УДК 351.746.1:004.056.5
DOI https://doi.org/10.32782/pdu.2025.1.61

О. О. Колесник
аспірант
Науково-дослідного інституту публічного права

НОРМАТИВНО-ІНСТИТУЦІЙНІ ЗАСАДИ ФОРМУВАННЯ НАЦІОНАЛЬНОЇ СИСТЕМИ КІБЕРБЕЗПЕКИ УКРАЇНИ

Статтю присвячено теоретико-правовому обґрунтуванню архітектури національної системи кібербезпеки України як інтегрованої складової національної безпеки та державної стійкості в умовах цифрової трансформації й збройної агресії. На основі системного та інституційно-правового підходів розкрито нормативні засади (Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII, Стратегію кібербезпеки та План її реалізації, базові акти інформаційного права, законодавство про критичну інфраструктуру) й інституційну структуру системи (Рада національної безпеки і оборони України, Національний координаційний центр кібербезпеки, Державна служба спеціального зв'язку та захисту інформації, Служба безпеки України, Міністерство оборони, Національний банк і Національна поліція). Визначено ключові проблеми функціонування системи – фрагментарність підзаконного регулювання, дублювання компетенцій, недостатню координацію між суб'єктами, кадрові обмеження та відсутність єдиних процедур аудиту, сертифікації і реагування на кіберінциденти. Обґрунтовано напрями вдосконалення нормативно-інституційної моделі: посилення координаційної ролі Національного координаційного центру кібербезпеки, розроблення уніфікованих процедур взаємодії між державними та приватними структурами, запровадження державних стандартів підготовки фахівців, створення національної системи моніторингу кіберзагроз і підвищення рівня відповідальності операторів критичної інфраструктури. У межах євроінтеграційного курсу України доведено необхідність гармонізації національного законодавства з правом Європейського Союзу, зокрема імплементації Директиви (ЄС) 2022/2555 (NIS2), Регламенту (ЄС) 2016/679 (GDPR) та практик Європейського акта про кіберсолідарність. Запропонована концепція передбачає перехід до інтегрованої, ризик-орієнтованої та стійкої системи кібербезпеки, спроможної забезпечити захист державного суверенітету, прав громадян і стабільність критичної інфраструктури у цифровому середовищі.

Ключові слова: *кібербезпека, національна безпека, Національний координаційний центр кібербезпеки, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, кібероборона, критична інфраструктура.*

Актуальність теми. Стрімка цифровізація суспільних відносин зумовила якісно новий етап у переосмисленні сутності безпеки держави та змісту її базових функцій. Кіберпростір, який ще донедавна розглядався переважно як технологічне середовище, нині набув статусу стратегічного виміру реалізації політичних, економічних і воєнних інтересів держав. Його глобальний, мережевий і водночас децентралізований характер актуалізував складний комплекс викликів для національних систем управління безпекою, що потребують адекватного правового реагування та інституційного упорядкування.

Як слушно зазначають С. Вдовенко, Є. Живило та інші дослідники, ефективність кібероборони безпосередньо залежить від гармонійного поєднання правових, організаційних і технічних засад діяльності суб'єктів системи безпеки, адже сучасна держава вимірює рівень своєї захищеності не лише територіальною цілісністю, а й стійкістю цифрових інфраструктур [1].

Для України, яка перебуває в умовах триваючої збройної агресії та постійного інформаційно-технологічного тиску, формування дієвої системи кібербезпеки набуває не просто галузевого, а системоутворюючого значення. Саме в площині кібербезпеки сьогодні концентруються ключові показники спроможності держави забезпечувати національний суверенітет, захищати демократичний устрій, права громадян і безпеку критичної інфраструктури. Як справедливо наголошується у міжнародній науковій літературі, український досвід кібероборони під час воєнного конфлікту став унікальним прикладом практичного переосмислення меж дії міжнародного права у сфері збройних і інформаційних відносин [14].

Разом із тим, нормативно-правове забезпечення кібербезпеки в Україні досі залишається фрагментарним, а інституційна архітектура – лише частково скоординованою. Попри закріплення базових засад державної політики у Законі України «Про основні засади забезпечення кібербезпеки України» [21] та у Стратегії кібербезпеки України [26], залишається очевидною потреба у формуванні цілісної нормативно-інституційної моделі, здатної забезпечити стабільну взаємодію державних і недержавних суб'єктів на засадах партнерства, відповідальності та сумісності зі стандартами Європейського Союзу і НАТО.

