Інформаційне право

УДК 351.71:004.056.5 (477)

DOI https://doi.org/10.5281/zenodo.18035430

Правове регулювання кібербезпеки в Україні: сучасні виклики та перспективи розвитку

Цимбалюк Валерій Іванович,
кандидат юридичних наук, професор кафедри правоохоронної діяльності та спеціальних юридичних дисциплін, Україна, https://orcid.org/0000-0003-0542-6644

Багатко Анастасія Сергіївна,
асистент кафедри інформаційного права та юридичної журналістики, Україна, https://orcid.org/0000-0003-4673-7406

Прийнято: 09.12.2025 | Опубліковано: 23.12.2025

Анотація: У статті розглянуто сучасний стан правового регулювання кібербезпеки в Україні. Було розглянуто в першу чергу тлумачення терміну «кібербезпека» як науковцями, так і законодавством України. Визначено основні нормативно-правові акти, які здійснюють регулювання кібербезпеки в Україні. Встановлено основні об'єкти, які підпадають під кібератаки.

Визначено, що основними викликами правового регулювання є значне відставання нормативної бази від технологічного прогресу, транскордонний характер кіберзлочинів, а також відсутність загальновизнаних міжнародних стандартів у цій сфері. Для розв’язання зазначених проблем доцільно використовувати напрацювання провідних держав і організацій.

У дослідженні було представлено та надано короткий опис провідних документів, що визначає базові положення та напрямки політики країни у

сфері кібербезпеки. Було спрямовано увагу на підзаконні нормативно-правові документи, що дозволяють регулювати визначену сферу.

Визначено, що процес правового врегулювання кібербезпеки часто зустрічається з великою кількістю перешкод, що потребують швидкого реагування та адаптування законодавчої бази до стрімких змін у цифровому оточенні. Було з'ясовано, що серед основних складнощів можна відзначити суттєве відставання законодавчої бази від технологічного прогресу, міжнародний характер кібернебезпеки, брак єдиної для всіх системи міжнародних стандартів для цієї сфери.

Разом з тим, для підвищення якості національного кіберзахисту було представлено систему скоординованих заходів за короткостроковим, середньостроковим та довгостроковим спрямуванням, тим самим підтримуючи стабільний та систематичний підхід для розв'язання цієї важливої проблеми.

Вивчаючи наявну проблематику та подальші перспективи розбудови правового регулювання кібербезпеки в нашій державі, було визначено потребу у суттєвому покращенні законодавчої системи, оскільки наявна законодавча база часто залишає можливість подвійного трактування, прослідковуються наявні прогалини, що суперечить принципам правової визначеності.

Наукова новизна дослідження полягає в аналізі реального стану кібербезпеки у нашій державі, визначається зростання чисельності кіберпрецедентів та кібератак на інформаційні бази та основні критичної інфраструктури, що визначає інтерес до цього питання.

Ключові слова: кібербезпека, кібератака, законодавство, національна безпека, регулювання, загрози, критична інфраструктура.

ISSN: 3041-2110

Legal Regulation of Cybersecurity in Ukraine: Current Challenges and Development Prospects

Valeriy Tsymbalyuk,
Candidate of Law, Professor of the Department of Law Enforcement and Special Legal Disciplines, Ukraine, https://orcid.org/0000-0003-0542-6644

Anastasia Bahatko
Assistant Professor, Department of Information Law and Legal Journalism, Ukraine, https://orcid.org/0000-0003-4673-7406

Abstract: The article examines the current state of legal regulation of cybersecurity in Ukraine. First of all, the interpretation of the term "cybersecurity" by both scientists and the legislation of Ukraine was considered. The main regulatory and legal acts that regulate cybersecurity in Ukraine were identified. The main objects that fall under cyberattacks were identified. The main subjects that regulate cybersecurity were also identified.

It was determined that the main challenges of legal regulation are the significant lag of the regulatory framework from technological progress, the cross-border nature of cybercrimes, as well as the lack of generally recognized international standards in this area. To solve these problems, it is advisable to use the experiences of leading states and organizations.

