу знаходимо у дисертації А. В. Туніка «Правові основи захисту персональних даних», де автор обґрунтовує необхідність комплексної законодавчої бази за європейським зразком. На відміну від систем, що обмежуються лише законом Про захист даних, європейська модель базується на синергії двох нормативних актів: закону Про захист даних та закону Про свободу інформації, які, як правило, розробляються і ухвалюються одночасно. Це дозволяє збалансувати право на приватність із правом суспільства на доступ до інформації [215, с. 141].

Для практичної реалізації цього балансу дослідник пропонує поєднання двох комплементарних методів: реалістичного та ліберального. Реалістичний підхід фокусується на зміцненні внутрішнього кола безпеки інформаційних систем. Він передбачає мінімізацію ризиків, спричинених вразливістю програмного забезпечення або людським фактором, через моніторинг, створення захищених мереж та суворе обмеження доступу до персональних баз. В той час як, ліберальний підхід, акцентує увагу на розбудові взаємозалежності та довіри між державою і власником даних. Це реалізується через мережу спеціалізованих організацій та договірні механізми, що робить обмін інформацією більш прозорим та зручним для громадянина [215, с. 178].

Таким чином, сучасна стратегія захисту персональних даних не повинна обирати між технічними обмеженнями та свободою обміну. Оптимальний шлях полягає у синтезі цих підходів, де реалістична технічна захищеність створює

необхідний фундамент для ліберального та відкритого інформаційного простору, гарантуючи при цьому непорушність цифрових прав особи».

Водночас здатність держави забезпечити такий баланс безпосередньо залежить від обраної моделі інформаційної політики та стратегічного бачення її місця у глобальних цифрових процесах. Важливим компонентом та джерельною базою у цьому напрямі виступають безпекові дослідження сфери інформаційної політики [6; 9; 96; 97; 100; 113; 152], одним із яких є кандидатська дисертація О. М. Яхно «Україна в сучасному геополітичному просторі (політико-медійний аспект)» [233].

На думку дослідниці, рівень розвитку інформаційної складової тісно пов'язаний із безпекою держави: період становлення механізмів інформаційного суспільства є критично вразливим, оскільки країна ризикує інтегруватися у світові інфраструктури, не створивши при цьому власних надійних механізмів захисту [233, с.10]. Моделі інформаційної політики держави, сформульовані О. М. Яхно, відображають різні стратегічні підходи до управління інформаційним простором, що дозволяє оцінити ризики та перспективи переходу України від реактивного захисту до проактивного формування безпечного цифрового середовища.

Класифікація моделей інформаційної політики, О. М. Яхно, стала підґрунтям розподілу стратегічного вектору державного управління інформаційним простором залежно від рівня активності та відкритості суб'єкта:

Перша модель інформаційної експансії. Вона характеризується наступальною стратегією, де держава прагне масштабувати власний інформаційний вплив, культуру та ідентичність за межі національних кордонів. Основним інструментарієм тут виступає активна пропаганда та безпосереднє втручання в інформаційні процеси інших суб'єктів.

Друга модель паритетної відкритості (взаємний доступ) базується на принципах інтеграції та кооперації. Держава свідомо відкриває інформаційний

сегмент для зовнішніх партнерів у обмін на рівноправний доступ до глобальних інформаційних потоків та безпосередню участь у їх формуванні.

Третя модель пасивної відкритості передбачає забезпечення вільного доступу до національного інформаційного простору для внутрішніх та іноземних суб'єктів без спроб держави впливати на світову інформаційну систему чи брати участь у формуванні глобального порядку денного.

Четверта модель ігнорування інформаційного суверенітету, відрізняється відсутністю чіткої державної стратегії та байдужістю до захисту національних інтересів у цифровій сфері, що фактично нівелює суб'єктність країни.

З огляду на євроінтеграційний вектор розвитку та необхідність зміцнення правової стійкості, найбільш перспективною для України, на думку О. М. Яхно, є II модель, що дозволяє гармонійно поєднати відкритість демократичного суспільства із активним захистом національного кіберпростору через механізми міжнародної координації та взаємного обміну ресурсами [233, с.9].

Водночас, попри теоретичну привабливість моделі паритетної відкритості, реалії повномасштабної міждержавної агресії та системних гібридних загроз вимагають переосмислення цієї стратегії. В умовах воєнного стану, масованих кібератак на критичну інфраструктуру та агресивних ІІСО, класична модель «відкритості в обмін на доступ» (друга модель) може виявитися недостатньою для забезпечення національної безпеки.

Більш доцільною, на нашу думку, в сучасних умовах локальних і глобальних загроз, у тому числі обумовлених воєнним станом, вбачається модель, що базується на пріоритеті інформаційного суверенітету та активному кіберзахисті з ефективними механізмами стратегічного стримування. Це можна обґрунтувати наступними чинниками: а) необхідність автономного захисту, коли у критичні моменти агресії держава повинна мати внутрішні механізми ізоляції та захисту національного сегменту мережі, які не залежать виключно від зовнішніх домовленостей; б) ризики надмірної відкритості, які в умовах гібридної війни «відкриття інформаційного простору» створює додаткові

вразливості для проникнення ворожої пропаганди та технічного шпигунства під виглядом легітимних інформаційних потоків; в) суверенітет над даними щодо забезпечення правової стійкості вимагає жорсткого контролю над стратегічно важливими базами даних та національними інформаційними ресурсами, що часто суперечить ідеї повної відкритості.

Відтак, хоча євроінтеграційний вектор залишається незмінним, механізм взаємодії з партнерами («Талліннський механізм») [208] має розглядатися не як «відкриття простору», а як надійний інструмент зміцнення національного кіберкордону. Таким чином, сучасна парадигма повинна еволюціонувати від «балансу відкритості» до «центричної моделі безпеки», де міжнародна координація є засобом посилення власної суверенної стійкості, а не самоціллю, що вимагає поступок у питанні контролю над інформаційним простором.

Такий підхід знаходить логічне підтвердження в принципах Регламенту Європейського Парламенту і Ради (ЄС) 2016/679 (GDPR), який виступає не лише правовим фундаментом захисту даних, а й інструментом забезпечення інформаційного суверенітету. Згідно з положеннями Регламенту, зокрема принципом «захисту за замовчуванням», держава має не просто «відкривати» дані для міжнародного обміну, а гарантувати їх цілісність та захищеність від маніпулятивного впливу на рівні цілісної систем [188]. Відповідно до ст. 44–46 GDPR, передача персональних даних третім сторонам або міжнародним організаціям можлива лише за умови забезпечення належного рівня захисту [188]. Це означає, що міжнародна співпраця, зокрема в межах «Талліннського механізму», повинна відбуватися через жорстко регламентовані канали, де національна держава зберігає роль арбітра та контролера безпекових процесів.

Отже, «центрична модель безпеки» базується на імперативі повної відповідальності держави за безпеку свого цифрового простору: міжнародне партнерство допомагає нам запроваджувати кращі технічні та правові практики, але не звільняє нас від обов'язку формувати «когнітивний щит» та забезпечувати невторчання у свідомість громадян з боку деструктивних зовнішніх суб'єктів.

Гібридна агресія демонструє, що деструктивний вплив на свідомість та інфраструктуру здійснюється не лише через ідеологічну пропаганду, а й через інструментарій високотехнологічних кібератак, які мають чітко виражений державний мотив.

Підтвердженням цієї тенденції є діяльність спеціалізованих угруповань, які інтегрують злочинні методи у стратегію масштабного військового вторгнення. Зокрема, у гібридних операціях державні групи, такі як Sandworm (APT44), застосовують техніки кіберзлочинців - DDoS, фішинг - для досягнення стратегічних цілей. Так, атака на Viasat 24 лютого 2022 року, виконана за годину до повномасштабного вторгнення, вивела з ладу 30 000 модемів в Україні та Європі, використовуючи wiper-malware AcidRain. Технічно це виглядало як деструктивна атака, характерна для кіберзлочинності, проте її безпосередня синхронізація з початком військових дій вказувала на державне замовлення та реалізацію геополітичного мотиву через цифрові інструменти [4, с. 28].

Додатковою складністю у протидії кіберзлочинності є транснаціональний характер цих правопорушень, що дозволяє вчиняти їх з будь-якої точки світу, уникаючи юрисдикції національних правоохоронних органів. Адже тільки через чітко структуровану суверенну стійкість держава здатна стати дієвим суб'єктом міжнародної правової допомоги, забезпечуючи невідворотність покарання за злочини, що вчиняються в глобальному цифровому просторі. У зв'язку з цим актуальності набуває розвиток системи кібербезпеки, а також удосконалення законодавства, яке надасть правоохоронним органам необхідні інструменти для ефективного виявлення, розслідування і запобігання таким злочинам. Однак ця взаємодія не повинна бути хаотичною. Правовим фундаментом для транскордонної співпраці у сфері безпеки стає Регламент (ЄС) 2016/679 (GDPR). Зокрема, ст. 44–46 Регламенту встановлюють чіткі принципи передачі персональних даних третім країнам або міжнародним організаціям, вимагаючи гарантій належного рівня захисту [188]. Для української правоохоронної системи це означає, що ефективна міжнародна правова допомога можлива лише коли

держава виступає як надійний суб'єкт, здатний забезпечити цілісність даних (згідно з принципом ст. 5(1)(f) GDPR) рівня захисту [188].

На мезорівні кримінологічна превенція виконує роль ключового транслятора, забезпечуючи перехід від стратегічних державних рішень до безпосереднього практичного захисту прав людини. Саме тут відбувається адаптація міжнародних стандартів, зокрема Регламенту (ЄС) 2016/679 (GDPR), до реальних правоохоронних практик. Рівень кримінологічної превенції фокусується на діяльності територіальних громад та правоохоронних структур, створюючи інституційне середовище, де право на приватність і цифрову безпеку стає реальністю, а не декларативною нормою. Ця ланка є важливою, оскільки саме на мезорівні здійснюється правоохоронний нагляд за дотриманням прав суб'єктів даних (зокрема, ст. 32 GDPR безпека опрацювання даних) [188]. Проте, попри наявність чітких законодавчих алгоритмів, ефективність цього рівня обмежена людським фактором.

Підтвердженням тези про недостатність суто технічних заходів безпеки та необхідність посилення превентивної роботи на мезорівні є результати емпіричного дослідження Юхно О. О. та Загуменним О. О., проведеного серед активної аудиторії соціальної мережі «Facebook» [230, с. 58-59]. Отримані науковцями дані демонструють тривожну невідповідність між високим рівнем цифрової активності та низьким рівнем «інтелектуального імунітету» користувачів. Це стосується ілюзії приватності, коли попри наявність технічних інструментів захисту, 80 % респондентів свідомо ігнорують налаштування приватності, а 74 % розкривають автентичну особисту інформацію. Це створює ідеальні умови для соціальної інженерії та сталкінгу, оскільки користувачі добровільно нівелюють власні «кіберкордони». Також, це стосується психологічної готовності до девіацій. Критичним показником для кримінологічної превенції є ставлення до протиправної комунікації. Лише 30 % опитаних категорично відкидають можливість обговорення чи вчинення

неправомірних дій у приватному листуванні. Натомість 70 % користувачів демонструють різний рівень латентної готовності до такої взаємодії [230, с. 59].

Аналіз цих показників дозволяє зробити висновок про те, що превентивні заходи, які базуються виключно на інформуванні про небезпеку, є малоефективними. Проблема полягає не у відсутності знань про налаштування безпеки, а у психологічній установці користувача, який довіряє цифровому середовищу більше, ніж власній безпеці.

У сучасному цифровому світі загрози для людини виходять далеко за межі традиційного викрадення даних чи фінансового шахрайства. Дедалі більшої актуальності набуває поняття когнітивної безпеки, а саме, здатності людини критично сприймати та опрацьовувати інформацію, захищаючи власну свідомість від маніпуляцій, дезінформації та цілеспрямованого психологічного впливу. Це безпосередньо стосується превенції злочинності проти людини, оскільки маніпуляції свідомістю часто є першим кроком до вчинення шахрайства, вимагання, або навіть вербування у злочинні угруповання.

Кобетяк А. Слушно зазначає, що у сучасних геополітичних умовах когнітивне протиборство стало ключовим елементом глобальної конкуренції. Держави-ініціатори використовують технології гібридної когнітивної експансії для цілеспрямованої трансформації світогляду населення. Цей процес є багатошаровим: він реалізується через соціальні мережі, медіа, рекламу, через маніпуляції в освітніх програмах і наукових теоріях [83, с. 26-32].

Критична вразливість суспільства до таких впливів стала очевидною під час глобальних криз, коли масовий перехід життєдіяльності в кіберпростір усунув бар'єри для зовнішнього втручання. Інформаційні платформи, ставши домінуючим джерелом знань, перетворилися на інструменти ментального впливу. Усвідомлення цієї загрози робить освіту та критичне мислення не просто соціальними інститутами, а стратегічними ресурсами держави. Якщо когнітивна безпека покликана захищати «інтелектуальний імунітет» особи, то протидія експансії вимагає від держави не лише пасивного захисту, а й активного

формування стійкого світогляду громадян, здатного протистояти спробам зовнішнього маніпулювання переконаннями та цінностями

В умовах гібридної війни та поширення інформації, безпека людини охоплює не лише її фізичну цілісність чи фінансове благополуччя, а й ментальну стійкість та здатність до об'єктивного мислення. Злочинність проти людини в цифровому просторі тепер включає також психологічний тиск, кібербулінг, створення фейкових новин для дезорієнтації та інші форми впливу на її когнітивні процеси. При цьому, стійке цифрове суспільство не може бути таким без когнітивно стійких громадян. Тому формування критичного мислення та медіаграмотності є невід'ємною частиною цифрової стійкості [147, с. 177-182].

У сучасних умовах воєнної агресії наукова думка Д. Тінін та О. Мисливої акцентує увагу на трансформації інформації у стратегічний ресурс, контроль над яким безпосередньо детермінує хід військових операцій та стійкість національної оборони. Безпекова функція у цій сфері виходить за межі технічного захисту, інтегруючи комунікаційний компонент, спрямований на збереження морального духу суспільства через соціальні мережі [211, с. 138].

Реалізація цієї стратегії в Україні знайшла відображення у нормативному закріпленні особливих правил функціонування медіапростору. Відповідно до Закону України «Про медіа», запроваджено механізм обмеження доступу до аудіовізуальних сервісів та платформ, що мають безпосередній зв'язок із країною-агресором [174]. Ключовим інструментом тут постає формування Національною радою з питань телебачення і радіомовлення переліку заборонених ресурсів (платформ Okko, Premier та ін.), діяльність яких базується на законодавстві РФ або спрямована на поширення окупаційного контенту.

Процедура блокування таких інтернет-ресурсів та мобільних застосунків, що здійснюється за рішенням Національної комісії, що відповідає за регулювання у сферах електронних комунікацій, є необхідним кроком для мінімізації ризиків маніпулятивного впливу. Водночас інституційні зусилля держави мають доповнюватися підвищенням рівня медіаграмотності громадян,

оскільки кінцева ефективність правових заборон безпосередньо залежить від здатності суспільства до критичного сприйняття інформації та протидії психологічному тиску в цифровому середовищі [195, с. 43-46].

Когнітивна безпека реалізується через просвітницькі кампанії з медіаграмотності, розвитку критичного мислення, навчання розпізнаванню маніпулятивних технік та фейків [162]. Це включає не лише захист даних, а й захист свідомості користувача від шкідливого інформаційного контенту. Технічні засоби можуть допомагати у виявленні ботів та тролів, але кінцеве рішення про довіру інформації приймає людина.

Пропаганда та маніпулювання інформацією застосовуються з метою впливу на когнітивні процеси людини шляхом формування спеціально сконструйованих інформаційних повідомлень, здатних активізувати певні шаблони та упередження. Щоб протистояти подібному впливу, необхідно розвивати критичне мислення, перевіряти інформацію через різноманітні джерела та здійснювати її самостійний аналіз. Когнітивна безпека є прикладом синергії між інформаційною безпекою та кримінально-правовою політикою. Водночас, освіта та підвищення свідомості громадян є спільним завданням обох сфер, що безпосередньо впливає на здатність людини захистити себе від цифрових загроз на когнітивному рівні.

В умовах воєнного стану інформаційний простір часто використовується як інструмент впливу на громадську свідомість, дестабілізацію суспільства та втручання у політику держави. Забезпечення інформаційної безпеки передбачає створення ефективної системи протидії таким загрозам, розвиток кіберзахисту, моніторинг і нейтралізацію дезінформації, зміцнення інформаційної інфраструктури держави, а також удосконалення механізмів інформаційної протидії та контрпропаганди [19; 191, с. 189].

Сучасна парадигма забезпечення інформаційної безпеки України базується на синергії освітнього потенціалу, професійної відповідальності медіа та міжнародної стратегічної інтеграції. Вирішального значення набуває

формування кадрового резерву, здатного реалізовувати стратегічні комунікації та протидіяти зовнішнім впливам через систематичне проведення тренінгів і кіберсимуляцій на рівні державних органів. Розвиток загальної кіберграмотності населення при цьому розглядається як фундамент суспільної стійкості до деструктивних інформаційних операцій [113].

Якісна трансформація ролі медіа в умовах воєнного стану перетворює журналістику на активного суб'єкта інформаційного протистояння, де професійна відповідальність та точність подання даних детермінують стабільність державного управління та психологічний стан соціуму. Водночас інституційна спроможність України посилюється через поглиблення міжнародного співробітництва, що передбачає спільні кібероперації та обмін технологіями в межах інтеграції з безпековими структурами НАТО і ЄС.

У сучасних умовах, особливо зважаючи на агресивну гібридну війну, людська свідомість перетворилася на основне поле бою. Метою ведення так званої когнітивної війни є не просто зміна поглядів людини, а й фундаментальна трансформація її способу мислення та подальших дій. Це підкреслює критичну важливість концепції когнітивної безпеки COGSEC, яка, становить захист від масштабних маніпуляцій і інформаційної зброї, була вперше сформульована американським експертом Р. Валтцманом у 2017 році. Він обґрунтував її необхідність у контексті протидії інформаційній війні із використанням соціальних мереж. Він підкреслив, що інформаційні операції сучасності націлені на комп'ютерні мережі та безпосередньо на пізнавальні процеси людини та процеси прийняття рішень суспільством [315].

COGSEC виходить за рамки традиційної інформаційної безпеки, акцентуючи увагу на усвідомленні того, як інформація може бути цілеспрямовано використана для маніпуляції думками, переконаннями та поведінкою людей у сучасному перенасиченому інформаційному середовищі. На відміну від традиційної кібербезпеки, яка захищає інфраструктуру, когнітивна безпека захищає людський розум від цілеспрямованих кампаній впливу (ІПСО).

Когнітивна війна це, форма конфлікту, де психологічний та інформаційний вплив застосовується для досягнення стратегічних цілей. Основною метою COGSEC є збереження когнітивної системи забезпечення об'єктивності, незалежності при прийнятті рішень [186].

Мета інформаційної агресії – людська когніція. Як пряма відповідь на цей стратегічний виклик та заклик до дій, була заснована неполітична позапартійна організація Cognitive Security & Education Forum (COGSEC), яка сьогодні слугує ключовою платформою для академічного дослідження та розробки освітніх і превентивних методологій у цій критичній галузі [254].

Адаптація завдань COGSEC до умов локальних та глобальних загроз у сучасній Україні набуває важливого значення, оскільки вимагає фокусування на протидії прямій гібридній агресії. Це включає створення спеціалізованих навчальних програм для формування критичного мислення серед населення, забезпечення оперативного дебанкування російської дезінформації та інтеграцію COGSEC-підходів у діяльність правоохоронних органів для кваліфікації злочинів, вчинених шляхом маніпуляції свідомістю (шахрайство, вербування, провокації).

Берзиньш Янис наголошував, що «російський погляд на сучасну війну ґрунтується на ідеї, що основним полем бою є погляди, і, як наслідок, у війнах нового покоління має домінувати інформаційно-психологічна війна з метою змусити військове та цивільне населення супротивника підтримати нападника на шкоду власному уряду та країні» [285, с. 5-13].

Людський елемент не лише робить кіберпростір вразливим, а й ускладнює кримінологічну превенцію. Сучасні дослідження свідчать, що традиційне моделювання лише мережевих вразливостей є недостатнім. Необхідно зосередитися на найбільш мінливому аспекті - поведінці особи, яка здійснює атаку, його навичках, правилах та процесі прийняття рішень [270; 284; 299; 313; 316; 344; 345].

Когнітивна безпека особи як фінальний контур запропонованої багаторівневої системи захисту інформаційної безпеки знаходить своє найбільш гостре відображення у питаннях безпеки неповнолітніх. У сучасних умовах забезпечення цифрової безпеки дитини перестає бути суто технічним завданням (фільтрація контенту чи встановлення обмежень), трансформуючись у фундаментальний пріоритет кримінологічних студій.

На актуальності цієї проблеми наголошують вчені, звертаючи увагу на стрімкій віртуалізації соціальних зв'язків, де дитина постає як найбільш вразливий суб'єкт віктимізації [6; 111; 228, с. 506-228]. Попри активне впровадження освітніх програм, спрямованих на формування медіаграмотності, емпіричні дослідження все частіше фіксують їх обмежену результативність. Це пояснюється психологічними особливостями підліткового віку, схильністю до ризикованої поведінки та високим рівнем довіри до цифрового середовища, що часто нівелює теоретичні знання про безпеку.

Відтак, слушно зазначає професор А.М. Бабенко, проблема захисту неповнолітніх демонструє обмеженість «зовнішніх» технічних бар'єрів. Якщо свідомість користувача (особливо молодого) не сформована як стійкий до маніпуляцій «когнітивний щит», будь-які технічні обмеження будуть обійдені зловмисниками. Таким чином, зазначає вчений, цей рівень безпеки вимагає переходу від моделі «заборони» до моделі «формування інтелектуального імунітету» [6, с. 416].

Такий стан речей є індикатором неефективності превенції, орієнтованої лише на «захист від загроз». Наш підхід, що базується на формуванні інтелектуального імунітету, вимагає суттєвого розширення кримінологічної превенції: а) від пасивного захисту до корекції, де превентивна стратегія держави має передбачати не лише блокування деструктивного контенту, а й педагогічно-психологічну корекцію поведінки неповнолітніх, що вже потрапили у коло агресії; б) розрив циклу насильства, коли відбувається визнання того, що «жертва

сьогодні це агресор завтра», перетворює когнітивну безпеку на інструмент розриву циклу віртуальної злочинності.

Слушно зазначає канадський соціолог Малкольм Гладуелл, що людина порушує закон не тільки через генетичну схильність чи виховання; визначальний вплив на поведінку має оточення та те, що індивід спостерігає навколо себе [293]. Ця теза знаходить своє підтвердження у відомій теорії «розбитих вікон» Дж. Вілсона та Дж. Келлінга. Згідно з нею, негласне схвалення дрібного безладу (незамінене скло у вікні) провокує ланцюгову реакцію ігнорування соціальних норм, що врешті призводить до мародерства та тяжких злочинів [334]. У цифровому середовищі роль таких «розбитих вікон» відіграють неконтрольований кібербулінг, агресивна пропаганда, мова ненависті та безкарність за цифрові девіації. Якщо віртуальний простір насичений ознаками когнітивного безладу, це деформує свідомість користувача, поступово знімаючи моральні та правові заборони.

Різноманітність загроз, виділена О. М. Лисенком, підкреслює, наскільки високою є ціна «когнітивної вразливості» неповнолітніх. Автор слушно акцентує увагу на широкому спектрі ризиків: від кібербулінгу, пропаганди насильства та порнографічного контенту до таких латентних явищ, як грумінг, кібершахрайство та формування адиктивної поведінки [116].

У контексті нашої багаторівневої системи інформаційної безпеки, ці загрози свідчать про критичну неспроможність реагування лише на рівні заборони доступу. Оскільки згадані явища (наприклад, грумінг чи формування залежності) базуються на маніпулюванні психологічними станами дитини, вони не можуть бути нейтралізовані лише технічними фільтрами чи блокуваннями.

Це актуалізує потребу в перегляді кримінологічної превенції. По-перше, трансформації об'єкта превенції. Трансформація полягає у переході від боротьби з «контентом» до захисту «психологічного простору» дитини. Якщо кібербулінг чи грумінг діють через соціальну інженерію, то єдиним ефективним превентивним бар'єром стає здатність неповнолітнього ідентифікувати

маніпулятивні елементи поведінки зловмисника. По-друге, відповідальність держави. Державна стратегія інформаційної безпеки повинна інтегрувати ці ризики у систему кримінологічного моніторингу, де превенція виступає не лише покаранням за вчинене кримінальне правопорушення, а й своєчасною корекцією когнітивних навичок дитини, що здатна запобігти її залученню до деструктивних сценаріїв. Таким чином, класифікація О. М. Лисенка стає картою загроз, на основі якої кримінологічна превенція має будувати проактивну стратегію: не чекати настання віктимізації, а розвивати у неповнолітніх внутрішні механізми захисту від адикцій та маніпуляцій.

Слушною є думка професора Н.С. Юзікової щодо актуальних напрямків забезпечення безпеки неповнолітніх в інформаційно-телекомунікаційній мережі Інтернет. Серед яких, захист від інформації і дій, що спонукають до небезпечної для життя дитини поведінки («трейнсерфінг», руфрайдинг (проїзд на даху поїзда) або «зацепинг», «руфінг» (незаконне проникнення на дах висотних будівель), екстрим фото тощо), суїциду, протиправної активності. Це має відноситися до ключових завдань національної безпеки і майбутнього суспільства [229, с. 157].

Ефективність превентивних заходів у сфері інформаційної безпеки, значною мірою, залежить від її спроможності захистити найбільш вразливу категорію суспільства - неповнолітніх. Аналіз сучасних загроз (кібербулінг, грумінг, адиктивна поведінка) в сучасних умовах тривалої воєнної агресії засвідчує неспроможність традиційних технічних фільтрів та класичних віктимологічних підходів. Феномен конвергенції ролей «жертва-агресор» доводить, що без формування «інтелектуального імунітету» превенція залишається лише боротьбою з наслідками, ігноруючи глибинні психологічні детермінанти злочинності, що призводять до агресії. Тому, для оптимізації цього процесу необхідна розробка спеціалізованих інтерактивних платформ превентивного спрямування. Впровадження подібних інклюзивних механізмів дозволить не лише оперативно реагувати на локальні безпекові виклики, а й системно формувати когнітивну стійкість молоді, зміщуючи акцент від

реактивного покарання до проактивного запобігання деструктивним поведінковим сценаріям.

Підсумовуючи слід зазначити, що кримінологічна превенція в умовах цифрової трансформації має еволюціонувати від фрагментарних технічних рішень до багаторівневої людиноцентричної системи інформаційної безпеки. Ця система поєднує стратегічний державний суверенітет (макрорівень), інституційну правоохоронну превенцію (мезорівень) та когнітивну безпеку особи (мікрорівень) у цілісний безпековий контур.

Висновки до другого розділу

1. Доведено, що правовий режим воєнного стану фундаментально трансформував парадигму інформаційної безпеки України від пасивного технічного захисту до проактивної стратегії національної кіберстійкості. Сучасна кримінологічна характеристика кіберзлочинності в умовах війни охоплює новітні чинники криміногенного ризику, зумовлені експансією штучного інтелекту. У зв'язку з цим обґрунтовано необхідність стратегічного переходу сектору безпеки до випереджального реагування та доцільність криміналізації нових цифрових загроз, зокрема створення і поширення згенерованого за допомогою ШІ синтетичного контенту експлуатації дітей (дипфейків).

Ефективна протидія гібридній агресії та масштабним інформаційно-психологічним операціям (ІПСО) вимагає одночасної імплементації чотирьох взаємопов'язаних напрямів: міжнародно-правового, який полягає у легалізації цифрових доказів кібератак для доведення умислу та притягнення агресора до відповідальності у міжнародних трибуналах; інституційно-оборонного щодо консолідації потенціалу через розбудову та нормативне закріплення функцій Кіберсил ЗСУ; інфраструктурного через перехід критичних реєстрів та об'єктів інфраструктури до моделі «нульової довіри»; антропоцентричного (правозахисного) шляхом збереження демократичного балансу між розширеними повноваженнями спецслужб і конституційними правами особи за стандартами ЄСПЛ.

Системна реалізація цих напрямів, спільно з інформаційною реінтеграцією деокупованих територій, дозволяє сформувати багаторівневу модель когнітивного суверенітету та утвердити українську громадянську ідентичність як інструмент загальнонаціональної єдності.

2. Розкрито сучасні законодавчі та інституційні засади забезпечення інформаційної безпеки в Україні, які розвиваються в умовах гострої державно-правової діалектики яка виражається у постійному пошуку компромісу між інформаційно-правовим підходом (дотримання прав людини) та спеціально-

режимним підходом (вимушена мілітаризація ІТ-сектору). Встановлено, що діюча інституційна модель має розгалужений багаторівневий характер і охоплює органи технічного й контррозвідального захисту (СБУ, Держспецзв'язку, Департамент кіберполіції), структури когнітивної безпеки (ЦПД при РНБО) та суб'єктів віктимологічного захисту неповнолітніх (ювенальна превенція).

Водночас виявлено системні вади цієї моделі: фрагментацію (дублювання) повноважень між відомствами та переважно цивільно-правоохоронний характер їхньої діяльності, що обмежує спроможність держави здійснювати наступальні кібероперації. Ліквідація наявних правових прогалин має базуватися на впровадженні випереджальних превентивних механізмів, що враховують поведінкові ризики. З метою нейтралізації системних загроз обґрунтовано дворівневий розподіл категорії «кіберстійкість»:

- «кіберстійкість держави» (публічно-правовий рівень): стратегічна спроможність підтримувати критичні функції, адаптуватися до гібридних загроз та відновлювати цифрову інфраструктуру на основі жорсткої координації сектору безпеки (МВС, Нацполіція, ЦПД).
- «кіберстійкість особи» (людиноцентричний рівень): сукупність когнітивних навичок, правової обізнаності та кібергігієни індивіда.

Подолання інституційних викликів вимагає впровадження масштабованих, дата-центричних інструментів управління та безперервного когнітивного розвитку кадрового потенціалу.

3. Визначено специфіку та багаторівневу структуру кримінологічної превенції крізь призму забезпечення справедливої рівноваги між захистом державного суверенітету (макрорівень), правоохоронною діяльністю (мезорівень) та когнітивною безпекою особи (мікрорівень). Доведено, що формування балансу між свободою та безпекою є ключовим викликом інформаційної політики: надмірний контроль загрожує порушенням прав людини, тоді як його відсутність створює умови для безкарної кіберзлочинності. Оптимальне рішення полягає у поєднанні глобальних принципів із національною

правовою традицією, де права людини стають не об'єктом обмежень, а головним орієнтиром державної суб'єктності.

У цьому контексті обґрунтовано концепцію «когнітивного імунітету» нації як невід'ємного виміру інформаційної безпеки, що передбачає перехід від захисту технічного периметра до формування стійкості людського капіталу. Запропоновано визначення «когнітивного імунітету суспільства» як самостійної кримінологічної та віктимологічної категорії, що визначає здатність громадян виступати внутрішнім самозахисним бар'єром проти транснаціональних ПСО та цифрового шахрайства.

