УДК 351/354.1 (477)

А. В. Кузьменко,
аспірант, ДЗВО "Університет менеджменту освіти" НАПН України
ORCID ID: https://orcid.org/0009-0000-4159-355X

DOI: 10.32702/2306-6814.2025.9.260

ФОРМУВАННЯ ТА РЕАЛІЗАЦІЯ ДЕРЖАВНОЇ ПОЛІТИКИ УКРАЇНИ У СФЕРІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

A. Kuzmenko,
Postgraduate Student, State Educational Institution "University of Educational Management" of the National Academy of Sciences of Ukraine

FORMATION AND IMPLEMENTATION OF STATE POLICY OF UKRAINE IN THE SPHERE OF INFORMATION SECURITY IN THE CONDITIONS OF DIGITAL TRANSFORMATION

У статті удосконалено систему правового регулювання забезпечення інформаційної безпеки в умовах цифрової трансформації шляхом внесення змін до нормативно-правових актів України, а саме: органам публічного управління заборонити використовувати у роботі іноземні програмні продукти, що мають засоби захисту, та співпрацювати з іноземними виробниками даних комп'ютерних програм у контексті додаткових заходів щодо забезпечення інформаційної безпеки України; прийняти Концепцію формування та розвитку культури інформаційної безпеки громадян України, яка має бути націленою на формування знань, умінь і навичок з питань інформаційної безпеки з урахуванням стратегічних цілей державної політики у сфері інформаційного права; у рамках зовнішньополітичної діяльності здійснити просування національних інтересів України, української культури, оскільки втрата культурної ідентичності українського народу детермінує ризики та загрози державного суверенітету; вдосконалити законодавство про освіту та систему заходів підготовки фахівців із захисту інформації на основі моніторингу існуючих потреб у контексті вдосконалення освітніх програм і стандартів у цій сфері, у тому числі за допомогою посилення отримуваних компетенцій щодо забезпечення кібербезпеки, комп'ютерної експертизи та розслідування цифрових злочинів.

Визначено значний дефіцит фахівців у галузі інформаційних технологій та захисту інформації через недостатність спеціалізованих освітніх установ з підготовки кадрів у цій сфері. У зв'язку з цим важливими є прогнози потреб у фахівцях та підвищення якості підготовки відповідних наукових та технічних кадрів. Тому одним із ключових напрямів державної політики є вдосконалення законодавства про освіту та системи заходів підготовки фахівців із захисту інформації на основі моніторингу існуючих потреб. Пріоритетним є вдосконалення освітніх програм і стандартів у цій сфері, у тому числі за допомогою посилення отримуваних компетенцій щодо забезпечення кібербезпеки, комп'ютерної експертизи та розслідування цифрових злочинів. З метою реалізації даних заходів у запропонованій Концепції формування та розвитку культури інформаційної безпеки громадян України запропоновано визначити основне завдання — вироблення комплексного підходу до підвищення рівня культури інформаційної безпеки громадян та формування у них навичок протидії загрозам інформаційної безпеки. Цим правовим актом слід передбачити низку положень, спрямованих на формування знань, умінь та навичок з питань інформаційної безпеки на основі регулярного моніторингу рівня грамотності громадян з питань інформаційної безпеки.

The article improves the system of legal regulation of ensuring information security in the context of digital transformation by making amendments to the regulatory legal acts of Ukraine, namely: to prohibit public administration bodies from using foreign software products that have means of protection in their work and from cooperating with foreign producers of these computer programs in the context of additional measures to ensure the information security of Ukraine; to adopt the Concept of Formation and Development of Information Security Culture of Ukrainian Citizens, which should be aimed at forming knowledge, skills and abilities on information security issues, taking into account the strategic goals of state policy in the field of information law; to promote the national interests of Ukraine and Ukrainian culture within the framework of foreign policy activities,

since the loss of the cultural identity of the Ukrainian people determines risks and threats to state sovereignty; improve the legislation on education and the system of measures for training information protection specialists based on monitoring existing needs in the context of improving educational programs and standards in this area, including by strengthening the acquired competencies in cybersecurity, computer forensics, and digital crime investigation.