The study presented and provided a brief description of the leading documents that define the basic provisions and directions of the country's policy in the field of cybersecurity. Attention was drawn to the subordinate regulatory and legal documents that allow regulating the specified area.

It has been determined that the process of legal regulation of cybersecurity often encounters a large number of obstacles that require rapid response and adaptation of the legislative framework to rapid changes in the digital environment.

It was found that among the main difficulties, one can note the significant lag of the legislative framework from technological progress, the international nature of cybersecurity, and the lack of a single system of international standards for this area. At the same time, a system of coordinated measures in the short, medium and long term was presented to improve the quality of national cyber defense, thereby supporting a stable and systematic approach to solving this important problem.

Studying the existing problems and further prospects for developing legal regulation of cybersecurity in our country, the need for a significant improvement of the legislative system was identified, since the existing legislative framework often leaves room for double interpretation, and existing gaps are observed, which contradicts the principles of legal certainty.

The scientific novelty of the study lies in the analysis of the real state of cybersecurity in our country, which is determined by the growth in the number of cyber precedents and cyber attacks on information bases and basic critical infrastructure, which determines the interest in this issue.

Keywords: cybersecurity, cyberattack, legislation, national security, regulation, threats, critical infrastructure.

Постановка проблеми. Правове регулювання кібербезпеки в Україні є динамічною сферою, яка постійно адаптується до нових загроз та викликів у цифровому просторі. В умовах повномасштабної війни, гібридних атак та наростаючої ролі цифрових технологій у всіх сферах життя, ефективність цього регулювання набуває критичного значення для національної безпеки, функціонування критичної інфраструктури та захисту прав громадян.

Україна на сучасному етапі виступає одним із ключових учасників глобальної кіберпросторової екосистеми. З моменту початку повномасштабної війни у 2022 р. було зафіксовано безпрецедентне збільшення кількості кібератак, спрямованих як на державний, так і приватний сектори. Наслідками таких атак стали локальні порушення функціонування українських

 ISSN: 3041-2110

вебресурсів, що утворюють загрозу для стабільності національного ринку, тісно інтегрованого в міжнародні цифрові мережі та організаційні структури.

У зв'язку із цим питання забезпечення кібербезпеки набуває критичного значення і потребує комплексного аналізу в контексті чинного національного та міжнародного нормативно-правового регулювання, які відіграють визначальну роль у захисті кіберпростору.

Аналіз останніх досліджень і публікацій. Дослідники пропонують кілька трактувань поняття кібербезпеки. Зокрема, В. Фурашев визначає кібербезпеку як стан, що відображає здатність особистості, нації та держави в цілому запобігати та нейтралізувати цілеспрямовані негативні впливи, пов'язані з інформацією [14, с. 164].

Д. Ширяєв наголошує, що кібербезпека є складним і багатогранним завданням, яке потребує спільних і безперервних зусиль усіх зацікавлених сторін. Лише через співпрацю, спрямовану на розробку передових практик, обмін інформацією та активне впровадження інноваційних технологій, можна забезпечити ефективний захист як особистих, так і глобальних цифрових інфраструктур від кіберзагроз [15, с. 602].

Л. Бєлкін, Ю. Юринець, М. Бєлкін та Є. Криволап наголошують, що поняття кібербезпеки є специфічним аспектом ширшого концепту інформаційної безпеки, при цьому акцентуючи на інформації, яка циркулює у кіберпросторі.

Особливий інтерес до кіберзагроз та забезпечення кібербезпеки обумовлений висхідною значущістю обігу даних у комп'ютерних системах та електронно-комунікаційних мережах, що відображає сучасні тенденції цифровізації та переходу до інформаційного суспільства [1, с. 80].

Здіснений аналіз джерельної бази дослідження дозволяє нам визначити, що тема досить популярна для вивчення, оскільки з кожним роком зростає кількість кіберзлочинів різного формату, які потребують вивчення кожен

ISSN: 3041-2110

окремо. Також нині відсутні дослідження, що комплексно розглядали б кіберзаконодавства кожної держави та єдину нормативно-правову базу.