Ключовим маркером ефективності такої системи превенції визначено її здатність захистити найбільш вразливу категорію - дитину. Аналіз цифрових загроз (кібербулінг, грумінг, інтернет-адикції неповнолітніх) в умовах війни доводить, що класичні технічні фільтри та заборони є недостатніми. Феномен конвергенції ролей «жертва-агресор» свідчить, що без формування інтелектуального імунітету у дитини держава лише боротиметься з наслідками, не усуваючи психологічних детермінант протиправної поведінки.

Таким чином, кримінологічна превенція трансформується з інструменту державного примусу на інституційний міст, який захищає свободу особи від маніпуляцій. Подальше вдосконалення державної політики має базуватися на людиноцентричній моделі, де інформаційна стійкість держави є похідною від інтелектуального імунітету кожного її громадянина, перетворюючи технічну безпеку на дієву безпеку людської особистості.

РОЗДІЛ 3. ЗАРУБІЖНИЙ ДОСВІД ТА ВДОСКОНАЛЕННЯ НАЦІОНАЛЬНОЇ СИСТЕМИ КРИМІНОЛОГІЧНОГО РЕАГУВАННЯ

3.1 Порівняльно-правовий аналіз передового зарубіжного досвіду забезпечення інформаційної безпеки та формування кіберстійкості

Порівняльно-правовий аналіз відіграє фундаментальну роль у формуванні сучасної системи інформаційної безпеки, оскільки транскордонна природа кіберзагроз вимагає гармонізації національного законодавства та механізму правозастосування з ефективними зарубіжними практиками. Дослідження зарубіжного досвіду дозволяє імплементувати найбільш дієві превентивні механізми та інституції запобігання кіберзлочинності.

У цьому контексті вивчення та запровадження передового зарубіжного досвіду виступає не просто науковим завданням, а умовою забезпечення стабільно високого рівня загальної інформаційної безпеки держави. Водночас найвищим критерієм ефективності правової позиції є дотримання балансу, що будь-які запозичені безпекові заходи повинні бути суворо підпорядковані меті захисту важливих інтересів, прав і свобод людини і громадянина у сфері цифрових технологій. Безпека глобального кіберпростору прямо пропорційна рівню захищеності кожної держави, що у підсумку визначає здатність держав до нормального соціально-економічного розвитку, функціонування державних інститутів та досягнення Цілей сталого розвитку 2030 (зокрема в частині розбудови стійкої інфраструктури, стимулювання інновацій та забезпечення миру, справедливості і сильних інституцій) [156].

Комплексне дослідження зарубіжного законодавства у сфері кібербезпеки, оцінка його сильних та слабких сторін, дозволяє глибоко проаналізувати вітчизняне законодавство з тим, щоб зрозуміти цінності та пріоритети, тенденції та перспективи його розвитку. Невипадково видатний вчений О. Ф. Кістяківський закликав до вивчення вітчизняного права у порівнянні з іноземним з метою вдосконалення першого [220, с. 33].

З огляду на мету дослідження, доцільним є проведення порівняльно-правової характеристики нормативно-правового регулювання та діяльності державних і приватних інституцій із забезпечення інформаційної безпеки, протидії транснаціональній кіберзлочинності та механізму правозастосування у зарубіжних країнах. У доктрині порівняльного правознавства традиційно виокремлюють два типи критеріїв порівняльно-правового аналізу: перший - через загальні параметри порівняння правових систем; другий - через порівняння законодавств різних країн [209]. У межах нашого дослідження ми виходимо з другого типу критеріїв, який передбачає визначення відповідності критеріям першого типу; аналіз системи законодавства та окремих його інститутів; дослідження галузей і правових інститутів, що стосуються визначеної безпекової проблематики; розгляд механізму правозастосування відповідних норм у цифровому середовищі.

Поділяючи наукову позицію О. В. Таволжанського, варто наголосити, що для оптимізації національних стратегічних підходів до забезпечення інформаційної безпеки необхідно імплементувати передовий досвід зарубіжних країн. При цьому фундаментальною основою мають стати не лише ефективні практики урядових структур, але й досягнення недержавного сектору та міжнародних організацій у сфері нейтралізації кіберзагроз [207, с. 155].

Варто зауважити, що окремі аспекти використання зарубіжного досвіду у запобіганні злочинності у сфері інформаційних технологій вже ставали об'єктом кримінологічних розвідок таких вітчизняних учених, як А. Бабенко, О. Бодунова П. Біленчук, Л. Варунц, М. Карчевський, Т. Лисько, Н. Лугіна, А. Лучук, М. Малій, В. Марков, В. Меланіч, Ю.Славіта, О. Таволжанський, Р. Черниш, Н. Юзікова, Ю. Якубівська та ін. Спираючись на цей потужний науковий фундамент, наголосимо, що компаративний аналіз формування інститутів інформаційної безпеки та кіберстійкості, як і будь-яке інше порівняльне дослідження, вимагає максимально систематичного підходу та застосування чіткої методології. Адже

будь-які висновки та рекомендації сформовані без урахування системності, позбавляються своєї практичної цінності. [23; 45; 117; 124; 223; 225; 228; 279].

Кримінологічний аналіз зарубіжного законодавства та практики формування безпечного інформаційного простору і протидії загрозам високотехнологічного характеру дозволяє представити національну правову систему у співставленні з правовими системами інших країн. З огляду на геополітичні виклики та різний рівень технологічного розвитку, у сьогоденному світі можна виокремити три макромоделі нормативно-правового регулювання кіберпростору та формування кіберстійкості.

Перша – романо-германська (континентальна) модель (на прикладі правової системи країн ЄС) характеризується прагненням до глибокої нормативної уніфікації, жорстким інституційним контролем та превентивним регулюванням. Вибір європейського досвіду (зокрема стандартів ENISA та директив ЄС) [239; 263; 264; 265] як базису для гармонізації вітчизняного законодавства зумовлений генетичною спорідненістю правових систем. Україна, як і більшість держав ЄС, належить до континентальної (романо-германської) правової сім'ї, що визначає специфіку механізмів регулювання інформаційної безпеки. Її фундаментом є пріоритет захисту фундаментальних прав людини у цифровому середовищі та створення стандартизованого європейського ринку кібербезпеки (відповідно до директиви (EU) 2022/2555 та Регламенту (ЄС) 2024/2847) [263; 264; 318]. Флагманами цієї моделі виступають Німеччина та Франція, а також Естонія, чий передовий досвід є інституційним орієнтиром для інших країн, Польщі, Литви, Латвії, Хорватії, України та ін.).

Друга - англосаксонська модель яка демонструє принципово іншу, прагматичну правову систему. Спираючись на гнучкість загального права, у системі превалює ризик-орієнтований підхід, децентралізації, дерегуляції технологічного сектору та розбудови потужного державно-приватного партнерства. Замість тотальної кодифікації, країни англосаксонської традиції роблять акцент на оперативному реагуванні, розбудові потенціалу («*saracity*

building») [258; 301] та активному захисті національних інтересів через стратегії кіберстримування. Потенціал «capacity building» це стратегічний перехід від технологічного та поліцейського захисту інформаційного простору до системного формування масового «кіберіунітету» суспільства через безперервну освіту, міжсекторальну взаємодію та інституалізацію цифрової гігієни [258; 300; 303; 309, с. 83-92]. Говорячи простими словами це коли держава не просто будує високі стіни навколо своїх даних, а вчить пересічних громадян бути розумними і відповідальними та не відчиняти двері ворогу зсередини. Представниками цієї моделі є Австралія, Великобританія, Канада, США, та технологічний союзник - Японія), де буде досліджено ефективні інструменти правового регулювання та державно-приватного партнерства.

Третя модель (держав в умовах геополітичної турбулентності та перманентного конфлікту) об'єднує правові системи, інформаційна безпека яких формується під постійним тиском гібридних та військових загроз. Інституційним прикладом у цій системі виступає Ізраїль, який демонструє успішну побудову «мілітаризованої кіберфортеці» із жорсткою централізацією управління, доктриною проактивного кіберстримування та глибокою інтеграцією армії з приватним ІТ-сектором.

Не менший науковий інтерес становить досвід транзитних юрисдикцій (Грузії, Молдови, Азербайджану), які демонструють складний процес розбудови кіберстійкості в умовах активної протидії агресору [231]. Ці країни змушені балансувати між демократичною євроатлантичною інтеграцією та необхідністю запровадження жорстких суверенних механізмів виживання держави. До цієї групи також доцільно віднести Естонію, Тайвань та Південну Корею, чий досвід дозволяє виокремити специфічні об'єкти правового регулювання, що охоплюють механізми атрибуції кібератак, правові режими «надзвичайного кіберстану», нормативне забезпечення «держави у хмарі» (резервування національних реєстрів) та законодавче регулювання когнітивної безпеки.

Для забезпечення релевантності компаративного аналізу, дослідження світового досвіду забезпечення інформаційної безпеки та формування кіберстійкості буде здійснено не за географічним, а за проблемно-тематичним принципом, крізь призму єдиного комплексного підходу, який дозволяє системно зіставити виокремлені макромоделі у чотирьох фундаментальних вимірах: 1) стратегічному, 2) нормативно-правовому, 3) інституційному, 4) екосистемному. Застосування такого кримінологічного аналізу зі специфікою кожного виміру дає можливість розкрити успішні зарубіжні практики, що дасть змогу об'єктивно оцінити реальну ефективність різноманітних механізмів формування кіберстійкості та визначити оптимальні шляхи їх імплементації у вітчизняну правову систему.

I. Стратегічний вимір, полягає у концептуальному баченні кіберзагроз, детермінує фундаментальну філософію держави щодо природи кіберпростору та способів реагування на інциденти. Від концептуального бачення залежить, чи розглядає юрисдикція цифрове середовище переважно як простір економічного розвитку та реалізації прав громадян (цивільний підхід), чи як повноцінний напрям воєнних дій (мілітаризований підхід).

В межах романо-германської макромоделі (наприклад, у Франції) домінує доктрина «стратегічної автономії», спрямована на захист цифрового суверенітету та економічної незалежності від зовнішніх впливів [311;320]. Досвід Франції становить особливий науковий інтерес, оскільки держава виступає головним ідеологом доктрини «стратегічної автономії» та «цифрового суверенітету» [228]. Цей підхід базується на переконанні, що інформаційна безпека є не просто технічним завданням, а фундаментальною умовою збереження геополітичної та економічної незалежності держави.

Стратегічна автономія означає здатність держави самостійно, без опору на технологічні спроможності чи політичну волю третіх країн (насамперед таких як США чи КНР), здійснювати ідентифікацію кіберзагроз, приймати незалежні рішення та реалізовувати ефективні заходи протидії [226; 247; 261]. Цей підхід

спрямований на подолання технозалежності та захист національного економічного простору від екстериторіального впливу іноземних юрисдикцій.

Для практичної реалізації доктрини стратегічної автономії Франція вибудувала унікальну інституційну систему, в основі якої лежить принцип суворого «цивільно-військового дуалізму». На відміну від багатьох інших держав, де функції захисту та нападу можуть бути сконцентровані в одному органі (як, наприклад, у мілітаризованих макромоделях), французьке законодавство чітко розмежує кіберзахист цивільної критичної інфраструктури та проведення військових кібероперацій [320; 261; 291; 292].

Цивільний напрям представляє Національне агентство з безпеки інформаційних систем (ANSSI) [261]. Інституційний статус ANSSI підкреслює пріоритетність його завдань. Агентство підпорядковане Генеральному секретаріату з питань оборони та національної безпеки (SGDSN), який, у свою чергу, звітує безпосередньо Прем'єр-міністру Франції. До виключної компетенції ANSSI належить превентивне регулювання операторів критично важливої інфраструктури, управління кризовими ситуаціями загальнонаціонального масштабу та жорстка сертифікація засобів криптографічного й антивірусного захисту.

Військовий напрям національної кібербезпеки представляє Командування кібероборони (COMCYBER) [291]. Створене у 2017 році, воно консолідувало під егідою Міністерства збройних сил усі військові підрозділи, дотичні до кіберпростору. Унікальність функціоналу COMCYBER полягає у легалізації двох паралельних напрямів, таких як оборонної та наступальної кіберборотьби. Франція є однією з небагатьох європейських держав, яка на рівні офіційної військової доктрини відкрито визнала наявність наступального кіберпотенціалу та легітимізувала право на превентивні або дії у відповідь у кіберпросторі противника, якщо цього вимагають вищі інтереси національної безпеки [291].

Такий інституційний дуалізм дозволяє Франції зберігати баланс, коли ANSSI забезпечує стійкість держави та економіки, тоді як COMCYBER виконує

функцію проактивного стримування, формуючи комплексну та самодостатню модель національної інформаційної безпеки [261; 291].

Узагальнюючи доцільність використання французького досвіду, варто наголосити, що для України ключовим орієнтиром має стати перехід від фрагментарного ІТ-захисту до комплексної доктрини «цифрового суверенітету». Практична імплементація цієї парадигми вимагає запровадження концепту державного контролю за трьома стратегічними напрямками: а) забезпеченням юрисдикційного контролю над державними даними (через механізм «довірених хмар»); б) інституалізацією безальтернативної безпекової сертифікації ІТ-рішень для об'єктів критичної інфраструктури; в) цілеспрямованим протекціонізмом національної індустрії кібербезпеки. У своєму поєднанні ці інструменти дозволять Україні перетворити національну кіберстійкість із суто технічної функції на фундаментальний гарант інституційного виживання держави в умовах гібридної війни.

У межах англосаксонської моделі США демонструють принципово іншу, проактивну парадигму забезпечення кіберстійкості, ядром якої є військово-стратегічна доктрина «захисту на випередження» та нерозривно пов'язана з нею концепція «безперервної взаємодії». Формування цього підходу стало наслідком визнання того факту, що класичне статичне стримування не працює у кіберпросторі, оскільки цифрові загрози генеруються переважно у «сірій зоні» нижче порогу традиційного збройного конфлікту. Натомість американські кіберсили повинні превентивно проникати у ворожі мережі, виявляти загрози на етапі їхнього формування, деградувати інфраструктуру супротивника та «накладати на нього витрати» безпосередньо в місцях зародження атак.

Сучасна еволюція цього підходу, закріплена у Кіберстратегії Міністерства оборони США 2023 року, розширила дію «захисту на випередження» за межі національних кордонів через механізм «полювання на випередження» [293; 302; 336]. У США Інститут безпеки ШІ був створений на базі Національного інституту стандартів і технологій (NIST) [306;307]. Інститут використовує

попередні напрацювання NIST щодо стандартів для технологій ШІ та створює нові проекти з безпеки ШІ на основі ключових цілей органу [251]. По-перше, Інститут має на меті підвищити безпеку ШІ за допомогою досліджень, тестувань та оцінок систем. По-друге, Інститут займається розвитком та поширенням практики безпечного застосування ШІ. Це передбачає створення та публікацію метрик, інструментів та методів оцінювання ризиків систем ШІ та поширення рекомендацій для відповідального дизайну, розробки та використання передових моделей ШІ. Заходи підтримки включають сприяння діалогу між державними розробниками, експертами та користувачами і розвиток міжнародної співпраці у напрямку безпечного ШІ.

Для ефективної співпраці уряду США із приватним сектором було створено Консорціум Інституту безпеки ШІ. За даними NIST, об'єднання складається з понад 200 організацій, які спільно з урядом США займається розробкою принципів управління ШІ. До складу консорціуму вже увійшли такі провідні компанії, як OpenAI, Google Alphabet, Anthropic і Microsoft [68].

Своєю чергою, держави, що перебувають у стані перманентного конфлікту (Ізраїль), формують радикальнішу доктрину, яка легітимізує нанесення превентивних кібернетичних (а іноді й кінетичних) ударів для нейтралізації загроз ще на етапі їх формування .

2. Нормативно-правовий вимір полягає у захисті критичної інфраструктури та криміналізації деліктів. Цей критерій відображає механізми трансляції стратегічних цілей у площину обов'язкових правових норм. Головним предметом порівняння тут виступають підходи держав до регламентації захисту об'єктів критичної інфраструктури та притягнення до відповідальності за високотехнологічні правопорушення.

Романо-германська правова система є базовою для більшості країн Європи, включаючи Україну, що робить досвід європейських інституцій (таких як ENISA) найбільш релевантним для дослідження забезпечення інформаційної безпеки [239]. Континентальна правова сім'я (орієнтиром якої є Німеччина та

наднаціональне законодавство ЄС, зокрема Директива NIS2) тяжіє до тотальної кодифікації, встановлюючи жорсткі вимоги та безпрецедентні фінансові санкції за недбалість операторів критичної інфраструктури.

Досліджуючи межі криміналізації цифрових деліктів в англосаксонській макромоделі, варто звернути увагу на небезпечну тенденцію розширення репресивного апарату держави. Показовим у цьому контексті є нормотворчий досвід Великої Британії у сфері протидії кібертероризму, який став предметом гострої доктринальної критики через непропорційне втручання у свободу вираження поглядів та право на приватність [269, с. 1123]. Зокрема, імплементація британського Закону про боротьбу з тероризмом та безпеку кордонів 2019 року запровадила механізми кримінального переслідування за факт доступу та перегляду екстремістських матеріалів у мережі. Фактично, особу піддають стигматизації та покаранню не за вчинення суспільно небезпечного діяння, а за її когнітивний інтерес, що є прямим порушенням фундаментальної свободи переконань [338].

Британський кейс ілюструє концептуальну правову колізію, прагнучи мінімізувати криміногенний вплив цифрового середовища, уряди готові жертвувати основоположними правами людини задля превалювання інтересів національної безпеки. Водночас такий жорсткий нормативний тиск з боку держави формує специфічну дихотомію на рівні приватного сектору, що проявляється у гіперфінансуванні на тлі фактичної інституційної вразливості. Як свідчать дані глобального дослідження KPMG Global Tech Report (2026), жорстка державна політика змушує британський бізнес безпрецедентно збільшувати бюджети на кібербезпеку (57% організацій планують зростання витрат понад 10%, що значно вище за середньосвітовий показник). Пріоритетними напрямками інвестицій стають системи штучного інтелекту (ШІ) та аналітика даних. Однак наявність фінансування не конвертується в автоматичну кіберзахищеність: лише 13% британських технологічних лідерів вважають свої системи кібербезпеки повністю масштабованими [77, с.16].

Цей концептуальний розрив між інвестиціями та реальною готовністю підтверджується дослідженням Absolute Security щодо корпоративної кіберстійкості у США та Великій Британії. Попри мільйонні бюджети, організації залишаються не готовими до серйозних інцидентів. Так, середній час повного відновлення після атак становить понад 4,5 днів, а прямі фінансові втрати сягають 2,5 млн доларів за один інцидент [77, с. 22-23].

У цьому контексті законодавство Великої Британії генерує ще один негативний побічний ефект, кризу відповідальності. Страх перед жорсткими юридичними санкціями та тотальним контролем кардинально трансформує роль керівників служб інформаційної безпеки (CISO). Понад 59% CISO стурбовані загрозою особистої юридичної відповідальності та звільнення, а 61% стикаються з очікуваннями керівництва щодо відсутності інцидентів [257].

Узагальнюючи цей досвід, можна констатувати, що виключно карально-репресивна модель державного регулювання не здатна сформувати реальну кіберстійкість нації. Ефективна система інформаційної безпеки вимагає переходу від моделі «покарання за вразливість» до моделі «екосистемної підтримки», де безпека вбудовується в системі технологій від самого початку, а держава виступає наглядачем і партнером у масштабуванні захисних практик.

Ризики надмірного розширення меж нормативно-правового регулювання інформаційного простору особливо яскраво проявляються в авторитарних макромоделях. Показовим прикладом інструменталізації кіберзаконодавства з метою політичних репресій є досвід Саудівської Аравії. Уряд цієї держави активно застосовує Закон про боротьбу з кіберзлочинністю та антитерористичне законодавство для легалізації арештів правозахисників і журналістів за їхню онлайн-адвокацію та громадську діяльність у мережі [269, с. 1136]. З точки зору міжнародного права, така репресивна нормотворчість та правозастосовна практика призводять до системних порушень фундаментальних прав людини, насамперед права на свободу вираження поглядів, імеративно закріпленого у ст. 19 Міжнародного пакту про громадянські та політичні права [128]. Це доводить,

що без належних демократичних запобіжників законодавство у сфері кібербезпеки здатне трансформуватися на механізм державного терору.

У контексті нормативно-правового виміру особливий науковий інтерес становить досвід моделі на прикладі Азербайджанської Республіки, яка демонструє високу динаміку розвитку техніко-юридичних механізмів захисту цифрових прав. Значним практичним здобутком цієї юрисдикції є швидка імплементація процесів загальнонаціональної електронізації, впровадження систем електронної ідентифікації та криптографічного захисту, що дозволило суттєво мінімізувати ризики несанкціонованого втручання у право громадян на недоторканність приватного життя [322, с. 37].

Водночас нормативно-правова база Азербайджану ілюструє складнощі кваліфікації та розслідування цифрових деліктів, зокрема у сфері порушення прав інтелектуальної власності [231]. Як зазначається у національній правовій доктрині, сучасна юриспруденція стикається з двома ключовими викликами. По-перше, це знецінення інтелектуального продукту через технологічну простоту його нелегального копіювання та поширення. По-друге, феномен тотальної анонімності безпосередніх правопорушників у мережі. Неможливість ідентифікації та притягнення до відповідальності кінцевого делінквента створює правовий вакуум, що змушує правозастосовні органи переносити правові претензій на посередників (інтернет-провайдерів) [322, с. 37].

Сучасна вітчизняна практика доводить, що кібернетичний простір залишається одним із ключових елементів гібридної агресії РФ проти України. Усвідомлюючи неможливість автономного протистояння таким масштабним загрозам, стратегічним пріоритетом нашої держави стає глибока європейська інтеграція та гармонізація вітчизняних підходів із континентальною макромоделлю. Важливим інституційним кроком у цьому напрямі стало підписання у 2023 році Робочої угоди між Україною та Агентством ЄС з кібербезпеки (ENISA) [239, с. 3-4]. Ця угода концептуально закріплює перехід від

ситуативного обміну інформацією до системного впровадження європейських практик кіберстійкості.

3. Інституційний напрям характеризується централізацією управління кіберризиками. Дослідження цього виміру дозволяє зрозуміти інституційну складову системи національної безпеки, а саме, який суб'єкт наділений ключовими повноваженнями щодо протидії кіберзагрозам і як розподілені ролі між військовими, розвідувальними та цивільними відомствами.

Англосаксонський підхід (досвід Великої Британії) демонструє успішну практику створення єдиних, потужних координаційних центрів (NCSC), які акумулюють експертизу та виступають єдиним «вікном» як для урядового сектору, так і для приватного бізнесу. Континентальна макромодель (на прикладі Естонії) тяжіє до високо скоординованої, але децентралізованої мережі уповноважених органів із залученням наднаціональних інституцій (таких як Центр передового досвіду НАТО) [300; 303; 304]. На противагу їм, держави (Азербайджан, Ізраїль) вибудовують систему з тотальним домінуванням спецслужб та оборонних відомств, що забезпечує швидке реагування, проте суттєво обмежує прозорість ухвалення рішень.

Сучасна еволюція інституційного підходу до кібербезпеки демонструє концептуальний перехід від техноцентричного підходу до безпосереднього захисту фундаментальних прав людини. Наукової уваги заслуговує інституційний досвід Австралії, яка продемонструвала концептуальний перехід від техноцентричного захисту інформації до захисту фундаментальних прав громадян. Революційним кроком стало створення спеціалізованого регуляторного органу Офісу Комісара з електронної безпеки (eSafety Commissioner) [268]. На відміну від класичних кіберкомандувань чи поліцейських структур, ця інституція функціонує як єдина національна система онлайн-безпеки, що поєднує нормативне регулювання, розгляд скарг та оперативне реагування на такі специфічні цифрові делікти, як кібербулінг, онлайн-насильство та незаконне поширення інтимних матеріалів. Австралійська

програма eSafety має офіційні освітні ресурси та річні звіти про діяльність. Так, у 2023-2024 рр. eSafety отримала 2 693 скарги, що підлягають розгляду, які стосувались кібербулінгу дітей, що було на 37% більше, ніж попереднього року; це підтверджує функціонування системи як реального каналу реагування, а не лише інформаційного ресурсу [268].

Розглядаючи інституційну складову континентальної моделі, варто виокремити фундаментальну роль Агентства Європейського Союзу з кібербезпеки (ENISA). Воно функціонує не як традиційний силовий орган, а як методологічний центр, що формує єдиний простір стандартів для всіх європейських держав [239].

Для України, яка перебуває у стані гібридної війни, співпраця з ENISA стає інструментом розбудови власної кіберстійкості. Зокрема, імплементація методології оцінки національної спроможності ENISA дозволяє об'єктивно визначити рівень вітчизняної кіберзрілості за двома ключовими критеріями: а) наявністю стратегічних документів; б) реальною інституційною спроможністю реагувати на інциденти [239].

4. Екосистемний вимір полягає у розбудові потенціалу та державно-приватному партнерстві. Це найновітніший та динамічний вимір формування кіберстійкості, який виходить за межі суто державних інституцій. Сучасна парадигма визнає, що захист цифрового простору неможливий без глибокої інтеграції приватного технологічного сектору та розвитку когнітивного імунітету громадян.

Фундаментальною складовою екосистемного виміру забезпечення інформаційної безпеки є розвиток людського капіталу та інституціалізація освітніх шляхів підготовки фахівців. Сучасна зарубіжна практика доводить, що системні ризики у кіберпросторі можна суттєво мінімізувати через переосмислення кваліфікаційних вимог до знань та навичок випускників вищої школи при їх виході на ринок праці. Так, показовим є досвід країн англосаксонської (Австралія, Великобританії, США) і континентальної

(Франція) моделей, які запровадили механізми синхронізації академічних ступенів з практичними професійними сертифікаціями, що дозволяє поєднати теоретичну підготовку з актуальними вимогами індустрії безпеки.

На наднаціональному рівні в межах Європейського Союзу цей процес координується Агентством ЄС з кібербезпеки (ENISA) [239]. Важливим інструментом екосистемної розбудови потенціалу стало створення бази даних вищої освіти з кібербезпеки. Ця інтерактивна платформа, що охоплює країни ЄС та Швейцарію, виконує роль стратегічного орієнтира для громадян у виборі освітніх траєкторій та одночасно виступає інструментом залучення молодих талантів до підтримання колективної кібербезпеки Європи.

Для України адаптація такого досвіду є критично важливою у контексті реформування національних стандартів ІТ-освіти та створення прозорої системи підготовки кадрів, здатної забезпечити інституційну стійкість держави перед сучасними високотехнологічними викликами

Особливу наукову цінність для України становить досвід транзитних і континентальних держав-сусідів (Грузії, Польщі) у сфері «capacity building» інституалізації механізмів протидії інформаційно-психологічним операціям (ІПСО), розбудови масової цифрової грамотності та захисту когнітивного суверенітету нації від зовнішньої дезінформації.

В межах англосаксонської макромоделі концепція екосистемної кіберстійкості «capacity building» набуває масштабу загальнонаціональної інформаційної гігієни. Прикладом такої екосистемної розбудови є досвід Канади, зокрема урядова програма «Get Cyber Safe» [276]. На відміну від суто поліцейських чи регуляторних практик, ця ініціатива є перманентною національною просвітницькою кампанією, очолюваною Центром безпеки комунікацій та Канадським центром кібербезпеки. Програма спрямована на децентралізоване формування кіберіммунітету в усіх без винятку соціальних групах від молоді та літніх людей до суб'єктів малого і середнього підприємництва. Вона формує практичні поведінкові патерни (зокрема,

імплементацию багатофакторної автентифікації, розпізнавання фішингу та безпечно налаштування пристроїв), розглядаючи їх як базову громадянську навичку. Практичні результати реалізації «Get Cyber Safe» доводять, що системне інформування населення мінімізує ризики успішного застосування методів соціальної інженерії та компрометації персональних даних [276].

Фундаментальним пріоритетом континентальної моделі є захист прав і свобод людини у цифровому середовищі. Практична реалізація цього концепту на екосистемному рівні яскраво простежується у досвіді Польщі. Польський підхід у забезпеченні інформаційної безпеки та формуванні кіберстійкості поєднує соціальну профілактику, правоохоронні практики та цифрову освіту, що забезпечує цілісну кіберстійкість освітніх та локальних спільнот [343]. Так, у межах Центру навчання та відпочинку Капер у Джураті за ініціативою Департаменту соціальної профілактики Бюро профілактики Національного управління поліції проведений навчальний семінар «Діяльність поліції у сфері мови ворожнечі, ненависті, злочинів на ґрунті ненависті та кіберзагроз» [328]. Навчальний проєкт для координаторів профілактики Komenda Wojewódzka Policji (KWP), Komenda Stołeczna Policji (KSP) і викладачів поліцейських шкіл був спрямований на підвищення професійних компетентностей у сферах протидії мові ворожнечі та кіберзагрозам. Координатори профілактики KWP та KSP це фахівці, які відповідають за організацію й реалізацію профілактичних програм, взаємодію зі школами, громадами та партнерами у сферах соціальної профілактики, кібербезпеки й превенції правопорушень [343].

Важливою складовою польської моделі реалізації завдань протидії кіберзагрозам є участь експертів NASK. Вони опрацьовують алгоритми реагування на кібербулінг з ролями школи, родини та інституцій; висвітлюють реальні та потенційні ризики у цифровому середовищі щодо практики дітей і молоді (зокрема публікації інтимного контенту) із наголосом на правових і психологічних наслідках [286]. Акцент зроблено на протидії дезінформації через фактчекінг, верифікацію джерел і навчальні ігри «Dezinfo» та «Koryntia», які

рекомендовані МОН Польщі для розвитку медіаграмотності школярів. У блоці щодо незаконного та шкідливого контенту експерти показали механізми скарг до Dużurnet.pl, критерії відмежування шкідливого й кримінального контенту та сучасні загрози, включно з контентом, створеним за допомогою ШІ. Додатково вони інтегрували практики CERT Polska щодо кібергігієни, фішингових атак і технік самозахисту [328].

Значну увагу приділяється протидії дезінформації через розвиток критичного мислення, верифікацію джерел і формування психологічної стійкості як компонента кіберстійкості. У цьому напрямі важливо звернути увагу на формування цифрового благополуччя, балансування онлайн та офлайн активностей, профілактику зловживань технологіями та соціальну профілактику, зокрема презентований на науковому семінарі інструмент «Свідомий – мобільний» як приклад «just-in-time» освітніх інтервенцій [328].

Прикладом того, як ця концепція працює на загальнонаціональному рівні, виступають просвітницькі кампанії, координовані Агентством з кібербезпеки та безпеки інфраструктури (CISA) спільно з Міністерством внутрішньої безпеки США. Саме така синергія державних інституцій та суспільства дозволяє мінімізувати ризики цифрового середовища на ранніх етапах їх формування. Так, Secure Our World - це офіційна американська кампанія (програма) CISA з підвищення кіберобізнаності та формування базових правил кібергігієни. Мета програми є формування навичок у громадян, сім'ї, бізнесу і організації простих дій, які зменшують ризик кіберзагроз. Матеріали можуть використовуватися протягом року. Виконавцями програми Secure Our World виступають: CISA, партнери кампанії, школи, організації, роботодавці [325]

Важливим елементом четвертого виміру забезпечення кіберстійкості є розбудова когнітивного суверенітету нації та формування стійкості суспільства до інформаційно-психологічних операцій (ІПСО) і дезінформації. Практичний інтерес представляє досвід Фінляндії, де медіаграмотність інтегрована на рівні національної політики безпеки. Фінська модель становить собою глибоко

інституалізовану систему освіти, орієнтовану на навчання протягом усього життя [294]. Головною метою цієї політики є формування здатності громадян оцінювати масиви даних, розпізнавати маніпулятивні технології та безпечно діяти в медійному середовищі. Для України фінський досвід доводить, що держава здатна нейтралізувати гібридні загрози інформаційного простору не лише через поліцейське блокування деструктивного контенту, а через системне формування у населення міцного суспільного «когнітивного імунітету».

