СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про Національну поліцію: Закон України від 02.07.2015 № 580-VIII. URL: https://zakon.rada.gov.ua/laws/show/580-19 (дата звернення: 23.09.2026).
2. Декларація про поліцію: Резолюція № 690 (1979) Парламентської асамблеї Ради Європи від 08.05.1979 р. URL: https://zakon.rada.gov.ua/laws/show/994_803#Text (дата звернення: 23.09.2026).
3. Кодекс України про адміністративні правопорушення: Закон України від 07.12.1984 № 8073-X. URL: https://zakon.rada.gov.ua/laws/show/80731-10 (дата звернення: 24.09.2026).
4. Про Дисциплінарний статут Національної поліції України: Закон України від 15 березня 2018 року № 2337-VIII. URL: https://zakon.rada.gov.ua/laws/show/2337-19 (дата звернення: 24.09.2026).
5. Панасенко А. О. Особливості адміністративної відповідальності поліцейських за корупційні правопорушення. *Науковий вісник Ужгородського національного університету*. Серія Право. 2015. Вип. 35(2.2). С. 166-169. URL: https://nbuv.gov.ua/UJRN/nvuzhpr_2015_35%282.2%29__44 (дата звернення: 25.09.2026).

Філіппов О.С., здобувач,
Науковий керівник: Ситніченко Олена МихайлівнО.М.,
к.ю.н., доцент, доцент кафедри правового забезпечення безпеки бізнесу,
ЗВО «Державний торговельно-економічний університет»

КІБЕРЗАГРОЗИ ТА ПРАВОВА ПОЛІТИКА УКРАЇНИ: СУЧАСНИЙ СТАН ТА ШЛЯХИ ВДОСКОНАЛЕННЯ

Сьогодні важко уявити життя без цифрових технологій – державні послуги, банки, освіта, бізнес і навіть спілкування перейшли в онлайн. Водночас із зручностями зросли й ризики: кібератаки стали щоденним явищем, а з початком повномасштабного вторгнення кіберпростір перетворився на повноцінне поле бою поряд із фронтом. Фахівці зазначають, що інформаційна безпека – це стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого мінімізується завдання шкоди через неповноту, невчасність та недостовірність інформації або через негативний інформаційний вплив [1, с. 38]. Саме тому питання протидії кіберзагрозам вийшло на перше місце в правовій політиці України.

Законодавство визначає кібербезпеку як захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, а кібератаку – як спрямовані дії в кіберпросторі для порушення конфіденційності, цілісності та доступності електронних інформаційних ресурсів [2]. На практиці це десятки різних сценаріїв: distributed denial-of-service атаки, що паралізують сайти і сервіси, програми-вимагачі, які шифрують дані компаній, цільовий фішинг керівників і бухгалтерів, компрометація постачальників програмного забезпечення, а також складні тривалі операції проти державних органів і критичної інфраструктури. Особливістю сучасних атак є їх комбінований характер, коли кібератака супроводжується інформаційно-психологічним впливом та спробами фізичного ураження інфраструктури.

Масштаб проблеми підтверджується офіційними даними. Урядова команда реагування CERT-UA, що діє при Державній службі спеціального зв’язку та захисту інформації України, щороку опрацьовує тисячі кіберінцидентів, більшість з яких пов’язана з російськими хакерськими угрупованнями [3]. Найбільш резонансними стали атака на оператора зв’язку «Київстар» у грудні 2023 року, що призвела до багатоденного збою мобільного зв’язку та інтернету для мільйонів абонентів, атаки на державні реєстри Міністерства юстиції України наприкінці 2024 року, а також постійні атаки на енергетику, логістику, банки та медіа. Ці приклади показали, що від кіберстійкості приватного бізнесу напряму залежить національна безпека, адже оператори зв’язку, банки та енергетичні компанії є одночасно і бізнесом, і критичною інфраструктурою.

У відповідь держава сформувала систему стратегічних і організаційних рішень. Стратегія кібербезпеки України визначає пріоритетами стримування агресора в кіберпросторі, розвиток кіберстійкості держави, державно-приватне партнерство та поглиблення співпраці з Європейським Союзом і НАТО [4]. Координацію здійснюють Національний координаційний центр кібербезпеки при Раді національної безпеки і оборони України, Державна служба спеціального зв'язку та захисту інформації України, Кіберполіція Національної поліції України та Служба безпеки України, кожна в межах своєї компетенції. Важливим кроком стало прийняття Закону України «Про критичну інфраструктуру» та розвиток галузевих центрів реагування, що мають забезпечити обмін інформацією про загрози між державою і бізнесом.

Водночас науковці справедливо звертають увагу на фрагментарність правового регулювання. Поняття «інформаційна безпека», «кібербезпека», «захист інформації», «критична інформаційна інфраструктура» вживаються в різних законах без повного узгодження, що ускладнює розуміння бізнесом своїх обов'язків [5, с. 64]. Наприклад, вимоги до захисту інформації в інформаційно-комунікаційних системах детально прописані для державних органів, а для більшості приватних компаній вони мають переважно рекомендаційний характер. Це створює парадокс: бізнес фактично тримає на собі значну частину критичної інфраструктури, але не завжди має чіткі юридичні стимули вкладати кошти в кіберзахист.

Окремим викликом є гармонізація українського права з правом Європейського Союзу. Директива Європейського Союзу 2022/2555 про заходи для високого спільного рівня кібербезпеки в межах Союзу суттєво розширила коло суб'єктів, які зобов'язані управляти кіберризиками та повідомляти про значні інциденти протягом 24 годин, а також посилила відповідальність керівництва організацій [6]. В Україні обов'язок повідомлення про інциденти поки що повною мірою стосується переважно об'єктів критичної інфраструктури, тоді як малий і середній бізнес часто приховує факти атак через страх репутаційних втрат і недовіру до державних органів. Подібна ситуація і у сфері захисту персональних даних, де європейський регламент встановлює значно суворіші вимоги та штрафи, ніж чинний український закон.