A significant shortage of specialists in the field of information technology and information protection has been identified due to the lack of specialized educational institutions for training personnel in this area. In this regard, forecasts of needs for specialists and improving the quality of training of relevant scientific and technical personnel are important. Therefore, one of the key areas of state policy is to improve the legislation on education and the system of measures for training information protection specialists based on monitoring existing needs. The priority is to improve educational programs and standards in this area, including by strengthening the acquired competencies in cybersecurity, computer forensics, and digital crime investigation. In order to implement these measures, the proposed Concept for the Formation and Development of Information Security Culture of Ukrainian Citizens proposes to define the main task — to develop a comprehensive approach to increasing the level of information security culture of citizens and developing their skills to counter information security threats. This legal act should provide for a number of provisions aimed at the formation of knowledge, skills and abilities in information security based on regular monitoring of the level of citizens' literacy in information security.

Ключові слова: державна політика України, сфері забезпечення інформаційної безпеки, цифрова трансформація.

Key words: state policy of Ukraine, information security, digital transformation.

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Державне регулювання забезпечення інформаційної безпеки багато в чому визначається державною політикою в питаннях розробки, використання цифрових технологій в публічному управлінні, бізнесі, громадянському суспільстві, спрямованої на формування стійкого технологічного суверенітету держави в інформаційно-комунікаційній сфері в умовах сучасних викликів і ризиків; правовідносин, забезпечення національних інтересів України. Основними цілями державної політики у сфері інформаційного права є: розвиток вітчизняних інформаційних ресурсів та забезпечення громадян суспільно значущою достовірною інформацією; розвиток національного сегменту мережі та ЗМІ, що відображають українську позицію по ключових питаннях політики; консолідуються у єдину систему завдань, створені задля досягнення цифрового і технологічного суверенітету України у інформаційної сфері, як основи економічного розвитку та забезпечення суверенітету.

Основні напрямки інформаційно-правової державної політики України реалізуються за допомогою стратегічного планування і вдосконалення законодавства, реалізації заходів, спрямованих на досягнення стратегічних пріоритетів. що забезпечують доступ до цифрових даних громадян та організацій. При цьому триває процес формування системи організаційних заходів захисту інформації в інтересах національної безпеки.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Значну роль теоретичному осмисленні особливостей формування та реалізація державної політики у сфері забезпечення інформаційної безпеки в умовах цифрової трансформації зіграли роботи українських і зарубіжних авторів. Окремим питання реалізація державної політики у сфері забезпечення інформаційної безпеки присвячені праціТ. Запорожець, А. Осьмака, С. Чукут та ін. Різноманітним напрямам дослідження цифрової трансформації присвячено праці М. Гребенюк, О. Звоздецька, Б. Леонов, О. Тронько, Р. Черниш та ін. Аналізу компетенції агентств США проведено у роботах Р. Пірса, П. Веркюля, А. Вермюля, Є. Каган, К. Санстейн, Д. Валдо. При аналізі французького права теоретичною базою послужили роботи Ж. Ріверо, Ж. Валін, а щодо питань правового статусу незалежних адміністративних відомств — Ж. Шевальє, Ж.Л. Отан. У контексті розгляду проблем формування державних систем електронної ідентифікації, використання електронного підпису слід зазначити роботи зарубіжного дослідника С. Мейсона.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою статті є пошук шляхів модифікації нині діючого механізму формування та реалізація державної політики у сфері забезпечення інформаційної безпеки в умовах цифрової трансформації.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

Результати порівняльно-правового аналізу Доктрин інформаційної безпеки України 2009 р. [1] та 2017 р. [2], відповідно, свідчать про підвищення значущості досліджуваної підгалузі в українському законодавстві. Ці доктрини мають стратегічний характер і спрямовані на вдосконалення правових норм у сфері інформаційної безпеки. Так, одним із головних нововведень у Доктрині інформаційної безпеки України 2017 р. є обов'язковість моніторингу виконання положень Доктрини та подання щорічного звіту Президенту України, що спрямоване на підвищення ефективності органів публічної влади та недержавних організацій у межах своїх повноважень.

Водночас одним з основних нормативних правових актів у галузі інформаційної безпеки є Стратегія розвитку інформаційного суспільства в Україні [3]. У цьому нормативному правовому акті визначено основні напрямки щодо внутрішньої та зовнішньої політики держави у сфері забезпечення інформаційної безпеки. У свою чергу, за нових геополітичних умов державна політика у сфері забезпечення інформаційної безпеки змінилася. В даний час проблема забезпечення інформаційної безпеки має першорядне значення і вимагає ухвалення нових правових рішень. Одним із основних способів вирішення питань забезпечення кібербезпеки стало створення Комітету Верховної Ради України з питань цифрової трансформації [4], Комітету з технологій розвитку та кібербезпеки НАБУ [5], Комітету Національної комісії з цінних паперів та фондового ринку комітету з питань інформаційних технологій та кібербезпеки [6].