У межах континентальної моделі екосистемний підхід до формування кіберстійкості реалізується не лише на рівні суверенних держав, а й через потужну наднаціональну координацію. Фундаментальним прикладом такого синергетичного підходу є загальноєвропейська стратегія «Better Internet for Kids» (ВІК+). На відміну від директивних регуляторних актів (спрямованих на захист інфраструктури), вона фокусується виключно на соціальному та когнітивному вимірах інформаційної безпеки.

Головною метою ВІК+ є забезпечення прав, поваги та захисту найвразливішої категорії громадян в онлайн-просторі через масову розбудову медіаграмотності та системну протидію кібербулінгу. З погляду інституційної логіки, стратегія розгортається у три етапи: 1) інженерія безпечного цифрового простору; 2) правове забезпечення захисту користувачів; 3) проактивне залучення цільової аудиторії до організації заходів безпеки. Саме третій етап становить найбільшу наукову цінність. Так, європейська екосистема кібербезпеки трансформує користувачів із пасивних об'єктів захисту на активних співтворців інноваційного та безпечного цифрового досвіду. Для вітчизняної практики цей досвід доводить, що ефективна протидія криміногенному впливу цифрового середовища неможлива без глибокої соціальної інтеграції та просвітницьких ініціатив на рівні всього суспільства

Екосистемний характер сучасної інформаційної безпеки зумовлює появу нових типів загроз, пов'язаних із вразливістю ланцюгів постачання та аутсорсингу технологічних послуг. Яскравим прецедентом 2025 р. стала серія

кіберінцидентів у глобальних франчайзингових мережах (McDonald's, Burger King, Popeyes), яка виявила системну незахищеність бізнес-моделей, що критично залежать від програмного забезпечення третіх сторін [77, с. 24-25].

Дослідження вразливостей чат-платформи McHire засвідчило, що навіть за умови значних інвестицій у цифровізацію, базові недоліки технічного контролю з боку постачальника такі як використання стандартних адміністративних паролів здатні поставити під загрозу персональні дані десятків мільйонів користувачів. Статистичні дані підтверджують небезпечну тенденцію, коли кількість порушень безпеки, пов'язаних із діями третіх осіб, подвоїлася і наразі становить 30% від загальної кількості інцидентів у секторі послуг. При цьому латентний період виявлення таких втручань у середньому складає 212 днів, що надає зловмисникам необмежені можливості для компрометації фінансових транзакцій [310].

Окрему увагу слід приділити механізмам фінансового відшкодування та кіберстрахування. Практика доводить неефективність формального підходу до страхових полісів у випадках, коли реальні збитки франчайзі сягали 3,7 млн доларів, а фактичні виплати за загальними корпоративними полісами становили лише 400 тис. доларів [77, с. 24]. Так, для забезпечення реальної інформаційної безпеки необхідний перехід від мінімального виконання регуляторних вимог до індивідуалізованого управління ризиками, де кожна нова інтеграція цифрової системи розглядається як розширення площі потенційної атаки, що потребує специфічного страхового покриття та експертного супроводу.

3.2. Роль міжнародного співробітництва та уніфікації у протидії кіберзагрозам транснаціонального характеру: загальний та спеціальний рівні

Роль міжнародного співробітництва та уніфікації у сфері кібербезпеки полягає у створенні глобальних підходів стійкості та єдиного правового простору

для ефективної нейтралізації загроз, які через свою транскордонну природу не можуть бути подолані зусиллями однієї держави.

Міжнародна співпраця у сфері протидії кіберзагрозам транснакордонного характеру є ключовим чинником забезпечення глобальної безпеки, особливо в умовах цифровізації та транскордонного характеру кримінальних правопорушень. Злочинність, обумовлена кіберзагрозами, часто виходять за межі однієї держави, що потребує узгоджених дій між країнами. Одним із основних шляхів є гармонізація законодавства відповідно до міжнародних стандартів, зокрема рекомендацій FATF, директив ЄС та конвенцій ООН. Це дозволяє створити єдині правила інформаційного моніторингу та запобігання кіберзагрозам безпекового характеру.

Питанням міжнародного співробітництва у сфері інформаційної безпеки та протидії транснаціональній кіберзлочинності та кіберзагрозам присвячені праці багатьох вітчизняних та зарубіжних науковців [17; 112; 204; 212; 235; 241; 245; 246; 279]. Сучасна правова доктрина виходить із того, що безальтернативність міжнародного співробітництва у протидії кіберзагрозам зумовлена глобальною взаємопов'язаністю інформаційних систем та транскордонною природою самих кібератак.

Стратегія інформаційної безпеки України передбачає активне залучення до міжнародного співробітництва в сфері кібербезпеки та обміну досвідом з іншими країнами. Україна прагне підтримувати спільні стандарти та процедури для захисту інформації, а також взаємно надавати допомогу в разі кібератак чи інших загроз, які можуть виникнути. Міжнародне співробітництво у сфері захисту цифрового середовища відіграє ключову роль у зміцненні національної та глобальної інформаційної безпеки.

Останніми роками Україна зазнає системного впливу масштабних, скоординованих і технологічно складних кібератак, які стали важливою складовою гібридної агресії проти держави. Ці дії не мають випадкового чи поодинокого характеру, вони є цілеспрямованими та стратегічно спланованими,

спрямованими на дестабілізацію системи державного управління, порушення роботи критичної інфраструктури, підриг довіри суспільства та ослаблення національної безпеки [218, с. 487-496]. Цифровий фронт цієї боротьби охоплює не лише технічні аспекти, а й складні інформаційно-психологічні операції, маніпулювання даними та системні спроби вивести з ладу державні сервіси. У таких безпрецедентних умовах кібербезпека об'єктивно стає базовим елементом національної обороноздатності, а правове регулювання кіберпростору одним з інструментів стратегічного захисту [151, с. 257].

Проте ефективна протидія цим загрозам неможлива в межах ізолюваної національної інституційної системи. Побудова сучасної, адаптивної системи кібербезпеки вимагає імплементації міжнародних стандартів та активного міжнародного співробітництва. Результати дослідження свідчать, що ця вимога набуває особливого значення в умовах воєнного стану, коли обмеженість внутрішніх ресурсів та територіальні виклики безальтернативно диктують необхідність глобальної інтеграції безпекового сектору. Так, система превенції вже не може спиратися виключно на внутрішні інструменти реагування. Ключовою умовою стає залучення наднаціональних правових механізмів, спільне проведення транскордонних оперативно-розшукових заходів та безперервний обмін розвідувальною інформацією з державами-партнерами.

Науковий інтерес у контексті дослідження ролі міжнародного співробітництва у системі протидії кіберзагрозам представляє дисертаційне дослідження П. П. Галушко. Автор зазначає, що сучасна інтеграція зумовлює фундаментальну зміну самої філософії безпеки: необхідність остаточного переходу від традиційної вітчизняної реактивної моделі (зосередженої на розслідуванні постфактум) на користь системної міжнародної проактивної стратегії. Як засвідчили реалії повномасштабної гібридної війни, реагування на наслідки є неефективним; головною метою стає виключно превенція катастрофічних ударів по критичній інфраструктурі. Це змусило Україну на практиці стрімко імплементувати проактивну міжнародну парадигму,

об'єднавши зусилля державного апарату, приватного ІТ-сектору та глобальних партнерів [30, с. 168-174].

Міжнародна взаємодія у сфері інформаційної безпеки трансформувалася у стратегічний детермінант зміцнення обороноздатності України, забезпечуючи перехід від локального протистояння до участі у глобальній системі колективної кіберстійкості. Синергія зусиль із міжнародними партнерами, що реалізується через спільні високотехнологічні кібероперації, оперативний обмін розвідувальними даними та трансфер передових технологій, суттєво інтенсифікувала спроможності національних суб'єктів безпеки у протидії гібридним загрозам [113, с. 98-104].

Міжнародне співробітництво у сфері запобігання та протидії злочинності виступає наріжним каменем будь-якої дієвої безпекової стратегії, адже, як справедливо зазначається в науковій літературі, що жодна, навіть наймогутніша держава, не в змозі самотійно протистояти транснаціональним загрозам [27, с. 109]. У контексті кіберзлочинності ця аксіома набуває абсолютного значення, тому що транскордонність та екстериторіальність цифрових деліктів перетворюють міждержавну взаємодію на безальтернативну умову захисту національних інтересів [242]. Водночас слід визнати, що конвенційні (традиційні) механізми міжнародної правової допомоги обтяжені низкою критичних структурних вад. Їхня бюрократична інертність, тривалі процедури опрацювання запитів та асиметрія національних юрисдикцій створюють небезпечний розрив у часі, роблячи ці класичні інструменти вкрай малоефективними перед обличчям блискавичних і масштабованих кіберзагроз у сучасному цифровому суспільстві.

Подолання цієї інституційної кризи вимагає концептуального переходу від епізодичної міжнародної правової допомоги до глибокої взаємодії в межах передових наднаціональних альянсів. Інформаційна та нормативна інтеграція з безпековими структурами НАТО і ЄС наразі є засадничим вектором Стратегії національної безпеки, що дозволяє Україні не лише адаптувати вітчизняне

законодавство до світових стандартів (зокрема, Директиви NIS2), а й виступати активним донором унікального бойового досвіду. Доповненням цієї співпраці є розбудова спільних центрів аналізу загроз та залучення України до програм кіберзахисту критичної інфраструктури, що створює багаторівневий «щит» проти транскордонної злочинності та державного кібертероризму.

На загальному рівні роль міжнародного співробітництва полягає у забезпеченні колективної безпеки в кіберпросторі та спільного реагування на відповідні ризики та кризи. По-перше, це формування спільних стратегій, що полягає у розробці універсальних норм, правил та принципів поведінки держав у кіберпросторі (наприклад, під егідою ООН або НАТО) для запобігання конфліктам та ескалації. По-друге, це інформаційний та практичний обмін, що характеризується створенням механізмів (наприклад, через цілодобові контактні пункти, як вимагає Директива 2013/40/EU) для оперативного обміну даними про нові загрози, індикатори компрометації (IoC) та технічні рішення [264]. Так, виявлення та повідомлення про загрози та ризики, що виникають внаслідок кібератак, та пов'язана з ними вразливість інформаційних систем є важливим елементом ефективного запобігання кібератак та реагування на них, а також підвищення безпеки інформаційних систем. Забезпечення стимулів для повідомлення про прогалини в безпеці може сприяти цьому ефекту. Держави-члени повинні прагнути забезпечити можливості для правового виявлення та повідомлення про прогалини в безпеці [264]. У Директиві наголошено на підвищенні міри покарання у тих випадках, коли атаку на інформаційну систему скоює злочинна організація, як це визначено в Рамковому рішенні Ради 2008/841/JHA від 24 жовтня 2008 р. про боротьбу з організованою злочинністю [308], коли кібератака здійснюється у великих масштабах, що впливає на значну кількість інформаційних систем, зокрема, коли вона має на меті створити ботнет, або коли кібератака завдає серйозної шкоди, зокрема, коли вона здійснюється через ботнет [264]. Доцільним виступає зміни до кримінального законодавства щодо

більш суворого покарання у випадках, коли кібер атака здійснюється проти критичної інфраструктури держав-членів або Союзу.

Трете, охоплює розбудову потенціалу як стратегічний процес зміцнення здатності держави або суспільства ефективно виявляти кіберзагрози, протидіяти їм та відновлюватися після інцидентів. Нагальна, потреба у такому системному зміцненні національного та колективного імунітету продиктована глобальними макроекономічними та політичними трансформаціями.

Сучасний світ стрімко вступає в нову еру геополітичної конкуренції, де технологічні зрушення докорінно переформатовують механізми функціонування держав і транснаціональних корпорацій. Як переконливо свідчать міжнародні аналітичні прогнози (зокрема, Global Cybersecurity Outlook 2026), кібербезпека трансформувалася із суто технічної проблеми ІТ-сектору на фундаментальний стратегічний імператив міжнародних відносин [277].

Така взаємодія зумовлюється трьома ключовими детермінантами: а) нерозривним злиттям кібербезпеки з геополітикою; б) фрагментацією міжнародного нормативно-правового поля (через прагнення держав до цифрового суверенітету); в) критичною потребою в інституційній стійкості. Сучасні транскордонні кібероперації стали базовим інструментом державного управління в умовах гібридної війни, що використовується для системного шпигунства, економічного саботажу та інформаційно-психологічного впливу. Поява багатополярного світу, посилення впливу недержавних суб'єктів створили високонепередбачуваний ландшафт загроз, де гібридні атаки розмивають межі між класичною державною та недержавною діяльністю, ускладнюючи процеси ідентифікації та атрибуції деліктів [267].

Ситуація додатково загострюється тим, що уряди посилюють контроль над національними сегментами кіберпростору (шляхом суворого регулювання локалізації даних та експортного контролю). Це неминуче призводить до розбіжностей у юрисдикціях, породжуючи ризики концентрації та порушення глобальних ланцюгів постачання. Зрештою, усвідомлення того факту, що

процеси у кіберпросторі сьогодні безпосередньо формують економіку, стійкість демократичних інститутів та загальний баланс сил, вимагає відмови від застарілих реактивних підходів [78, с. 4-5].

Стратегія розбудови потенціалу полягає у закупівлі обладнання та системному підході до створення стійкої екосистеми цифрового захисту. У межах ЄС та міжнародних організацій (ООН, ОБСЄ) охоплює IV ключові рівні.

Нормативно-правовий рівень формує допомогу у створенні національних стратегій кібербезпеки та адаптації законодавства. Для України, в контексті ст. 83 Договору про функціонування ЄС [253], це означає гармонізацію визначень кіберзлочинів, щоб забезпечити принцип «подвійної кримінальності» та юридичну сумісність.

Технічно оперативний рівень охоплює створення та навчання команд реагування на різноманітні комп'ютерні надзвичайні події, загрози, атаки. Це включає передачу технологій, спільні кібернавчання та налагодження каналів обміну даними про загрози в реальному часі.

Освітньо кадровий потенціал полягає у підготовці фахівців, підвищенні кваліфікації суддів та працівників правоохоронних органів (особливо у сфері збору, передачі цифрових доказів), а також просвітницькій програмі цифрової грамотності для населення. У контексті інформаційної безпеки це є фундаментом, адже система стійка лише тоді, коли люди знають, як діяти в умовах гібридних атак.

Політичний рівень забезпечує навчання фахівців для участі в міжнародних переговорах щодо норм відповідальної поведінки держав у кіберпросторі. Це дозволяє Україні бути не просто отримувачем допомоги, а активним учасником формування європейських стандартів.

На спеціальному рівні міжнародна співпраця має ключове значення, по-перше, уніфікація кримінального законодавства. Так, гармонізація національних кримінальних кодексів (за прикладом Будапештської конвенції та Директиви 2013/40/EU Європейського Парламенту та Ради про атаки на інформаційні

системи спрямована на забезпечення однакового визначення ключових кіберзлочинів. У Директиви 2013/40/EU визначені ст. 3 Незаконний доступ до інформаційних систем, ст. 4 Незаконне втручання в систему; ст. 5 Незаконне втручання в дані, ст. 6 Незаконне перехоплення [264].

Реалізація стратегії «захищеної інтеграції» України в безпековий простір ЄС потребує глибокої синхронізації складів кримінальних правопорушень, визначених у Директиві 2013/40/EU, із національним законодавством. Дана Директива, прийнята на виконання Статті 83 Договору про функціонування ЄС, встановлює мінімальні стандарти криміналізації діянь, що посягають на інформаційні системи. Аналіз відповідності КК України положенням Директиви 2013/40/EU дозволяє констатувати високий рівень нормативної конвергенції, що є фундаментом для забезпечення принципу подвійної кримінальності та ефективної транскордонної співпраці. Зокрема, положення Статті 3 Директиви 2013/40/EU (незаконний доступ до інформаційних систем) в українському правовому полі імплементовані через ст. 361 КК України, яка карає за несанкціоноване втручання в роботу інформаційно-комунікаційних систем. В умовах війни, вітчизняний законодавець трансформував цю норму, посиливши відповідальність за дії, вчинені в умовах воєнного стану, що свідчить про адаптивність системи до екстремальних викликів.

Втручання в систему та дані, регламентовані Ст. 4 та 5 Директиви 2013/40/EU, знайшли своє відображення у ст. 361 та ст. 362 КК України відповідно. Якщо європейський стандарт фокусується на забезпеченні цілісності та доступності даних, то українська модель додатково акцентує увагу на суб'єктному складі правопорушень (зокрема, щодо осіб, які мають право доступу), що посилює внутрішню інституційну стійкість організацій. Питання незаконного перехоплення даних (Стаття 6 Директиви 2013/40/EU) в Україні вирішується через комплексну дію ст. 163 КК України, що захищає конституційну таємницю спілкування, та ст. 361 КК України, у частині, що стосується витоку інформації.

Така гармонізація перетворює КК України з суто карального інструмента на елемент розбудови потенціалу. Синхронізація дефініцій дозволяє Україні повноцінно використовувати інфраструктуру Європолу та Євроюсту, оскільки ідентичність правового сприйняття кіберзагроз знімає процесуальні бар'єри при транскордонному зборі цифрових доказів. Детальна кореляція між статтями 3–6 Директиви 2013/40/EU та відповідними нормами Розділу XVI КК України є практичним втіленням парадигми «захищеної інтеграції». Це підтверджує, що правова стійкість України будується на здатності національного закону виступати частиною глобальної системи безпеки, де ідентичність кримінально-правових стандартів забезпечує функціонування колективного «правового щита» в умовах гібридних загроз.

По-друге, Директива 2013/40/EU та Будапештська конвенція забезпечує принцип подвійної кримінальності для ефективної екстрадиції та правової допомоги. Цей принцип виступає фундаментальною основою міжнародного співробітництва у кримінальних справах. Відповідно до Директив ЄС та загальної практики правової допомоги, він означає, що діяння, щодо якого запитується екстрадиція або правова допомога, має бути визнане кримінальним правопорушенням (злочином) відповідно до законодавства обох держав: країни, що запитує допомогу, та країни, до якої звертаються. Для України, яка перебуває в умовах воєнної агресії та постійних локальних кібератак на критичну інфраструктуру, така інтеграція та співробітництво стають критичним елементом національної стійкості та міжнародного захисту.

На спеціальному рівні міжнародної співпраці роль уніфікації та співробітництва полягає у сприянні прямій взаємодії правоохоронних органів (наприклад, через Інтерпол чи Європол) для оперативного розслідування транскордонних злочинів, де час є критичним фактором.

Сучасні цифрові технології відкривають нові, безпрецедентні можливості для міжнародної співпраці. Водночас вони формують глобальні виклики, ключовим з яких є питання безпеки штучного інтелекту (ШІ). Оскільки більшість

ризиків, пов'язаних із впровадженням інтелектуальних систем, мають яскраво виражений екстериторіальний характер і становлять загрозу міжнародного масштабу, їх ефективна нейтралізація неможлива в межах ізольованих національних юрисдикцій і вимагає міждержавної взаємодії.

Справедливість цієї тези підтверджується глобальними аналітичними маркерами: незважаючи на превентивну оцінку систем ШІ перед їх впровадженням, абсолютна більшість експертів (87%) визначають алгоритмічні вразливості як загрозу, що масштабується найшвидше. На цьому тлі спостерігається небезпечна асиметрія у регіональній спроможності держав захищати свою критичну інфраструктуру: рівень інституційної впевненості коливається від 84% у країнах Близького Сходу та Північної Африки до критичних 13% у державах Латинської Америки [78, с. 7-8].

Індикатором системної кризи є і розбіжність стратегічних пріоритетів на корпоративному рівні: тоді як топ-менеджмент фокусується переважно на протидії масовому кібершахрайству (яке зачіпає понад 73% суб'єктів), профільні фахівці з безпеки вбачають головну небезпеку в цілеспрямованих атаках з використанням програм-вимагачів (ransomware). Реальність цих загроз змушує урядові інституції вдаватися до жорсткого нормативного регулювання. Наприклад, у зв'язку з чотирикратним зростанням кількості атак на комунікаційні мережі, регуляторні органи США (зокрема, Федеральна комісія з питань зв'язку) зобов'язують провайдерів безальтернативно імплементувати модель «нульової довіри», забезпечувати сегментацію мереж та протоколювати інциденти у взаємодії з федеральними агентствами [234].

У цьому контексті світова спільнота налаштована на інклюзивну співпрацю задля забезпечення розвитку людиноцентричного, надійного та відповідального ШІ, який гарантує безпеку та працює на суспільне благо. Ця взаємодія реалізується через ключові міжнародні форуми та ініціативи, спрямовані на подолання всього спектра технологічних ризиків. Така політика має максимізувати технологічні переваги при одночасному жорсткому контролі

загроз, що включає запровадження адаптивної категоризації ризиків з урахуванням національних обставин та діючих правових рамок [332].

Практичним втіленням цих принципів та знаковим етапом інституціоналізації міжнародного співробітництва у сфері глобальної інформаційної безпеки став Глобальний саміт з безпеки штучного інтелекту (листопад 2023 року, Велика Британія). За його підсумками 28 держав, включаючи Україну, підписали історичну Декларацію Блетчлі (The Bletchley Declaration), яка вперше на найвищому рівні консолідувала зусилля для мінімізації ризиків так званого «передового ШІ» [332].

Для України, як повноправного підписанта Декларації, це відкриває стратегічні перспективи глибокої інтеграції у міжнародні кіберкоаліції (зокрема, через практичну взаємодію з новоствореними Інститутами безпеки ШІ, перші [з](#) яких були створені урядами Британії та Сполучених Штатів за підсумками Саміту з безпеки ШІ, проведеного у 2023 році.) [68]. Така інституційна синергія є безальтернативною умовою для формування механізмів колективного реагування на транскордонні алгоритмічні загрози, що дозволяє гарантувати захист критичної інформаційної інфраструктури держав та загальну стабільність світового цифрового простору.

Уніфікація цих механізмів вимагає постійної співпраці для розробки спільних міжнародних принципів та кодексів етичної поведінки. Особливої уваги потребують високотехнологічні загрози, що генеруються так званним «передовим» ШІ. Для протидії їм держави-лідери зобов'язуються посилювати інституційну координацію та розширювати партнерську мережу. Це дозволить своєчасно ідентифікувати, аналізувати та проактивно реагувати на глобальні кіберзагрози через спеціалізовані платформи, включно з проведенням регулярних міжнародних самітів з безпеки ШІ [332].

Практичним виміром такої інституційної координації стало формування глобальної моделі спеціалізованих Інститутів безпеки штучного інтелекту. Піонерами у цій сфері виступили США та Великобританія, чий досвід нині

інтенсивно масштабується на міжнародному рівні. Зокрема, під час травневого Саміту з безпеки ШІ 2024 року десять провідних держав світу та ЄС уклали угоду про створення єдиної мережі таких інститутів задля забезпечення транскордонної сумісності методологій тестування та оцінювання алгоритмічних систем. Наміри інтегруватися до цієї мережі вже задекларували Японія, Південна Корея та Канада [331]

Поглиблення міждержавної синергії, як зазначила Міністерка торгівлі США Джина Раймондо, проявилось у підписанні Меморандуму про взаєморозуміння між США та Великобританією (квітень 2024 року) [331]. Цей документ запроваджує обов'язкову спільну розробку програми тестування передових ШІ-моделей із використанням уніфікованого інструментарію, спрямованого прискорити реагування на виклики безпеці. Водночас, як зазначила виконавча віце-президентка Європейської Комісії М. Вестагер, стратегічну роль у цьому процесі на європейському континенті відіграє новостворений Офіс штучного інтелекту Європейського Союзу [331]. Окрім функцій наглядового органу за дотриманням AI Act, Офіс фактично перебирає на себе повноваження європейського Інституту безпеки ШІ. Його партнерство з американськими інституціями виходить за межі суто технічного тестування і передбачає глибинне узгодження регуляторних підходів, орієнтирів та загальної методології протидії кіберзагрозам в обох юрисдикціях.

У контексті зазначених трансформацій важливим є питання залучення України до описаної міжнародної безпеки ШІ. Враховуючи статус нашої держави як підписанта Декларації Блетчлі та наявність унікального практичного досвіду вітчизняних фахівців у протидії гібридним кіберзагрозам в умовах воєнного стану, Україна має значний потенціал не лише як реципієнт безпекової допомоги, а й як активний контриб'ютор колективної кіберстійкості.

Стратегічним вектором для нашої держави має стати ініціювання створення національного Інституту безпеки ШІ (або відповідного спеціалізованого центру компетенцій при національних суб'єктах кібербезпеки)

з його подальшим включенням до згаданої глобальної мережі. Крім того, процес євроінтеграції відкриває Україні прямі можливості для тісної секторальної взаємодії з Офісом штучного інтелекту ЄС. Така інституційна інтеграція дозволить вітчизняним правоохоронним та безпековим структурам отримати доступ до передових інструментів оцінки алгоритмічних вразливостей, спільних баз даних інцидентів та новітніх методик розслідування високотехнологічних кіберзлочинів, зміцнюючи загальнонаціональний імунітет перед загрозами цифрового майбутнього.

Практична реалізація такого партнерства безпосередньо відкриває шлях до впровадження комплексних інноваційних рішень у найбільш вразливих сферах. Зокрема, застосування нових цифрових інструментів, коли використання технології блокчейн дозволяє забезпечити процесуальну прозорість транзакцій та жорсткий контроль за цільовим розподілом гуманітарної чи фінансової допомоги. При цьому, алгоритми штучного інтелекту та технології Big Data дають змогу здійснювати предиктивний аналіз надвеликих масивів фінансових даних, що забезпечує миттєве виявлення аномалій та точне прогнозування складних, багаторівневих шахрайських схем.

Використання блокчейну дозволяє забезпечити прозорість транзакцій та контроль за розподілом гуманітарної допомоги, а штучний інтелект і Big Data дають змогу аналізувати великі масиви фінансових даних для виявлення аномалій та прогнозування шахрайських схем. Важливим є також проведення спільних навчань і тренінгів для правоохоронців та фінансових аналітиків, що сприяє підвищенню кваліфікації та обміну досвідом. Наприклад, у Сінгапурі впроваджено сучасну систему міжнародної співпраці у боротьбі з економічними злочинами COSMIC, яка була запущена Monetary Authority of Singapore у квітні 2024 р. Платформа дозволяє банкам обмінюватися даними про підозрілі транзакції, використовуючи стандартизований формат, що полегшує інтеграцію з аналітичними інструментами й забезпечує оперативну реакцію на іноземні загрози [329].

Аналізуючи процес імплементації міжнародних нормативно-правових актів, важливо розуміти, що кримінальне законодавство будь-якої держави займає центральне місце в системі регулювання суспільних відносин. З огляду на прагнення України до повномасштабної участі в політичному й економічному житті Європи, наближення вітчизняного законодавства до міжнародного досвіду є логічно зумовленим і критично важливим для забезпечення національної кібербезпеки. Це вимагає не лише гармонізації складів злочинів (як було обговорено через Директиву 2013/40/EU), але й впровадження ефективних механізмів міжнародного співробітництва у сфері розслідування, превенції та оперативного обміну інформацією.

Заходи, спрямовані на підвищення ефективності боротьби з транснаціональною кіберзлочинністю, вимагають посилення міжнародної взаємодії та обміну інформацією між державами-учасницями. Ці механізми, ґрунтуються на принципах Конвенції ООН Проти транснаціональної організованої злочинності, прийнятої 15.11.2000 р. [90]. Вони включають:

- стимулювання осіб, що беруть участь у діяльності злочинних груп, до активної співпраці з правоохоронними органами, що включає надання інформації про структуру, діяльність та ресурси кіберзлочинних груп;
- розгляд можливості пом'якшення покарання або навіть надання імунітету від кримінального переслідування для осіб, які співробітничать у розслідуванні або переслідуванні злочинів. Такі заходи є визначальними для розкриття внутрішніх зв'язків транснаціональної кіберзлочинності.
- надання ефективних режимів захисту особам, які співробітничать зі слідством, що здійснюється відповідно до встановлених міжнародних та внутрішніх правових норм.

Крім заходів розслідування, міжнародне співробітництво охоплює проактивні заходи попередження, відповідно до принципів Конвенції ООН проти транснаціональної організованої злочинності [90]. Ці превентивні заходи мають пряме відношення до формування інформаційної безпеки:

- вжиття спільних законодавчих та адміністративних заходів для запобігання зловживань з боку кіберзлочинних груп у торгових процедурах, фінансових операціях та отриманні субсидій. Це передбачає підтримку співробітництва між правоохоронними органами та приватними організаціями.
- запобігання зловживанням шляхом створення та обміну інформацією між компетентними органами щодо реєстрів кінцевих бенефіціарів та інших даних про юридичні особи, які можуть використовуватися для легалізації доходів від кіберзлочинів;
- проведення періодичної міжнародної оцінки існуючих правових документів та адміністративної практики з метою виявлення їхньої вразливості до зловживань з боку кіберзлочинців.
- сприяння поглибленню розуміння суспільством сутності транснаціональної кіберзлочинності через інформаційні кампанії, а також сприяння реінтеграції в суспільство осіб, засуджених за ці злочини, для зниження рецидиву.

Доцільність такого, системного підходу підтверджується актуальними аналітичними прогнозами розвитку безпекового середовища до 2026 року. Експерти наголошують на остаточному вичерпанні реактивних моделей захисту та виокремлюють три глобальні, глибоко взаємопов'язані тенденції, що диктують необхідність переходу до проактивної, розвідувальної кіберстійкості:

- геополітична детермінація кіберризиків щодо перенесення глобальних конфліктів у кіберпростір, що вимагає безперервного моніторингу стратегічних ланцюгів постачання та інтеграції геополітичної розвідки в національні системи безпеки;
- критична вразливість глобальної морської логістики шляхом перетворення базової інфраструктури міжнародної торгівлі на пріоритетну мішень для атак, що диктує необхідність скоординованого міждержавного моніторингу транскордонних операцій у режимі реального часу;
- ескалація загроз «тіньового штучного інтелекту» шляхом масового та нерегламентованого використання генеративних нейромереж, що формує

нову масштабну поверхню ризиків, нейтралізація якої потребує жорсткого інституційного контролю за алгоритмами та походженням даних [77, с. 7-8].

Жоден із трьох викликів (геополітичний, логістичний чи алгоритмічний) не може бути подоланий в ізолюваному національному полі. Їхня нейтралізація об'єктивно вимагає консолідованих наднаціональних механізмів управління ризиками та ефективного міжнародного співробітництва

Ключовим інструментом доступу до такої моделі інформаційної безпеки є поглиблення інституційної та нормативної взаємодії з європейськими структурами. З огляду на це, одним з важливих чинників членства України у Раді Європи виступає необхідність інтеграції країни та національної правової бази у єдиний європейський правовий простір шляхом приведення національного законодавства у відповідність до міжнародних норм. У контексті протидії кіберзагрозам, це означає, зокрема, уніфікацію кримінально-правових механізмів відповідно до стандартів РЄ (Будапештська конвенція) [92]. Імплементация цих положень посилює міжнародну взаємодію з ЄС, оскільки уніфіковані склади злочинів полегшують процедури екстрадиції та надання міжнародної правової допомоги на основі принципу подвійної кримінальності, що є критично важливим для протидії транснаціональній кіберзлочинності.