Недостатня координація між органами сектору безпеки та оборони, нечіткий розподіл компетенцій між ключовими суб'єктами – Службою безпеки України, Державною службою спеціального зв'язку та захисту інформації, Національним координаційним центром кібербезпеки – а також обмежена інтеграція приватного сектору й наукової спільноти у процеси кіберзахисту формують істотні інституційні дисбаланси та знижують рівень ефективності національної політики у цій сфері.

У зв'язку з цим проблематика нормативно-інституційного забезпечення національної системи кібербезпеки України постає як один із провідних напрямів сучасної адміністративно-правової доктрини. Йдеться не лише про вдосконалення законодавчого регулювання, а й про становлення нової моделі публічного управління – кібербезпеки як інтегрованого елементу національної безпеки, заснованого на принципах верховенства права, інституційної взаємодії, публічно-приватного партнерства та стійкості держави до гібридних загроз.

Аналіз останніх досліджень і публікацій. Питання правового та інституційного забезпечення кібербезпеки ґрунтовно досліджувалися у працях вітчизняних учених, зокрема І. В. Діордіци, Л. А. Веселової, Н. І. Логінової, С. М. Мазепи, А. В. Тарасюка, О. Д. Довганя, Ю. Г. Даника, В. Л. Бурячка, М. Т. Гаврильціва, О. І. Марущака, Ю. А. Гульванської, С. В. Демедюка, а також у дослідженнях С. Вдовенка, Є. Живила, О. Черноног і В. Докіля [1–8]. Вагоме місце посідають сучасні праці, присвячені аналізу правових механізмів кібероборони держави, науковому осмисленню стратегічних засад реалізації Стратегії кібербезпеки України та адаптації національного законодавства до стандартів ЄС і НАТО. Вагомий порівняльно-правовий доробок належить М. Кравчуку, В. Кравчуку, А. Грубінку, Т. Подковенку та В. Ухачу, які на матеріалі української практики окреслюють тенденції еволюції правового регулювання кібербезпеки в руслі європейської інтеграції [13]. Додатково, системний аналітичний масив узагальнено у колективній монографії НІСД, присвяченій правовим аспектам кібербезпеки в умовах гібридної агресії, що забезпечує комплексне бачення проблематики та верифікує порівняльні висновки [10].

Водночас, попри наявність істотних наукових напрацювань, дискусійними залишаються питання нормативної узгодженості компетенцій суб'єктів системи, механізмів державно-приватної взаємодії та гармонізації вітчизняного законодавства з правом Європейського Союзу.

Метою цієї статті є комплексне теоретико-правове обґрунтування нормативно-інституційних засад формування національної системи кібербезпеки України, а також визначення основних напрямів удосконалення правового регулювання та оптимізації інституційної взаємодії суб'єктів державного і недержавного секторів у контексті євроатлантичної інтеграції.

Завдання дослідження полягають у тому, щоб проаналізувати чинну нормативно-правову базу, що регулює сферу кібербезпеки України; розкрити інституційну структуру національної системи кібербезпеки та окреслити компетенції її ключових суб'єктів; визначити проблемні аспекти функціонування системи та сформулювати напрями її вдосконалення відповідно до міжнародних стандартів і кращих практик.

Отже, дослідження спрямоване на виявлення закономірностей становлення національної системи кібербезпеки як складової державної політики у сфері національної безпеки та вироблення концептуальних пропозицій щодо підвищення її ефективності в умовах сучасних викликів цифрової епохи.

1. Нормативно-правові засади формування національної системи кібербезпеки України.

