УДК 338.46:002+356.35

Деревянко Богдан Володимирович
доктор юридичних наук, професор,
провідний науковий співробітник
відділу господарсько-правових досліджень проблем економічної безпеки
Державна установа «Інститут економіко-правових досліджень імені В.К. Мамутова
Національної академії наук України»
Derevyanko Bogdan
Doctor of Law, Professor,
Leading Researcher of the Department of
economic and legal studies of economic security and safety issues
State Organization "V. Mamutov Institute of Economic and Legal Research
of the National Academy of Sciences of Ukraine"
ORCID: 0000-0001-7408-8285

Ніколенко Людмила Миколаївна
доктор юридичних наук, професор,
провідний науковий співробітник
відділу господарсько-правових досліджень проблем економічної безпеки
Державна установа «Інститут економіко-правових досліджень імені В.К. Мамутова
Національної академії наук України»
Nikolenko Liudmyla
Doctor of Law, Professor,
Leading Researcher of the Department of
economic and legal studies of economic security and safety issues
State Organization "V. Mamutov Institute of Economic and Legal Research
of the National Academy of Sciences of Ukraine"
ORCID: 0000-0002-3437-6968

Дутов Михайло Михайлович
кандидат юридичних наук,
старший науковий співробітник
відділу господарсько-правових досліджень проблем економічної безпеки
Державна установа «Інститут економіко-правових досліджень імені В.К. Мамутова
Національної академії наук України»
Dutov Mykhaylo
Candidate of Law Sciences (PhD), Senior Researcher
State Organization "V. Mamutov Institute of Economic and Legal Research
of the National Academy of Sciences of Ukraine"
ORCID: 0000-0002-4661-2833

DOI: 10.25313/law-2026-3-97-6

ІННОВАЦІЙНЕ ІНВЕСТУВАННЯ У ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УМОВАХ ВОЄННОГО СТАНУ ТА ПОВОЄННОГО ВІДНОВЛЕННЯ

INNOVATIVE INVESTMENT IN CYBERSECURITY PROVISION IN THE CONDITIONS OF MARTIAL LAW AND POST-WAR RECOVERY

Анотація. *Вступ. Сучасна економіка світу і будь-якої більш або менш розвиненої країни не може розвиватися без застосування досягнень науково-технічного прогресу, передусім у площині цифрових техногій. Проте розвиток НТП та поширення цифровізації (диджиталізації), як і будь-які суспільно-політичні чи економічні явища або процеси, різнополярно впливають на суспільство та економіку. Крім переваг з'являються і нові загрози.*

Мета. За мету статті поставлено з урахуванням підходів, що реалізуються у державах-членах ЄС згідно із Новим інноваційним порядком денним Європи та Цифровим порядком денним для Європи, обґрунтувати напрями формування збалансованої моделі сталого інвестування в інноваційно значущу сферу забезпечення кібербезпеки із наданням відсічі агресору в особливий період та убезпеченням кіберпростору у повоєнний час.

Матеріали і методи. Досягнення сформульованої достатньо складної і комплексної мети передбачає необхідність застосування комплексу відомих методів наукового пізнання. Серед них пріоритет має бути наданий застосуванню методу порівняння (компаративному методу) під час дослідження актів європейського та українського законодавства, застосуванню аналітико-синтетичного методу під час дослідження правозастосовної практики. Комплексні історико-правовий та економіко-правовий методи мають пояснити причинно-наслідковий зв'язок між багатьма досліджуваними явищами і процесами. Системно-структурний метод повинен сприяти з'ясуванню обсягів господарської й адміністративної компетенції суб'єктів державного регулювання забезпечення кібербезпеки. Застосування методу аналогії дозволяє екстраполювати фізичні і біологічні явища і процеси на соціальні з метою розкриття природи останніх. Метод сходження від абстрактного до конкретного і від простого до складного, що спирається і випливає із аналітико-синтетичного методу, повинен сприяти дослідженню складових моделі сталого інвестування в інноваційно значущу сферу забезпечення кібербезпеки і формулюванню частин нової концепції. Також використовувалися й інші методи, що будуються на матеріалістичній діалектиці, а також сучасні методи, підґрунтям яких є синергетика і герменевтика, що дозволяє характеризувати спорадичні нелінійні і непрогнозовані явища і процеси, які можуть позитивно чи негативно впливати на забезпечення кібербезпеки в Україні в умовах воєнного стану та повоєнного відновлення.