Виклад основного матеріалу дослідження Відповідно до положень Закону України «Про основні засади забезпечення кібербезпеки України», поняття кібербезпеки визначається як стан захищеності життєво важливих інтересів особи, громадянина, суспільства та держави в межах кіберпростору. Цей стан забезпечує стабільний розвиток інформаційного суспільства, функціонування цифрового комунікативного середовища, а також ефективне виявлення, запобігання та нейтралізацію як актуальних, так і потенційних загроз національній безпеці України у сфері кіберпростору [8].

Головна мета кібератак в Україні, особливо після повномасштабного вторгнення Росії у 2022 р., є комплексною і спрямована на досягнення як військових, так і політичних, економічних та соціальних цілей. Ці кібератаки є невід'ємною частиною гібридної війни.

Ключовим документом, що визначає основні засади та напрями державної політики у сфері кібербезпеки, є Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 р. № 2163-VIII [8]. Цей Закон:

- визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини й громадянина, суспільства та держави у кіберпросторі;
- закріплює основні принципи державної політики у сфері кібербезпеки;
- визначає основні об'єкти кіберзахисту (критична інформаційна інфраструктура, державні електронні інформаційні ресурси тощо);
- розмежовує повноваження суб'єктів забезпечення кібербезпеки (Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язку), Служба безпеки України (СБУ), Національна поліція України, Міністерство оборони України тощо);

– визначає поняття кіберінциденту, кібератаки, кіберзлочину та інші ключові терміни.

Крім цього Закону, правове регулювання кібербезпеки ґрунтується на низці інших нормативних актів (табл. 1).

Таблиця 1

Нормативно-правові акти з регулювання кібербезпеки в Україні

Нормативний акт	**Напрям регулювання**
Конституція України [3]	Закріплює основи національної безпеки, права на інформацію та захист персональних даних.
Стратегія кібербезпеки України [12]	Стратегічний документ, що визначає цілі, пріоритети та напрями розвитку системи кібербезпеки. Остання редакція була затверджена Указом Президента України від 26 серпня 2021 р. № 447/2021.
Закон України «Про національну безпеку України» [7]	Визначає кібербезпеку як складову національної безпеки.
Кримінальний кодекс України [4]	Містить статті, що встановлюють відповідальність за кіберзлочини (наприклад, несанкціоноване втручання в роботу комп'ютерів, систем, мереж, створення шкідливих програм, поширення шкідливого ПЗ).
Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [5]	Регулює питання захисту інформації
Закон України «Про захист персональних даних» [6]	Регулює збір, зберігання, використання та захист персональних даних.

Доцільно також приділити належну увагу підзаконним нормативно-правовим актам, які регулюють зазначену сферу. Зокрема, варто виокремити Укази Президента України, як-от «Про Стратегію національної безпеки України» [13] та «Про Стратегію інформаційної безпеки» [11].

У рамках цих нормативних документів передбачено стратегічні напрями, спрямовані на забезпечення розвитку кіберпростору, що характеризується свободою, безпекою, стабільністю та відкритістю, з метою гарантування прав людини в Україні.

Водночас слід враховувати, що обсяги інформаційних ресурсів неухильно зростають, а кількість користувачів, які взаємодіють у цифровому середовищі без територіальних обмежень, постійно збільшується. У таких умовах кіберзлочинці активно використовують складні методи для несанкціонованого доступу до цифрових ресурсів, викрадення конфіденційних даних, а також здійснення актів саботажу щодо діяльності компаній з метою подальшого вимагання грошових коштів.

Проаналізувавши чинне законодавство, можно зазначити, що воно нажаль у своєму розвитку не встигає за сучасними викликами, розвитком нових стратегій кіберзлочинності та засобів які для цього застосовуються. Нині ефективність кіберполіції, СБУ та Держспецзв'язку знаходиться на високому рівні, однак вище описані фактори, військова агресія в інформаційному просторі підтримує їх у постійному тонусі.

Розглядаючи роботу різних структур, варто зазначити, що між кіберполіцією та слідчими СБУ існує певне дублювання повноважень, оскільки на дослідчому етапі вони виконують тотожну діяльність.