Нормативно-правове регулювання у сфері кібербезпеки України становить багаторівневу систему актів, що охоплює закони, укази Президента, постанови Кабінету Міністрів, а також міжнародні договори, ратифіковані Україною. Центральним елементом цієї системи є Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII [21], який визначає правові та організаційні засади забезпечення кібербезпеки, встановлює повноваження суб'єктів системи (зокрема Служби безпеки України, Державної служби спеціального зв'язку та захисту інформації, Міністерства оборони, Національної поліції, Національного банку тощо) та закріплює принципи взаємодії між державними і приватними структурами. Цей акт став основою для формування сучасної моделі національної системи кібербезпеки та заклав підґрунтя для подальшого розвитку нормативно-інституційної бази. Варто підкреслити, що Закон України «Про національну безпеку України» [22] визначає кібербезпеку як складову загальної системи національної безпеки, чим закладає стратегічні основи для формування її інституційної архітектури.

Важливим стратегічним документом є Стратегія кібербезпеки України, затверджена Указом Президента України від 26 серпня 2021 року № 447/2021 [26], яка визначає цілі, пріоритети та напрями державної політики у сфері кіберзахисту. Документ формує рамкову політичну основу національної безпеки у кіберпросторі, передбачає розвиток спроможностей сил оборони та правоохоронних органів, створення умов для кіберстійкості критичної інфраструктури, удосконалення системи реагування на інциденти, а також інтеграцію у спільний євроатлантичний безпековий простір. Її імплементацію забезпечує План реалізації Стратегії кібербезпеки України, затверджений Указом Президента від 1 лютого 2022 року № 37/2022 [27], що деталізує конкретні заходи, строки виконання та відповідальні органи.

У системі законодавства важливе місце посідають також базові акти інформаційного права, зокрема Закон України «Про інформацію» від 2 жовтня 1992 року № 2657-XII [17] та Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 5 липня 1994 року № 80/94-ВР [18], які визначають правові засади доступу, використання, зберігання й захисту інформації, у тому числі в електронних комунікаціях. Закон «Про критичну інфраструктуру» від 15 липня 2021 року № 1882-IX [23] деталізує організаційно-правові механізми управління безпекою об'єктів критичної інформаційної інфраструктури, а Постанова Кабінету Міністрів України від 19 червня 2019 року № 518 [29] установлює Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури, що конкретизують технічні та процедурні стандарти безпеки.

Суттєву роль у розбудові інституційного середовища відіграє Національний координаційний центр кібербезпеки при Раді національної безпеки і оборони, правовий статус якого визначено Указом Президента України від 07.06.2016 № 242/2016, яким затверджено Положення про Національний координаційний центр кібербезпеки [28]. Він забезпечує міжвідомчу взаємодію, координацію діяльності державних органів і реалізацію єдиної державної політики у сфері кіберзахисту.

Важливою складовою нормативної системи залишається міжнародно-правова

основа. Україна є стороною Конвенції про кіберзлочинність (Будапештська конвенція) [16], яка визначає єдині стандарти криміналізації кіберзлочинів і співпраці між державами у розслідуванні кіберінцидентів. Її положення лягли в основу національних норм, що регулюють кіберпростір і кримінальну відповідальність за порушення у сфері інформаційної безпеки.

Законодавство України поступово адаптується до правових стандартів Європейського Союзу, зокрема до вимог Директиви (ЄС) 2016/1148 про безпеку мережевих і інформаційних систем [11], а також її оновленої версії – Директиви (ЄС) 2022/2555 (NIS2), яка передбачає посилення обов'язків держав щодо управління кіберризиками та реагування на інциденти. У цьому контексті важливе місце посідає й Закон України «Про захист персональних даних» [20], положення якого є основою для гармонізації з Регламентом (ЄС) 2016/679 (GDPR) у частині правового режиму обробки та захисту даних у цифровому середовищі. Україна бере курс на гармонізацію своєї політики з європейськими підходами, що підтверджується даними Національного індексу кібербезпеки (National Cyber Security Index) [15], де простежується позитивна динаміка розвитку нормативних механізмів і відповідності міжнародним практикам.

Як зазначає С. М. Мазепа, ефективність нормативного регулювання у сфері кібербезпеки безпосередньо залежить від узгодженості законодавчих норм, інституційної спроможності органів державної влади та наявності єдиної стратегічної візії [7]. Подібної позиції дотримуються О. І. Марущак [8] і Л. А. Веселова [2], які підкреслюють, що імплементація європейських стандартів та розвиток інституційної архітектури кібербезпеки є необхідною умовою для досягнення кіберстійкості держави.