Зазначені державні структури здійснюють діяльність з формування заходів безпеки критично важливої інфраструктури та контроль за державними органами, до повноважень яких входять питання забезпечення технологічної незалежності об'єктів інформаційної інфраструктури. Аналізуючи динаміку показників кібератак на вітчизняні інформаційні об'єкти не можна не наголосити на важливості діяльності вищевказаних спеціальних органів державної влади, які на постійній основі здійснюють прогнозування, виявлення та оцінку внутрішніх та зовнішніх ризиків та загроз, що впливають на національну безпеку у галузі розвитку та вдосконалення інформаційних технологій.

Водночас однією з основних загроз безпеці у вищезгаданих документах стратегічного планування визнано кіберзлочинність. У юридичній доктрині неодноразово зазначалося, що у час проблема інформаційної безпеки у кримінально-правовому контексті має першорядне значення, у зв'язку з цим необхідне прийняття нових правових рішень, обумовлених сучасними викликами і загрозами інформаційній безпеці.

Сучасна динаміка злочинних діянь з використанням комп'ютерних та інформаційних пристроїв показує, що масштаби суспільно небезпечних діянь мають особливу динаміку зростання у фінансовій, соціальній та економічній сферах життєдіяльності. Основною причиною зростання кіберзлочинності є революційний розвиток інформаційних технологій, що використовуються у всіх секторах, водночас інформаційні технології впроваджуються в роботу органів публічної влади (державної, органів місцевого самоврядування та інших організацій, що реалізують державні функції).

Зростання кіберзлочинності залежить багатьох чинників, зокрема від світових процесів. Наприклад, під час пандемії нової коронавірусної інфекції COVID-19 відбулося багаторазове збільшення операцій в електронному вигляді, передача інформації обмеженого доступу та інформації персональних даних. У свою чергу, масова електронна взаємодія та використання інформаційних технологій з великим масивом цифрових даних призвели до великої кількості злочинів у сфері інформаційної безпеки. Російська кібер-агресія спричинила негативну тенденцію інформаційних атак та кіберпротиборства, що визначили збільшення показників суспільно небезпечних діянь та появу в умовах трансформації права нових видів посягань на життєво важливі об'єкти, включаючи об'єкти критичної інформаційної інфраструктури. Вивчення соціально-кримінологічних даних свідчить про ефективність заходів у рамках державної політики щодо захисту об'єктів критичної інформаційної інфраструктури та технічної взаємодії щодо протидії комп'ютерним злочинам у сфері інформаційної безпеки, що й визначило динаміку аналізованих показників. Звертаючись до питання про протидію загрозам скоєння злочинів в інформаційному середовищі в рамках державної політики у сфері забезпечення інформаційної безпеки, слід зазначити участь України в активному обговоренні питань безпеки в інформаційній сфері. Так, державна політика України спрямована на розвиток системи забезпечення безпеки в інформаційній сфері з урахуванням національних інтересів держави та сприяння формуванню правових механізмів щодо врегулювання конфліктів в інформаційному суспільстві. Водночас основним напрямом реалізації державної політики у галузі міжнародної інформаційної безпеки виступає підвищення ефективності інформаційного обміну під час розслідування суспільно небезпечних діянь з використанням інформаційних та комунікаційних технологій. При цьому одним із завдань державної політики є вдосконалення механізмів обміну інформації під час розслідування цієї категорії злочинів.

В умовах наростання загроз і ризиків кібербезпеки Україна бере активну участь у розробці міжнародно-правових документів у сфері протидії інформаційній злочинності. Так, ЄС та Україна провели третій раунд кібердіалогу у Брюсселі, в Україні вперше перевірили кібербезпеку системи delta за стандартами рівня НАТО тощо [7].

Таким чином, етап розвитку інформаційно-правових відносин у сфері забезпечення інформаційної безпеки в умовах цифрової трансформації пов'язують як із проблемами міжнародного права, так і невирішеністю багатьох інформаційно-правових питань у національній системі права.