Результати. Під час дослідження враховано підходи, що реалізуються у державах-членах ЄС згідно із Новим інноваційним порядком денним Європи та Цифровим порядком денним для Європи. Визначено потребу в оновленні концептуальних актів українського законодавства у бік розширення напрямів і способів інвестування інноваційної діяльності, покликаної забезпечити кібербезпеку із наданням відсічі агресору в особливий період та убезпеченням кіберпростору у повоєнний час. Вказано на пріоритетність доповнення чинних актів, аніж розробку і прийняття нових. Запропоновано доповнити Розділ III «Формування та виконання Національної програми інформатизації» чинного Закону України «Про національну програму інформатизації». Імплементація, навіть у переробленій формі, загальних положень про поширення диджиталізації та забезпечення кібербезпеки двох названих «порядків» для Європи сприятиме об'єднанню українського та європейського кіберпросторів і відбуватиметься у загальній канві імплементації Acquis communautaire до українського законодавства. Запропоновано імплементувати положення обох названих «порядків» для Європи про інноваційне інвестування та фінансування діяльності із забезпечення кібербезпеки до Розділу IV «Фінансове забезпечення Національної програми інформатизації» Закону України «Про національну програму інформатизації». Також підтримано прийняття проєкту закону України «Про Кіберсили Збройних Сил України», завдяки чому буде підтверджено першість України в утворенні нових сил у складі ЗСУ, а також підвищено спеціалізацію у протидії ворожим кібератакам в умовах дії правового режиму воєнного стану та ефективній роботі в часи повоєнного відновлення.

Перспективи. Подальші дослідження мають спрямовуватися на розробку змін і доповнень до законодавства України про розвиток диджиталізації і забезпечення кібербезпеки, особливо до Закону України «Про національну програму інформатизації».

Ключові слова: *інвестиційна діяльність, інноваційна діяльність, кібербезпека, воєнний стан, повоєнне відновлення, законодавство, державне регулювання, Новий інноваційний порядок денний Європи, Цифровий порядок денний для Європи, диджиталізація, стартап, кіберпростір, кіберінцидент, Збройні Сили України.*

Summary. *Introduction. The modern economy of the world and any more or less developed country cannot develop without the application of scientific and technological progress, primarily in the field of digital technologies. However, the development of scientific and technological progress and the spread of digitalization, like any socio-political or economic phenomena or processes, have a multipolar impact on society and the economy. In addition to the advantages, new threats also appear.*

Purpose. The purpose of the article is to substantiate the directions of forming a balanced model of sustainable investment in the innovatively significant sphere of cybersecurity, taking into account the approaches implemented in the EU Member States in accordance with the New European Innovation Agenda for Europe and the Digital Agenda for Europe, with the aim of repelling the aggressor in a special period and securing cyberspace in the post-war period.

Materials and methods. Achieving the formulated rather complex and comprehensive goal requires the use of a set of well-known methods of scientific knowledge. Among them, priority should be given to the use of the comparison method (comparative method) when studying acts of European and Ukrainian legislation, and the use of the analytical-synthetic method when studying law enforcement practice. Complex historical-legal and economic-legal methods should explain the cause-and-effect relationship between many studied phenomena and processes. The system-structural method should help clarify the scope of economic and administrative competence of subjects of state regulation of cybersecurity. The use of the analogy method allows

extrapolating physical and biological phenomena and processes to social ones in order to reveal the nature of the latter. The method of ascending from the abstract to the concrete and from the simple to the complex, which is based on and follows from the analytical-synthetic method, should contribute to the study of the components of the model of sustainable investment in the innovatively significant sphere of ensuring cybersecurity and the formulation of parts of the new concept. Other methods based on materialist dialectics were also used, as well as modern methods based on synergetics and hermeneutics, which allow characterizing sporadic nonlinear and unpredictable phenomena and processes that can positively or negatively affect the provision of cybersecurity in Ukraine under martial law and post-war recovery.

Results. The study took into account the approaches implemented in the EU Member States in accordance with the New European Innovation Agenda for Europe and the Digital Agenda for Europe. The need to update the conceptual acts of Ukrainian legislation towards expanding the areas and methods of investing in innovative activities designed to ensure cybersecurity with repelling the aggressor in a special period and securing cyberspace in the post-war period was identified. The priority of supplementing existing acts rather than developing and adopting new ones was indicated. It is proposed to supplement Section III "Formation and Implementation of the National Informatization Program" of the current Law of Ukraine "On the National Informatization Program". The implementation, even in a revised form, of the general provisions on the spread of digitalization and ensuring cybersecurity of the two named "orders" for Europe will contribute to the unification of the Ukrainian and European cyberspaces and will take place in the general framework of the implementation of the Acquis communautaire into Ukrainian legislation. It is proposed to implement the provisions of both named "orders" for Europe on innovative investment and financing of cybersecurity activities into Section IV "Financial support of the National Informatization Program" of the Law of Ukraine "On the National Informatization Program". The adoption of the draft law of Ukraine "On Cyber Forces of the Armed Forces of Ukraine" was also supported, which will confirm Ukraine's primacy in the formation of new forces within the Armed Forces of Ukraine, as well as increase specialization in countering hostile cyberattacks under the legal regime of martial law and effective work during post-war reconstruction.