2. Інституційна структура національної системи кібербезпеки України

Розбудова національної системи кібербезпеки (НСКБ) України відбувається на основі поєднання принципів централізованого державного управління та багаторівневої координації між органами сектору безпеки, оборони, правопорядку і спеціальними суб'єктами, уповноваженими на здійснення функцій у сфері захисту інформаційного простору. У правовому полі така модель визначена Законом України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р. № 2163-VIII [21], який закріпив систему суб'єктів забезпечення кібербезпеки, їхні повноваження, принципи взаємодії та порядок координації діяльності.

Роль Ради національної безпеки і оборони України та Національного координаційного центру кібербезпеки. Відповідно до Стратегії кібербезпеки України, затвердженої Указом Президента України від 26.08.2021 р. № 447/2021 [26], стратегічне управління у сфері кібербезпеки здійснює Рада національної безпеки і оборони України (РНБО), яка координує діяльність усіх органів державної влади щодо запобігання, виявлення і нейтралізації кіберзагроз. Безпосереднім координаційним органом РНБО є Національний координаційний центр кібербезпеки (НКЦК), правовий статус якого визначено Указом Президента України від 07.06.2016 № 242/2016 «Про затвердження Положення про Національний координаційний центр кібербезпеки» [28]. НКЦК виконує роль головного міжвідомчого майданчика для оперативного обміну інформацією, аналізу кіберінцидентів, координації дій суб'єктів системи безпеки та ініціювання відповідних управлінських рішень. Відповідно до Положення, Центр здійснює координацію та контроль діяльності суб'єктів сектору безпеки й оборони у сфері кібербезпеки, аналіз стану кіберзахисту критично важливих об'єктів та готовності суб'єктів до протидії кіберзагрозам, а також бере участь у розробленні галузевих індикаторів кібербезпеки та прогнозуванні загроз [28]. Крім того, НКЦК готує концептуальні пропозиції РНБО щодо підвищення ефективності державної політики, розвитку нормативної бази й узгодження діяльності органів сектору безпеки, а також забезпечує моніторинг стану впровадження національних стандартів у сфері кіберзахисту, гармонізованих зі стандартами ЄС та НАТО [28].

Як відзначає А. І. Марущак, діяльність НКЦК є ключовим чинником ефективного управління у сфері кібербезпеки, оскільки забезпечує «інституційне з'єднання» секторів оборони, внутрішніх справ, інформаційної політики та цифрової трансформації держави [8].

Повноваження Державної служби спеціального зв'язку та захисту інформації України

Центральним органом виконавчої влади, який реалізує державну політику у сфері технічного та криптографічного захисту інформації, урядового зв'язку і кіберзахисту, є Державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІ). Її правовий статус визначено Законом України «Про Державну службу спеціального зв'язку та захисту інформації України» від 23.02.2006 р. № 3475-IV [19].

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» [21], ДССЗЗІ є національним координатором у сфері кіберзахисту, що забезпечує розроблення стандартів, організацію технічного аудиту, реагування на кіберінциденти та взаємодію з міжнародними структурами. При ДССЗЗІ діє національний центр реагування на комп'ютерні надзвичайні події (CERT-UA), який виконує аналітичні, експертні та комунікаційні функції. Як засвідчено у звітах служби [9], CERT-UA забезпечує обмін технічною інформацією між державними установами, операторами критичної інфраструктури та приватними компаніями, що дозволяє своєчасно виявляти і локалізувати кіберінциденти.

З метою підвищення технічної стійкості об'єктів критичної інфраструктури Постановою Кабінету Міністрів України від 19.06.2019 р. № 518 затверджено Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури [29], які передбачають обов'язок суб'єктів господарювання створювати внутрішні системи управління інформаційною безпекою під методичним наглядом ДССЗЗІ.

Функції Служби безпеки України, Міністерства оборони, Національного банку та Національної поліції. У структурі національної системи кібербезпеки особливе місце посідає Служба безпеки України (СБУ), яка відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII [21] є ключовим суб'єктом протидії кіберзагрозам воєнного, розвідувально-підривного та терористичного характеру. На СБУ покладено контррозвідувальні, оперативно-розшукові та превентивні функції, спрямовані на виявлення, запобігання та нейтралізацію кібератак, що становлять загрозу суверенітету, конституційному ладу, обороноздатності та інформаційній безпеці держави. В умовах триваючої збройної агресії проти України діяльність СБУ у цій сфері має системний, комплексний характер і здійснюється у тісній взаємодії з іншими складовими сектору безпеки та оборони.