Дослідники наголошують, що понад дві третини успішних кібератак починаються не зі зламу технічних систем, а з помилки людини – переходу за фішинговим посиланням, використання слабкого пароля або порушення правил роботи з даними [7, с. 112]. Це означає, що правова політика не може обмежуватися лише технічними стандартами і покараннями, вона має включати освіту, формування культури кібергігієни та зрозумілі для бізнесу комплаєнс-процедури. Особливо вразливим є малий і середній бізнес, який не має власних фахівців з безпеки, не проводить аудит інформаційних систем і не укладає договори страхування кіберризиків. Кадрова проблема стосується і юристів: ринок потребує правників, які розуміють природу електронних доказів, вміють складати політики інформаційної безпеки, договори про нерозголошення та обробку даних, супроводжувати розслідування інцидентів.

Законодавство про захист інформації вимагає від власників інформаційно-комунікаційних систем забезпечувати конфіденційність, цілісність і доступність інформації, зокрема шляхом розмежування доступу, антивірусного захисту, резервного копіювання та реагування на інциденти [8]. На практиці виконання цих вимог означає для підприємства необхідність затвердити внутрішні політики безпеки, призначити відповідальних осіб, регулярно навчати персонал і фіксувати всі дії з даними. Великі компанії вже створюють власні центри моніторингу безпеки або передають цю функцію на аутсорсинг, укладаючи договори з чіткими умовами про відповідальність провайдера та збереження конфіденційності. Позитивним прикладом є розвиток співпраці бізнесу з CERT-UA, яка публікує індикатори компрометації та практичні рекомендації, доступні кожному підприємству.

На нашу думку, кіберзагрози вже стали головним викликом для правової політики України, не менш важливим за традиційні військові загрози.

Зазначимо, що чинні закони загалом правильно визначають напрями захисту, але вони відстають від швидкості розвитку технологій і тактики хакерів. Таким чином, держава має не лише посилювати контроль і відповідальність, а й допомагати бізнесу зрозумілими правилами, доступним аудитом безпеки та навчанням працівників.

Відмітимо, що майбутнє – за чесним партнерством держави і бізнесу, коли компанії не бояться повідомляти про атаки, а держава швидко надає допомогу. Також зазначимо, що правнича освіта має готувати юристів нового типу, які однаково добре розуміють і право, і цифрові технології. Тільки поєднання сильних законів, освічених людей і сучасних технологій зможуть зробить Україну по-справжньому стійкою до кіберзагроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Баранов О. А. Правове забезпечення інформаційної безпеки : підручник. – Київ : Юрінком Інтер, 2023. – 376 с.
2. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII : станом на 1 серп. 2026 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 11.10.2026).
3. Урядова команда реагування на комп'ютерні надзвичайні події CERT-UA. Офіційний сайт. URL: https://cert.gov.ua (дата звернення: 11.10.2026).
4. Стратегія кібербезпеки України : затв. Указом Президента України від 26.08.2021 р. № 447/2021. URL: https://www.president.gov.ua/documents(дата звернення: 11.10.2026).
5. Кормич Б. А. Інформаційна безпека : організаційно-правові основи : навч. посіб. – Київ : Кондор, 2024. – 268 с.
6. 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 (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 (дата звернення: 11.10.2026).
7. Діордіца І. В. Кіберзлочинність та електронні докази у кримінальному провадженні : монографія. – Київ : Алерта, 2024. – 312 с.
8. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 р. № 80/94-ВР : станом на 1 серп. 2026 р. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр (дата звернення: 11.10.2026).

Флісак С.М.,здобувач
Науковий керівник: Загурський О. Б.,
кандидат юридичних наук, доцент,
ЗВО «Університет Короля Данила»

МІЛІТАРИЗАЦІЯ УКРАЇНСЬКОЇ МОЛОДІ НА ТИМЧАСОВО ОКУПОВАНИХ ТЕРИТОРІЯХ: МІЖ ІНДОКТРИНАЦІЄЮ ТА ДОБРОВІЛЬНИМ ВСТУПОМ ДО ЗБРОЙНИХ СИЛ РФ

Актуальність дослідження зумовлена поширенням практик мілітаризації та ідеологічної індоктринації українських дітей і молоді на тимчасово окупованих територіях України. Залучення неповнолітніх до військово-патріотичних організацій, воєнізованих заходів та освітніх програм із відповідним ідеологічним змістом актуалізує питання про можливий вплив такого середовища на формування їхньої ідентичності й подальші життєві рішення. Показовим у цьому контексті є випадок Олександра Мустяце, якого, за повідомленнями відкритих джерел, згодом виявили серед військовослужбовців російської федерації, а також його неповнолітнього брата, залученого до руху «Юнармія» [1, 2]. Метою дослідження є міжнародно-правова оцінка зазначених практик на прикладі кейсу родини Мустяце.

Перейдемо до історії Олександра Мустяце, уродженця села Кринки Херсонської області 2007 року народження, який після початку повномасштабного вторгнення опинився на території російської федерації. У 2026 році громадська ініціатива Back to Ukraine повідомила про виявлення його серед військовослужбовців російської армії. За оприлюдненими даними, Олександр підтвердив участь у війні на боці рф, а в листуванні з представниками ініціативи заявив, що «Росія завжди була в моєму серці» [1,3].