Примітно, що питання міжнародного співробітництва щодо забезпечення інформаційної безпеки вирішують низку проблем щодо подолання загроз, викликів та ризиків. Водночас підвищений інтерес держави зумовлює необхідність створення механізмів щодо запобігання інформаційним атакам на критично важливі об'єкти інформаційного середовища, передбачає неприпустимість використання інформаційних технологій як засобу для вчинення протиправних дій, що посягають на національну безпеку держави, впливу та заподіяння економічної, соціальної, політичної шкоди. Внаслідок цього державна політика у сфері забезпечення інформаційної безпеки України визначає завдання з розробки та впровадження ефективних засобів захисту ресурсів від зазіхань та атак в умовах нових викликів, загроз та ризиків. При цьому, як і раніше, постає питання про створення уніфікованих норм у рамках окремих міждержавних об'єднань, які дозволяли б орієнтувати правову політику держави з урахуванням національних особливостей кожної держави-учасниці. Вважаємо, що в цих умовах необхідне формування дієвого правового механізму, який сприяв би якості та стійкості окремих елементів забезпечення інформаційної безпеки з урахуванням сучасних інформаційних атак та загроз в умовах динамічного розвитку нових інформаційних технологій.

У свою чергу серед стратегічних напрямів правового регулювання інформаційної безпеки виділяється не-

обхідність удосконалення національної нормативно-правової бази з урахуванням сучасного стану інформаційної безпеки. У зв'язку з цим звертає увагу посилення оперативності реагування держави на сучасні кіберзагрози.

Нами пропонується у контексті додаткових заходів щодо забезпечення інформаційної безпеки України органам публічного управління заборонити використовувати у роботі іноземні програмні продукти, що мають засоби захисту, та співпрацювати з іноземними виробниками даних комп'ютерних програм. Ці заходи викликані глобальними інформаційними змінами, що відбулися внаслідок посилення геополітичних викликів та нових інформаційних загроз. Реалізація таких загроз тягне за собою щорічне збільшення кількості кібератак на вітчизняні інформаційні об'єкти. У зв'язку з цим правове забезпечення інформаційної безпеки стає одним із найважливіших напрямів у внутрішній політиці держави. Вважаємо, що сформулювати дану пропозицію необхідно в Указі Президента України щодо додаткових заходів забезпечення інформаційної безпеки, які спрямовані на підвищення якості правового забезпечення інформаційної безпеки та недопущення загроз на критично важливі об'єкти інформаційного середовища. При цьому необхідне подальше формування системи безпеки в інформаційній сфері на національному та міждержавному рівнях через ухвалення відповідних нормативних правових актів у сфері інформаційної безпеки. Слід враховувати, що формування, вдосконалення та розвиток заходів щодо забезпечення інформаційної безпеки сприяє встановленню ефективних та дієвих заходів для боротьби з інформаційними атаками та припинення інформаційних війн загалом.

У свою чергу, певні проблеми реалізації державної політики у сфері, що розглядається, посилюються в процесі обробки персональних даних та іншої інформації обмеженого доступу на різних цифрових платформах та програмних ресурсах в інформаційно-комунікаційній мережі Інтернет. У зв'язку з цим право відповідним чином реагує на нові виклики та погрози. Так, постановою Кабінету Міністрів України "Про затвердження Технічного регламенту засобів криптографічного захисту інформації" від 21 жовтня 2020 р. № 991 [8] визначено порядок використання криптоалгоритмів та засобів шифрування відомостей, що стосуються діяльності органів публічного управління. Дані алгоритми та засоби захисту будуть проходити вітчизняну сертифікацію з метою підвищення ефективності використання та збереження інформаційних ресурсів.

Стратегія розвитку інформаційного суспільства України [3] спрямована на формування правової культури у громадян у частині правильного та безпечного використання інформаційних ресурсів, встановлення порядку з отримання, зберігання та використання достовірної інформації, а також підвищення ефективності захисту інформаційної інфраструктури, формування правових механізмів виявлення інформаційних загроз.

Тому пропонується прийняти Концепцію формування та розвитку культури інформаційної безпеки громадян України, яка має бути націленою на формування знань, умінь і навичок з питань інформаційної безпеки з урахуванням стратегічних цілей державної політики у сфері інформаційного права. При цьому розвиток цифрових технологій потребує посилення відповідальності за порушення встановленого порядку їх використання суб'єктами інформаційних відносин, у зв'язку з цим слід зазначити адміністративно-правову та кримінально-правову політику у цій сфері та розвиток інформаційно-правового інституту юридичної відповідальності. Посилення відповідальності за правопорушення в інформаційній сфері обумовлено підвищенням проблем захисту прав людини, включаючи необхідність посилення правового забезпечення безпеки обробки персональних даних.