Важливою ланкою у структурі НСКБ є Міністерство оборони України (МОУ), яке реалізує державну політику кібероборони відповідно до Стратегії кібербезпеки України, затвердженої Указом Президента України від 26.08.2021 № 447/2021 [26], та Плану її реалізації (Указ Президента України від 01.02.2022 № 37/2022) [27]. Послідовність реалізації стратегічних завдань підтверджується розпорядженням Кабінету Міністрів України від 7 березня 2025 року № 204-р, яким затверджено план заходів на 2025 рік з імплементації Стратегії кібербезпеки [30]. МОУ забезпечує кіберзахист інформаційних ресурсів Збройних Сил України, захист систем управління військами, урядових комунікацій, а також участь у формуванні оперативних спроможностей щодо відбиття кіберагресії. Як зазначається у Стратегії, кібероборона розглядається як складова національної оборонної політики, що інтегрує інформаційно-аналітичні, розвідувальні та технічні компоненти [26].

У фінансовому секторі важливу роль відіграє Національний банк України (НБУ), який відповідно до Закону № 2163-VIII [21] виконує функції національного регулятора безпеки банківських інформаційних систем і платіжної інфраструктури. НБУ встановлює обов'язкові вимоги до кіберзахисту фінансових установ, здійснює моніторинг інцидентів у платіжних системах, а також координує діяльність банківського сектору з питань інформа-

ційної безпеки. З урахуванням цифровізації фінансових послуг роль НБУ як системного суб'єкта забезпечення кіберстійкості набула особливої ваги, що відповідає європейським стандартам NIS2 та практиці центральних банків держав – членів ЄС [11].

Національна поліція України (НПУ) виконує завдання щодо протидії кіберзлочинності та проведення досудового розслідування у сфері кіберзлочинів. Важливим кроком у посиленні цих функцій стало ухвалення Закону України від 15.03.2022 № 2137-IX, яким внесено зміни до Кримінального процесуального кодексу України та Закону «Про електронні комунікації» з метою підвищення ефективності досудового розслідування кібератак «за гарячими слідами» [24]. Згідно із зазначеним актом, НПУ отримала розширені процесуальні повноваження для оперативного реагування на кібератаки, у тому числі щодо фіксації цифрових доказів та взаємодії з міжнародними правоохоронними структурами.

Як слушно зазначають О. Д. Довгань та М. В. Тарасюк, ефективність діяльності зазначених органів визначається не лише обсягом їхніх компетенцій, а насамперед рівнем міжвідомчої координації та інтеграції інформаційних ресурсів у межах єдиної системи кіберзахисту [5, с. 137]. Злагоджена взаємодія СБУ, МОУ, НБУ та НПУ сприяє зміцненню обороноздатності держави у кіберпросторі, формуванню комплексного підходу до управління кіберризиками та підвищенню загальної стійкості національної системи кібербезпеки.

Принципи взаємодії державних і недержавних суб'єктів, та євроінтеграційний аспект. Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII [21], одним із ключових принципів побудови національної системи кібербезпеки є державно-приватне партнерство, спрямоване на поєднання потенціалу держави, бізнесу та наукової спільноти для досягнення належного рівня кіберзахисту. Цей принцип передбачає залучення операторів критичної інфраструктури, приватних ІТ-компаній, банківського сектору, телекомунікаційних операторів і закладів науки до процесу формування та реалізації державної політики у сфері кібербезпеки. Суб'єкти господарювання, які забезпечують функціонування критично важливих об'єктів, зобов'язані дотримуватися державних стандартів безпеки, повідомляти про кіберінциденти та взаємодіяти з компетентними органами, зокрема Державною службою спеціального зв'язку та захисту інформації (ДССЗЗІ) і командою реагування на комп'ютерні надзвичайні події CERT-UA [29].