Prospects. Further research should be aimed at developing amendments and additions to the legislation of Ukraine on the development of digitalization and ensuring cybersecurity, especially to the Law of Ukraine "On the National Informatization Program".

Key words: *investment activity, innovation activity, cybersecurity, martial law, post-war recovery, legislation, state regulation, the New European Innovation Agenda for Europe, the Digital Agenda for Europe, digitalization, startup, cyberspace, cyber incident, Armed Forces of Ukraine.*

Постановка проблеми. Сучасна економіка світу і будь-якої більш або менш розвиненої країни не може розвиватися без застосування досягнень науково-технічного прогресу (НТП), передусім у площині цифрових технологій. Проте розвиток НТП та поширення цифровізації (диджиталізації), як і будь-які суспільно-політичні чи економічні явища або процеси, різнополярно впливають на суспільство та економіку. Крім переваг з'являються і нові загрози.

Перевагами диджиталізації (цифровізації) економіки і життя суспільства є значне спрощення життя людини і діяльності суб'єктів господарювання через усунення значної кількості бюрократичних процедур. Завдяки застосуванню сучасних цифрових технологій спрощується державне регулювання різноманітних явищ і процесів в економіці і суспільстві. Представники бізнесу можуть дистанційно зареєструвати новий суб'єкт господарювання, отримати ліцензію та/або дозвіл на здійснення певного виду господарської діяльності, сплатити податки, подати заяву чи скаргу, висунути претензію і здійснити ще тисячі операцій. Можна згадати як ще 10–20 років тому для цього треба було готувати і роздруковувати значну кількість документів, вистоювати черги перед їх поданням до органів виконавчої та/або судової влади, інколи навіть їхати до іншого міста.

Та окрім переваг тотальна диджиталізація (цифровізація) спричинила активізацію зловмисників і злочинців, які створили тисячі загроз інтересам людини, суб'єктів бізнесу, держави та суспільства. Внутрішні або міжнародні шахраї, «рейдери», кібертерористи різноманітними способами намагаються викрасти персональні дані інших людей, компаній, фінансових інституцій, дізнатися номери карток і рахунків, вивідати паролі входу до електронних фінансових інструментів, гаманців криптовалюти, викачати промислові і військові таємниці тощо. Майже кожен громадянин України щодня отримує так звані фішингові повідомлення у скриньку своєї електронної пошти та/або через акаунт телефону та встановлені у ньому додатки. Протидія цим явищам, а також подальший інноваційний розвиток цифрових технологій потребують значних інвестицій у сферу диджиталізації (цифровізації). При цьому чим більш розвиненою є ця сфера у державі, тим більших інвестицій для подальшого розвитку вона потребує. І пропорційно цим інвестиціям потрібні інвестиції у забезпечення безпеки у кіберпросторі держави.

Аналіз останніх досліджень і публікацій. Різноманітні правові, управлінські, економічні аспекти розвитку інформатизації, державного регулювання процесів диджиталізації (цифровізації) суспільства і держави, зокрема у різних галузях і сферах економіки і суспільства, а також питання забезпечення кібербезпеки уже були предметом численних досліджень українських молодих і досвідчених вчених. Так, група дослідників зосереджує увагу на механізмах процесу диджиталізації