Основні об'єкти кібератак в Україні відображають стратегічні цілі агресора – дестабілізацію держави, порушення її функціонування та зниження обороноздатності. Після повномасштабного вторгнення Росії у 2022 р., ці об'єкти стали ще більш чітко визначеними та систематично зазнавали атаки.

Ось головні об'єкти кібератак в Україні:

1. об'єкти критичної інформаційної інфраструктури (КІІ): Це пріоритетна ціль, оскільки їхній вихід з ладу має каскадні наслідки для функціонування держави та життєдіяльності населення;
2. державні органи та установи:

– урядові портали та сайти: сайти міністерств, відомств, місцевих органів влади. Мета – дефейс (зміна зовнішнього вигляду), порушення доступу до державних послуг, поширення пропаганди та дезінформації;

ISSN: 3041-2110

– електронні державні реєстри та бази даних: системи Пенсійного фонду, податкової служби, Єдиний державний реєстр. Мета – викрадення конфіденційних даних, їхнє спотворення або знищення;
– системи документообігу: системи внутрішнього листування та електронного документообігу в державних установах. Мета – шпигунство, викрадення службової інформації, порушення комунікації;

3. сектор безпеки та оборони:

– військові інформаційні системи: командно-штабні системи, системи розвідки, зв'язку, логістики. Мета – отримання розвідувальної інформації, порушення координації військ, дезорієнтація;
– оборонно-промисловий комплекс: підприємства, що виробляють або ремонтують військову техніку. Мета – шпигунство, саботаж виробництва. Згідно з даними СБУ, російські спецслужби активно використовують кібератаки для отримання інформації про військові плани та оборонну промисловість;

4. медіа та інформаційний простір: новинні сайти та телеканали: Сайти ЗМІ, сервери трансляції. Мета – блокування доступу до правдивої інформації, поширення пропаганди через зламані ресурси, дискредитація журналістів. Інститут масової інформації (ІМІ) регулярно фіксує кібератаки на українські ЗМІ [2, с. 403].

Загалом, об'єктами кібератак в Україні є всі елементи, що забезпечують функціонування держави, її обороноздатність, економічну стабільність та інформаційний суверенітет.

Реальний стан сьогодення, це те, що сьогодні фахівці фіксують збільшення кількості кіберінцидентів та кібератак на державні інформаційні резерви та об'єкти критичної інфраструктури України.

Згідно з положеннями Закону України «Про основні засади забезпечення кібербезпеки України», до суб’єктів, відповідальних за реалізацію заходів у сфері кібербезпеки, належать міністерства та інші центральні органи

виконавчої влади, місцеві державні адміністрації, органи місцевого самоврядування, а також правоохоронні, розвідувальні та контррозвідувальні структури.

До цього переліку входять також суб'єкти оперативно-розшукової діяльності, Збройні сили України, інші військові формування, створені відповідно до законодавчих норм, а також Національний банк України, підприємства, установи й організації, які належать до об'єктів критичної інфраструктури. Крім того, важливу роль у забезпеченні кібербезпеки відіграють Служба безпеки України, Міністерство оборони України, Національна поліція України та Державна служба спеціального зв'язку та захисту інформації України [8].

Зазначені установи виконують стратегічні функції у сфері забезпечення кібербезпеки, що включають виявлення, запобігання та подальше розслідування кіберзлочинів, захист об'єктів критичної інфраструктури та інформаційних ресурсів держави, а також розроблення і впровадження комплексних стратегій та заходів із кіберзахисту.

Крім того, їх діяльність охоплює активну співпрацю з міжнародними партнерами для посилення глобальних механізмів кібербезпеки й реалізації заходів з підвищення рівня кіберсвідомості серед населення та представників бізнес-спільноти. Важливу роль у механізмах забезпечення національної кібербезпеки відіграє Рада національної безпеки й оборони України. Її функціональні обов'язки та повноваження чітко регламентовані законодавством, особливо у контексті положень, викладених в статті 4 Закону України «Про Раду національної безпеки й оборони України» [9].