Основні напрями співробітництва України та РЄ, зокрема, забезпечення прав людини, реформування судової системи та боротьба із корупцією та відмиванням грошей, покладено в основу Плану дій Ради Європи для України на 2023-2026 роки «Стійкість, відновлення та відбудова» [160]. Як наголосив директор Директорату з координації програм РЄ д-р Клаус Нойкірх, пріоритети співпраці безпосередньо стосуються забезпечення інформаційної безпеки у широкому сенсі. Це стосується: а) роботи в напрямках протидії відмиванню грошей (що часто є наслідком кіберзлочинів та фінансового шахрайства); б) розвитку незалежної, ефективної та надійної системи правосуддя (необхідно для розслідування, переслідування транснаціональних кіберзлочинців); в) підтримки

свободи слова та медіа (що важливо для захисту від дезінформації та забезпечення когнітивної безпеки) [203].

Важливо зауважити, що міжнародне співробітництво з Радою Європи є комплексною правовою та інституційною основою для підвищення кіберстійкості України та ефективної протидії глобальним кіберзагрозам. Практичним втіленням цієї багатосторонньої взаємодії та логічним розширенням безпекової координації стало створення у 2023 р. «Талліннського механізму». Дана ініціатива, об'єднана зусиллями міністерств закордонних справ України, Канади, Данії, Естонії, Франції, Німеччини, Нідерландів, Польщі, Швеції, Великобританії та США, виступає новим інструментом оперативної підтримки національної цифрової стійкості [208]. Оцінюючи роль проекту, зазначимо, що він спрямований на посилення координації у сфері захисту критичної інфраструктури України від агресивних кібероперацій. Необхідність такого формату тривалої допомоги була продиктована інтенсифікацією зовнішніх втручань у 2023 році, що вимагало не лише правового реагування, а й розбудови реального цивільного кіберпотенціалу.

Потреба у посиленні саме цивільного та корпоративного сегментів підтверджується глобальними тенденціями. Так, недавній аналітичний звіт Vodafone Business демонструє критичний рівень кібервразливості корпоративного сектору: понад 10% компаній визнають, що серйозна кібератака стане для них екзистенційним вироком, після якого бізнес не виживе. Ця безпрецедентна незахищеність зумовлена людським фактором понад 70% керівників вбачають головну загрозу у вразливості власних співробітників до фішингових атак. Хоча гучні інциденти (злами Jaguar Land Rover та Marks & Spencer) змусили 45% організацій запровадити базове навчання з питань безпеки, загальна картина ризиків лише погіршується. Так, 63% респондентів почуваються більш вразливими, ніж рік тому. Причиною є низька кібергігієна: працівники дублюють паролі в середньому в 11 особистих акаунтах, створюючи для зловмисників «точки входу» до корпоративних систем [77, с. 21; 305].

Ситуація додатково загострюється стрімким розвитком генеративного штучного інтелекту та технологій deepfake. Вони виводять соціальну інженерію на новий рівень ускладнення, дозволяючи злочинцям імітувати цифрову особистість керівників для несанкціонованої авторизації платежів [77, с. 21-22]. З огляду на ці тенденції, міжнародні ініціативи Талліннського механізму стають необхідними: а) забезпечують державу інструментами для термінового посилення інфраструктурних технічних бар'єрів та когнітивної обізнаності персоналу, без якого захист цивільного сектору в умовах війни є неможливим.

Сьогодні, «Талліннський механізм» має стати основою міжнародної підтримки, забезпечуючи синергію між державами-партнерами та іншими групами допомоги. Для досягнення максимальної ефективності союз країн-учасниць пропонує трирівневу координацію за короткостроковим, середньостроковим та довгостроковим напрямками. Це забезпечує комплексний та стійкий алгоритм захисту, де стратегічні правові стандарти РЄ доповнюються конкретними технічними заходами підтримки важливих систем держави. А стратегічна координація та розбудова технічного захисту на макрорівні є лише однією складовою комплексної кіберстійкості. Міжнародна співпраця потребує синергії між інституційною обороною та правоохоронним наступом на транснаціональні кримінальні мережі.

Практичним виміром такої інтеграції є безпосередня участь Національної поліції України у 22 міжнародних спецопераціях (17 з них проведено у 2024 р.), що дозволило нейтралізувати низку глобальних хакерських мереж. Прикладами цієї взаємодії є: операція «Vicarius» спільно з правоохоронцями Латвії з ліквідації транскордонної мережі шахрайських call-центрів у сфері псевдо-криптоінвестицій (збитки склали 340 тис. євро, арештовано активів на понад 500 тис. дол. США); спільні з Молдовою заходи зі знешкодження угруповання, що ошукувало громадян під виглядом постачання автомобілів для ЗСУ; а також скоординована Європолем операція з блокування масштабного криптоджекінгу

на серверах «Amazon Web Services» (компрометація понад 5 тис. акаунтів зі збитками корпорації у 4 млн дол. США) [42].

Окрім оперативно-розшукової реалізації, фундаментом міжнародної інтеграції є щоденний інформаційно-аналітичний обмін, розбудова інституційного потенціалу правоохоронних органів. Системним інструментом комунікації вітчизняних поліцейських із європейськими партнерами виступає захищена платформа Європолу SIENA. Лише протягом 2025 року через цей канал забезпечено безперебійне опрацювання масиву розвідувальних даних щодо ключових транскордонних деліктів: комп'ютерних злочинів, фішингу, відмивання кримінальних активів та сексуальної експлуатації дітей. Найбільш результативну взаємодію зафіксовано з правоохоронними структурами Польщі, Чехії, Литви, Німеччини, Франції та Австрії [64].

Логічним доповненням оперативної співпраці є активна участь українських фахівців у формуванні глобальної системи інформаційної безпеки. Це реалізується через взаємодію з міжнародними інституціями: Управлінням ООН з наркотиків і злочинності, Радою Європи, НАТО, ОБСЄ та Консультативною місією ЄС. Підтвердженням зростання суб'єктності України на міжнародній арені є залучення представників вітчизняної поліції до роботи Спеціального комітету ООН з розробки конвенції протидії кіберзлочинності. Паралельно забезпечується імплементація передового зарубіжного досвіду через участь у стратегічних тренінгах Ради Європи (проекти CyberEast та CyberEast+), що у підсумку працює на загальне підвищення кіберстійкості та захист критичної інфраструктури держави [42].

В умовах сьогодення, міжнародне співробітництво у сфері інформаційної безпеки трансформується з формальної взаємодії у динамічну систему правової стійкості. На загальному рівні уніфікація забезпечує легітимність та політичну єдність, а на спеціальному створює практичний інструментарій «sarasity building» для нейтралізації транснаціональних кіберзагроз. Для України це

означає остаточний перехід від ролі об'єкта, що потребує захисту, до статусу активного контриб'ютора європейської кібербезпеки.

3.3. Основні напрями вдосконалення кримінологічного забезпечення інформаційної безпеки та формування національної кіберстійкості в Україні

Забезпечення інформаційної безпеки України вимагає переходу від реактивної моделі реагування на кіберінциденти до проактивної системи, заснованої на кіберстійкості та верховенстві права. Цей процес є важливим для євроінтеграційного курсу країни і потребує комплексних реформ за трьома основними напрямками: законодавча гармонізація, інституційна стійкість та превентивна освіта. Протидія кіберзлочинності та забезпечення прав людини у цифровому просторі вимагає не лише реактивних, а й проактивних кримінологічних заходів. Це означає перехід від простої фіксації кіберзлочинів до системного впливу на їхні детермінанти та зниження віктимності громадян.

Метою вдосконалення є синтез міжнародних превентивних моделей (правової, технічної, когнітивної) та їх адаптація до національного законодавства, що створює багаторівневий бар'єр проти загроз. Тому, синтез превентивних моделей на рівні держави та особи розглядається як єдина стратегічна умова для досягнення інтегрованої *національної кіберстійкості*, яка охоплює захист не лише технологічних систем, а й людського чинника.

У контексті кримінологічного забезпечення інформаційної безпеки, кіберстійкість необхідно розглядати як бінарну систему, що складається з макрорівня (держави) та мікрорівня (індивіда).

Кіберстійкість держави (макрорівень) представляє інституційну, технічну та правову здатність урядового апарату та критичної інфраструктури протистояти, швидко відновлюватися та адаптуватися до кібератак, зберігаючи при цьому виконання своїх ключових функцій.

Кіберстійкість індивіда (мікрорівень) є кримінологічною складовою і відображає поведінкову, освітню та психологічну здатність громадян розпізнавати, уникати, мінімізувати вплив кіберзагроз, що спрямовані на них.

Практична реалізація такого макро- та мікрорівневого синтезу вимагає комплексного оновлення державних механізмів протидії кіберзагрозам. Відповідно, ефективне вдосконалення кримінально-правової політики безпосередньо залежить від імплементації трьох взаємопов'язаних моделей: конвенційно-правової, інституційно-технічної та когнітивно-освітньої моделей.

Об'єктивна необхідність імплементації запропонованої архітектури національної кіберстійкості (конвенційно-правової, інституційно-технічної та когнітивно-освітньої моделей) безпосередньо підтверджується глобальними прогностичними трендами розвитку кібербезпеки на період до 2026 року [77, с.12-13]. Сучасна трансформація безпекового середовища відбувається під впливом низки системних факторів, які ставлять на перший план інтелектуальну автоматизацію, конфіденційність даних та інституційну довіру.

По-перше, визначальним вектором еволюції стає алгоритмізація наступальних та оборонних дій. У цих умовах штучний інтелект інтегрується як стратегічний «другий пілот» для команд з кібербезпеки, автоматизуючи виявлення загроз та частково компенсуючи гострий дефіцит кваліфікованих кадрів. Однак, попри стрімку автоматизацію, експертне середовище консолідовано визнає: штучний інтелект не здатен замінити тонке розуміння контексту. Саме тому збереження безапеляційного людського контролю для прийняття стратегічних рішень залишається критичним, що цілком підтверджує пріоритетність розбудови когнітивно-освітньої моделі.

По-друге, перехід до хмарних систем постійного моніторингу в режимі реального часу радикально змінює вимоги до управління даними. На відміну від абстрактних збоїв у системах, витік персональних медичних чи фінансових даних має безпосередній деструктивний вплив на громадян. Це стимулює суспільний запит на жорсткіше регулювання та розширення вимог щодо згоди.

Навіть в умовах певного відставання законодавства у сфері ШІ, імплементація існуючих рамок управління даними (стандартів GDPR та NIST AI Risk Management Framework) стає більш суворою, змушуючи розробляти системи з архітектурою вбудованої прозорості та підзвітності [317]. Зрештою, інтеграція зазначених технологічних та правових викликів формує новий глобальний критерій оцінки безпеки - довіру. У найближчій перспективі інституційна зрілість держави визначатиметься не формальним проходженням періодичних перевірок, а здатністю безперервно демонструвати проактивну стійкість, прозорість і надійність перед суспільством та міжнародними партнерами [288].

З огляду на те, що наведені глобальні макротренди підтверджують життєздатність та безальтернативність запропонованої архітектури національної кіберстійкості, виникає необхідність здійснити глибинний аналіз кожного її структурного елемента. Відтак, для повного розуміння того, як саме формується синергетичний ефект цієї багаторівневої системи, доцільно послідовно розкрити концептуальну сутність та практичне призначення конвенційно-правової, інституційно-технічної та когнітивно-освітньої моделей.

Перша, конвенційно-правова модель, яка передбачає глибинну гармонізацію національного законодавства з ключовими європейськими та міжнародними стандартами, зокрема з Директивою NIS2, Загальним регламентом про захист даних (GDPR) та Будапештською конвенцією. Ця модель створює необхідний нормативний каркас для уніфікованої кваліфікації новітніх кіберзлочинів. Лише за умови єдиного розуміння складу цифрового делікту з одночасним дотриманням балансу між високим рівнем мережевої безпеки (NIS2) та захистом прав суб'єктів даних (GDPR). стає можливим його результативне переслідування у транскордонному просторі.

Конвенційний підхід дозволяє нівелювати об'єктивні перешкоди у розслідуванні кіберінцидентів (транзитивність цифрових доказів, генерованих автономними алгоритмами, та заплутаність юрисдикційних меж). Це важлива складова національної та інформаційної безпеки, яка гарантує здатність

державних інституцій витримувати цифрові удари, адаптуватися до мінливих векторів атак та забезпечувати невідворотність покарання для кіберзлочинців через механізми міжнародної правової допомоги.

Онопрієнко С. та Онопрієнко О., визначають головною метою Конвенції досягнення синергії між кримінальним законодавством держав-учасниць, оптимізацію процесуальних процедур та інтенсифікацію міжнародної правової допомоги. Вчені констатують, що визнання глобального масштабу кіберзлочинності вимагає від міжнародної спільноти впровадження уніфікованих правових матриць, які дозволяють державам здійснювати синхронну та ефективну протидію кіберделіктам, повністю долаючи обмеження національних юрисдикцій [151, с. 257-259].

Нормативне закріплення складів кіберзлочинів у межах конвенційно-правової моделі є лише передумовою, ступінь дієвості цих матеріальних норм зводиться нанівець, якщо правоохоронна система не володіє адекватним інструментарієм для збору доказової бази та доведення вини у транскордонному середовищі. Продовженням удосконалення кримінально-правової політики є перехід від оновлення матеріального права до модернізації кримінального процесу, де ключовий напрям, відповідає думці С. М. Князева, щодо глобальної систематизації профільних нормативно-правових актів. За сучасних умов, на думку автора, обґрунтованою видається розробка окремого Закону України «Про інформаційну безпеку України» або комплексне рамкове оновлення чинних актів із визначенням їх місця системі. Реалізація цієї парадигми вимагає створення кодифікованого нормативно-правового акту, який визначав би фундаментальні принципи, об'єкти, суб'єктів, види актуальних загроз, інструменти правового реагування, гарантії прав людини, дієві форми парламентського, судового і громадського контролю. При цьому обов'язковою умовою такого рамкового акту має стати його системне та збалансоване співвідношення із суміжними законами про кібербезпеку, медіа, персональні дані, державну таємницю, електронні комунікації та критичну інфраструктуру, що дозволить усунути правові колізії та

забезпечить процесуальну ефективність правозастосування в цифровій екосистемі [82, с. 132].

В умовах повномасштабної кібервійни та формування архітектури повоєнної кіберстійкості, стратегічним напрямом вдосконалення вітчизняного законодавства є глибока імплементація спеціалізованих процесуальних механізмів Будапештської конвенції. Традиційні норми кримінального процесуального права виявляються недостатньо ефективними у транскордонному цифровому середовищі, де електронні докази можуть бути модифіковані або безповоротно знищені за лічені секунди, а сліди диверсій розпорошені між десятками іноземних юрисдикцій.

Відтак, першочерговим завданням реформування КПК України є адаптація наступних конвенційних інструментів до реалій правового режиму воєнного стану та повоєнного відновлення. По-перше, це стосується механізму превентивного збереження даних (ст. 16–17 Конвенції) [92]. Інтеграція процедур негайного збереження комп'ютерних даних дозволить вітчизняним слідчим упереджувати втрату критичної інформації ще до початку формального слідства та отримання тривалих міжнародних погоджень. По-друге, це торкається екстериторіального обшуку та вилучення цифрової інформації (ст. 19 Конвенції) [92]. Законодавство має забезпечити легітимний доступ правоохоронних органів до розподілених комп'ютерних систем, носіїв та хмарних сервісів. Можливість оперативного копіювання, блокування або вилучення даних є критичною умовою розслідування високотехнологічних воєнних злочинів та транснаціональних шахрайств. Третє, це динамічний моніторинг (ст. 20–21 Конвенції) [92]. Перехоплення трафіку та доступ до переданих даних у режимі реального часу формують техніко-юридичний базис для виявлення та документування триваючих кібероперацій агресора або транснаціональних злочинних синдикатів.

Еволюція конвенційно-правової моделі не обмежується технічними чи фінансовими деліктами, а системно охоплює захист суспільної моралі та

цінностей у цифровому вимірі. Етапом такої еволюції стало прийняття у 2003 році Додаткового протоколу до Будапештської конвенції, який імперативно вимагає криміналізації діянь расистського та ксенофобського характеру, вчинених із використанням комп'ютерних систем (CETS No. 189) [49]. Він розширює сферу дії Конвенції, офіційно визнаючи на глобальному рівні, що транскордонне цифрове середовище становить собою не лише технологічну інфраструктуру, а й потужний інструмент масової трансляції нетерпимості, дискримінації та мови ворожнечі. У цьому контексті, О. Онопрієнко та С. Онопрієнко зазначають, позитивне прагнення України не лише механічно адаптувати міжнародні стандарти до специфіки національного контексту, а й виступати повноправним, спроможним суб'єктом міжнародного права. Вона підтверджує готовність України бути активним учасником глобального процесу формування правової моделі цифрової епохи, здатної ефективно протистояти гібридним загрозам та інформаційно-психологічним операціям [151].

Гончарук В. доводить, що внесення комплексних змін до матеріального та процесуального законодавства України є не теоретичною забаганкою, а нагальною потребою правозастосовної практики. Ця необхідність продиктована системними процесуальними колізіями, які виникають на етапах досудового розслідування високотехнологічних деліктів та безпосередньо під час судового провадження, де ключовим каменем спотикання залишається верифікація та належна правова оцінка електронних доказів [34, с. 181].

Другим напрямом вдосконалення національної політики є імплементація інституційно-технічної моделі, яка забезпечує практичну життєздатність оновлених матеріальних та процесуальних норм. Ця модель базується на двох елементах: забезпеченні балансу між безпекою та правами людини, а також розбудові інфраструктури транскордонної взаємодії.

З внесенням змін до Закону України «Про захист інформації в інформаційно-комунікаційних системах» [169] змінено підходи до захисту інформації в інформаційно-комунікаційних системах від несанкціонованого

доступу, витоку технічними каналами, поки що залишено без змін. Так, державні інформаційні ресурси або інформація з обмеженим доступом мають оброблятися в авторизованих системах з безпеки чи шляхом отримання сертифіката відповідності стандарту інформаційної безпеки (не застосовується до інформаційно-комунікаційних систем, в яких обробляється державна таємниця) [153, с. 184-185].

Водночас, класична парадигма безпеки, що базується на статичній сертифікації та формальних контрольних списках відповідності, вичерпує свою ефективність перед обличчям безпрецедентної еволюції глобальних кіберзагроз. Сьогодні фундаментальним викликом для інституційного контролю стає феномен «тіньового штучного інтелекту» - масове використання несанкціонованих або неліцензованих алгоритмічних систем, що функціонують в організаціях поза межами офіційних контурів безпеки. Відсутність регламентованих політик управління такими інструментами (що фіксується у 60% організацій) підвищує вартість ліквідації наслідків витоків даних [287].

Більше того, технологічний ландшафт загроз стрімко ускладнюється. Значне зростання технологій генерування дипфейків (на 1500% у період 2023–2025 рр.) вивело соціальну інженерію, дезінформаційні кампанії та шахрайство з ідентифікаційними даними на якісно новий рівень переконливості. Сучасні транснаціональні злочинні угруповання активно використовують ШІ для розробки адаптивного, поліморфного шкідливого програмного забезпечення, експлуатації вразливостей великих мовних моделей та повної автоматизації фішингових операцій [77, с.11-12]. Ця асиметрія загроз безальтернативно змушує державні та корпоративні сектори впроваджувати власні контрзаходи на базі ШІ для безперервної предиктивної оцінки небезпек.

Окремим стратегічним викликом, що ставить під загрозу існуючі стандарти захисту інформації з обмеженим доступом, є наближення ери квантових обчислень. Їхня прогнозована здатність дешифрувати сучасну криптографію з відкритим ключем вимагає від держави невідкладного

планування переходу до квантово-стійких алгоритмів шифрування. Паралельно розширення екосистеми автономних ШІ-агентів формує нові вектори атак, зокрема експлойти нульового кліку та складні сценарії підвищення привілеїв, які вкрай важко ідентифікувати традиційними засобами моніторингу [77, с.11].

У відповідь на ці виклики система забезпечення інформаційної безпеки вимагає комплексної трансформації. Окрім жорсткого інституційного контролю за використанням ШІ та безперервного когнітивного тренування персоналу необхідна модернізація технічних протоколів, зокрема, перехід до безпарольних стандартів аутентифікації, що є стійкими до фішингу. Для забезпечення національної кіберстійкості у перспективі держава повинна здійснити концептуальний перехід від реактивної моделі відповідності стандартам до проактивної, дата-центричної системи безперервного управління ризиками.

Розширення процесуальних повноважень правоохоронних органів вимагає вдосконалення інституційних механізмів стримувань і противаг. З урахуванням євроінтеграційного курсу України, імплементація таких інструментів має супроводжуватися дієвими гарантіями. Законодавчі та інституційні зміни повинні забезпечити безумовний судовий контроль за кіберслідчими діями, процедурну прозорість та повну відповідність стандартам захисту персональних даних, зокрема вимогам європейського GDPR [275].

Практичне дотримання цього правозахисного балансу залишається надзвичайно складним викликом, оскільки об'єктивна реальність диктує свої суворі умови. Безперечно, сучасні високотехнологічні кримінальні правопорушення, вчинені з використанням новітніх гід- та блокчейн-технологій, генерують колосальні економічні збитки. У таких реаліях навіть незначний програмний збій чи цілеспрямоване несанкціоноване втручання здатні спровокувати пряму загрозу життю людей та призвести до катастроф національного чи навіть глобального масштабу. Більше того, експоненційне зростання глобальних комп'ютерних і телекомунікаційних мереж та повсюдний, неконтрольований доступ до них багаторазово посилюють можливості їх

використання для здійснення професійної кримінальної діяльності транснаціональним організованим злочинним світом [126].

Князев С. М. зазначає, що інформаційна безпека не повинна бути сформульована лише мовою ризиків і загроз, вона має залишатися юридично сумісною з правом на інформацію, свободою поглядів, правом на приватність та загальними гарантіями захисту прав і свобод людини та громадянина. Саме тому будь-які обмеження в інформаційній сфері повинні мати чітку законодавчу основу, бути предметно визначеними, пропорційними та прозорими. У практичному вимірі це означає необхідність уникати розмитих підстав для втручання у сфері медіа, запроваджувати сучасні європейські стандарти обробки, мінімізації та безпечного зберігання інформації у сфері персональних даних, а також унеможливити у сфері доступу до публічної інформації перетворення безпекових потреб на підставу для необґрунтованого обмежування доступу до суспільно значущих відомостей [82, с. 132-133].

Окремим, техніко-юридичним напрямом розбудови цієї моделі є повноцінне включення України у міжнародний контур протидії кіберзагрозам. Будапештська конвенція закладає фундамент такої транскордонної взаємодії через механізми взаємної правової допомоги (ст. 25–34), екстрадиції (ст. 24) та функціонування мережі контактних пунктів «24/7» (ст. 35) [92]. Україна ратифікувала Будапештську конвенцію із певними застереженнями. Цей крок був продиктований об'єктивною необхідністю узгодження універсальних міжнародних норм із фундаментальними принципами національного кримінального права. Насамперед це стосувалося збереження жорстких вимог щодо чіткого визначення складу кримінального правопорушення, встановлення пропорційних меж кримінальної відповідальності та регламентації допустимості використання технічних засобів як об'єкта і засобу правового регулювання. Застосування такого підходу дозволило Україні зберегти рівень гнучкості у формуванні суверенної внутрішньої правової політики, не порушуючи загальної логіки та духу міжнародної співпраці.

Свідченням того, що ці застереження не стали кроком до ізоляції, є глибока інтеграція нашої держави у глобальний безпековий простір. Україна не лише імплементує іноземний досвід, а й виступає активним співтворцем міжнародного кіберправа коли бере постійну участь у роботі Комітету Конвенції про кіберзлочинність Ради Європи (Т-СУ) та безпосередньо долучається до розробки стратегічних директивних записок. Водночас повноцінна інтеграція в європейську систему цифрової безпеки забезпечується через поглиблену співпрацю з ключовими агентствами Європол, INTERPOL та Агентством ЄС з кібербезпеки (ENISA). Спільні масштабні тренінги, оперативний обмін розвідувальною інформацією та розробка уніфікованих стандартів дозволяють українським правоохоронним структурам нарощувати власний інституційний потенціал та ефективно реагувати на транснаціональні загрози будь-якого рівня складності.

Для України розбудова цієї інфраструктури означає перехід від ситуативного реагування до системної та технічно захищеної співпраці у режимі реального часу. Наявність безпечних каналів зв'язку та уніфікованих протоколів дозволяє вітчизняним правоохоронцям оперативно обмінюватися розвідувальною інформацією з іноземними партнерами, долати бар'єри національних юрисдикцій та формувати єдиний фронт переслідування транснаціональних кіберзлочинців. Нагальність розбудови такої транскордонної взаємодії зумовлена тим, що кіберзагрози давно вийшли за межі традиційних фінансових чи технічних посягань, набувши форми глобальних інформаційно-психологічних операцій. У цьому контексті показовим є аналітичний висновок експерта Google Дж. Коена щодо специфіки російських інформаційних атак, які сьогодні реалізуються за кількома ключовими векторами [164].

Зокрема, масштабні дезінформаційні кампанії цілеспрямовано розгортаються для штучного стимулювання соціального невдоволення українськими біженцями на території європейських держав. Шляхом поширення у соціальних мережах фейкових наративів про нібито злочинну діяльність та

привілейоване становище переміщених осіб, держава-агресор намагається підірвати рівень суспільної та політичної підтримки України у світі. Крім того, інформаційна війна безпосередньо проникає у повсякденний когнітивний простір громадян інших держав, де зусилля агресора фокусуються на дискредитації українців та маніпулюванні свідомістю на користь Росії [164].

Важливо наголосити, що технічне забезпечення цих атак базується на комбінованому використанні людського ресурсу (тролів) та вдосконалених алгоритмічних систем (ШІ-чатботів), швидкості яких більшість транснаціональних технологічних платформ наразі не здатні ефективно протистояти. Зрештою, найбільш радикальним вектором цієї дезінформаційної агресії є використання медійних маніпуляцій для прямого підбурювання та виправдання актів крайнього насильства.

Слушно зазначає Ільницька У., що національний інформаційний простір України, на жаль, зазнає суттєвих загроз, викликів, які становлять небезпеку функціонування держави, її політичного та економічного розвитку, інтеграції у європейські та євроатлантичні структури [67, с. 29].

Третім, інтегруючим вектором вдосконалення національної політики виступає імплементація когнітивно-освітньої моделі, яка концептуально поєднує розвиток людського капіталу з інноваційними технологіями. Її фундаментальним пріоритетом є розбудова програм кібергігієни для громадян та спеціалізованої техніко-юридичної підготовки для співробітників правоохоронних органів і сектору безпеки. Оскільки лєвова частка сучасних технологічних деліктів базується на експлуатації «людського фактора», саме превентивна освітня діяльність стає базою оборони інформаційного простору.

Окремим викликом для сучасної системи забезпечення інформаційної безпеки та оновлення освітньої моделі є стрімка інтеграція технологій ШІ у сферу оборони та національної безпеки, що маркує перехід до так званих «війн шостого покоління» [38]. Це технологічно-правові виклики інституціоналізації обумовлені фактором тотального використання штучного інтелекту.

Слушно зазначають, Бібік А. В., Городиський Р. О., Ваврічен О. А, що практичний досвід відсічі збройній агресії РФ засвідчив, що ШІ став чинником підвищення ефективності управління, через функціонування системи обізнаності Delta та програмно-аналітичних комплексів розвідки, які забезпечують новий рівень обробки даних із супутників, БпЛА та джерел OSINT [10, с.34-35]. Проте широке впровадження таких інтелектуальних систем зумовлює не лише технічні, а й фундаментальні когнітивно-правові виклики. Комплексне реформування підготовки фахівців має спиратися на законодавче фіксування принципу «людина в контурі управління». У межах когнітивної моделі цей принцип означає навчання операторів взаємодіяти зі штучним інтелектом виключно як з аналітичним радником. Навичка критичного осмислення машинних висновків є життєво необхідною, оскільки фінальне рішення має залишатися за людиною, це критично важливо для дотримання норм міжнародного гуманітарного права та чіткого визначення меж кримінально-правової відповідальності.

Паралельно з цим, спеціалізована підготовка має охоплювати сферу інформаційно-психологічної протидії та когнітивного захисту. Використання ШІ для виявлення бот-мереж, автоматизованого аналізу деструктивних кампаній та верифікації фейків дозволяє суттєво мінімізувати ризики поширення неправдивих даних, які безпосередньо загрожують стабільності управлінських рішень у зоні бойових дій [10, с. 35]. Саме розбудова спроможності персоналу працювати в межах цієї гібридної моделі, коли машина швидко опрацьовує дані, а людина зберігає безапеляційний контроль над етичними, гуманітарними та стратегічними аспектами, є кінцевою метою сучасної когнітивно-освітньої моделі забезпечення кіберстійкості.

У контексті практичної реалізації когнітивно-освітньої моделі, її організаційний аспект має першочергово включати створення спеціалізованих навчальних програм для офіцерського складу та правоохоронців у межах національних проєктів цифрової трансформації. Саме безперервне навчання

дозволить сформуванню стійкої гібридної моделі прийняття рішень на практиці. Безпечна інтеграція ШІ вимагає створення нової когнітивно-етичної рамки, у якій технологічна перевага машинних алгоритмів гармонізується з жорстким правовим регулюванням, етичними стандартами та збереженням людського контролю над стратегічно важливими процесами. Саме за умови впровадження таких когнітивних та етичних запобіжників (фахово підготовленого персоналу та захищених даних) відкривається можливість повноцінної, безпечної реалізації операційного потенціалу штучного інтелекту. Сьогодні він перетворюється на інструмент протидії новітнім кіберзагрозам. Ця технологічна перевага базується на здатності ШІ здійснювати надшвидкий глибинний аналіз надвеликих масивів даних (Big Data), ідентифікувати латентні закономірності в аномальній мережевій активності та вибудовувати високоточні предиктивні сценарії розвитку кібератак ще до моменту їхньої активної фази.

Формування таких професійних компетенцій у межах когнітивно-освітньої моделі забезпечує фундаментальну зміну методології кіберзахисту. Навчений персонал, взаємодіючи з інтелектуальними системами, отримує можливість здійснити остаточний перехід від застарілих методів реагування на інциденти до сучасних адаптивних і проактивних парадигм. Такий гібридний підхід здатний ідентифікувати та нейтралізувати загрози випереджально, ще на етапі мережевої розвідки чи підготовки інфраструктури правопорушниками.