місцевих органів влади і конкретизовує суб'єктний склад правовідносин, що виникають під час формування та виконання Національної програми інформатизації [1]. Н. Васиньова вказала на окремі досягнення у розвитку диджиталізації в країні, запровадженні цифрових трендів у діяльності органів державної влади та місцевого самоврядування, проте наголосила на потребі вирішення певних завдань на шляху до європейської інтеграції [2, с. 51]. Окремі дослідження присвячено диджиталізації судового процесу. Зокрема О. Шминдрук вважає, що диджиталізація цивільного судочинства відкриває нові можливості для забезпечення справедливого судового процесу, проте водночас створює виклики, особливо в контексті доступу до суду через електронні системи [3]. В. Рудюк доводить, що цифровізація серйозно змінила ландшафт традиційних сфер суспільних відносин і стала причиною істотних змін у сфері правозастосування, зокрема функціонування «електронного суду» [4, с. 84]. О. Барабаш приділяє увагу диджиталізації вітчизняної освіти, виділяючи як позитивні аспекти варіативність використання соціальних мереж в освітніх цілях, у навчанні, у викладацькій діяльності, а як аспекти, що вимагають особливої уваги, — низький рівень грамотності в ІТ-галузі, інертність переходу від традиційної форми трудової діяльності до диджиталізованої, що вимагає певного часу на перегляд її нормативного регулювання [5]. О. Вінник доводить, що цифровізацією є складне явище з притаманними йому незаперечними достоїнствами (як-от, можливість вирішувати надскладні завдання) і ризиками (загроза втрати людиною контролю над штучними інтелектом, зловживання цифровими можливостями, посилення вуглецевого сліду через надмірне споживання у процесі цифровізації електроенергії тощо) [6].

Протягом кількох попередніх років збільшилася кількість досліджень, покликаних сприяти захисту кіберпростору від різноманітних кіберінцидентів. Так, Л. Дешко та К. Бондарєва підтверджують висловлено нами на початку статті: «збільшення оцифрування послуг та дуже активне використання Інтернету призвело до еволюції кіберпростору, що також викликало значні проблеми для безпеки урядів у всьому світі щодо злочинів, вчинених за допомогою комп'ютерних систем» [7, с. 380]; В. Поліщук та Л. Панасевич вказують на перспективність спільної боротьби проти кіберзагроз разом з іншими державами та міжнародними безпековими [8, с. 506]. Проте питання залучення внутрішніх та іноземних інвестицій для розвитку інноваційних цифрових технологій, зокрема і безпекових, покликаних захистити кіберпростір держави, піднімають дуже нечасто. Цим викликана потреба у проведенні дослідження.

Метою статті є: з урахуванням підходів, що реалізуються у державах-членах ЄС згідно із Новим інноваційним порядком денним Європи та Цифровим порядком денним для Європи, обґрунтувати напрями формування збалансованої моделі сталого інвестування в інноваційно значущу сферу забезпечення кібербезпеки із наданням відсічі агресору в особливий період та убезпеченням кіберпростору у повоєнний час.

Методи наукового дослідження. Досягнення щойно сформульованої достатньо складної і комплексної мети передбачає необхідність застосування комплексу відомих методів наукового пізнання. Серед них пріоритет має бути наданий застосуванню методу порівняння (компаративному методу) під час дослідження актів європейського та українського законодавства, застосуванню аналітико-синтетичного методу під час дослідження правозастосовної практики. Комплексні історико-правовий та економіко-правовий методи мають пояснити причинно-наслідковий зв'язок між багатьма досліджуваними явищами і процесами. Системно-структурний метод повинен сприяти з'ясуванню обсягів господарської й адміністративної компетенції суб'єктів із забезпечення кібербезпеки. Застосування методу аналогії дозволяє екстраполювати фізичні і біологічні явища і процеси на соціальні з метою розкриття природи останніх. Метод сходження від абстрактного до конкретного і від простого до складного, що спирається і випливає із аналітико-синтетичного методу, повинен сприяти дослідженню складових моделі сталого інвестування в інноваційно значущу сферу забезпечення кібербезпеки і формулюванню частин нової концепції. Також використовувалися й інші методи, що будуються на матеріалістичній діалектиці, а також сучасні методи, підґрунтям яких є синергетика і герменевтика, що дозволяє характеризувати спорадичні нелінійні і непрогнозовані явища і процеси, які можуть позитивно чи негативно впливати на забезпечення кібербезпеки в Україні в умовах воєнного стану та повоєнного відновлення.

Виклад основного матеріалу дослідження. В Україні законодавство із забезпечення захисту та розвитку інформаційних технологій формувалося чи не з початку відновлення незалежності у 1990-х роках. Так, 5 липня 1994 року було прийнято Закон України «Про захист інформації в інформаційно-комунікаційних системах» [9]. На початку XXI століття на міжнародному рівні, під егідою Ради Європи 23 листопада 2001 року було підписано Конвенцію про кіберзлочинність, яку Україною було ратифіковано із застереженнями і заявами через прийняття відповідного Закону від 7 вересня 2005 року [10]. Під час ратифікації Конвенції в Україні розуміли її сенс і значення, адже вже у 2000-х роках Україна входила у світову десятку держав за поширенням Інтернету, а на початку 2010-х років — входила у світову десятку держав-лідерів диджиталізації (цифровізації), тисячі громадян України мали гаманці криптовалюти біткойн, а пізніше й інших видів криптовалюти, багато адміністративних послуг надавалося в електронній