Як наголошується у офіційних публікаціях ДССЗЗІ [9], забезпечення ефективної кібербезпеки неможливе без тісної взаємодії з приватним сектором, оскільки саме бізнес є власником і оператором більшості елементів національної кіберінфраструктури – від телекомунікаційних мереж до платіжних систем і промислових технологічних процесів. ДССЗЗІ виступає координатором цього партнерства, формуючи єдині стандарти взаємодії, обміну інформацією та реагування на інциденти в межах системи CERT-UA, що відповідає міжнародній практиці управління кіберризиками.

Розвиток національної системи кібербезпеки відбувається у тісному зв'язку з європейськими інтеграційними процесами. Україна послідовно гармонізує своє законодавство із положеннями Директиви (ЄС) 2016/1148 про безпеку мережевих та інформаційних систем (NIS Directive) [11] і її оновленої редакції – Директиви (ЄС) 2022/2555 (NIS2), яка встановлює нові стандарти кіберстійкості для державних і приватних суб'єктів критичної інфраструктури. Як зазначає С. М. Мазепа, адаптація до європейської моделі кіберуправління, що ґрунтується на взаємодії державних компетентних органів із національними CERT/CSIRT, є передумовою підвищення стійкості української системи до кібератак і забезпечення стратегічної сумісності з безпековими структурами ЄС та НАТО [7, с. 169].

У свою чергу, за даними IFES Ukraine, Україна вже досягла суттєвого прогресу у формуванні інституційної архітектури, наближеної до європейських стандартів, зберігаючи водночас власну специфіку, обумовлену умовами гібридної війни [12].

Високі показники Національного індексу кібербезпеки (NCSI) [15] підтверджують позитивну динаміку розвитку нормативно-правових і організаційних механізмів кіберзахисту, що є результатом комплексного підходу до реалізації євроінтеграційного курсу у цій сфері.

Проблеми та напрями вдосконалення нормативно-інституційної системи кібербезпеки України. Незважаючи на суттєвий поступ у формуванні нормативно-правового та інституційного підґрунтя кібербезпеки, національна система залишається у процесі становлення та потребує подальшого вдосконалення. Як слушно зазначають С. М. Мазепа та А. І. Марущак, одним із ключових викликів є недостатня координація між відомствами сектору безпеки і оборони, що призводить до дублювання функцій і зниження ефективності реагування на кіберзагрози [7; 8]. Відсутність єдиного механізму обміну інформацією між державними та недержавними суб'єктами, попри існування НКЦК при РНБО України, ускладнює оперативне прийняття рішень та реалізацію превентивних заходів.

Окрему проблему становлять прогалини у підзаконному регулюванні, що стосуються реалізації положень Закону України «Про основні засади забезпечення кібербезпеки України» [21]. Як вказує Ю. А. Гульванська, низка підзаконних актів не забезпечує достатньої конкретизації процедур взаємодії суб'єктів кіберзахисту, зокрема у питаннях аудиту безпеки, сертифікації інформаційних систем та стандартизації технічних вимог [3, с. 48]. Подібні висновки підтверджуються й у дослідженні IFES Ukraine, де наголошується на необхідності розроблення чітких регламентів реалізації міжвідомчої політики кіберзахисту [12, с. 56].

Важливим системним викликом залишається кадрове забезпечення та підготовка фахівців, спроможних ефективно діяти в умовах зростання кількості і складності кіберінцидентів. Як підкреслює Н. І. Логінова, забезпечення кадрової стійкості національної системи вимагає формування державних стандартів сертифікації фахівців у галузі кібербезпеки та посилення освітньої складової підготовки кадрів для сектору безпеки [6, с. 178]. Цю тезу підтримують і О. Д. Довгань та М. В. Тарасюк, які акцентують на важливості розвитку аналітичного та наукового потенціалу для підтримки національної політики у сфері кібероборони [5, с. 139].

З огляду на євроінтеграційні пріоритети України, стратегічним напрямом розвитку системи кібербезпеки є гармонізація законодавства з правом Європейського Союзу, насамперед у контексті імплементації Директиви (ЄС) 2022/2555 (NIS2), Регламенту (ЄС) 2016/679 (GDPR) та Європейського акту про кіберсолідарність (Cyber Solidarity Act). Як зазначається у матеріалах ENISA [11] та IFES Ukraine [12], ефективне впровадження цих стандартів забезпечить підвищення рівня кіберстійкості критичної інфраструктури, інтеграцію українських механізмів управління ризиками у європейський простір та зміцнення спроможностей держави у сфері стратегічної кібероборони. Важливим кроком у подоланні нормативних прогалин стало ухвалення Закону України № 4336-IX «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів» [25], який конкретизував вимоги до кіберзахисту державних систем і об'єктів критичної інформаційної інфраструктури.