Необхідність стратегічного фокусу на компетентнісному підході підтверджується актуальними світовими тенденціями. Зокрема, результати глобального дослідження «Кадри в галузі кібербезпеки до 2025 року» (на основі опитування понад 16 тисяч фахівців) засвідчують фундаментальний зсув на ринку праці: вразливістю сучасних безпекових підрозділів є не кількісний дефіцит персоналу, а якісний брак спеціалізованих навичок [260]. Незважаючи на стабілізацію економічного тиску та оптимізацію бюджетів, близько третини організацій досі констатують фінансову неспроможність залучити фахівців належної кваліфікації. Наслідки такого голоду є критичними: 88% респондентів

знали щонайменше одного серйозного інциденту безпеки, безпосередньо зумовленого недостатнім рівнем підготовки персоналу.

Емпіричні дані вказують на те, що найбільш гострий дефіцит знань фіксується у сферах безпеки хмарних технологій та експлуатації штучного інтелекту. На тлі стрімкої інтеграції ШІ-інструментів (які вже імплементують або тестують 69% організацій), майже половина практиків змушена опановувати ці технології шляхом несистемної самоосвіти. Водночас професійна спільнота чітко усвідомлює масштаб трансформацій: понад 70% експертів прогнозують, що ШІ згенерує нові спеціалізовані ролі та вимагатиме від фахівців поглибленого стратегічного мислення [260].

Така трансформація вимог до когнітивних здібностей фахівців оголює системну кризу класичних механізмів кадрового забезпечення. Сьогодні формування кадрового резерву у сфері кібербезпеки перетворилося на інституційний виклик: еволюція загроз відбувається значно швидше, ніж відтворення кваліфікованої робочої сили. Як наслідок, державні та приватні структури втрачають здатність оперативно укомплектовувати критично важливі підрозділи. Згідно з аналітичною доповіддю Всесвітнього економічного форуму «Глобальний прогноз у сфері кібербезпеки на 2024 рік» (Global Cybersecurity Outlook 2024), 71% організацій констатують наявність незакритих вакансій. Цей дефіцит залишається головною перешкодою для розбудови кіберстійкості, адже він відображає кількісну нестачу персоналу, а саме брак висококваліфікованих аналітиків, здатних захищати складні гібридні системи [277, с. 18-25].

Усвідомлюючи ризики, передові інституції починають змінювати кадрову парадигму: на зміну формальній оцінці дипломів приходить пріоритетизація реальних прикладних компетенцій. У межах сучасного компетентнісного підходу роботодавці все частіше застосовують сценарно-орієнтовані співбесіди (симуляції). Це дозволяє об'єктивно оцінити саме когнітивні здібності кандидата: швидкість стратегічного мислення під стресовим тиском, алгоритми

пріоритетизації ризиків та здатність до прийняття рішень, що є набагато ціннішим за формальний перелік регалій [280].

Крім того, базовою вимогою функціонування сучасних команд стає організаційна гнучкість. З огляду на те, що високотехнологічні інциденти не прив'язані до географічного розташування, відмова від гнучких або дистанційних моделей роботи штучно і безпідставно звужує кадровий резерв. Потреба у вузькопрофільних фахівцях (з хмарної безпеки, реагування на інциденти та управління ризиками) формує стійкий глобальний тренд: кількість незакритих вакансій у світі зростає з 1 мільйона у 2013 році до стабільних 3,5 мільйонів у період 2021–2023 років [77, с.15].

Окремим викликом для когнітивно-освітньої моделі стає психоемоційний стан персоналу. Попри високий загальний рівень професійної мотивації та впевненості у затребуваності своєї спеціальності, майже половина фахівців відчуває хронічне виснаження та перевантаження через необхідність безперервного моніторингу еволюціонуючих загроз.

З огляду на це, стратегічним імперативом для інституційного сектору безпеки стає зміна управлінської парадигми. Як підсумовують аналітики ISC2, сьогодні пріоритетом є не звичайний найм нових співробітників, а інтенсивний розвиток наявного кадрового потенціалу. Це вимагає системних інвестицій у підвищення кваліфікації та впровадження моделей управління робочим навантаженням [77, с. 8]. Експертиза у сфері штучного інтелекту не може розглядатися як опціональна навичка, вона стає стратегічною необхідністю для подолання кадрового дефіциту та мінімізації ризиків інституційних збоїв.

Системне вирішення цих технологічних вразливостей, поєднане з ефективним правовим регулюванням, здатне гарантувати безперебійність і високу надійність систем кіберзахисту. У глобальному вимірі це створює передумови для формування стійкої, інтелектуальної інформаційної безпеки України, здатної адаптуватися до мінливого ландшафту транснаціональних кіберзагроз майбутнього [38, с. 17].

Водночас, практична розбудова такої інноваційної екосистеми неможлива без її концептуального закріплення на рівні державного планування. Як слушно зазначає професор Н. С. Юзікова, для України, враховуючи перманентний характер гібридних атак, критично важливо мати комплексну та багаторівневу стратегію кібербезпеки. Ця стратегія повинна ґрунтуватися на досвіді та практиках зарубіжних країн, враховуючи унікальні оборонні потреби та виклики нашої держави [227].

Відповідно до такого підходу, оновлена Національна стратегія кібербезпеки має охоплювати низку ключових елементів. Насамперед, ідеться про системне збільшення інвестицій у сферу кібербезпеки, а також про формування потужного кадрового резерву кіберфахівців. Цей резерв має бути готовим до оперативної мобілізації у разі виникнення критичних кіберінцидентів для безпосереднього посилення штатних кіберпідрозділів у складі ЗСУ та СБУ; підвищення обізнаності широкого кола громадян України про кіберзагрози та формування навичок захисту від них; співпрацю з міжнародними партнерами, такими як НАТО, ЄС та ін.

Кіберстійкість держави (макрорівень) представляє інституційну, технічну та правову здатність урядового апарату та критичної інфраструктури протистояти, швидко відновлюватися та адаптуватися до кібератак, зберігаючи при цьому виконання своїх ключових функцій.

Своєю чергою, кіберстійкість індивіда (мікрорівень) є віктимологічною та кримінологічною складовою, що відображає поведінкову, освітню та психологічну здатність громадян розпізнавати, уникати та мінімізувати вплив спрямованих на них кіберзагроз.

Ці рівні є взаємозалежними елементами. Практика доводить, що найслабша ланка (зокрема, особа, яка піддається маніпуляціям соціальної інженерії) здатна скомпрометувати найбільш захищену державну систему. Усвідомлення цієї бінарності є елементом, де національна кіберстійкість виступає як стратегічна мета, яка досягається лише тоді, коли державні

механізми (макрорівень) створюють надійну безпекову рамку, а суспільство (мікрорівень) володіє достатнім когнітивним імунітетом, перетворюючись на самозахисний бар'єр проти кіберзагроз.

Безпосереднім практичним кроком виступає перспективна інтеграція результатів даного дослідження у навчальний процес Дніпровського національного університету імені Олеся шляхом запровадження спецкурсу «Правові засади кіберстійкості та цифрова держава», у межах якого, буде розглянуто багаторівневу модель національної кіберстійкості як складної бінарної системи, що органічно поєднує макрорівень (інституційні та правові механізми держави) та мікрорівень (віктимологічну безпеку індивіда). Міждисциплінарна програма охоплюватиме аналіз державно-правової діалектики між забезпеченням фундаментальних прав людини та імперативами національної безпеки, вивчення впливу алгоритмічних систем (зокрема штучного інтелекту) на публічне управління, а також аналіз сучасних транснаціональних інформаційно-психологічних операцій.

Висновок до третього розділу

1. Проведений компаративний аналіз світових макромоделей нормативно-правового регулювання кіберпростору свідчить про трансформацію підходів: від стратегії статичного захисту периметра до моделі активної кіберстійкості. Універсальної моделі не існує; її ефективність досягається через поєднання чотирьох вимірів: стратегічного (кіберпростір як сфера національних інтересів), нормативного (гнучке законодавство, орієнтоване на реальну шкоду), інституційного (мережеві структури типу ENISA чи CISA) та екосистемного (розбудова потенціалу, *capacity building*).

Зарубіжна практика дозволяє виокремити три ключові макромоделі: англосаксонську з гнучким державно-приватним партнерством, стимулюванням приватних інвестицій та гнучким правозастосуванням; континентальну з наднаціональною стандартизацією, жорстким контролем та пріоритетом захисту прав людини і транзитну з високою динамікою інституційного розвитку та прискореним впровадженням технічних засобів в умовах перманентних гібридних загроз.

Для України механічне копіювання однієї парадигми є недоцільним, прийнятним є синтез найкращих елементів: імплементація мілітаризованої проактивної доктрини за зразком США та Ізраїлю (активне кіберстримування); суворо гармонізація законодавства з Директивою ЄС NIS2 та актом CRA (персональна відповідальність керівництва критичної інфраструктури); запозичення британського досвіду створення єдиного міжвідомчого координаційного центру, а також адаптація досвіду країн Балтії та Польщі щодо захисту когнітивного суверенітету.

2. Обґрунтовано загальний та спеціальний рівні міжнародного співробітництва у сфері протидії транснаціональній кіберзлочинності, що дозволило визначити зміну міжнародно-правового статусу України. Екстериторіальна природа кіберправопорушень, їх масштабування за рахунок штучного інтелекту та перетворення на інструмент гібридної війни диктують

безальтернативну необхідність інтеграції держави у глобальний безпековий простір на двох рівнях:

- загальний (стратегічний та нормативно-правовий) рівень, що забезпечує політичну єдність та подолання асиметрії національних юрисдикцій шляхом гармонізації вітчизняного законодавства з міжнародними актами (Будапештська конвенція, Директива NIS2, нова Конвенція ООН про боротьбу з кіберзлочинністю 2025 року), а також стимулює формування макрорегіональних коаліцій (Талліннський механізм) для захисту критичної інфраструктури;
- спеціальний (інституційний та оперативно-тактичний) рівень який втілюється у правозастосовну практику завдяки мережевій взаємодії правоохоронних органів України. Вона включає безперервний обмін розвідувальними даними та індикаторами компрометації в режимі реального часу через канали Європолу за підтримки НАТО та ОБСЄ.

Доведено, що завдяки успішній інтеграції у спільні поліцейські операції відбувся остаточний перехід України від ролі пасивного реципієнта допомоги до статусу активного і важливого учасника колективної європейської безпеки. Ключовим кроком у цьому напрямі визначено секторальну інтеграцію України до міжнародної екосистеми безпеки ШІ шляхом заснування національного Інституту безпеки ШІ (за прикладом Інституту безпеки штучного інтелекту Великобританії та Офісу ШІ ЄС), що виступатиме головним транскордонним хабом.

3. Доведено, що вдосконалення кримінологічного забезпечення інформаційної безпеки України потребує фундаментального переходу від реактивної моделі до проактивної системи управління ризиками, яка базується на розумінні кіберстійкості як складної бінарної системи. Ефективність цієї системи безпосередньо залежить від синергії макрорівня (захищеності державних інституцій) та мікрорівня (віктимологічної безпеки індивіда), де головним інструментом інтеграції є формування суспільного «когнітивного імунітету». Без

належної когнітивної стійкості громадян навіть найдосконаліші технічні системи безпеки залишатимуться вразливими, оскільки саме людина є головною мішенню ворожої соціальної інженерії.

Авторська модель розвитку національної кіберстійкості об'єднує три превентивні складові: а) конвенційно-правову, яка полягає у гармонізації стандартів управління даними та регулювання ризиків штучного інтелекту; б) інституційно-технічну, що полягає у безперервному моніторингу загроз, контролі «тіньового ШІ»; в) когнітивно-освітню, яка проявляється у компетентнісному підході до подолання кадрової кризи, підвищенні правової культури та віктимологічній безпеці населення через масштабні просвітницькі кампанії проти алгоритмізованого шахрайства.

Прикладним інструментом практичного впровадження результатів дослідження в освітній процес визначено розробку та впровадження в Дніпровський національний університет імені Олеся Гончара авторського міждисциплінарного спецкурсу «Правові засади кіберстійкості та цифрова держава». Навчальна дисципліна спрямована на формування у майбутніх фахівців (правників, політологів, психологів, журналістів, соціологів) крос-функціональних компетентностей для ефективної протидії гібридним загрозам, захисту критичної інфраструктури, подолання «техногенної віктимності» організацій та забезпечення сталого повоєнного розвитку України.

ВИСНОВКИ

За результатами дисертаційного дослідження, здійснено комплексне обґрунтування кримінологічних засад забезпечення інформаційної безпеки в міжнародному, національному та зарубіжному вимірах в умовах воєнного стану, гібридної війни та активного розвитку технологій штучного інтелекту. Основні результати дослідження, що відображають вирішення поставлених наукових завдань, полягають у наступному:

1. Наукове осмислення сутності, змісту та рівнів інформаційної безпеки як об'єкта кримінологічного захисту та правової превенції полягає у розробці комплексної тривірневої моделі, яка базується на розширеній міжнародній матриці безпеки Тріаді СІА (конфіденційність, цілісність, доступність), яку доповнено процесуальними елементами автентичності й неспростовності та структурно розподілено на інфраструктурний, правовий (інформаційно-регуляторний) і соціально-психологічний (когнітивний) рівні. Такий підхід дозволяє виявити наскрізний характер сучасних кіберзагроз, визначити специфічні напрями проактивної превенції для кожного з рівнів та обґрунтувати антропоцентричний пріоритет захисту суспільної свідомості, процесу формування волі й цифрових прав і свобод людини від протиправних маніпулятивних впливів.

2. Проаналізовано генезис вітчизняної наукової думки, що пройшла шлях від вузького розуміння безпеки як технічного захисту даних (І етап: 1991–1996 рр.), через правову концептуалізацію (ІІ етап: 1997–2000 рр.) та міжнародну гармонізацію (ІІІ етап: 2001–2013 рр.) до обґрунтованого нами четвертого етапу (з 2014 року до сьогодні), який зумовлений воєнними викликами і кардинально відрізняється від попередніх періодів своєю онтологічною природою, оскільки характеризується переходом від реактивного технічного захисту до формування цілісної державної функції та стратегічної кіберстійкості держави. У межах цього етапу уточнено понятійно-категоріальний апарат через

чітке розмежування загального поняття «інформаційна безпека» (як захисту свідомості та нецифрових даних) і вузких технологічних категорій «кібербезпека» та «цифрова безпека», що дозволило конкретизувати межі предмета кримінологічного захисту.

На основі узагальнення зарубіжної наукової думки з'ясовано, що на відміну від вітчизняних досліджень, орієнтованих на правову кодифікацію та стратегічне планування, західна доктрина відзначається високим рівнем математизації та техноцентризму (використання Байєсівських мереж, теорії ігор та марковських моделей для прогнозування атак). Однак доведено, що ключовим недоліком західних моделей є ігнорування динамічної поведінки правопорушника та людського фактора, що обмежує їхню ефективність для повної кримінологічної превенції й актуалізує потребу впровадження антропоцентричного підходу.

3. З'ясовано, що принципи та механізми міжнародно-правового забезпечення інформаційної безпеки у протидії транснаціональним кіберзагрозам потребують адаптації до умов глобальної кризи доведення джерела атак. Обґрунтовано науковий підхід до розуміння сутності інформаційної безпеки держави, що ґрунтується на інтеграції правових, соціальних та етичних аспектів у єдину систему захисту й гармонізації міжнародних стандартів (зокрема, Будапештської конвенції та GDPR) із національними правовими традиціями. Визначено засади реалізації принципу невідворотності кримінальної відповідальності у цифровому середовищі шляхом інтеграції техніко-юридичного елемента «неспростовності» до системи доказування, що дозволяє юридично нейтралізувати використання злочинцями систем анонімізації та транскордонної маршрутизації трафіку.

Обґрунтовано чотирирівневий механізм, який через поєднання процесуальних можливостей Будапештської конвенції та матеріальних норм міжнародного гуманітарного права забезпечує алгоритм притягнення агресора до юридичної відповідальності за вчинені кібератаки на рівнях: процесуальної

атрибуції атак; легітимізації цифрових доказів для міжнародних трибуналів; доведення транснаціонального злочинного умислу; техніко-юридичної кваліфікації кібератак як воєнних злочинів.

Визначено, що прийняття у 2025 році під егідою УНП ООН Конвенції про запобігання, припинення та боротьбу з кіберзлочинністю закладає основу для уніфікації криміналізації та оперативного обміну даними. Доведено, що гармонізація законодавства України з принципами FISMA, Директиви NIS2 та нової Конвенції ООН дозволяє трансформувати унікальний вітчизняний бойовий досвід у системний правовий механізм захисту національних інтересів і цифрового суверенітету держави.

4. Доведено, що функціонування системи забезпечення інформаційної безпеки в умовах правового режиму воєнного стану вимагає стратегічного переходу сектору безпеки від реактивної моделі до проактивного реагування. Сформульовано кримінологічну характеристику кіберзлочинності в умовах воєнного стану, до якої включено новітні фактори криміногенного ризику штучного інтелекту та Інтернету речей (IoT). Обґрунтовано доцільність криміналізації нових цифрових загроз, зумовлених воєнним станом та технологічним прогресом, зокрема, створення та поширення згенерованого за допомогою ШІ синтетичного контенту експлуатації дітей (дипфейків).

5. Розкрито сучасні законодавчі та інституційні засади забезпечення інформаційної безпеки в Україні. Ліквідація наявних правових прогалів має базуватися на впровадженні випереджальних превентивних механізмів, які враховують поведінкові ризики та соціальні фактори протиправності. З метою нейтралізації системних кіберзагроз обґрунтовано дворівневий розподіл поняття «кіберстійкість» на державний (публічно-правовий) та особистісний (людиноцентричний) рівні. «Кіберстійкість держави» визначено як стратегічну спроможність підтримувати критичні функції, адаптуватися до гібридних загроз та відновлювати цифрову інфраструктуру на основі інституційної координації

сектору безпеки (МВС, Нацполіція, ЦПД), управління ризиками ланцюгів постачання та впровадження метрик кіберзрілості.

6. Формування балансу між свободою та безпекою є ключовим викликом сучасної інформаційної політики. Надмірний контроль загрожує порушенням прав людини, тоді як його відсутність створює умови для кіберзлочинності та інформаційних атак. Оптимальне рішення полягає у поєднанні глобальних принципів із національною правовою традицією, що забезпечує ефективність кримінологічного захисту та збереження демократичних цінностей. Такий підхід дозволяє створити правову систему, здатну реагувати на сучасні загрози, не порушуючи фундаментальних прав і свобод.

Розкрито специфіку та багаторівневу структуру кримінологічної превенції крізь призму забезпечення справедливої рівноваги між свободою слова, захистом державного суверенітету та цифровими правами людини. У цьому контексті обґрунтовано концепцію «когнітивного імунітету» нації як невід’ємного виміру інформаційної безпеки, що базується на зарубіжному досвіді розбудови потенціалу (capacity building) та передбачає докорінний перехід від захисту виключно технічного периметра до формування стійкості людського капіталу. Запропоновано визначення «когнітивного імунітету суспільства» як самостійної кримінологічної та віктимологічної категорії, що визначає здатність громадян виступати внутрішнім самозахисним бар’єром проти транснаціональних інформаційно-психологічних операцій (ІПСО) та цифрового шахрайства.

7. Проаналізовано досвід зарубіжних стратегій забезпечення інформаційної безпеки та запропоновано підхід до класифікації моделей забезпечення кіберстійкості. Виокремлено чотири взаємозалежні виміри цих моделей: стратегічний, нормативний, інституційний та екосистемний, що дозволяє комплексно оцінювати рівень кіберзрілості держави і суспільства за міжнародними стандартами та визначати конкретні шляхи модернізації українського законодавства. Представлено віктимологічний підхід до запобігання кіберзлочинності через обґрунтування змісту «техногенної

віктимності» організацій (на основі аналізу міжнародного досвіду використання хмарних сервісів), де провідним чинником посягань визначено організаційну недбалість у налаштуваннях конфігурацій та договірній підзвітності.

8. Обґрунтовано загальний та спеціальний рівні міжнародного співробітництва у сфері протидії транснаціональній кіберзлочинності, що дозволило визначити зміну міжнародно-правового статусу України в системі європейської кібербезпеки. Доведено, що завдяки успішній інтеграції правоохоронних органів України у спільні транскордонні поліцейські операції та системи обміну розвідувальними даними (Європол, мережа SIENA), відбувся остаточний перехід України від ролі пасивного реципієнта (об'єкта захисту) до статусу активного, стратегічно важливого учасника колективної європейської безпеки.

9. Запропоновано перспективні напрями вдосконалення кримінологічного забезпечення інформаційної безпеки в Україні в умовах розвитку технологій штучного інтелекту. Для практичної реалізації європейських безпекових стандартів розроблено концептуальний підхід щодо приєднання до європейської системи кібербезпеки та інтеграції авторської пропозиції стосовно заснування національного Інституту безпеки ШІ (за прикладом Інституту безпеки штучного інтелекту Великої Британії). Зазначена інституція має виступати головним координаційним хабом для впровадження міжнародних стандартів у вітчизняну практику запобігання, виявлення і розслідування високотехнологічних кіберзлочинів. Крім того, з метою практичного впровадження результатів дослідження в освітній процес, запропоновано авторський міждисциплінарний спецкурс «Правові засади кіберстійкості та цифрова держава» для підготовки нової генерації фахівців, здатних забезпечувати когнітивний імунітет суспільства та сталий повоєнний розвиток України.

10. Запропоновано авторський міждисциплінарний спецкурс «Правові засади кіберстійкості та цифрова держава» як прикладний інструмент практичного впровадження результатів дисертаційного дослідження в освітній

процес Олеся Гончара Дніпровського національного університету. Навчальна дисципліна спрямована на підготовку нової генерації фахівців (правників, політологів, соціологів), які володітимуть крос-функціональними компетентностями для ефективної протидії гібридним загрозам, захисту критичної інфраструктури та формування когнітивного імунітету суспільства в умовах сталого повоєнного розвитку України.

Список використаних джерел

1. Авдєєва Г.К. Проблеми використання спеціальних знань у кримінальному провадженні в умовах воєнного стану в Україні. Збірник статей: *Питання боротьби зі злочинністю*. 2022. № 43 том 1. URL: <http://pbz.nlu.edu.ua/issue/view/15815> . (дата звернення: 15.04.2024)
2. Азаров Д. С. Кримінальна відповідальність за злочини у сфері комп'ютерної інформації : дис. ... канд. юрид. наук : 12.00.08 / НАНУ. Інститут держави і права ім. В.М. Корецького. К., 2002. 228 с
3. Аніщук В. В. Інформаційна безпека як об'єкт посягання злочинів проти основ національної безпеки України. *Науковий вісник Ужгородського національного університету*. 2023. С. 139-143. DOI <https://doi.org/10.24144/2307-3322.2023.77.2.23> URL: <https://visnyk-juris-uzhnu.com/wp-content/uploads/2023/06/25-2.pdf> (дата звернення 25.12.25).
4. Антоненко О. А. , Береза В. В. Розмиття меж між кіберзлочинністю та кібервійною в телекомунікаційній інфраструктурі: моделі атрибуції. Системи і технології зв'язку, інформатизації та кібербезпеки: актуальні питання і тенденції розвитку: збірник матеріалів V Міжнародної науково-технічної конференції. К.: Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, 2025. С. 28. URL: <https://mitit.mil.gov.ua/api/files/2572> (дата звернення 15.12.25).
5. Бабенко А. М., Матвєєвський О. В., Саїнчин С. О., Проблеми проведення судових експертиз під час розслідування воєнних злочинів за рекомендаціями «Протокола Берклі» *Право та державне управління*. 2024. № 3. С. 271-281. DOI <https://doi.org/10.32782/pdu.2024.3.39> (дата звернення 15.12.25).
6. Бабенко А.М., Резніченко Г.С, Теслиук І.О. Безпека малолітніх та неповнолітніх осіб в соціальних інтернет-мережах: сучасні підходи до запобігання правопорушенням. *Юридичний науковий електронний журнал* № 10/2025. С. 415-417. DOI <https://doi.org/10.32782/2524-0374/2025-10/94> URL: <https://lsej.org.ua/index.php/arkhiv-nomeriv?id=191> (дата звернення 15.12.25).

7. Бабійчук В. С. Кібертероризм та протидія йому. *Young Scientist*. 2019. No 4 (68). С. 103-107.
8. Барабаш О.О. Право на інформаційну безпеку як складова права людини на безпеку: концептуальні положення захисту інформаційних прав. *Юридичний науковий електронний журнал*. № 2.2024. С. 560-563. URL: http://www.lsej.org.ua/2_2024/140.pdf (дата звернення 25.12.25).
9. Белкін Л. М., Юринець Ю. Л., Белкін М. Л., Криволап Є. В. Проблеми формування та реалізації державної політики у сфері інформаційної безпеки України. *Юридичний вісник*. 2022. № 3 (64). С. 78-86. DOI: <https://doi.org/10.18372/2307-9061.64.16893> (дата звернення 15.12.24).
10. Бібік А. В., Городиський Р. О., Ваврічен О. А. Вплив штучного інтелекту на прийняття військового рішення (з урахуванням досвіду війни в Україні). Системи і технології зв'язку, інформатизації та кібербезпеки: актуальні питання і тенденції розвитку: збірник матеріалів V Міжнародної науково-технічної конференції. К.: Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, 2025. С. 34-35. URL: <https://mitit.mil.gov.ua/api/files/2572> (дата звернення 15.01.26).
11. Білаш О. В., Сорокатиий М.І. Захист інформаційної інфраструктури України в умовах воєнних дій. Системи і технології зв'язку, інформатизації та кібербезпеки: актуальні питання і тенденції розвитку: збірник матеріалів V Міжнародної науково-технічної конференції. К.: Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, 2025. С. 36. URL: <https://mitit.mil.gov.ua/api/files/2572> (дата звернення 15.01.26).
12. Бірюков Д. Концепція захисту критичної інфраструктури як елемент загальноєвропейської безпекової політики. *Журнал Наукові записки*. 6(68). http://www.ipiend.gov.ua/uploads/nz/nz_68/birukov_kontseptsia.pdf (дата звернення 05.02.26).

13. Бодунова О. М. Criminology principles of digitalization of state structures: global experience. *Соціологія права*. 2022. Випуск 1-2 (40-41). С. 7-10. <http://soclaw.idpnan.kyiv.ua/archive/2022/1-2/1.pdf> (дата звернення 05.02.26).
14. Бодунова О. М. Запобігання злочинності у сфері інформаційних технологій в умовах воєнного стану в Україні. *Науковий вісник Ужгородського національного університету*. 2023. № 75. Т. 2. С. 83-87. <http://visnyk-pravo.uzhnu.edu.ua/article/view/276140> (дата звернення 05.02.26).
15. Бодунова О. М. Теоретико-прикладні основи запобігання злочинності у сфері інформаційних технологій: моногр. Луцьк: Вежа-Друк, 2023. 344 с.
16. Бодунова О. М., Топчій В. В. Система кримінальних правопорушень у сфері інформаційних технологій: міжнародно-правовий вимір. *Ірпінський юридичний часопис*. 2023. № 1(10). С. 187-195.
17. Бодунова О. М., Топчій В. В., Дідківська Г. В. та ін. Кримінологічні засади участі України у міжнародній системі запобігання злочинності: монографія: / Вінниця, ТОВ «ТВОРИ». 2021, 376 с.
18. Бойченко О. В. Міжнародна інформаційна безпека: проблеми і перспективи. *Форум права*. 2009. № 3. С. 74–79.
19. Бондаренко В. О. Інформаційна безпека сучасної держави: концептуальні роздуми. URL: <http://www.crime-research.iatp.org.ua/library/strateg.htm> (дата звернення 05.02.26).
20. Будапештська конвенція про кіберзлочинність: Конвенція Ради Європи від 23.11.2001 р. Ратифікована Законом України від 07.09.2005 р. № 2824-IV. Редакція чинна. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 11.01.2025).
21. Валюшко І. О. Інформаційна безпека України в контексті російсько-українського конфлікту: дис... канд. політичних наук: спец. 23.00.04. К., 2018. 210 с

- 22.Валюшко І. О. Інформаційна безпека України: трансформація законодавства після російського вторгнення. Історико-політичні студії. 2017. № 2 (8). С. 30-43.
- 23.Варунц Л. Д. Досвід організації діяльності Королівської канадської кінної поліції та шляхи його використання в Україні : дис. канд. юрид. наук : 12.00.07. Дніпропетровськ, 2012. 203 с.
- 24.Василова О.В. Роль інноваційних технологій у розслідуванні та попередженні злочинів: сучасні виклики. Науковий вісник Ужгородського Національного Університету. Серія ПРАВО. 2025. Вип.87, ч.4. С.45–49. DOI <https://doi.org/10.24144/2307-3322.2025.87.4.6>
- 25.Виходець Ю.О., Тетерятник Г.К. Окремі питання використання osint при розслідуванні злочинів в умовах військової агресії РФ. Правові новели. 2022. № 18. С. 70-76. URL: https://legalnovels.in.ua/journal/18_2022/10.pdf. DOI <https://doi.org/10.32847/ln.2022.18.10> (дата звернення 05.02.26)
- 26.Войціховський А.В. Міжнародне співробітництво в боротьбі з кіберзлочинністю // Право і безпека. – 2011. – № 4. – С. 107-112.
- 27.Войціховський А.В. Формування системи інформаційної безпеки в рамках ООН. Правоохоронна функція держави: теоретико-методологічні та історико-правові проблеми. Харків, 2019. URL: https://univd.edu.ua/general/publishing/konf/17_05_2019/pdf/17.pdf
- 28.Гаврильців М.Т. Інформаційна безпека держави в системі національної безпеки України. Юридичний науковий електронний журнал. 2020. № 2. С. 200–203.
- 29.Галушко П. П. Кіберзлочинність як загроза національній безпеці України в умовах війни // Гуманітарні аспекти цифрового суспільства : тези доп. учасників міжн. наук.-практ. конф. (Харків, 8 груд. 2022 р.), С. 133–136. URL: https://library.pp-ss.pro/index.php/ndippsn_20221208/article/view/halushko

- 30.Галушко П. П. Кримінологічна характеристика та протидія кіберзлочинності в Україні в умовах війни : дис. ... д-ра філософії : 081. Харківський національний університет внутрішніх справ. Харків, 2025. 236 с.
- 31.Глобалізація і суспільство: національний, міжнародний та за рубіжний виміри: монографія / Т. В. Корнякової, О. Л. Соколенко, В. С. Гошовського та ін.; за заг. ред. д-ра.юрид.наук Т. В. Корнякової, д-ра.юрид.наук Н. С. Юзікової). Дніпро: ЛПРА, 2021. 492с.
- 32.Гловюк І.В. Оцінка результатів OSINT у судовій практиці: окремі питання. Науковий вісник Ужгородського Національного Університету. Серія ПРАВО. 2025. Вип.91, ч.4. С.251–259. DOI <https://doi.org/10.24144/2307-3322.2025.91.4.35>
- 33.Гогонянц С.Ю., Грицай П.М., Шапран О.О.. (2019) «Загальні положення методики оцінювання рівня воєнної небезпеки на основі таксономічних методів», *Сучасні інформаційні технології у сфері безпеки та оборони*. Київ, Україна, 34(1), с. 29–36. <https://doi.org/10.33099/2311-7249/2019-34-1-29-36> URL: <https://sit.nuou.org.ua/article/view/164783> (дата звернення 05.02.26).
- 34.Гончарук В. Л. Правові механізми боротьби з кіберзлочинністю: світова практика та вітчизняний контекст. *Питання боротьби зі злочинністю*. 2025. № 49. С. 178–184. URL: <https://pbz.nlu.edu.ua/article/view/338617/326961>. (дата звернення: 02.04.2026)
- 35.Голіна В. В. Кримінологічна профілактика злочинності: поняття, специфіка, структура, об'єкт запобіжного впливу. *Питання боротьби зі злочинністю*. 2015. Вип. 29. С. 145–154.
- 36.Горелова В. Ю. Кібербезпека: виклики цифрової ери через призму Конгресу ООН у Кіото. *Legal Bulletin*. 2024. С. 98–104. DOI: <https://doi.org/10.31732/2708-339X-2024-14-A13> (дата звернення: 11.01.2025).
- 37.Горелова В.Ю., Вихрист С.М., Правове забезпечення та перспективи розвитку державної політики у сфері інформаційної безпеки. *Legal Bulletin*. 2024. №13. С. 79-85. DOI: <https://doi.org/10.31732/2708-339X-2024-13>