Відповідно до зазначеного положення, Рада національної безпеки й оборони України несе відповідальність за розробку та розгляд питань, що стосуються захисту стратегічних національних інтересів, зокрема у сфері кібербезпеки, яка є важливою складовою національної безпеки. Її діяльність охоплює також заходи інформаційної безпеки, спрямовані на захист

ISSN: 3041-2110

інформаційної інфраструктури, тоді як кібербезпека передбачає протидію цифровим атакам у кіберпросторі.

Рада проводить стратегічну оцінку стану та перспектив забезпечення кібербезпеки, аналізуючи дані, отримані від структур, залучених до системи кіберзахисту країни. Це підкреслює критичне значення координаційної функції Ради у контексті гарантування кібербезпеки в масштабах України. Одним із ключових напрямів роботи в цій сфері є зміцнення міжнародного співробітництва.

Правове регулювання кібербезпеки стикається з численними викликами, що вимагають оперативного реагування та адаптації законодавства до швидких змін у цифровому середовищі. Основні труднощі включають значне відставання нормативної бази від технологічного прогресу, транскордонний характер кіберзлочинів, а також відсутність загальновизнаних міжнародних стандартів у цій сфері.

Однією з ключових проблем є затримка в оновленні законодавства, яке часто не встигає за появою нових цифрових загроз. Технологічні інновації рухаються вперед значно швидше, ніж розробляються відповідні норми, що призводить до появи «правового вакууму».

В таких умовах злочинці успішно використовують юридичні прогалини для вчинення незаконних дій. Наприклад, розвиток штучного інтелекту та квантових технологій створює потенціал для виникнення нових ризиків, але більшість країн поки що не впровадили чіткі регуляторні положення для контролю цих галузей.

У 2023 р. міністерства закордонних справ України та низки інших держав, серед яких Канада, Данія, Естонія, Франція, Німеччина, Нідерланди, Польща, Швеція, Велика Британія та Сполучені Штати Америки, оголосили про створення нового механізму співпраці в галузі кібербезпеки, який отримав назву «Талліннський механізм» [10].

ISSN: 3041-2110

Аналізуючи значення цього проєкту у сфері зміцнення кібербезпеки, необхідно підкреслити його ключову функцію, що полягає у вдосконаленні координації зусиль та наданні підтримки Україні в захисті критично важливої інфраструктури від ймовірних кіберзагроз.

Проєкт розроблено з урахуванням впливу постійних російських кібероперацій на критичну інфраструктуру України, що значно активізувалися упродовж 2023 року і стали причиною необхідності довготривалої міжнародної допомоги для зміцнення кіберзахисних механізмів. Співпраця в межах зазначеного проєкту має потенціал стати ключовим елементом підтримки з боку держав-учасниць, сприяючи розвитку цивільного кіберзахисного потенціалу України та налагодженню взаємодії з іншими організаціями, які залучені до надання допомоги.

Для підвищення ефективності українського кіберзахисту учасники проєкту пропонують координацію заходів за короткостроковим, середньостроковим та довгостроковим напрямами, забезпечуючи тим самим системний і стійкий підхід до вирішення цієї надзвичайно важливої проблеми.

Практичні результати Талліннського механізму полягають у мобілізації значних фінансових ресурсів (понад 200 млн євро станом на листопад 2025 р.) та технічної підтримки для посилення кіберстійкості нашої держави від 13 країн-партнерів, включаючи фінансування конкретних проєктів, як-от модернізація серверного обладнання для регіонів, що сприяє сталому функціонуванню критичної інфраструктури України в умовах війни.

Для розв’язання зазначених проблем доцільно використовувати напрацювання провідних держав і організацій, таких як США, НАТО і Швейцарія. Україні варто звернути особливу увагу на практики ЄС та НАТО, спрямовані на формування інтегрованої системи сертифікації в галузі кібербезпеки.

Головними завданнями мають стати розробка національної системи реагування на масштабні кіберінциденти та кризи з охопленням як

 ISSN: 3041-2110

загальнонаціональних планів, так і окремих стратегій для об'єктів критичної інфраструктури. Ключовим аспектом є активізація державно-приватного партнерства та проведення поглиблених наукових досліджень у цій сфері.