Однією з основних зовнішніх державних функцій є зовнішньополітична діяльність — співробітництво зі світовим співтовариством, іншими державами у рамках міжнародних, міждержавних регіональних об'єднань та організацій. Ключову роль у такій взаємодії грає просування національних інтересів України, української культури, оскільки втрата культурної ідентичності українського народу детермінує ризики та загрози державного суверенітету. Разом з тим у цій сфері реалізація політики України стикається з певними труднощами, для подолання яких необхідно вживати рішучих заходів щодо вдосконалення національної системи правового забезпечення інформаційної безпеки в Україні.

Дослідження показує, що через зростання ризиків в інформаційній сфері з метою вдосконалення інформаційно-правового забезпечення доцільно грунтуватися на ризик-орієнтованому підході, який в даний час повинен базуватися на системі скоординованих заходів з оцінки існуючих ризиків, їх ранжуванні та подальшому розвитку України в інформаційному просторі.

Розвиток національної системи правового забезпечення інформаційної безпеки в Україні повинен мати системний характер, який на постійній основі виявлятиме прогалини та колізії правового регулювання в галузі інформаційної безпеки. Реалізація державної політики у сфері забезпечення інформаційної безпеки пов'язана з посиленням контролю за інформаційною безпекою, використанням сучасних криптографічних, інженерно-технічних та інших засобів захисту інформації. У сфері контролю та моніторингу відносин при використанні інформаційно-комунікаційних мереж та діяльності засобів масової інформації істотний внесок у забезпечення інформаційної безпеки робить система державних та недержавних інститутів.

Важливе значення в рамках дослідження цієї теми грає питання формування кадрового резерву. Сьогодні відзначається значний дефіцит фахівців у галузі інформаційних технологій та захисту інформації через недостатність спеціалізованих освітніх установ з підготовки кадрів у цій сфері. У зв'язку з цим важливими є прогнози потреб у фахівцях та підвищення якості підготовки відповідних наукових та технічних кадрів. Тому одним із ключових напрямів державної політики є вдосконалення законодавства про освіту та системи заходів підготовки фахівців із захисту інформації на основі моніторингу існуючих потреб. Пріоритетним є вдосконалення освітніх програм і стандартів у цій сфері, у тому числі за допомогою посилення отримуваних компетенцій щодо забезпечення кібербезпеки, комп'ютерної експертизи та розслідування цифрових злочинів. З метою реалізації даних заходів пропонуємо у запропонованій Концепції формування та розвитку культури інформаційної безпеки громадян України визначити

основне завдання — вироблення комплексного підходу до підвищення рівня культури інформаційної безпеки громадян та формування у них навичок протидії загрозам інформаційної безпеки. Цим правовим актом слід передбачити низку положень, спрямованих на формування знань, умінь та навичок з питань інформаційної безпеки на основі регулярного моніторингу рівня грамотності громадян з питань інформаційної безпеки.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Вважаємо, що реалізація цих заходів дозволить сформувати у громадян відповідальне ставлення до правового забезпечення інформаційної безпеки та побудувати довіру до національного інформаційного простору, тим самим знизивши загрози та ризики інформаційної безпеки. Разом з тим положення вищезгаданого правового акта повинні лягти в основу регіональних програм у сфері інформаційної безпеки, які забезпечують стратегічні завдання при реалізації державної правової політики у сфері інформаційної безпеки України.

Важливою складовою державної інформаційної політики є розвиток системи законодавства у сфері забезпечення інформаційної безпеки. Загальними принципами реалізації політики держави з досліджуваної теми є: дотримання міжнародного та українського законодавства щодо забезпечення інформаційної безпеки; розвиток міждержавного співробітництва; рівність всіх суб'єктів інформаційно-правових відносин; вдосконалення цифрових технологій та їх компонентів; формування цифрового довіреного середовища; забезпечення доступу до достовірної інформації, цифрового та технологічного суверенітету України; пріоритет запобіжних (превентивних) заходів захисту інформації, невідворотності покарання за протиправні дії інформаційної сфері.