Отже, подальший розвиток національної системи кібербезпеки України має бути спрямований на посилення міжвідомчої координації, усунення нормативних прогалин, розбудову кадрового потенціалу, а також на повну адаптацію до стандартів ЄС і НАТО. Реалізація цих завдань сприятиме формуванню стійкої, скоординованої та інституційно зрілої моделі кібербезпеки, здатної ефективно протидіяти сучасним загрозам і забезпечувати національні інтереси України у цифровому середовищі.

Висновки. Здійснений аналіз показав, що нормативно-інституційна модель кібербезпеки України має достатній базовий каркас (закон № 2163-VIII, Стратегія та План її реалізації), проте зберігає «вузькі місця» у координації суб'єктів, підзаконній конкретизації процедур взаємодії, а також у кадровому та науково-аналітичному

забезпеченні. Пріоритетами подальшого розвитку є: інституційне посилення НКЦК як центру координації; уніфікація підзаконних регламентів (аудит, сертифікація, повідомлення про інциденти); запровадження стандартів підготовки і сертифікації фахівців; повноцінна імплементація підходів NIS2/GDPR та практик кіберсолідарності ЄС. Їх реалізація забезпечить цілісність, керованість і стійкість НСКБ, підвищивши здатність держави протидіяти сучасним кіберзагрозам.

Список використаної літератури:

1. Вдовенко С., Живило Є., Черноног О., Докіль В. Аналіз особливостей функціонування системи кібероборони. Нормативно-правові аспекти. *Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка*. 2022. Вип. 74. С. 52–72. URL: https://doi.org/10.17721/2519-481X/2022/74-06
2. Веселова Л. А. Адміністративно-правові засади кібербезпеки в умовах гібридної війни : дис. … д-ра юрид. наук : 12.00.07. Одеса : Одеський держ. ун-т внутр. справ, 2021. 410 с.
3. Гульванська Ю. А. Правове регулювання кібербезпеки в Україні: сучасний стан та перспективи розвитку. *Інформація і право*. 2024. № 2(49). С. 45–52.
4. Діордіца І. В. Адміністративно-правове регулювання кібербезпеки України : дис. … д-ра юрид. наук : 12.00.07. Запоріжжя : Запорізький нац. ун-т, 2018. 519 с.
5. Довгань О. Д., Тарасюк М. В. Національні інтереси України в кібернетичній сфері. *Інформація і право*. 2021. № 1. С. 134–142.
6. Логінова Н. І. Кібернетична безпека держави: теоретико-правовий аспект : монографія. Харків : Право, 2023. 224 с.
7. Мазепа С. Кібербезпека в Україні: сучасні виклики та шляхи вдосконалення законодавчого регулювання. *Актуальні проблеми правознавства*. 2025. № 2(42). С. 164–172.
8. Марущак А. І. Стратегія кібербезпеки України: правові засади та механізми реалізації. *Вісник Національного університету «Львівська політехніка». Юридичні науки*. 2024. № 2(38). С. 112–119.
9. Національна система кібербезпеки функціонуватиме ефективніше. Державна служба спеціального зв'язку та захисту інформації України. 2023. URL: https://cip.gov.ua/ua/news/nacionalna-sistema-kiberbezpeki-funkcionuvatime-efektivnishe
10. Україна в умовах гібридної агресії: правові аспекти кібербезпеки : колективна монографія. За ред. В. М. Фурашева. Київ : НІСД, 2024. 312 с.
11. ENISA. Directive on security of network and information systems (NIS Directive). URL: https://www.enisa.europa.eu/topics/nis-directive
12. IFES Ukraine. *Cybersecurity in Ukraine: Legal Framework Analysis*. Kyiv : IFES Ukraine, 2024. 156 p.
13. Kravchuk M., Kravchuk V., Hrubinko A., Podkovenko T., Ukhach V. Cyber security in Ukraine: Theoretical view and legal regulation // *Law, Policy and Security*. 2024. Vol. 2, No. 2. P. 28–38. https://doi.org/10.62566/lps/2.2024.28.
14. Legal Aspects of Cybersecurity During Armed Conflicts: Ukrainian Case Study // *International Journal of Cyber Law*. 2024. Vol. 12, Issue 3. P. 45–67.
15. Ukraine. National Cyber Security Index. URL: https://ncsi.ega.ee/country/ua/
16. Конвенція про кіберзлочинність (Будапештська конвенція) : ратифікована із застереженнями і заявами Законом України від 07.09.2005 № 2824-IV. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text
17. Про інформацію : Закон України від 02.10.1992 № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text
18. Про захист інформації в інформаційно-телекомунікаційних 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
19. Про Державну службу спеціального зв'язку та захисту інформації України : Закон України від 23.02.2006 № 3475-IV. URL: https://zakon.rada.gov.ua/laws/show/3475-iv#Text
20. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text
21. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
22. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text