Потенційним кроком для України може стати приєднання до Центру передового досвіду НАТО з кібероборони. Це надасть змогу впроваджувати найкращі світові практики та посилити координацію з Альянсом. Крім того, варто наголошувати на нарощуванні технічного потенціалу для захисту кіберпростору. Серед видів співробітництва НАТО-Україна у сфері кібербезпеки варто відзначити наступне:

- НАТО надає Україні критично важливі дані про плани та дії противника (зокрема РФ), що допомагає у плануванні оборони та превентивних заходів у кіберпросторі;
- надання сучасних технологій, тренінги для фахівців, допомога у розбудові спроможностей центрів кібербезпеки;
- участь у спільних кібер-навчаннях (Cyber Coalition, Locked Shields) та кібероперацій для відпрацювання реагування на інциденти;
- Україна є членом Програми розширених можливостей НАТО (ЕОР), що забезпечує більш тісну співпрацю у всіх сферах безпеки, включно з кібербезпекою;
- адаптація українського законодавства у сфері кібербезпеки до норм ЄС та НАТО для глибшої інтеграції та можливості спільного реагування.

Додаткову складність становить транснаціональний характер кіберзлочинів, які часто виходять за межі юрисдикцій окремих держав. Це суттєво ускладнює розслідування таких злочинів і притягнення винних до відповідальності, оскільки національні правові норми зазвичай обмежені територіальним застосуванням і не діють за межами країни їх походження.

Досліджуючи актуальні проблеми та перспективи розвитку правового регулювання кібербезпеки в Україні, можна відзначити необхідність значного вдосконалення національного законодавства у цій галузі. Чинні нормативно-

ISSN: 3041-2110

правові акти нерідко залишають місце для неоднозначного трактування, містять навмисні або випадкові прогалини, що суперечить принципам правової визначеності.

Труднощі доказування у кіберзлочинах полягають у складності ідентифікації та локалізації злочинця, технічній специфіці доказів (електронні докази, їхня зміна, видалення), міжнародному аспекті (юрисдикція, співпраця), швидкому розвитку технологій, що ускладнює правозастосування, та потребі у висококваліфікованих експертах для аналізу даних, а також дотриманні правил належності та допустимості доказів при їх зборі.

Така ситуація ускладнює ефективне виконання завдань і функцій кібербезпеки та кібероборони, водночас створюючи підґрунтя для конфліктів між уповноваженими органами. Це порушує фундаментальні принципи адекватності правового регулювання.

Висновки. Агресія росії проти України суттєво змінила динаміку кіберзахисту, загострившись необхідність систематизації нових підходів і стратегій у сфері кібероборони. На основі цих трансформацій слід розробити комплекс законодавчих змін, які б забезпечили ефективне функціонування кібербезпеки в умовах сучасних викликів і загроз.

Недостатня адаптація законодавства до умов воєнного стану ускладнює оперативне реагування на кіберзагрози, обмежує ефективність судової практики та перешкоджає притягненню до відповідальності за транснаціональні правопорушення. Ці про галини підтверджують нагальну потребу в комплексному вдосконаленні правового регулювання для забезпечення стійкості інформаційного простору перед кібератаками та маніпулятивним контентом, які є основними інструментами гібридної агресії.

Створення міжнародного хабу кіберзахисту як юридичної особи сприятиме координації зусиль із міжнародними організаціями, такими як НАТО, та приватними компаніями, що забезпечить обмін передовими правовими і технічними рішеннями.

ISSN: 3041-2110

Посилення відповідальності через включення до Кримінального кодексу України категорії «кібердиверсія» та механізму «цифрових санкцій» створить ефективний інструмент стримування кіберзлочинів. Ці пропозиції ґрунтуються на міжнародних стандартах, зокрема Директиві ЄС NIS2 та Стратегії кібербезпеки НАТО, адаптованих до українських реалій воєнного часу.