Таким чином, правове забезпечення інформаційної безпеки є важливою складовою системи забезпечення національної безпеки України, що визначається завданнями протидії: внутрішнім та зовнішнім інформаційним загрозам при використанні цифрових технологій; деструктивним процесам, що розвиваються, спрямованим на інформаційний простір України, порушення прав і свобод громадян, безпеки суспільства і держави, а також завданнями забезпечення соціально-економічного розвитку країни та вітчизняних цифрових технологій, технологічного суверенітету України.

Література:

1. Про Доктрину інформаційної безпеки України: Указ Президента України від 8 липня 2009 року № 514/2009. URL: https://zakon.rada.gov.ua/laws/show/514/2009#Text (Дата звернення: 01.04.2025).

2. 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 року № 47/2017. URL: https://zakon.rada.gov.ua/laws/show/47/2017#Text (Дата звернення: 01.04.2025).

3. Розпорядження Кабінету Міністрів України "Про схвалення Стратегії розвитку інформаційного суспільства в Україні" від 15.05.2013 р. № 386-р. URL: https://zakon.rada.gov.ua/laws/show/386-2013-%D1%80#Text (Дата звернення: 03.04.2025).

4. Комітет Верховної Ради України з питань цифрової трансформації (2025). URL: https://komit.rada.gov.ua/ (Дата звернення: 01.04.2025).

5. НАБУ. Комітет з технологій розвитку та кібербезпеки (2025). URL: https://nabu.ua/ua/komitet-z-tehnologiy-rozvitku-ta-kiberbezpeki.html (Дата звернення: 01.04.2025).

6. Національна комісія з цінних паперів та фондового ринку. Комітет з питань інформаційних технологій та кібербезпеки (2025). URL: https://www.nssmc.gov.ua/komitet-z-pytan-informatsiinykh-tekhnolohii-ta-informatsiinoi-bezpeky/ (Дата звернення: 01.04.2025).

7. РНБО. Огляд подій в сфері кібербезпеки, липень 2024. URL: https://www.rnbo.gov.ua/files/%D0%9D%D0%9A%D0%A6%D0%9A/2024%2007%20Cyber%20digest_UA.pdf (Дата звернення: 01.04.2025).

8. Постанова Кабінету Міністрів України "Про затвердження Технічного регламенту засобів криптографічного захисту інформації" від 21 жовтня 2020 р. № 991. URL: https://zakon.rada.gov.ua/laws/show/991-2020-%D0%BF#Text (Дата звернення: 01.04.2025).

References:

1. President of Ukraine (2009), Decree "About the Information Security Doctrine of Ukraine", available at: https://zakon.rada.gov.ua/laws/show/514/2009#Text (Accessed 01 April 2025).

2. President of Ukraine (2017), Decree "On the decision of the National Security and Defense Council of Ukraine" "About the Information Security Doctrine of Ukraine", available at: https://zakon.rada.gov.ua/laws/show/47/2017#Text (Accessed 01 April 2025).

3. Cabinet of Ministers of Ukraine (2013), Resolution "On the approval of the Strategy for the Development of the Information Society in Ukraine", available at: https://zakon.rada.gov.ua/laws/show/386-2013-%D1%80#Text (Accessed 03 April 2025).

4. Committee of the Verkhovna Rada of Ukraine on Digital Transformation (2025), available at: https://komit.rada.gov.ua/ (Accessed 01 April 2025).

5. NABU. Committee on Development Technologies and Cybersecurity (2025), available at: https://nabu.ua/ua/komitet-z-tehnologiy-rozvitku-ta-kiberbezpeki.html (Accessed 01 April 2025).

6. National Securities and Stock Market Commission. Committee on Information Technology and Cybersecurity (2025), available at: URL: https://www.nssmc.gov.ua/komitet-z-pytan-informatsiinykh-tekhnolohii-ta-informatsiinoi-bezpeky/ (Accessed 01 April 2025).

7. NSDC (2024), "Overview of events in the field of cybersecurity", available at: https://www.rnbo.gov.ua/files/%D0%9D%D0%9A%D0%A6%D0%9A/2024%2007%20Cyber%20digest_UA.pdf (Accessed 01 April 2025).

8. Cabinet of Ministers of Ukraine (2020), Resolution "On approval of the Technical Regulations for cryptographic information protection means", available at: https://zakon.rada.gov.ua/laws/show/991-2020-%D0%BF#Text (Accessed 01 April 2025).

Стаття надійшла до редакції 16.04.2025 р.