23. Про критичну інфраструктуру : Закон України від 15.07.2021 № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text
24. Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам : Закон України від 15.03.2022 № 2137-IX. URL: https://zakon.rada.gov.ua/laws/show/2137-20#Text
25. Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури : Закон України від 27.03.2025 № 4336-IX. URL: https://zakon.rada.gov.ua/go/4336-20
26. Про Стратегію кібербезпеки України : Указ Президента України від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text
27. Про План реалізації Стратегії кібербезпеки України : Указ Президента України від 01.02.2022 № 37/2022. URL: https://zakon.rada.gov.ua/laws/show/37/2022#n5
28. Про Положення про Національний координаційний центр кібербезпеки при Раді національної безпеки і оборони України : Указ Президента України від 07.06.2016 № 242/2016. https://zakon.rada.gov.ua/laws/show/242/2016#Text
29. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури : постанова Кабінету Міністрів України від 19.06.2019 № 518. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF
30. Про затвердження плану заходів на 2025 рік з реалізації Стратегії кібербезпеки України : розпорядження Кабінету Міністрів України від 07.03.2025 № 204-р. URL: https://zakon.rada.gov.ua/go/204-2025-%D1%80

Kolesnyk O. O. Regulatory and institutional principles of forming the national cybersecurity system of Ukraine

The article is devoted to the theoretical and legal substantiation of the architecture of the national cybersecurity system of Ukraine as an integrated component of national security and state resilience in the conditions of digital transformation and armed aggression. Based on the systemic and institutional and legal approaches, the regulatory framework (Law of Ukraine «On the Basic Principles of Ensuring Cybersecurity of Ukraine» No. 2163-VIII, Cybersecurity Strategy and its Implementation Plan, basic acts of information law, legislation on critical infrastructure) and the institutional structure of the system (National Security and Defense Council of Ukraine, National Cybersecurity Coordination Center, State Service for Special Communications and Information Protection, Security Service of Ukraine, Ministry of Defense, National Bank and National Police) are revealed. Key problems of the system's functioning are identified – fragmentation of secondary legislation, duplication of competences, insufficient coordination between entities, staffing limitations and lack of unified audit, certification and cyber incident response procedures. Areas for improving the regulatory and institutional model are substantiated: strengthening the coordinating role of the National Cybersecurity Coordination Center, developing unified procedures for interaction between public and private structures, introducing state standards for training specialists, creating a national cyber threat monitoring system and increasing the level of responsibility of critical infrastructure operators. Within the framework of Ukraine's European integration course, the need for harmonization of national legislation with European Union law has been proven, in particular, the implementation of Directive (EU) 2022/2555 (NIS2), Regulation (EU) 2016/679 (GDPR) and the practices of the European Cyber Solidarity Act. The proposed concept envisages a transition to an integrated, risk-oriented and resilient cybersecurity system capable of ensuring the protection of state sovereignty, citizens' rights and the stability of critical infrastructure in the digital environment.

Key words: *cybersecurity, national security, National Cybersecurity Coordination Center, State Service of Special Communications and Information Protection of Ukraine, Security Service of Ukraine, cyber defence, critical infrastructure.*