Подальші наукові пошуки доцільно спрямувати на поглиблене вивчення правового регулювання штучного інтелекту в контексті кібербезпеки, зокрема його використання в дезінформаційних кампаніях, а також на розробку міжнародних правових механізмів для протидії кіберзагрозам, що виходять за межі національної юрисдикції.

Важливим залишається вдосконалення координації між державними органами, приватним сектором і міжнародними партнерами, що сприятиме реалізації реформ.

Правове регулювання кібербезпеки в Україні є живим організмом, що постійно вдосконалюється у відповідь на динамічний та агресивний кіберландшафт, прагнучи забезпечити надійний щит для цифрового простору країни.

Системний підхід до оновлення законодавства не тільки підвищить стійкість України до гібридних загроз у період війни, а й забезпечить передумови для сталого розвитку інформаційної безпеки в повоєнний період, зміцнюючи довіру суспільства до цифрових технологій і державних інститутів.

Список використаних джерел

1. Бєлкін Л. М., Юринець Ю. Л., Бєлкін М. Л., Криволап Є. В. Співвідношення понять «інформаційна безпека», «безпека інформації», «кібербезпека» в контексті безпекових стратегій України 2020 – 2021 років.

ISSN: 3041-2110

Scientific Works of National Aviation University. Series: Law Journal «Air and Space Law». 2022. №3(64). С. 78 – 86.

2. Колосовський Є. Ю. Сучасний стан кібербезпеки в Україні в умовах воєнного періоду. *Юридичний науковий електронний журнал*. 2023. №12. С. 402 – 405.

3. Конституція України. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96%D0%B2%D1%80#Text. (Дата звернення: 26.10.2025).

4. Кримінальний кодекс України Кодекс України. Закон від 05.04.2001 №2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text. (Дата звернення: 24.11.2025). (Дата звернення: 27.11.2025).

5. Про захист інформації в інформаційно-комунікаційних системах. Закон України від 05.07.1994. №80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text. (Дата звернення: 24.11.2025). (Дата звернення: 25.10.2025).

6. Про захист персональних даних. Закон України від 01.06.2010. №2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text. (Дата звернення: 25.11.2025). (Дата звернення: 29.10.2025).

7. Про національну безпеку України Закон України від 21.06.2018. №2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text. (Дата звернення: 26.11.2025). (Дата звернення: 26.10.2025).

8. Про основні засади забезпечення кібербезпеки України. Закон України від 05.10.2017. №2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/216319#Text. (Дата звернення: 22.10.2025).

9. Про Раду національної безпеки і оборони України. *Закон України. Відомості Верховної Ради України (ВВР)*. 1998. №35. ст. 237. URL: https://zakon.rada.gov.ua/laws/show/183/98-%D0%B2%D1%80#Text. (Дата звернення: 26.10.2025).

 ISSN: 3041-2110

10. Талліннський механізм: Україна та міжнародні партнери започаткували новий інструмент співпраці у кіберпросторі. *Урядовий портал.* 2023. URL: https://www.kmu.gov.ua/news/tallinnskyimekhanizmukrainatamizhnarodnipartnery-zapochatkuvaly-novyi-instrument-spivpratsi-u-kiberprostori. (Дата звернення: 26.10.2025).

11. Указ Президента України «Про Стратегію інформаційної безпеки» від 28.12.2021 р. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text. (Дата звернення: 21.10.2025).

12. Указ Президента України «Про Стратегію кібербезпеки України» від 26.08.2021 р.. №447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Tex. (Дата звернення: 23.10.2025).

13. Указ Президента України «Про Стратегію національної безпеки України» від 14.09.2020 р.. №392/2020. URL: https://zakon.radagov.ua/laws/show/392/2020#Text. (Дата звернення: 26.10.2025).

14. Фурашев В. М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. *Інформація і право.* 2012. №2. С. 162 – 169.

15. Ширяєв Д. О. Кібербезпека та сучасний світ. *Актуальні проблеми сучасної науки в дослідженнях молодих учених, курсантів та студентів*. 2023. С. 600 – 602.

 ISSN: 3041-2110