- 38.Грезіна О. М. Роль штучного інтелекту у виявленні та прогнозуванні кіберзлочинів. Роль та місце правоохоронних органів у розбудові демократичної правової держави : матеріали XVII Міжнар. наук.-практ. інтернет-конф., м. Одеса, 2025 р. Одеса : ОДУВС, 2025. Т. 1. С. 16. URL: http://repositsc.nuczu.edu.ua/bitstream/123456789/26624/1/%D0%A0%D0%BE%D0%BB%D1%8C_%D1%82%D0%B0_%D0%BC%D1%96%D1%81%D1%86%D0%B5_2025_%D0%A2%D0%9E%D0%9C1.pdf#page=16 (дата звернення: 11.01.2025)
- 39.Гурковський В.І. інформаційна безпека в Україні як складова національної безпеки. Зб. наук. праць УАДУ. К.: Вид-во УАДУ. 2002. Вип. 2. С. 9-18.
- 40.Давиденко В.Л. Цілі та завдання віктимологічного впливу на злочинність. *Актуальні проблеми вітчизняної юриспруденції*. 2017. № 1. Т. С. 141–143. URL: <https://dspace.univd.edu.ua/items/cae78617-62eb-43a0-89da-a8831849146e> (дата звернення 05.02.26).
- 41.Денисов С.Ф. Деякі аспекти сутності та предмета кримінології як на- уки. Вісник Кримінологічної асоціації України. 2021. № 1 (24). С. 151–159. URL: <https://dspace.univd.edu.ua/items/8d7669ce-66e2-4594-bb5c-3c1383a3ad55> . (дата звернення: 09.01.2026).
- 42.Департамент кіберполіції Національної поліції України. Офіційний звіт за 2025 рік. URL: <https://cyberpolice.gov.ua/news/shhorichnyj-zvit-7096/> . (дата звернення: 09.04.2026).
- 43.Деякі питання забезпечення функціонування інформаційнокомунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану : постанова Кабінету Міністрів України від 12.03.2022 № 263. URL: <https://zakon.rada.gov.ua/laws/show/263-2022-%D0%BF#Text> (дата звернення: 09.01.2026).
- 44.Діброва Т. А., Пісенко Д. О., Сметаніна Н. В. Кіберзлочинність та кібершахрайство в умовах воєнного стану. Юридичний науковий електронний

- журнал. 2022. № 11. С. 546–549. URL: http://lsej.org.ua/11_2022/132.pdf.
(дата звернення: 09.01.2026).
- 45.Дір І. Ю. Основні характеристики «acquis communautaire» Європейського Союзу. Науковий вісник Ужгородського Національного Університету. Серія «ПРАВО». 2023. Вип. 78. Ч. 2. С. 355. URL: <http://visnykpravo.uzhnu.edu.ua/article/view/286637/280490>
(дата звернення: 09.01.2026).
- 46.Діти в онлайн-стрімах – нова мішень для зловмисників. Що варто знати батькам? <https://chatovi.online/articles/nbMdo1> (дата звернення 05.02.26)
- 47.Добкіна К.Р. право на мир як основа правової політики постконфліктної реінтеграції. *Право і суспільство*. № 3. 2025. Т. 2. С. 516-522. URL: http://pravoisuspilstvo.org.ua/archive/2025/3_2025/part_2/72.pdf (дата звернення 15.02.25).
- 48.Довгань О. Д., Ткачук Т. Ю. Система інформаційної безпеки України: онтологічні виміри. *Інформація і право*. 2018. № 1(24). С. 89–103.
- 49.Додатковий протокол до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних. https://zakon.rada.gov.ua/laws/show/994_363#Text (дата звернення 15.02.25).
- 50.Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи: Протокол Ради Європи від 28.01.2003. Законотворчість : база даних. Верхов. Рада України. URL: https://zakon.rada.gov.ua/laws/show/994_687#Text (дата звернення 25.04.2025 р.)
- 51.Досягнення в сфері інформатизації та телекомунікацій в контексті міжнародної безпеки : резолюція Генеральної Асамблеї ООН A/RES/56/19 від 29 листоп. 2001 р. // БД «Документи» / Організація Об'єднаних Націй. URL: <https://undocs.org/ru/A/RES/56/19> (дата звернення 20.02.2026 р.)

52. Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки: резолюція Генеральної Асамблеї ООН A/RES/54/49 від 1 груд. 1999 р. База даних (БД) «Документи». Організація Об'єднаних Націй. URL: <https://undocs.org/ru/A/RES/54/49> (дата звернення 20.02.2026 р.)
53. Другий додатковий протокол до Конвенції про кіберзлочинність (Будапештська конвенція) URL.: <https://www.coe.int/uk/web/kyiv/-/enhanced-co-operation-and-disclosure-of-electronic-evidence-22-countries-sign-new-protocol-to-cybercrime-convention> (дата звернення 20.02.2026 р.)
54. Думчиков М.О. Використання OSINT технологій для виявлення корупційних правопорушень: сучасні підходи та виклики. Академічні візії. № 3. 2024. С. 1-6. DOI: <https://doi.org/10.5281/zenodo.13928363> (дата звернення: 28.02.2026р.)
55. Забара І. М. Міжнародна інформаційна безпека в міжнародному праві: до питання визначення. *Український часопис міжнародного права*. 2012. № 4. С. 63–69.
56. Забара І. М. Міжнародна інформаційна безпека: сучасні концепції в міжнародному праві. *Міжнародне право та філософія права*. 2013. том 2 № 4. URL: <http://tlaw.nlu.edu.ua/article/view/63695> (дата звернення 20.02.2026 р.)
57. Загальний регламент про захист даних: Регламент Європейського Парламенту і Ради (ЄС) від 27.04.2016 № 984_008-16. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення: 28.02.2026р.)
58. Загородня, А. С., & Кулик, А. В. Роль ООН у врегулюванні та підтримці міжнародної безпеки: миротворчість і превентивна дипломатія. *Сучасний науковий журнал*, (6(4)), (2024). 112-120. URL: <https://doi.org/10.36994/2786-9008-2024-6-14> (дата звернення 05.02.26)
59. Задорожна І.М. Великі дані як об'єкт управління. *Економіка та менеджмент*. 2016. № 1–2. С. 75–79. URL:

https://econommeneg.btsau.edu.ua/sites/default/files/visnyky/economika/zadorozhna_1-2_2016.pdf (дата звернення 05.12.25).

60. Закалюк А.П. Курс сучасної української кримінології: теорія і практика: у 3 кн. – Кн.1: Теоретичні засади та історія української кримінологічної науки / А.П. Закалюк. – К.: Видавничий дім «Ін Юре», 2007. 424с.
61. Збитки українців від кіберзлочинності торік зросли до 1 млрд грн – дослідження ЄМА. Офіційний сайт Forbes. URL: <https://forbes.ua/news/zbitki-ukraintsiv-vid-kiberzlochinnosti-torik-zrosli-do-1-mlrd-grn-doslidzhennya-ema-21022023-11884> (дата звернення 05.12.25)
62. Звіт Internet Watch Foundation за 2023 рік. <https://www.iwf.org.uk/annual-report-2023/> (дата звернення 05.12.25)
63. Звіт Національної поліції України про результати роботи у 2020 році. URL: <https://www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit2020/npu-zvit-2020.pdf>. (дата звернення 05.12.25)
64. Звіт про діяльність Департаменту кіберполіції Національної поліції України за 2025 рік. Департамент Кіберполіції. URL: <https://cyberpolice.gov.ua/news/shh-orichnyj-zvit7096/> (дата звернення: 09.04 2026)
65. Зінченко Д.А. Аналіз ризиків і стратегій захисту від кібератак у сучасному цифровому світі. Протидія кіберзлочинності та торгівлі людьми : зб. матеріалів міжнар. наук.-практ. конф. (м. Вінниця, 31 травня 2023). Вінниця: ХНУВС, 2023. С. 118–121. URL: <https://dspace.univd.edu.ua/handle/123456789/17463> (дата звернення: 09.01.2025).
66. Іванцов В., Зелінський В. Вплив цифровізації на розвиток кримінологічних досліджень: нові виклики та можливості : дис. Чернігів : Пенітенціарна академія України, 2024. URL: <https://dspace.univd.edu.ua/items/33a805aa-6e5c-43c3-a5a0-e44518a53847> (дата звернення: 11.01.2025).

67. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. *Політичні науки*. Vol. 2, No. 1, 2016. С.27-32. URL: <https://science.lpnu.ua/sites/default/files/journalpaper/2017/jun/4352/ilnicka0.pdf> (дата звернення: 09.01.2025).
68. Інститут безпеки ШІ: перспективи та виклики. <https://dc.org.ua/news/instytutu-bezpeky-shi-perspektyvy-ta-vyklyky> (дата звернення: 09.01.2026).
69. Інформаційна безпека (соціально-правові аспекти): Підручник / Остроухой Б. В., Петрик Б. М., Присяжнюк М. М. та ін. ; за заг- ред. Є. Д. Скулиша. К : КНТ, 2010. 776 с. URL: https://duikt.edu.ua/uploads/1_1352_84114000.pdf (дата звернення: 09.01.2025).
70. Інформаційна безпека України [Текст] : глосарій / Л.С. Харченко, Н.А. Ліпкан, О.В. Логінов [и др.] ; заг. ред. Р.А. Калюжний. К. : Текст, 2004. 135 с.
71. ІТ-право під час гібридної війни: від пошуку парадигми до прагматичних рішень: кол. монографія / за заг. ред. проф.: Є. Харитоновна, О. Харитоновної, І. Давидової. Одеса : Фенікс, 2025. 588 с. ISBN 978-617-8430-70-2
72. Калюжний Р.А., Новицька Н. Б. Становлення інформаційного суспільства. *Правова інформатика*. 2006. № 3 (11). С. 17-22
73. Караман К.В. Сучасна парадигма криміналістичного значення цифрових слідів у кримінальному провадженні. *Вісник Кримінологічної асоціації України*, 2025. № 2 (35). С. 224-232. URL: <https://vca.univd.edu.ua/index.php/vca/article/view/560/608> . (дата звернення: 09.01.2026).
74. Карчевський М, В. (2023) Протидія злочинності в Україні : інфорграфіка : інтерактивний довідник. Версія 3.0. URL : <https://karchevskiy.com/i-dovidnyk/> (дата звернення: 19.01.2025).
75. Карчевський М. В. Кримінально-правова охорона інформаційної безпеки України: монографія. Луганськ: РВВ ЛДУВС ім. ЕО Дідоренка, 2012. 230 с.
76. Кібер Брама <https://stopfraud.gov.ua> (дата звернення: 09.01.2026).

77. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О. Довгань; упоряд. О. Довгань, Л. Литвинова, С. Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В.І. Вернадського. К., 2026. № 1 (січень). 139 с. URL: <https://ippi.org.ua/sites/default/files/2026-1.pdf> (дата звернення: 22.03.2026).
78. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О. Довгань; упоряд. О. Довгань, Л. Литвинова, С. Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В.І. Вернадського. К., 2026. № 2 (лютий). 148 с. URL: <https://ippi.org.ua/sites/default/files/2026-2.pdf> (дата звернення: 03.03.2026).
79. Кіберзлочинність в Україні: кримінологічна характеристика та запобігання : монографія / за заг. ред. В. В. Голіни, М. Г. Колодяжного. Харків : Право, 2021. 296 с.
80. Кіберсвіт у новому тисячолітті. Хто вони: кіберзлочинці, кібершахраї, кібертерористи? Офіційний сайт видання «Lexinform». URL: <https://lexinform.com.ua/dumka-eksperta/kibersvit-u-novomu-tysyacholitti-htovony-kiberzlochynsi-kibershahrayi-kiberterorysty/> (дата звернення: 09.01.2026).
81. Кримінальний кодекс України. <https://zakon.rada.gov.ua/laws/show/2341-14#Text> (дата звернення: 19.01.2026).
82. Князев С.М. Теоретико-методологічні засади правового регулювання забезпечення інформаційної безпеки. *Наука і техніка сьогодні*. 2026. № 3(57). С. 124-136. DOI: [https://doi.org/10.52058/2786-6025-2026-3\(57\)-124-136](https://doi.org/10.52058/2786-6025-2026-3(57)-124-136)
83. Кобетяк, А. Когнітивна експансія в умовах інтенсивного розвитку кіберпростору як виклик національній безпеці: досвід України. *Society and Security*, 2025. № (6(12)), С. 26–32. [https://doi.org/10.26642/sas-2025-6\(12\)-26-32](https://doi.org/10.26642/sas-2025-6(12)-26-32). URL: <https://sas.ztu.edu.ua/article/view/349536> (дата звернення: 09.01.2026).

- 84.Кобко Є. Підрозділи ювенальної превенції національної поліції України в системі органів публічного адміністрування в умовах воєнного стану. *Юридичний вісник*, 2023 № 3. С. 47-52 https://yurvisnyk.in.ua/v3_2023/6.pdf (дата звернення: 09.01.2026).
- 85.Коваленко Є. В., Плетньов О. В. Передумови загроз у сфері інформаційної безпеки та перспективи їх подолання. *Актуальні проблеми управління інформаційною безпекою України* : зб. тез наук. доповідей X Всеукраїнська наук.-практ. конф., Київ, 4 квітня 2019 року. Нац. акад. СБУ. Київ, 2019. С. 57–61.
- 86.Коваленко А.В. Криміналістичне вчення про збирання, дослідження та використання доказів у кримінальному провадженні: монографія. К.: Алерта, 2024. 558с.
- 87.Колб О. Г., Бендовський Н. Г. Про деякі напрями діяльності, що стосується національної безпеки України. *Держава та регіони. Науково-виробничий журнал*. Серія: Право. 2021. № 2 (72). С. 82-87
- 88.Колб О. Г., Бендовський Н. Г. Сингулярність загроз інформаційній та національній безпеці України. *Злочинність і протидія їй в умовах сингулярності: тенденції та інновації*: зб. тез доп. наук.-практ. конф., присвяч. пам'яті члена Правління Кримінологічної асоціації України, професора Тетяни Андріївни Денисової (м. Харків, 16 квіт. 2021 р.). МВС України, Харків. нац. ун-т внутр. справ, Кримінол. асоц. України. Харків : ХНУВС, 2021. С. 313-314
- 89.Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних. https://zakon.rada.gov.ua/laws/show/994_326#Text (дата звернення: 09.12.2025).
- 90.Конвенція ООН Проти транснаціональної організованої злочинності від 15.11.2000 р. URL: https://zakon.rada.gov.ua/laws/show/995_789#Text (дата звернення: 09.12.2025).

91. Конвенція про захист прав людини і основоположних свободи (Рада Європи, 4 листопада 1950р.): <http://zakon4.rada.gov.ua/laws/show/-995004> (дата звернення: 09.12.2025).
92. Конвенція про кіберзлочинність. Додатковий протокол від 28.01.2003 до Конвенції. Конвенцію ратифіковано із застереженнями і заявами Законом N 2824-IV (2824-15) від 07.09.2005, ВВР, 2006, N 5-6, ст.71. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 09.12.2025).
93. Консолідовані версії Договору про Європейський Союз та Договору про функціонування Європейського Союзу з протоколами та деклараціями. URL: https://zakon.rada.gov.ua/laws/show/994_b06#Text (дата звернення: 09.12.2025).
94. Конституція України. URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text> (дата звернення: 09.12.2025).
95. Кормич Б. А. Інформаційне право України : підручник. Одеса : Видавничий дім «Гельветика», 2021. 384 с.
96. Кормич Б.А. Організаційно-правові засади політики інформаційної безпеки України: Монографія. Одеса: Юридична література, 2003. 472 с.
97. Корнякова Т.В., Юзікова Н.С. Основні напрями сучасної правоохоронної діяльності. Правова парадигма відновлення України: проблеми та перспективи: [Матеріали XIV Міжнародної науково-практичної конференції, м. Київ, Національний авіаційний університет, 23 лютого 2024 р.]. – Тернопіль: Вектор, 2024. С. 343-347 URL: <https://archer.chnu.edu.ua/bitstream/handle/123456789/9657/9.pdf?sequence=1&isAllowed=y> . (дата звернення: 09.12.2025).
98. Косевцов В. О., Бінько І. Ф., Матвієвський О. М. Методичний підхід до аналізу й оцінки рівня національної безпеки та її складових. *Наука і оборона*. 1995. № 1. С. 74-77
99. Косевцов В. О., Телелим В.М., Шевченко В. І. Оцінка стану воєнної безпеки України. *Наука і оборона*. 1998. № 2. С. 3-6.

100. Кравцова М. О., Литвинов О. М. Запобігання кіберзлочинності в Україні : монографія. Харків : Панов, 2016. 212 с.
101. Кримінальна відповідальність за несанкціоноване втручання в роботу ЕОМ : монографія. Ю. А. Бельський, П. А. Воробей, А. В. Савченко., О. Г. Колб. К.: Юрінком Інтер, 2019. 264 с.
102. Кримінально-правова охорона інформаційної безпеки України : монограф. / М.В. Карчевський ; МВС України, Луган. держ. ун-т внутр. справ ім. Е.О. Дідоренка. Луганськ : РВВ ЛДУВС ім. Е.О. Дідоренка, 2012. 528 с.
103. Кримінальне право України : Загальна частина : підручник / В. Я. Тацій та ін. ; за ред. В. Я. Тація, В. І. Тютюгіна, В. І. Борисова. 6-те вид., переробл. і допов. Харків : Право, 2020. 584 с.
104. Кримінальне право України. Загальна частина : підручник / за заг. ред. В. М. Бурдіна, В. І. Маркіна. К., 2025. 1148 с.
105. Кримінальне право України : Особлива частина : підручник / Ю. В. Баулін та ін. ; за ред. В. В. Сташиса, В. Я. Тація. 4-те вид., переробл. і допов. Харків : Право, 2010. 608 с.
106. Кримінальний процесуальний кодекс України : Закон України від 13 квітня 2012 р. № 4651-VI. Законодавство України : веб-сайт. URL: <https://zakon.rada.gov.ua/laws/show/4651-17> (дата звернення: 27.02.2026).
107. Кримінологія: підручник А. М. Бабенко, О. Ю. Бусол, О. М. Костенко та ін.; за заг. ред. Ю. В. Нікітіна, С. Ф. Денисова, Є. Л. Стрельцова. 2-ге вид., перероб. та допов. Харків: Право, 2018. 416 с.
108. Кримінологія: підручник /В.В. Голіна, Б.М. Головкін, М.Ю. Валуйська та ін.; за ред.. В.В. Голіни, Б.М. Головкіна. Х.: Право, 2020. 440с.
109. Кримінологія: Навчальний посібник для підготовки до екзаменів. Видання 3-те, перероб. та доп. / Т.В. Корнякова, Н.С. Юзікова. Дніпро, 2022. 168с.
110. Кудрявський І. В. (2025). Верифікація алгоритму підтримки прийняття рішень у ході застосування механізмів державного управління у сфері захисту

- безпеки інформаційного простору. *Соціальне Право*, (3), 217-229. вилучено із <https://soclaw.com.ua/index.php/journal/article/view/1313> (дата звернення: 09.01.2026).
111. Курінна О.О., Юзікова Н.С. Особливості кримінальної відповідальності за сексуальне насильство щодо дітей: теоретичні та практичні аспекти. *Актуальні проблеми вітчизняної юриспруденції*. 2024. № 6. С. 221-227. URL: http://apnl.dnu.in.ua/6_2024/36.pdf (дата звернення: 09.12.2025).
112. Леган І. М. Особливості міжнародного співробітництва щодо запобігання і протидії кіберзлочинності та кібертероризму. *Науковий вісник Міжнародного гуманітарного університету. Сер. : Юриспруденція*. 2021. № 50. С. 118–121. URL: <https://vestnikpravo.mgu.od.ua/archive/juspradenc50/27.pdf>. (дата звернення: 19.02.2024).
113. Лелет Я. Генеза інформаційної безпеки в умовах воєнно-політичного конфлікту. *Вісник Прикарпатського університету. Серія: Політологія*. 2024. № 19. С. 98–104. URL: <https://journals.pnu.if.ua/index.php/politology/article/view/185> (дата звернення: 09.12.2025).
114. Лизанчук В.В. Інформаційна безпека України: теорія і практика: підручник. Львів: ЛНУ ім. Івана Франка, 2017. 725 с
115. Линник Г.М. Адміністративно-правове регулювання інформаційної безпеки України : автореф. дис.... канд. юрид. наук : 12.00.07 / Г.М. Линник / Нац. ун-т біоресурсів і природокористування України. К., 2011. 20 с. 53.
116. Лисенко О. М. Міжнародно-правове регулювання прав дитини в кіберпросторі. *Соціологія права*. 2016. № 3 (18). URL: <http://soclaw.idpnan.kyiv.ua/archive/2016/3/8.pdf> (дата звернення: 19.12.2024).
117. Лисько Т. Д., Меланіч В. В., Славіта Ю. В. Протидія кіберзлочинності: сучасний стан вітчизняного законодавства та досвід зарубіжних країн. *Актуальні проблеми держави і права*. 2022. № 96. С. 44–49. DOI: <https://doi.org/10.32782/apdp.v96.2022.4>.

118. Литвиненко О.В. Інформаційні впливи та операції. Теоретикоаналітичні нариси: монографія / О.В. Литвиненко. – К.: НІСД, 2003. 240 с.
119. Ліпкан В. А., Максименко Ю. Є., Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції : навч. посіб. К.: КНТ, 2006. 280 с.
URL:<https://duikt.edu.ua/ua/lib/1/category/2402/view/1350>
(дата звернення: 09.12.2025).
120. Ліпкан В.А. Національна і міжнародна безпека у визначеннях та поняттях [Текст] / В. А. Ліпкан, О. С. Ліпкан. – Вид. 2-ге, доп. і переробл. – К.: Текст, 2008. 400 с
121. Ліпкан В.А. Теоретико-методологічні засади управління у сфері національної безпеки України. / В.А. Ліпкан ; Національна академія внутрішніх справ України. К., 2005. 350 с.
122. Логинов О.В. Адміністративно-правове забезпечення інформаційної безпеки органів виконавчої влади: Автореф. дис... канд. юрид. наук: 12.00.07 / О.В. Логінов; Нац. акад. внутр. справ України. К., 2005. 20 с.
123. Лугівська Л. Р., Яцишин О. О., Любавіна В. П. Тенденції розвитку кримінальної відповідальності за кіберзлочини в умовах цифровізації суспільства. *Dictum Factum*. 2024. № 2 (16). С. 258–264. URL: <https://df.duit.in.ua/index.php/dictum/article/view/363> (дата звернення: 11.01.2025).
124. Лугіна Н. А., Лучук А. М. Порівняльний аналіз вітчизняного та європейського законодавства з питань запобігання кіберзлочинності. *Ірпінський юридичний часопис: науковий журнал*. 2023. Вип. 1 (10). С. 180–186 URL : <https://ojs.dpu.edu.ua/index.php/irplegchr/article/view/83/82>
(дата звернення: 09.12.2025).
125. Максименко Ю. Є. Теоретико-правові засади забезпечення інформаційної безпеки України : дис... канд. юрид. наук : 12.00.01. К., 2007. 188 с.
126. Малій М., Біленчук П. Кіберсвіт у новому тисячолітті. Хто вони: кіберзлочинці, кібершахраї, кібертерористи? *Юридичний вісник України*.

URL: <https://lexinform.com.ua/dumka-eksperta/kibersvit-u-novomu-tysyacholitti-hto-vony-kiberzlochyntsi-kibershahrayi-kiberterorysty/>

(дата звернення: 09.12.2025).

127. Меленко О.В. *Методологія правознавства в науковій спадщині Б.О. Кістяківський дис. на здобуття наукового ступеня кандидата юридичних наук. за спеціальністю 12.00.01 – теорія та історія держави і права; історія політичних і правових учень* Одеса. 2008. 196с. . URI https://drive.google.com/file/d/1ADm7qlSWMdq_WNblAKinoFJsOQTc1ItL/view

(дата звернення: 09.12.2025).

128. Міжнародний пакт про громадянські і політичні права: Пакт Організації Об'єднаних Націй від 16.12.1966 (станом на 19 жовтня 1973 р.)

URL: https://zakon.rada.gov.ua/laws/show/995_043#Text

(дата звернення: 09.01.2026).

129. Мирошниченко Н. А. Суспільно небезпечні наслідки кримінальних правопорушень, їх вплив на кваліфікацію. *Європейські орієнтири розвитку України: науково-практичний вимір в умовах воєнних викликів* : матеріали Міжнар. наук.-практ. конф. (м. Одеса, 26 квітня 2024 р.) / за заг. ред. С. В. Ківалова. Одеса, 2024. С. 353–355.

130. Мордвинцев М. В., Пашнев Д. В., Наконечний В. С. Особливості використання технологій відеоаналізу та програмного забезпечення з розпізнавання облич у кримінальному аналізі. *Право і безпека*. 2025. № 1 (96). С. 90–103. URL: <https://pb.univd.edu.ua/index.php/PB/article/view/853/691>

(дата звернення: 09.01.2026).

131. Моса В.В. Теоретико-методологічні засади використання кримінального аналізу оперативними підрозділами правоохоронних органів України. *Науковий вісник Ужгородського Національного Університету. Серія ПРАВО*. Випуск 73: частина 2, 2022. С.141-147. URL: <https://visnyk-juris-uzhnu.com/wp-content/uploads/2022/11/24-1.pdf>

(дата звернення: 29.12.2025).

132. Мудриєвська Л. М. Роль права на забуття в реалізації особистих прав людини. Актуальні проблеми прав людини: від універсальних стандартів до національної практики : Міжнародна науково-практична конференція. Київський університет права Національної академії наук України, 11 грудня 2025 р. Львів – Торунь : Liha-Pres, 2025. С. 87-89. <http://catalog.liha-pres.eu/index.php/liha-pres/catalog/book/430> (дата звернення: 09.01.2026).
133. Мудриєвська Л.М. Чукаєва В.О. Права людини та сучасна конституційна реформа в Україні. Розділ у монографії Human rights and public governance : Scientific monograph. Riga, Latvia : «Baltija Publishing», 2025. 772 p.С. 434-456.
134. Навроцький В. О. Наступність кримінального законодавства України (порівняльний аналіз КК України 1960 р. та 2001 р.). К.: Атіка, 2001. 272 с.
135. Наливайко О. І., Братішко Н. А. Поняття та особливості міжнародно-правових стандартів прав людини. *Аналітично-порівняльне правознавство*. 2023. № 2. С. 411–416.
136. Науково-практичний коментар Кримінального кодексу України / за ред. М. І. Мельника, М. І. Хавронюка. 11-те вид., переробл. та допов. Київ : ВД «Дакор», 2019. 1384 с.
137. Національна бібліотека України ім. В.І. Вернадського. К., 2026. № 2 (лютий). 148 с. URL: <https://ippi.org.ua/sites/default/files/2026-2.pdf> (дата звернення: 09.02.2026).
138. Національна стратегія у сфері прав людини. Указ Президента від 24.03.2021 № 119/2021. URL: <https://zakon.rada.gov.ua/laws/show/119/2021#Text> (дата звернення: 19.08.2024).
139. Нашинець-Наумова А.Ю.. Інформаційна безпека: питання правового регулювання: монографія. К: Видавничий дім «Гельветика», 2017. 168 с. https://elibrary.kubg.edu.ua/id/eprint/18860/1/A_Nashinets-Naumova_monografia_1_FPMV.pdf (дата звернення: 19.08.2024).

140. Нестерова І.А. Впровадження цифрових технологій в кримінологічні дослідження. *Електронне наукове видання «Аналітично-порівняльне правознавство»*. Випуск № 01, 2026, частина 2. С. 421-425. URL <https://app-journal.in.ua/wp-content/uploads/2026/02/69-1.pdf> (дата звернення: 19.02.2026).
141. Нижник Н.Р. Національна безпека України (методологічні аспекти, стан і тенденції розвитку): навчальний посібник / Н.Р. Нижник, Г.П. Ситник, В.Т. Білоус. Ірпінь : Акад. ДПС України, 2000. 304 с.
142. Ніколайчук С. Захист прав дітей в умовах воєнного стану: проблеми теорії та практики. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2022. № 4. С. 94–105.
143. Новий звіт McAfee оцінює глобальні збитки від кіберзлочинності у розмірі у понад 1 трильйон доларів. URL: <http://teib.info/?p=5780> (дата звернення: 19.02.2026).
144. Новицький В.Я. Стратегічні засади забезпечення інформаційної безпеки в сучасних умовах. *Інформація і право*. 2022. Вип. 1 (40). С. 111–118. DOI: [https://doi.org/10.37750/2616-6798.2022.1\(40\).254349](https://doi.org/10.37750/2616-6798.2022.1(40).254349) .
<https://il.ippi.org.ua/article/view/254349> (дата звернення: 19.04.2025).
145. Одерій О.В., Кожевников О.А. Отримання криміналістично значущої інформації шляхом аналізу відкритих інтернет-джерел. *Правовий часопис Донбасу*. 2020. № 4 (73) 2020. С. 144 – 155. DOI: <https://doi.org/10.32366/2523-4269-2020-73-4-144-155> (дата звернення: 23.02.2024).
146. Олійник А. А. Сутність інформаційної безпеки як правового явища у національному та міжнародному просторі. *Актуальні проблеми вітчизняної юриспруденції* № 6. 2023. С.293-299.
147. Олійник А. А. Формування стійкого цифрового суспільства: превентивна роль інформаційної безпеки та кримінально-правової політики у запобіганні злочинності . *Актуальні проблеми вітчизняної юриспруденції* № 2. 2025. С. 177-182. DOI <https://doi.org/10.32782/2408-9257-2025-2-27>
URL:http://apnl.dnu.in.ua/2_2025/29.pdf (дата звернення: 19.12.2025).

148. Олійник А.А. Кіберстійкість та права людини: імплементація міжнародних превентивних моделей у цифровий простір в Україні . *Аналітичне порівняльне правознавство* № 6. Ч. 3. 2025. С. 84-90. URL: https://app-journal.in.ua/wp-content/uploads/2025/12/APP_06_2025_part-3.pdf (дата звернення: 19.01.2026).
149. Олійник А.А. Модель забезпечення цифрової безпеки в мережі internet крізь призму досвіду зарубіжних країн. Збірник тез Всеукраїнської науково-практичної конференції "Забезпечення принципів поваги, захисту та реалізації прав дитини у цифровому середовищі». (м. Дніпро 23.листопада 2023) Дніпровський національний університет імені Олеся Гончара, Дніпро, Ліра, 2023. С.349-352 URL: https://www.dnu.dp.ua/docs/ndc/2023/materiali%20konf/new_Zbirnyk_Konf_Zahyst%20prav_dytny_v_cifrovomu_sviti.pdf (дата звернення: 19.01.2026).
150. Олійник А.А. Окремі форми інформаційної агресії матеріали всеукраїнського науково-практичного круглого столу. Інформаційна агресія в сучасному світі: правовий аналіз та протидія Харків, 21 червня 2024 р. : електрон. наук. вид. / редкол.: В. С. Батиргарєєва та ін. – Харків : Майдан, 2024. С. 56-58. https://ivpz.kh.ua/wp-content/uploads/2024/11/%D0%97%D0%B1%D1%80%D0%BD%D0%B8%D0%BA_%D1%96%D0%BD%D1%84%D0%BE%D0%B0%D0%B3%D1%80%D0%B5%D1%81%D1%96%D1%8F_2024-%D0%BD%D0%B0-%D1%81%D0%B0%D0%B9%D1%82.pdf (дата звернення: 19.01.2026).
151. Онопрієнко О., Онопрієнко С. Конвенція ради Європи про кіберзлочинність: висновки для України. *Пропілеї права та безпеки*. 2025. № 8. С. 257–259. DOI: <https://doi.org/10.32620/pls.2025.8.66> URL: <https://nti.khai.edu/ojs/index.php/PLS/article/view/pls.2025.8.66> (дата звернення: 23.01.2026).

152. Орлов Ю. В. Злочинність і протидія їй в умовах війни: кримінальноправовий та кримінологічний виміри : монографія / Кримінол. асоц. України. Х.: Право, 2023. 252 с
153. Паламарчук С. А., Мартинюк В. В., Овсянніков В. В., Шугалій О. О., Перехідний період законодавчих змін щодо захисту інформації та кіберзахисту інформаційно-комунікаційних систем. Системи і технології зв'язку, інформатизації та кібербезпеки: актуальні питання і тенденції розвитку: збірник матеріалів V Міжнародної науково-технічної конференції. К.: Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, 2025. С. 184-185. URL: <https://mitit.mil.gov.ua/api/files/2572> (дата звернення: 09.01.2026).
154. Палій О.А. Національна безпека України в контексті євроатлантичної інтеграції: дис... канд. політ. наук: 21.01.01 / Палій Олександр Андрійович ; Національний ун-т «Києво-Могилянська академія». К., 2005. 205 с.
155. Пахомов В., Каріх І., Рєпін Д. Міжнародно-правове регулювання кіберпростору. *Молодий вчений*. 2021. № 4 (92). С. 269–272. URL: <https://doi.org/10.32839/2304-5809/2021-4-92-58> (дата звернення: 19.12.2024).
156. Перетворення нашого світу: Порядок денний у сфері сталого розвитку до 2030 року : Резолюція Генеральної Асамблеї ООН від 25 верес. 2015 р. № A/RES/70/1. *Організація Об'єднаних Націй*. URL: <https://undocs.org/ru/A/RES/70/1> (дата звернення: 23.01.2026).
157. Петрик В.М. Інформаційна безпека України: поняття, сутність та загрози / В.М. Петрик, М.В. Галамба // *Юридичний журнал*. 2006. №11. – С. 49-52.
158. Пісоцька К. О. Діяльність підрозділів ювенальної превенції Національної поліції України: адміністративно-правовий аспект : монографія. Дніпро : Видавець Біла К. О., 2023. 158 с.
159. Пісоцька К. О. Захист прав та інтересів дітей: фокус діяльності ювенальної превенції Національної поліції під час воєнного стану. 2025. *Наукові перспективи*. № 2(56). С. 1-13. DOI: <https://doi.org/10.52058/2708-7530-2025->

(дата звернення: 09.01.2026).

160. План дій Ради Європи для України на 2023-2026 роки «Стійкість, відновлення та відбудова» <https://rm.coe.int/action-plan-ukraine-2023-2026-ukr/1680aa8282> (дата звернення: 04.02.2025).
161. Погорецький М.А. Цифрові технології та докази у розслідуванні злочинів проти основ національної безпеки України: процесуальні проблеми та європейські стандарти. Аналітично-порівняльне правознавство. 2025. №5, ч. 3. С.239–255. DOI <https://doi.org/10.24144/2788-6018.2025.05.3.37>
162. Почепцов Г. Когнітивні війни в соцмедіа, масовій культурі й масових комунікаціях. К. : Фоліо. 2019. 314 с.
163. Правові засади забезпечення інформаційної безпеки України в умовах збройної агресії : колективна монографія / за заг. ред. О. В. Радченка. К.: Інститут держави і права ім. В. М. Корецького НАН України, 2022. 312 с.
164. Представник Google у Радбезі ООН: мета кібератак росії - виправдання воєнних злочинів. Укрінформ. 21.06.2022. URL:<https://www.ukrinform.ua/rubric-technology/3512169-predstavnik-google-u-radbezi-oon-meta-kiberatak-rosii-vipravdanna-voennih-zlociniv.html> (дата звернення: 19.12.2024).
165. Про Державну службу спеціального зв'язку та захисту інформації України. Закон України. <https://zakon.rada.gov.ua/laws/show/3475-15#Text> (дата звернення: 29.02.2025).
166. Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації: Рішення РНБО від 29.12.2016 р. Офіційний сайт ВРУ. URL: <https://zakon.rada.gov.ua/laws/show/n0015525-16#Text> (дата звернення: 29.02.2025).
167. Про затвердження Порядку взаємодії суб'єктів національної системи реагування на кіберінциденти, кібератаки, кіберзагрози із суб'єктами забезпечення кібербезпеки, правоохоронними, контррозвідувальними,

- розвідувальними органами та суб'єктами оперативно-розшукової діяльності: постанова Кабінету Міністрів України від 13.11.2025 № 1471. URL: <https://zakon.rada.gov.ua/laws/show/1471-2025-%D0%BF#Text> (дата звернення: 29.02.2025).
168. Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування: офіційний сайт Офісу Генерального прокурора. URL: <https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushehnyya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2> (дата звернення: 19.12.2025).
169. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР: станом на 20 квіт. 2025 р. URL: <https://zakon.rada.gov.ua/laws/show/80/94вр#Text> (дата звернення: 15.02.2026).
170. Про захист персональних даних. Закон України. <https://zakon.rada.gov.ua/laws/show/2297-17#Text> (дата звернення: 15.02.2026).
171. Про інформацію Закон України. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text> (дата звернення: 15.02.2026).
172. Про Кіберсили Збройних Сил України. Проект закону №12349. URL: <https://www.rada.gov.ua/news/razom/266780.html> (дата звернення: 15.02.2026).
173. Про критичну інфраструктуру Закон України URL: <https://zakon.rada.gov.ua/laws/show/1882-20#Text> (дата звернення: 15.02.2026).
174. Про медіа: Закон України №2849-IX від 13.12.2022 року. URL: <https://zakon.rada.gov.ua/laws/show/2849-20#Text> (дата звернення: 15.02.2026).
175. Про національну безпеку України. Закон України <https://zakon.rada.gov.ua/laws/show/2469-19#Text> (дата звернення: 15.02.2026).
176. Про Національну поліцію України. Закон України від 02.07.2015 р. № 580VIII URL: <https://zakon.rada.gov.ua/laws/show/58019#Text> (дата звернення: 15.02.2026).
177. Про основні засади забезпечення кібербезпеки України: Закон України 5 жовтня 2017 року № 2163-VIII. Офіційний сайт Верховної Ради України. URL: <http://zakon.rada.gov.ua/laws/show/2163-19> (дата звернення: 15.12.2025).

178. Про рішення Ради національної безпеки і оборони України «Про Стратегію національної безпеки України» Указ Президента України від 14 вересня 2020 року. URL: <https://www.president.gov.ua/documents/3922020-35037> (дата звернення: 19.12.2024).
179. Про рішення Ради національної безпеки і оборони України від 11.03. 2021 р. "Про створення Центру протидії дезінформації". Указ Президента України. <https://zakon.rada.gov.ua/laws/show/106/2021#Text> (дата звернення: 19.12.2024).
180. Про рішення ради національної безпеки і оборони України від 15 жовтня 2021 року «Про стратегію інформаційної безпеки»: Указ Президента України від 28 грудня 2022 року № 685/2021 / Офіційний веб-портал Президента України. URL: <https://zakon.rada.gov.ua/laws/show/685/2021#n33> (дата звернення: 19.12.2024).
181. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України». Указ Президента України від 25 лютого 2017 р. № 47/2017 <https://zakon.rada.gov.ua/laws/show/47/2017#Text> (дата звернення: 19.12.2024).
182. Про Службу безпеки України. Закон України. <https://zakon.rada.gov.ua/laws/show/2229-12#Text> (дата звернення: 19.08.2025).
183. Про утворення територіального органу Національної поліції. Постанова Кабінету Міністрів України від 13 січня 2023 р. № 30. <https://zakon.rada.gov.ua/laws/show/30-2023-%D0%BF#Text> (дата звернення: 09.12.2025).
184. Про Цілі сталого розвитку України на період до 2030 року. Указ Президента України. URL: <https://zakon.rada.gov.ua/laws/show/722/2019#Text> (дата звернення: 09.12.2025).
185. Проект нового Кримінального кодексу України: передумови розробки, концептуальні засади, основні положення : монографія / П. П. Андрушко та ін. ; за заг. ред. Ю. В. Бауліна, М. І. Хавронюка. Київ : АртЕк, 2024. 494 с.

186. Протидія когнітивній війні: інформованість і стійкість. НАТО Ревю. 20.05.2021. URL: <https://www.nato.int/docu/review/uk/articles/2021/05/20/protidya-kognitivnj-vjn-nformovanst-stjkst/index.html> (дата звернення: 19.12.2024).
187. Пчеліна О.В., ПчелінВ.Б. Використання новітніх технологій під час досудового розслідування кримінальних правопорушень. *Vědaaperspektivy*. 2025. №8 (51).С.336–348.DOI [https://doi.org/10.52058/2695-1592-2025-8\(51\)-336-348](https://doi.org/10.52058/2695-1592-2025-8(51)-336-348)
188. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви [95/46/ЄС](#) (Загальний регламент про захист даних). URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення: 09.12.2025).
189. Рзаєва, Г. Захист прав людини, порушених внаслідок кіберзлочинів у глобальному інформаційному суспільстві. *Науковий вісник Дніпровського державного університету внутрішніх справ*. 2025. (2). С. 35–41. <https://doi.org/10.31733/2078-3566-2020-2-35-41> (дата звернення: 09.01.2026).
190. Ричка Д. О. Особливості кримінально-правової кваліфікації злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Дис на здобуття наукового ступеня кандидата юридичних наук за спец. 12.00.08. Університет державної фіскальної служби України, Ірпінь 2019. 208 с. <https://www.nusta.edu.ua/wp-content/uploads/2016/11/Dis-Ричка.pdf> (дата звернення: 09.12.2025).
191. Ричка Д. О., Цифрова трансформація та її вплив на тіньову економіку в енергетичному секторі України. *Актуальні проблеми вітчизняної юриспруденції* № 3. 2025. С.189-196. DOI <https://doi.org/10.32782/2408-9257-2025-3-25> URL: https://apnl.dnu.in.ua/3_2025/27.pdf (дата звернення: 09.12.2025).

192. Рижков М.М., Рубан А. Стратегія інформаційної і кібербезпеки ЄС: сучасний вимір. Міжнародні відносини. Серія «Політичні науки». 2019. № 21. URL: http://journals.iir.kiev.ua/index.php/pol_n/article/view/3866 (дата звернення: 12.03.2026).
193. Сачко О.В. Хорошун О.В. Міжнародні стандарти та досвід зарубіжних країн забезпечення ефективності розслідування корупційних кримінальних правопорушень. *Держава та регіони*. Серія: Право. 2024. № 4. с. 112-116. URL: http://law.stateandregions.zp.ua/archive/4_2024/19.pdf (дата звернення: 09.12.2025).
194. Сачко О.В. Забезпечення публічної безпеки органами Національної поліції та органами Служби безпеки України під час воєнного стану. *Актуальні проблеми вітчизняної юриспруденції*. 2023. № 6. С. 128-133.
195. Селецький О. В., Крес Н. О. Інформаційна безпека в умовах воєнного стану як складова національної безпеки. *Актуальні проблеми політики*. 2025. Вип. 76. С. 43-46. DOI <https://doi.org/10.32782/app.v76.2025.6> URL: https://app.nuoua.od.ua/archive/76_2025/8.pdf (дата звернення: 09.01.2026).
196. Сироватченко, М. Правові аспекти забезпечення кібербезпеки в Україні: сучасні виклики та роль національного законодавства // *Вісник Національного університету «Львівська політехніка»*. Серія «Юридичні науки». 2024. Том 11, № 1(41), С. 314-320. DOI: <https://doi.org/10.23939/law2024.41.314> URL: <https://science.lpnu.ua/uk/law/vsi-vypusky/vypusk-11-nomer-1-41-2024/pravovi-aspekty-zabezpechennya-kiberbezpeky-v-ukrayini> (дата звернення: 09.12.2025).
197. Ситуаційний центр забезпечення кібербезпеки СБУ. <https://cybersecurity.gov.ua/en> (дата звернення: 19.01.2026).
198. Смотрич Д.В., Браїлко Л. Інформаційна безпека в умовах воєнного стану. *Науковий вісник Ужгородського Національного Університету*, 2023. Серія ПРАВО. Випуск 77. Ч. 2. С. 121-127. DOI <https://doi.org/10.24144/2307-3322.2023.77.2.20> URL: <https://visnyk-juris-uzhnu.com/wp-content/uploads/2023/06/22-2.pdf> (дата звернення: 09.12.2025).

199. Солових Є.П., Солових Є.М. Роль ООН у забезпеченні інформаційної безпеки у сучасному світі <https://ekhnuir.karazin.ua/server/api/core/bitstreams/c46e5d5d-1388-4d07-9700-06760be12451/content> (дата звернення: 19.12.2025).
200. Солодовник В. І., Шевчук Д. Л. Системи і технології зв'язку, інформатизації та кібербезпеки: актуальні питання і тенденції розвитку: збірник матеріалів V Міжнародної науково-технічної конференції. К.: Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, 2025. С. 260-261. URL: <https://mitit.mil.gov.ua/api/files/2572> (дата звернення: 09.01.2026).
201. Солончук, І. В. Теоретичні проблеми правового регулювання інформаційних відносин в умовах інформаційного суспільства / Солончук І. В. // Правові новели : науковий юридичний журнал. 2024. № 22. С. 126-133. DOI: <https://doi.org/10.32782/ln.2024.22.17> . URI <https://ela.kpi.ua/handle/123456789/68072> (дата звернення: 09.12.2025).
202. Степко О.М. Аналіз головних складових інформаційної безпеки держави. Наук. вісн. Ін-ту міжнар. відносин НАУ. Сер. : Економіка, право, політологія, туризм. К., 2011. Вип. 1 (3). С. 90–99.
203. Стійкість, відновлення та відбудова – презентація Плану дій Ради Європи для України та перше засідання Керівного комітету. 24 квітня 2023 року. URL: <https://www.coe.int/uk/web/kyiv/>
204. Столяр О. Міжнародно-правові проблеми визначення та класифікація кіберзлочинів. Юридичний журнал. 2017. № 4. С. 190–193. URL: <http://www.jurnaluljuridic.in.ua/archive/2017/4/43.pdf> (дата звернення: 09.12.2025).
205. Стрельцов Є. Л. Рациональний дискурс про кримінальне право : монографія. Київ : Юрінком Прес, 2024. 468 с.
206. Судова статистика. Форма No 7 «Звіт про склад засуджених»: URL: http://court.gov.ua/inshe/sudova_statystyka/ (дата звернення: 19.12.2025).

207. Таволжанський О. В. Особливості забезпечення кібербезпеки у сучасному світі: огляд суб'єктів запобігання кіберзлочинності. *Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького: Журнал. Серія Право*. 2018. № 6(18). С. 154-163
208. Талліннський механізм: Україна та міжнародні партнери започаткували новий інструмент співпраці у кіберпросторі (2023). Урядовий портал. URL: <https://www.kmu.gov.ua/news/tallinnskyi-mekhanizm-ukraina-tamizhnarodni-partnery-zapochatkuvaly-novyi-instrument-spivpratsi-u-kiberprostori> (дата звернення: 09.12.2025).
209. Тихомиров О. Д. Юридична компаративістика: філософські, теоретичні та методологічні проблеми. Київ : Знання, 2005. 334 с.
210. Тихомиров О. Забезпечення інформаційної безпеки: теоретико-правовий аспект. *Право України*. 2011. № 4. С. 252-259
211. Тінін Д., Мислива О. Деякі аспекти інформаційної безпеки українського населення на тимчасово окупованих територіях. Матеріали I Міжнародної наукової конференції «Теорія модернізації в контексті сучасної світової науки» (м. Полтава, 23 червня 2023). С. 137–138. URL: <https://archive.mcnd.org.ua/index.php/conference-proceeding/article/download/636/646/657> (дата звернення: 09.12.2025).
212. Топчій В. В., Бодунова О. М. Система кримінальних правопорушень у сфері інформаційних технологій : міжнародно-правовий вимір. Ірпінський юридичний часопис. Серія: право. 2023. Вип. 1 (10). С. 187–194.
213. Торбас О. О. OSINT при розслідуванні кримінальних правопорушень: підручник. Одеса: Видавництво «Юридика», 2024. 180 с.
214. Триняк В.Ю. Інформаційна безпека як соціокультурний феномен (соціально-філософський аналіз): автореф. дис... канд. філософ. наук : 09.00.03 / В.Ю. Триняк ; Дніпропетр. нац. ун-т ім. О.Гончара. Д., 2009. 19 с.
215. Тунік А. В. Правові основи захисту персональних даних : дис. ... канд. юрид. наук : 12.00.07. Київ, 2012. 229 с.

216. Турбулентність глобальних геополітичних процесів і проблеми національної безпеки : монографія / [О. М. Кириленко, М. А. Козловець, Г. Л. Рябцев та ін.] ; Аналіт. центр сучас. гуманітаристики. Харків: Право, 2025. 306 с.
217. Федчак І.А. Історія, сутність та поняття моделі здійснення правоохоронної діяльності на основі прогнозів (Predictive Policing). *Науковий Вісник Львівського державного університету внутрішніх справ*. № 3. 2023. С. 141-147. URL: <https://dspace.lvduvs.edu.ua/bitstream/1234567890/5944/1/18.pdf>
218. Філіпенко Н.Є., Лукашевич С.Ю. Діяльність судово-експертних установ щодо запобігання злочинності з використанням прогресивних інформаційних методик та технологій. *Наукові інновації та передові технології* 2023. № 14(28). С. 487-496.
219. Фролова О. М. Роль ООН в системі міжнародної інформаційної безпеки. *Міжнародні відносини. Серія «Політичні науки»*. 2018. №18-19. URL : http://journals.iir.kiev.ua/index.php/pol_n/article/view/3468.
(дата звернення: 09.12.2025).
220. Хейман С. Кістяківський. Боротьба за національні та конституційні права в останні роки царату. К. : Основні цінності, 2000. 304с.
221. Худолей, Я., & Загребельна, Н. (2023). Захист персональних даних у період дії в Україні правового режиму воєнного стану: загальнотеоретичні аспекти. *Legal Bulletin*, 75–82. <https://doi.org/10.31732/2708-339X-2023-08-75-82> (дата звернення: 09.12.2025).
222. Центр протидії дезінформації. Веб-сайт. URL: <https://cpd.gov.ua/warnin/fejkovyj-syuzhet-vid-imeni-united24-media-pro-uczimto-otruyennya-vijskovyih-zsu-yizheyu-z-magazyniv-u-kursku/> (дата звернення 15.12.2025)
223. Черниш Р. Правовий досвід країн європейського союзу у сфері протидії поширенню фейкової інформації. *Інформаційне право*. 2019. № 10. С. 123–128.
224. Шемчук В.В. Зарубіжний досвід забезпечення інформаційної безпеки держави. *Порівняльно-аналітичне право*. 2019. № 2. С. 188-191.

225. Шаблистий В.В. Цифрова ера кримінального процесу: можливості ІТ-систем у досудовому розслідуванні. Юридичний науковий електронний журнал. 2025. №1. С.630–633. DOI <https://doi.org/10.32782/2524-0374/2025-1/146>.
226. Шишко В.В., Горошко В.В. Вимір права на інформаційну безпеку у міжнародному праворозумінні. *Науковий вісник Ужгородського національного університету*, 2025. Серія ПРАВО. Вип. 91. Ч. 3. С. 275-281. URL: <https://visnyk-juris-uzhnu.com/wp-content/uploads/2025/11/43-1.pdf> (дата звернення: 09.12.2025).
227. Юзікова Н.С. Інформаційні загрози та заходи протидії інформаційній агресії: зарубіжний досвід.: матеріали всеукраїнського науково-практичного круглого столу. Інформаційна агресія в сучасному світі: правовий аналіз та протидія Харків, 21 червня 2024 р. : електрон. наук. вид. / редкол.: В. С. Батиргареева та ін. – Харків : Майдан, 2024. С. 35-42. URL: https://ivpz.kh.ua/wp-content/uploads/2024/11/%D0%97%D0%B1%D1%96%D1%80%D0%BD%D0%B8%D0%BA_%D1%96%D0%BD%D1%84%D0%BE%D0%B0%D0%B3%D1%80%D0%B5%D1%81%D1%96%D1%8F_2024-%D0%BD%D0%B0-%D1%81%D0%B0%D0%B9%D1%82.pdf (дата звернення: 19.12.2025).
228. Юзікова Н.С. Інформаційна безпека у системі заходів запобігання кримінальним правопорушенням у сфері інформаційних технологій: досвід країн ЄС та США. *Аналітично-порівняльне правознавство* 2023. № 5. С.506-512 <https://app-journal.in.ua/wp-content/uploads/2023/11/93.pdf> (дата звернення: 19.12.2025).
229. Юзікова Н.С. Кримінологічний аналіз деструктивного впливу інтернет-контенту на міжособистісне спілкування у ювенальному середовищі. Збірник тез Всеукраїнської науково-практичної конференції "Забезпечення принципів поваги, захисту та реалізації прав дитини у цифровому середовищі». (м. Дніпро 23 листопада 2023р.) Дніпровський національний університет імені Олеся Гончара, Д.: Ліра 2023. С. 154-160. URL:

https://www.dnu.dp.ua/docs/ndc/2023/materiali%20konf/Zbirnyk_Konf_Zahyst%20prav_dytny_v_cifrovomu_sviti.pdf (дата звернення: 09.12.2025).

230. Юхно О. О., Загуменний О. О. Використання сучасних інформаційних технологій працівниками поліції при проведенні негласних слідчих (розшукових) дій : навч. посіб. 2-ге вид., допов. і перероб. Х.: Колегіум, 2020. 116 с.
231. Якубівська Ю. Є. Світові тенденції розвитку кіберзлочинності. *Зовнішня торгівля: економіка, фінанси, право. Серія. Економічні науки*. 2014. № 5-6 (76-77). URL: [http://zt.knute.edu.ua/files/2014/5-6\(76-77\)/uazt_2014_5-6_14.pdf](http://zt.knute.edu.ua/files/2014/5-6(76-77)/uazt_2014_5-6_14.pdf) (дата звернення: 05.12.2024).
232. Яровой, Т. С. OSINT, як перспективний інструмент контролю за лобістською діяльністю в контексті державної безпеки. *Експерт: парадигми юридичних наук і державного управління*. 2019. (4(6), 201-208. [https://doi.org/10.32689/2617-9660-2019-4\(6\)-201-208](https://doi.org/10.32689/2617-9660-2019-4(6)-201-208) (дата звернення: 09.12.2025).
233. Яхно О. М. Україна в сучасному геополітичному просторі (політико-медійний аспект) : дис.... канд. політ. наук : 23.00.03. К., 2006. 170 с.
234. Akshay Joshi. The cyber threats to watch in 2026 – and other cybersecurity news // World Economic Forum. URL: <https://www.weforum.org/stories/2026/02/2026-cyberthreats-to-watch-and-othercybersecurity-news/> (дата звернення 18.02.2026).
235. Albanese Jay S. A Typology of Cybercrime: An Assessment of Federal Prosecutions. *Journal of Criminal Justice and Law*. 2022. Vol. 6. Issue 1. URL: <https://jcjl.pubpub.org/pub/vm45gchn/release/1> (дата звернення 21.03.25).
236. AI Safety Institutes: Prospects and Challenges. <https://dc.org.ua/news/instytuty-bezpeky-shi-perspektyvy-ta-vyklyky>
237. Andress, J. (2014). *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice*. 190p. https://web.xidian.edu.cn/yanzheng/files/20160919_170521.pdf

238. Artificial Intelligence Risk Management Framework (AI RMF 1.0) / National Institute of Standards and Technology. U.S. Department of Commerce, 2023. (NIST AI 100-1). URL: <https://doi.org/10.6028/NIST.AI.100-1>.
239. Assessment of National Cyber Capabilities: What is the Level of Cybersecurity Maturity r Capabilities: of Ukraine According to the ENISA Methodology? https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwj6hvj3iZCUAxXohSsGHULIDIUQFnoECCkQAQ&url=https%3A%2F%2Funderstandingcyberwar.org%2Fwp-content%2Fuploads%2F2024%2F09%2FProekt_1_en.pdf&usg=AOvVaw37i270N6QBNQHdSr1BeXqi&opi=89978449
240. Azerbaijan. Conference Paper. 2023. Dec. URL: https://www.researchgate.net/publication/376488076_International_Cooperation_a_gainst_Cybercrime_the_Perspective_of_Azerbaijan
241. Baezner M. Cyber and Information Warfare in the Ukrainian Conflict. Version 2. Zürich: Center for Security Studies (CSS). ETH Zürich. October 2018. URL: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-forsecurities-studies/pdfs/20181003_MB_HS_RUS-UKR%20V2_rev.pdf (дата звернення 21.03.25).
242. Balajanov E. International Cooperation against Cybercrime: the Perspective of Berkeley Protocol on Digital Open Source Investigations: A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law. URL:<https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source> (дата звернення 21.03.25).
243. Berkeley Protocol on Digital Open Source Investigations: A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law. URL:<https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source> (дата звернення 21.12.24)

244. Brichambaut M. P. de. The Indivisibility of Euro-Atlantic Security: Presentation at the 18th Partnership for Peace Research Seminar. 2010 // URL: <https://www.osce.org/les/f/documents/5/f/41452.pdf>
245. Bronk C., Collins G., Wallach D. The Ukrainian Information and Cyber War / The Cyber Defense Review. 2023. URL: https://cyberdefensereview.army.mil/Portals/6/Documents/2023_Fall/CDR_V8N3_Fall_2023_03-Bronk.pdf?ver=U0B1Cl6qzBlZrFPxIjqOEg%3D%3D.
246. Bruce M., Lusthaus J., Kashyap R., Phair N., Varese F. Mapping the global geography of cybercrime with the World Cybercrime Index. PLoS.One. 2024. April 10. DOI: <https://doi.org/10.1371/journal.pone.0297312>
247. Case of Benedik v. Slovenia (Application no. 62357/14) : Judgment / European Court of Human Rights. Strasbourg, 24 April 2018. URL: <https://hudoc.echr.coe.int/ukr?i=001-182455> (date of access: 01.03.2026).
248. Case of Delfi AS v. Estonia (Application no. 64569/09) : Judgment [GC] / European Court of Human Rights. Strasbourg, 16 July 2015. URL: <https://hudoc.echr.coe.int/eng?i=001-163044> (date of access: 01.03.2026).
249. Case of K.U. v. Finland (Application no. 2872/02) : Judgment / European Court of Human Rights. Strasbourg, 02 December 2008. URL: <https://hudoc.echr.coe.int/eng?i=001-89964> (date of access: 01.03.2026).
250. Case of Szabó and Vissy v. Hungary (Application no. 37138/14) : Judgment / European Court of Human Rights. Strasbourg, 12 January 2016. URL: <https://hudoc.echr.coe.int/eng?i=001-160020> (date of access: 01.03.2026).
251. Center for AI Standards and Innovation (CAISI). <https://www.nist.gov/caisi>
252. Convention on Cybercrime (Budapest Convention. 23.XI.2001). URL: <https://www.coe.int/en/web/cybercrime/the-budapest-convention> (дата звернення 21.03.25).
253. Consolidated version of the Treaty on the Functioning of the European Union. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016E%2FTXT-20200301>

254. Cognitive Security & Education Forum (COGSEC).
URL:<https://www.cogsec.org/>
255. Crimes related to computer networks: background paper for the Workshop on Crimes related to the Computer Network. Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders (Vienna, 10-17 April 2000). A/CONF.187/10. United Nations. URL: <https://digitallibrary.un.org/record/432653> (дата звернення 21.03.25).
256. Cuellar, M., et al. Accuracy and Fairness of Facial Recognition Technology in Low-Quality Police Images. URL: <https://arxiv.org/abs/2505.14320>.<https://doi.org/10.48550/arXiv.2505.14320>
257. Cyber Incidents and Attacks Disrupt Enterprise Business Operations for Two Weeks, Reveals First Comprehensive Global Cyber Resilience Survey. URL: <https://finance.yahoo.com/news/cyber-incidents-attacks-disrupt-enterprise131500647.html>
258. Cybersecurity Capacity Maturity Model for Nations (CMM). Revised Edition. *Global Cyber Security Capacity Centre, University of Oxford*. 2021. URL: <https://gcscc.ox.ac.uk/cmm-2021-edition> (дата звернення 21.03.25).
259. Cybersecurity is a fascinating and highly scientific field spanning a range of disciplines and involving a wealth of organisations and actors, from both the public sector and the business world, within France and internationally. URL: <http://www.ssi.gouv.fr/en/mission/word-from-director-general/>
260. Cybersecurity skills matter more than headcount in the AI era // FoundryCo, Inc. (<https://www.csoonline.com/article/4108270/cybersecurity-skills-matter-more-thanheadcount-in-the-ai-era.html>). 02.01.2026)
261. Décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information ». URL:https://www.legifrance.gouv.fr/loda/id/JORFTEXT0000_208_28212 (дата звернення 21.01.2026)

262. Diogenes, Y., & Ozkaya, E. (2022). *Cybersecurity – Attack and Defense Strategies: Countermeasure design tools for changing the security landscape* (3rd Edition). Packt Publishing, 2022. 570 p. ISBN: 9781803248776. <https://k.twirpx.link/file/4414375/> (дата звернення 21.03.25).
263. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). *Official Journal of the European Union*. 2022. L 333. P. 80–152. URL: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj> (дата звернення 21.01.2026).
264. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA/. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32013L0040> (дата звернення 21.03.25).
265. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995. *Official Journal of the European Communities* No L 281/31. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046> (дата звернення 20.12.2025)
266. Ellehuus R., Zagorski A. Restoring the European Security Order. 2019 // URL: <https://russiancouncil.ru/papers/CSIS-RIAC-Ellehuus-Zagorski-Restoring-EuropeanOrder.pdf> (дата звернення 21.03.25).
267. Ellie Winslow, Joanna Bouckaert. How cybersecurity can best navigate geopolitics to secure a resilient and open digital future 5 // World Economic Forum. <https://www.weforum.org/stories/2026/02/cybersecurity-and-geopolitics-the-challenges-to-build-resilience-in-a-fragmented-world/> (дата звернення 21.01.2026).
268. eSafety Commissioner: Online Safety Education and Reporting System. <https://www.esafety.gov.au> (дата звернення 21.01.2026).

269. Fatemah A. The Pivotal Role of International Human Rights Law in Defeating Cybercrime: Amid a (UN-Backed) Global Treaty on Cybercrime. *Vanderbilt Journal of Transnational Law*. 2022. Vol. 55, no. 5. P. 1117–1144. URL: <https://scholarship.law.vanderbilt.edu/cgi/viewcontent.cgi?article=2766&context=vjtl> (дата звернення 21.01.2026).
270. Fava, D. S., Byers, S. R., Yang, S. J. (2008). Projecting Cyberattacks Through VariableLength Markov Models. *IEEE Transactions on Information Forensics and Security*, 3 (3), 359–369. doi: <http://doi.org/10.1109/tifs.2008.924605> (дата звернення 21.03.25).
271. Federal Information Security Modernization Act of 2022-H.R.6497 ([FISMA 2022](#)) . URL: <https://www.congress.gov/bill/117th-congress/house-bill/6497> (дата звернення 21.01.2026)
272. Freeman, L. (2018). Digital Evidence and International Criminal Justice. *Journal of International Criminal Justice*, 16(1), 163-181. DOI: <https://doi.org/10.1093/jicj/mqy007> (дата звернення 21.03.25).
273. Fruhlinger J. What is information security? Definition, principles, and jobs. CSO United States. 17.01.2020. URL: <https://www.csoonline.com/article/3513899/what-is-information-security-definition-principles-and-jobs.html> (дата звернення 21.03.2025)
274. Garbis J., Chapman J. W. Zero Trust Security: An Enterprise Guide. Berkeley, CA : Apress, 2021. 300 p. DOI: <https://doi.org/10.1007/978-1-4842-6702-8>(дата звернення 21.03.25).
275. General Data Protection Regulation (GDPR). URL: <https://gdpr.eu> (дата звернення 21.01.2026)
276. Get Cyber Safe. <https://www.getcybersafe.gc.ca/en> (дата звернення 21.01.2026)
277. Global Cybersecurity Outlook 2024 : Insight Report / World Economic Forum. Geneva, 2024. 44 p. URL:

https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf

(дата звернення 21.01.2026)

278. Grunewald, D., Liitzenberger, M., Chinnow, J., Bye, R., Bsufka, K., Albayrak, S. (2011). Agent-based network security simulation. Proceedings of The 10th International Conference on Autonomous Agents and Multiagent Systems, 3, 1325–1326.
279. Heather J. Williams, Ilana Blum. Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise . Published May 17, 2018. URL: https://www.rand.org/pubs/research_reports/RR1964.html (дата звернення 21.03.25).
280. How Employers Are Rethinking Cybersecurity Jobs Recruitment // Cyber Management Alliance. URL: <https://www.cm-alliance.com/cybersecurity-blog/how-employers-are-rethinking-cybersecurity-jobs-recruitment> (дата звернення 12.01.2026)
281. Information security, cybersecurity and privacy protection. Information security management systems. Requirements. ISO/IEC 27001:2022. URL: <https://www.iso.org/standard/27001> (дата звернення 21.01.2026)
282. Information technology. Artificial intelligence. Guidance on risk management. ISO/IEC 23894:2023. URL: <https://www.iso.org/standard/77304.html> (дата звернення 18.05.2025 р.)
283. ISO (Online Browsing Platform). Офіційна платформа.URL: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en> (дата звернення 21.01.2026)
284. Jajodia, S., Noel, S. (2010) Advanced cyber attack modeling analysis and visualization. Technical report, DTIC Document. Available at: <https://apps.dtic.mil/dtic/tr/fulltext/u2/a516716.pdf> (14.01.2026р.)
285. Jānis Bērziņš. Russia's New Generation Warfare in Ukraine: *Implications for Latvian Defense Policy. Policy Paper*. April 2014. № 02. P. 5-13.

286. Jesteśmy państwowym instytutem badawczym. NASK. <https://www.nask.pl/instytut> (14.01.2026p.)
287. Julian Horsey. Cybersecurity Trends 2026 : From Unapproved AI to Passkeys, Clear Steps to Stay Safe. Geeky Gadgets. <https://www.geeky-gadgets.com/cybersecurity-trends-2026/> (14.01.2026p.)
288. Justin Rende. The 6 Cybersecurity Trends That Will Shape 2026. ISACA (<https://www.isaca.org/resources/news-and-trends/industry-news/2026/the-6-cybersecurity-trends-that-will-shape-2026>). (14.01.2026p.)
289. Kindervag J. Build Security Into Your Network's DNA: The Zero Trust Network Architecture. *Forrester Research*. 2010. URL: https://www.virtualstarmedia.com/downloads/Forrester_zero_trust_DNA.pdf (date of access: 23.12.2025)
290. Kounadi, O., Ristea, A., Araujo, A. et al. A systematic review on spatial crime forecasting. *CrimeSci* 9.7, 2020. URL: <https://doi.org/10.1186/s40163-020-00116-7> (14.01.2026p.)
291. Le Commandement de la cyberdéfense (COMCYBER). *Ministère des Armées*. URL: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiZy4C30ISUAxXvR_EDHfr-ASAQFnoECBUQAQ&url=https%3A%2F%2Fwww.defense.gouv.fr%2Fcomcyber%2Fcommandement-cyberdefense-comcyber&usg=AOvVaw2Vnk9zW-vwkW4-KVWSAxGF&opi=89978449 (дата звернення 21.01.2026).
292. LOI n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale. URL: <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000028338825> (дата звернення 21.01.2026).
293. Malcolm Gladwell. *The Tipping Point*. Little, brown and company. Boston. New York .London. URL: https://binyaprak.com/images/blog_articles/123/the-tipping-point.pdf (дата звернення 18.05.2025 p.)

294. Media Literacy in Finland / National Media Education Policy. <https://okm.fi/en/media-literacy> (дата звернення 21.03.25).
295. Michael Glassman, Min Ju Kang. Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT). *Computers in Human Behavior*. Volume 28, Issue 2. 2012. P. 673-682. URL:<https://doi.org/10.1016/j.chb.2011.11.014>. (дата звернення 18.05.2025 р.)
296. Milov, O., Kostyak, M., Milevsky, S., Pogasiy, S. (2019). Methods for modeling agent behavior in information and communication systems. *Control, Navigation and Communication Systems. Academic Journal*, 6 (58), 63–70. doi: <http://doi.org/10.26906/sunz.2019.6.063> (дата звернення 18.05.2025 р.)
297. Moskal, S., Kreider, D., Hays, L., Wheeler, B., Yang, S. J., Kuhl, M. (2013) Simulating attack behaviors in enterprise networks. *Proceedings of 2013 IEEE Conference on Communications and Network Security (CNS)*. National Harbor, 359–360. doi: <http://doi.org/10.1109/cns.2013.6682726> (дата звернення 21.03.25).
298. Moskal, S., Wheeler, B., Kreider, D., Kuhl, M. E., Yang, S. J. (2014). Context model fusion for multistage network attack simulation. *Proceedings of Military Communications Conference (MILCOM)*. Baltimore, 158–163. doi: <http://doi.org/10.1109/milcom.2014.32> (дата звернення 21.03.25).
299. M-trends 2016 (2016). Mandaint: A FireEye Company. Technical report. URL: <https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-mtrends-2016.pdf> (дата звернення 21.03.25).
300. National Cyber Security Framework Manual / ed. by A. Klimburg. Tallinn : *NATO CCD COE Publications*, 2012. 244 p. URL: https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf (дата звернення: 23.04.2026)
301. National Cyber Strategy 2022. *HM Government*. Policy paper. 2022. URL: <https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022> (дата звернення: 21.01.2026).
302. National Security Agency (NSA). *Mitigating Cloud Vulnerabilities*. Cybersecurity Information. U.S. Department of Defense. URL:

<https://www.nsa.gov/Press-Room/Cybersecurity-Advisories-Guidance/smdpage16681/15/smdcat16681/Cybersecurity/smdsort16681/title/>

(дата звернення 21.03.25).

303. NATO standard AJP-10. Allied Joint Doctrine for strategic communications. March 2023. URL: https://assets.publishing.service.gov.uk/media/6525459d244f8e00138e7343/AJP_10_Strat_Comm_Change_1_web.pdf (дата звернення – 05.05.2025).
304. NATO standard AJP-3.10.1(A) Allied Joint Doctrine for psychological operations. October 2007. URL: <https://info.publicintelligence.net/NATO-PSYOPS.pdf> (дата звернення 05.05.2025).
305. Naveen Goud. Over 10% of UK businesses unlikely to survive a Cyber Attack. Cybersecurity Insiders <https://www.cybersecurity-insiders.com/over-10-of-uk-businesses-unlikely-to-survive-a-cyber-attack/> (дата звернення 21.01.2026 р.).
306. NIST Risk Management Framework. Information Technology Laboratory. Computer Security Resource Center. URL: <https://csrc.nist.gov/projects/risk-management/fisma-background> (дата звернення 20.02.2026 р.) .
307. NIST SP 800-53 Control Overlays for Securing AI Systems Concept Paper August 14, 2025. URL: <https://csrc.nist.gov/csrc/media/Projects/cosais/documents/NIST-Overlays-SecuringAI-concept-paper.pdf> (дата звернення 20.02.2026 р.).
308. Official Journal of the European Union, L 300, 11 November 2008. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL%3A2008%3A300%3ATOC> (дата звернення 20.02.2026 р.).
309. Pawlak P. Capacity building in cyberspace as an instrument of foreign policy. *Global Policy*: Vol. 7, No. 1. P. 83–92. <https://doi.org/10.1111/1758-5899.12298>
URL: <https://onlinelibrary.wiley.com/doi/10.1111/1758-5899.12298> (дата звернення 21.01.2026).
310. Patrick Ryder. How Restaurants, Especially Franchises, Should Look at Cyber Security. WTWH Media, LLC. URL: <https://www.qsrmagazine.com/story/how->

- [restaurants-especially-franchisesshould-look-at-cyber-security/](#) (дата звернення 21.03.25).
311. Poland sees ‘Russian cyberattack’ behind fake military draft report. URL:<https://www.euractiv.com/section/elections/news/poland-sees-russian-cyberattack-behind-fake-military-draft-report/> (дата звернення 21.01.2026).
312. Principles of Information Security, Sixth Edition Michael E. Whitman and Herbert J. Mattord. URL: [https://unidel.edu.ng/focelibrary/books/Principles%20of%20Information%20Security%20by%20Whitman,%20Michael%20Mattord,%20Herbert%20\(z-lib.org\).pdf](https://unidel.edu.ng/focelibrary/books/Principles%20of%20Information%20Security%20by%20Whitman,%20Michael%20Mattord,%20Herbert%20(z-lib.org).pdf) (дата звернення 21.03.25).
313. Qin, X., Lee, W. (2004). Attack plan recognition and prediction using causal networks. Proceedings of 20th Annual Computer Security Applications Conference. Tucson, 370–379. doi: <http://doi.org/10.1109/csac.2004.7> (дата звернення 21.01.2026).
314. Qutaishat, M. A., & Al-Manasra, R. M. (2021). *Disentangling the Concept of Information Security Properties*. 29th European Conference on Information Systems. Enabling Effective Information Security Governance. June 2021. URL: <https://www.fim-rc.de/Paperbibliothek/Veroeffentlicht/1160/wi-1160.pdf> (дата звернення 21.01.2026).
315. Rand Waltzman. The Weaponization of Information The Need for Cognitive Security. URL: https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT473/RAND_CT473.pdf (дата звернення 20.10.2025 р.)
316. Riley, M., Elgin, B., Lawrence, D., Matlack, C. (2014). Missed alarms and 40 million stolen credit card numbers: How target blew it. Available at: <http://www.bloomberg.com/news/articles/2014-03-13/target-missed-warnings-in-epic-hack-of-credit-card-data> (дата звернення 21.03.25).
317. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive

- 95/46/EC (General Data Protection Regulation). Official Journal of the European Union. 2016. L 119. P. 1–88. URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>.
318. Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act). *Official Journal of the European Union*. 2024. L 2024/2847. URL: <https://eur-lex.europa.eu/eli/reg/2024/2847/oj> (дата звернення: 21.01.2026).
319. Resolution adopted by the General Assembly. Developments in the field of information and telecommunications in the context of international security 55/28. URL: <https://undocs.org/ru/A/RES/55/28> (дата звернення 21.01.2026).
320. Revue stratégique de cyberdéfense. *Secrétariat général de la défense et de la sécurité nationale (SGDSN)*. Paris, 2018. 166 p. URL: <https://www.sgdsn.gouv.fr/files/files/Publications/revue-cyber-resume-in-english.pdf> (дата звернення: 21.01.2026).
321. Riley, M., Elgin, B., Lawrence, D., Matlack, C. (2014). Missed alarms and 40 million stolen credit card numbers: How target blew it. Available at: <http://www.bloomberg.com/news/articles/2014-03-13/target-missed-warnings-in-epic-hack-of-credit-card-data> (дата звернення 20.10.2025 р.)
322. Rzayeva G. Protection of human rights violated by cybercrimes in global information. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2020. № 2 (105). С. 35–41. URL: <https://doi.org/10.31733/2078-3566-2020-2-35-41> (дата звернення 21.03.25).
323. Schimmelfennig F. NATO's Enlargement to the East: An Analysis of Collective Decision-Making: EAPC-NATO Individual Fellowship Report 1998–2000. 2000 // URL: <https://www.nato.int/acad/fellow/98-00/schimmelfennig.pdf> (дата звернення 21.01.2026).

324. Schmitt, M. N. (Ed.). (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2nd ed.). Cambridge University Press. DOI: <https://doi.org/10.1017/9781316822524> (дата звернення 21.03.25).
325. Secure Our World. <https://www.cisa.gov/secure-our-world> (дата звернення 21.01.2026).
326. Security and Privacy Controls for Information Systems and Organizations. NIST SP 800-53 Rev. 5 <https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final> (дата звернення 21.01.2026).
327. Security of NASA'S cloud computing services. February 7, 2017. Report No. IG-17-010. URL: <https://oig.nasa.gov/wp-content/uploads/2024/02/IG-17-010.pdf> (дата звернення 20.10.2025 р.)
328. Seminarium szkoleniowe pn. «Działania profilaktyczne policji w obszarze mowy nienawiści, hejtu, przestępstw z nienawiści oraz cyberzagrożeń» від 18.09.2025. Biuro Prewencji KGP. URL: <https://policja.pl/pol/aktualnosci/266636,Seminarium-szkoleniowe-pn-quotDzialania-profilaktyczne-Policji-w-obszarze-mowy-n.html> (дата звернення 21.01.2026).
329. Singapore introduces COSMIC platform for banks to flag money-laundering concerns. URL: <https://www.globalgovernmentfintech.com/singapore-cosmic-platform-launches/> (дата звернення 20.10.2025 р.)
330. Stotz, A., Sudit, M. (2007). Information fusion engine for real-time decisionmaking: A perceptual system for cyber attack tracking. Proceedings of 2007 10th International Conference on Information Fusion. Quebec, 1–8. doi: <http://doi.org/10.1109/icif.2007.4408113> (дата звернення 21.03.25).
331. The AI Seoul Summit. Published May 23, 2024. <https://www.csis.org/analysis/ai-seoul-summit> (дата звернення 20.10.2025 р.)
332. The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023. GOV.UK: Prime Minister's Office, 10 Downing Street. 2023. URL: <https://www.gov.uk/government/publications/ai-safety-summit-2023-the->

- [bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023](#) (дата звернення: 13.04.2026)
333. The NIST Controlled Unclassified Information Series SP 800-171, 800-171A, 800-172 and 800-172A Presentation - January 24, 2023. <https://csrc.nist.gov/Presentations/2023/nist-cui-guidance-update> (дата звернення 21.01.2026).
334. The police and neighborhood safety Broken windows by James Q. Wilson and George L. Kelling. URL: http://atlantic_monthly_broken_windows.pdf (дата звернення 21.01.2026).
335. The privacy act of 1974 (As Amended) <https://www.dodig.mil/Portals/48/Documents/Programs/Privacy%20Program/pa1974.pdf> (дата звернення 20.10.2025 р.)
336. The United Nations Convention against Cybercrime opens for signature in Hanoi. Office of Legal Affairs, United. URL: <https://www.un.org/ola/en/news/united-nations-convention-against-cybercrime-opens-signature-hanoi> (дата звернення 21.03.25).
337. The Federal Information Security Modernization Act of 2014 (FISMA 2014). URL: <https://www.cisa.gov/topics/cyber-threats-and-advisories/federal-information-security-modernization-act> (дата звернення 26.11.2025 р.)
338. UK Counter-Terrorism and Border Security Act 2019. URL: <https://www.legislation.gov.uk/ukpga/2019/3/contents> (дата звернення 20.10.2025 р.)
339. Valiullina, Z. V. (2016). Information security of corporate economics in the conditions of globalization. *European Journal of Management Issues*, 24(6), 34-43. <https://doi.org/10.15421/191604> (дата звернення 21.03.25).
340. Verizon. (2023). *Data Breach Investigations Report (DBIR)*. Basking Ridge, NJ: Verizon Enterprise Solutions. URL: <https://www.verizon.com/business/resources/reports/2023-data-breach-investigations-report-dbir.pdf> (дата звернення 26.11.2025 р.)

341. Wang, B., Cai, J., Zhang, S., Li, J. (2010). A network security assessment model based on attack-defense game theory. Proceedings of 2010 International Conference on Computer Application and System Modeling (ICCA SM). Taiyuan, 3, V3–639. doi: <http://doi.org/10.1109/iccasm.2010.5620536> (дата звернення 21.03.25).
342. Weber S. Shaping the Postwar Balance of Power: Multilateralism in NATO. International Organization. 1992. Vol. 46. № 3. P. 633–680
343. Wydziały prewencji KWP/KSP. URL: <https://www.policja.pl/pol/kgp/biuro-prewencji/wydzialy-prewencji-kwp/39264,dok.html> (дата звернення 26.11.2025 р.)
344. Xie, P., Li, J. H., Ou, X., Liu, P., Levy, R. (2010). Using bayesian networks for cyber security analysis. Proceedings of 2010 IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). Chicago, 211–220. doi: <http://doi.org/10.1109/dsn.2010.5544924> (дата звернення 21.03.25).
345. Yevseiev, S., Karpinski, M., Shmatko, O., Romashchenko, N., Gancarczyk, T., Falat, P. (2019). Methodology of the cyber security threats risk assessment based on the fuzzy-multiple approach. 19th International Multidisciplinary Scientific GeoConference SGEM2019, Informatics, Geoinformatics and Remote Sensing. Sofia, 437–444. doi: <http://doi.org/10.5593/sgem2019/2.1/s0> (дата звернення 21.03.25).
346. Yuzikova N. Criminology research of the influence of internet content on interpersonal communication and behavior of minors. Baltic Journal of Legal and Social Sciences, 2022 No. 3 DOI <https://doi.org/10.30525/2592-8813-2022-3-12 P. 94-101> (дата звернення 21.03.25).
347. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture*. NIST Special Publication 800-207. National Institute of Standards and Technology. URL: <https://csrc.nist.gov/publications/detail/sp/800-207/final> (дата звернення 21.09.24).

ДОДАТКИ

Додаток А

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

яких опубліковано основні наукові результати дисертації:

1. Олійник А. А. Сутність інформаційної безпеки як правового явища у національному та міжнародному просторі. *Актуальні проблеми вітчизняної юриспруденції* № 6. 2023. С.293-299. DOI <https://doi.org/10.32782/2408-9257-2023-6-45>.
2. Олійник А. А. Формування стійкого цифрового суспільства: превентивна роль інформаційної безпеки та кримінально-правової політики у запобіганні злочинності . *Актуальні проблеми вітчизняної юриспруденції* № 2. 2025. С. 177-182. DOI <https://doi.org/10.32782/2408-9257-2025-2-27>
3. Олійник А. А. Запобігання правопорушенням у сфері інформаційної безпеки: від захисту державного суверенітету до гарантування прав людини. *Актуальні проблеми вітчизняної юриспруденції* № 6. 2025. С.129-134. DOI <https://doi.org/10.32782/2408-9257-2025-6-19>
4. Олійник А.А. Кіберстійкість та права людини: імплементація міжнародних превентивних моделей у цифровий простір в Україні. *Аналітичне порівняльне правознавство* № 6. Ч. 3. 2025. С. 84-90. DOI <https://doi.org/10.24144/2788-6018.2025.06.3.12>
5. Юзікова Н.С., Олійник А. А. Напрями забезпечення правопорядку на звільнених територіях: інституційні підходи, довіра та практики взаємодії поліції й громади. *Науковий вісник УжНУ. Серія “Право”* № 93. Частина 4. 2026. С.247-255. DOI <https://doi.org/10.24144/2307-3322.2026.93.4.35>

які засвідчують апробацію матеріалів дисертації:

11. Олійник А.А. Організація безпеки інформаційного суверенітету для України як об'єкта глобальних інформаційних впливів Збірник тез Всеукраїнського науково-практичного юридичного форуму «Національна парадигма правового розвитку сучасної України» (Дніпровський національний університет імені Олеся Гончара, м. Дніпро, 18 травня 2023 року). Дніпро: Ліра, 2023. С. 334-340.

URL:<https://www.dnu.dp.ua/docs/ndc/>

[2023/materiali%20konf/new_NACIONALNA%20PARADIGMA.pdf](https://www.dnu.dp.ua/docs/ndc/2023/materiali%20konf/new_NACIONALNA%20PARADIGMA.pdf)

12. Олійник А.А. Модель забезпечення цифрової безпеки в мережі internet крізь призму досвіду зарубіжних країн. Збірник тез Всеукраїнської науково-практичної конференції "Забезпечення принципів поваги, захисту та реалізації прав дитини у цифровому середовищі». (м. Дніпро 23.листопада 2023) Дніпровський національний університет імені Олеся Гончара, Дніпро, Ліра, 2023. С.349-352 URL: https://www.dnu.dp.ua/docs/ndc/2023/materiali%20konf/new_Zbirnyk_Konf_Zahyst%20prav_dytny_v_cifrovomu_sviti.pdf

13. Олійник А.А. Окремі форми інформаційної агресії матеріали всеукраїнського науково-практичного круглого столу. Інформаційна агресія в сучасному світі: правовий аналіз та протидія Харків, 21 червня 2024 р. : електрон. наук. вид. / редкол.: В. С. Батиргареева та ін. – Харків : Майдан, 2024. С. 56-58. https://ivpz.kh.ua/wp-content/uploads/2024/11/%D0%97%D0%B1%D1%96%D1%80%D0%BD%D0%B8%D0%BA_%D1%96%D0%BD%D1%84%D0%BE%D0%B0%D0%B3%D1%80%D0%B5%D1%81%D1%96%D1%8F_2024-%D0%BD%D0%B0-%D1%81%D0%B0%D0%B9%D1%82.pdf

14. Олійник А. А. Міжнародне запобігання злочинності у сфері цифрових технологій у контексті захисту прав людини. Матеріали міжнародної науково-практичної конференції. Актуальні проблеми прав людини: від універсальних стандартів до національної практики : Київський університет права Національної академії наук України, 11 грудня 2025 р. Львів – Торунь : Liha-Pres, 2025. С. 100-104. DOI <https://doi.org/10.36059/978-966-397-557-3-27>

15. Олійник А.А. Методологічний потенціал генетичного підходу Б. О. Кістяківського у дослідженні генези прав людини. Матеріали Всеукраїнської науково-практичної конференції «Актуальні проблеми правової науки. Запоріжжя. 22.12. 2025. С.79-82. URL: https://www.znu.edu.ua/faculty_law/nauka_/2025/_vseukrayins_koyi_naukovo-praktichnoyi_konferents_yi_aktual_n_problemi_pravovoyi_nauki_ta_pravookhoronnoyi_d_yal_nost_.pdf

Додаток Б
Акти впровадження

«ЗАТВЕРДЖЕНО»

Проректор
з освітньої роботи

Наталія ГУК

“ 7 ” 2025 р.



АКТ
про впровадження результатів дисертаційного дослідження
Олійника Артема Андрійовича
на тему «Кримінологічні засади забезпечення інформаційної безпеки: міжнародний,
національний та зарубіжний виміри» в освітній процес Дніпровського національного
університету

Комісія у складі: декана юридичного факультету О.В. Сачка, т.в.о. завідувачою кафедрою адміністративного і кримінального права Т.В. Корнякова, голови методичної ради юридичного факультету І.В. Патерило, склали цей акт про те, що ними вивчені матеріали підготовлені аспірантом Олійником А.А. на тему «Кримінологічні засади забезпечення інформаційної безпеки: міжнародний, національний та зарубіжний виміри», подані на здобуття наукового ступеня доктора філософії.

Результати проведеного Олійником А.А. дослідження мають необхідний теоретичний і методологічний рівень та високу практичну цінність, оскільки надає комплексний кримінологічний аналіз сучасних загроз у кіберпросторі та інтегрує передовий міжнародний досвід для формування ефективної системи протидії кіберзлочинності в Україні. Матеріали дослідження Олійника А.А. запроваджені у освітній процес юридичного факультету, що дозволить підвищити кваліфікацію здобувачів вищої освіти за першим (бакалаврським) та другим (магістерським) рівнями вищої освіти спеціальності D8 Право.

Члени комісії дійшли висновку, що представлені Олійником А.А. матеріали дослідження ґрунтуються на значній кількості опрацьованих автором джерел, що охоплюють національне та зарубіжне законодавство, міжнародні кримінологічні дослідження та емпіричні дані щодо кіберзлочинності, підтверджуючи теоретичну обґрунтованість висвітлених кримінологічних засад інформаційної безпеки.

Голова комісії:

Сачко О.В.

Члени комісії:

Корнякова Т.В.

Патерило І.В.



Декан юридичного факультету,
д.ю.н., професор

Т.в.о. завідувача кафедри адміністративного
і кримінального права Дніпровського
національного університету імені Олесея
Гончара, д.ю.н., професор

Голова методичної ради юридичного
факультету Дніпровського національного
університету імені Олесея Гончара, д.ю.н.,
професор

«ЗАТВЕРДЖЕНО»

Проректор
з наукової роботи

Олег МАРЕНКОВ

“ 09 ” 2025 р.



А К Т

впровадження результатів дисертаційного дослідження
Олійника Артема Андрійовича
на тему «Кримінологічні засади забезпечення інформаційної безпеки: міжнародний,
національний та зарубіжний виміри»
у наукову діяльність Дніпровського національного університету
імені Олеся Гончара

Комісія у складі:

Голови комісії:
Сачко О.В.

Декан юридичного факультету
Дніпровського національного університету
імені Олеся Гончара, д.ю.н., професор

Членів комісії:
Корнякова Т.В.

професор кафедри адміністративного
і кримінального права Дніпровського
національного університету імені Олеся
Гончара, д.ю.н., професор

Живова Ю.В.

доцент кафедри адміністративного
і кримінального права юридичного
факультету Дніпровського національного
університету імені Олеся Гончара, к.ю.н.,
доцент

склала цей акт про те, що результати дисертаційного дослідження аспіранта Дніпровського національного університету імені Олеся Гончара Олійника Артема Андрійовича за темою «Кримінологічні засади забезпечення інформаційної безпеки: міжнародний, національний та зарубіжний виміри», використовується у межах виконання плану Науково-дослідницької теми кафедри адміністративного і кримінального права Дніпровського національного університету імені Олеся Гончара «Забезпечення реалізації та захист основних свобод, прав людини, національних інтересів держави в умовах гібридних загроз і безпекових викликів» (затвердженої Рішенням ради юридичного факультету, протокол № 7 від 08.01.25 р., номер держреєстрації 0125U002352). Зокрема, в межах теми були опубліковані наступні наукові статті та тези доповідей Олійника А.А.:

1. Олійник А. А. Сутність інформаційної безпеки як правового явища у національному та міжнародному просторі. *Актуальні проблеми вітчизняної юриспруденції* № 6. 2023. С.293-299. DOI <https://doi.org/10.32782/2408-9257-2023-6-45>.
2. Олійник А. А. Формування стійкого цифрового суспільства: превентивна роль інформаційної безпеки та кримінально-правової політики у запобіганні злочинності. *Актуальні проблеми вітчизняної юриспруденції* № 2. 2025. С. 177-182. DOI <https://doi.org/10.32782/2408-9257-2025-2-27>
3. Олійник А.А. Запровадження міжнародних стандартів захисту цифрового середовища до українського законодавства та правозастосування як основи боротьби з кіберзлочинністю. Аналітично-порівняльне правознавство журнал юридичного факультету ДВНЗ "Ужгородський національний університет". № 2. 2025. (прийнято редакцією до публікації)
4. Олійник А.А. Організація безпеки інформаційного суверенітету для України як об'єкта глобальних інформаційних впливів Збірник тез Всеукраїнського науково-практичного юридичного форуму «Національна парадигма правового розвитку сучасної України» (Дніпровський національний університет імені Олеся Гончара, м. Дніпро, 18 травня 2023 року). Дніпро: Ліра, 2023. С. 334-340. URL: https://www.dnu.dp.ua/docs/ndc/2023/materiali%20konf/new_NACIONALNA%20PARADIGMA.pdf
5. Олійник А.А. Модель забезпечення цифрової безпеки в мережі internet крізь призму досвіду зарубіжних країн. Збірник тез Всеукраїнської науково-практичної конференції "Забезпечення принципів поваги, захисту та реалізації прав дитини у цифровому середовищі". (м. Дніпро 23 листопада 2023) Дніпровський національний університет імені Олеся Гончара, Дніпро, Ліра, 2023. С.349-352 URL: https://www.dnu.dp.ua/docs/ndc/2023/materiali%20konf/new_Zbiryk_Konf_Zahyst%20prav_dytny_u_cifrovomu_sviti.pdf
6. Окремі форми інформаційної агресії матеріали всеукраїнського науково-практичного круглого столу. Інформаційна агресія в сучасному світі: правовий аналіз та протидія Харків, 21 червня 2024 р. : електрон. наук. вид. / редкол.: В. С. Батиргарєєва та ін. – Харків : Майдан, 2024. С. 56-58. https://ivpz.kh.ua/wp-content/uploads/2024/11/%D0%97%D0%B1%D1%96%D1%80%D0%BD%D0%B8%D0%BA_%D1%96%D0%BD%D0%B0%D0%B9%D1%82.pdf
7. Забезпечення конституційних прав людини в умовах кіберпростору: діалектика балансу між приватністю, безпекою та ефективністю протидії кіберзлочинності // Матер. Міжнародної науково-практичної конференції ДДУВС. Дніпро. 26.06.2025

Акт обговорено і схвалено на засіданні кафедри адміністративного і кримінального права Дніпровського національного університету імені Олеся Гончара протокол № 1 від 02.09.2025 року.

Голови комісії:

Сачко О.В.



Декан юридичного факультету
Дніпровського національного університету
імені Олеся Гончара, д.ю.н., професор

Членів комісії:

Корнякова Т.В.



професор кафедри адміністративного
і кримінального права Дніпровського
національного університету імені Олеся
Гончара, д.ю.н., професор

Живова Ю.В.



доцент кафедри адміністративного
і кримінального права юридичного
факультету Дніпровського національного
університету імені Олеся Гончара, к.ю.н.,
доцент