формі. Тобто не має сенсу доводити прогресивність України у технологічному розвитку. Важливішим є забезпечення захисту національних інтересів держави та громадян. Уже 15–20 років тому були загрози для власників гаманців криптовалюти й інших віртуальних активів, на чому нами раніше наголошувалося [11]. Серед іншого нами вказувалося на ризик втрати ID-гаманця та/або паролю (під втратою малося на увазі також і заволодіння іншими особами), і рекомендувалося не зберігати ID гаманця і пароль до нього у пам'яті підключеного до мережі Інтернет комп'ютеру тощо [11, с. 36].

Державне регулювання пішло у напрямку прийняття 23 лютого 2006 року відповідного Закону України та утворення Державної служби спеціального зв'язку та захисту інформації України [12], а потім із значною перервою 27 січня 2016 року Указом Президента України було уведено в дію рішення РНБО України «Про Стратегію кібербезпеки України» [13], яке сьогодні вже не є чинним, а замість нього діє рішення РНБО України від 14 травня 2021 року «Про Стратегію кібербезпеки України» [14]. Тобто законодавство про кібербезпеку у межах державного регулювання досліджуваних процесів постійно розвивалося і змінювалося. І так триває донині.

5 жовтня 2017 року було прийнято два закони України: «Про електронну ідентифікацію та електронні довірчі послуги» [15] та «Про основні засади забезпечення кібербезпеки України» [16]. Прийняття останнього стало відповіддю на збільшення загроз кіберпростору України після початку російської агресії 2014 року. За відсутності загроз прийняття такого Закону можна було б визнати позитивом у структурі безпекового законодавства і аналогом високої оцінки інноваційного розвитку держави, яка «доросла» до його прийняття. Але в ситуації боротьби за власну державу, ідентичність і навіть фізичне виживання, прийняття цього Закону є об'єктивною необхідністю.

16 грудня 2020 року було прийнято Закон України «Про електронні комунікації» [17], а 1 грудня 2022 року — Закон України «Про національну програму інформатизації» [18]. І на сьогодні процес формування законодавства у напрямку намагання підвищити рівень кібербезпеки триває. Та не менш важливою є потреба в поширенні інвестування інноваційних розробок, покликаних це реалізувати.

Пунктом 5 частини першої статті 1 «Визначення термінів» Закону України «Про основні засади забезпечення кібербезпеки України» надано поняття кібербезпеки як «5) кібербезпека — захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі» [16], а також надано кілька десятків визначень інших вузькоспеціалізованих релевантних понять, зокрема інцидент кібербезпеки (кіберінцидент), кібератака, кіберзахист, кіберзлочин (комп'ютерний злочин), кіберрозвідка, кібертероризм, кібершпигунство та ін. [16]. Також названим Законом визначено принципи його застосування, правові основи, об'єкти кібербезпеки та кіберзахисту, суб'єкти забезпечення кібербезпеки, принципи забезпечення кібербезпеки та ін. Важливе значення має характеристика національної системи кібербезпеки, надана у статті 8 [16]. Так, у частині другій цієї статті названо основні суб'єкти національної системи кібербезпеки та визначено їх компетенцію з огляду на завдання досліджуваного Закону України. Серед цих органів є: Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, СБУ, Міністерство оборони України та Генеральний штаб ЗСУ, розвідувальні органи України, НБУ, МЗС України [16].

Після початку повномасштабного вторгнення російської федерації в Україну та проголошення правового режиму воєнного стану названі у статті 1 «Визначення термінів» Закону України «Про основні засади забезпечення кібербезпеки України» негативні впливи у кіберпросторі (кіберінциденти, кібератаки, кіберзлочини. кібертероризм, кібершпигунство та ін.) значно поширилися. Можна навести нещодавній злом кіберзлочинцями (орієнтовно з російської федерації) сайту онлайн-магазину нумізматичної продукції НБУ у січні 2026 року та викрадення особистої інформації (П.І.Б., дата народження, адреса електронної пошти, номер телефону, адреса поштового відділення, окремі паролі) більш ніж 250 тисяч клієнтів, абсолютна більшість з яких є громадянами України. На підтвердження наведеного в аналітичному звіті про стан виконання Плану реалізації Стратегії кібербезпеки України за 2025 рік Державної служби спеціального зв'язку та захисту інформації України зазначено: «Упродовж 2025 року Оперативним центром реагування на кіберінциденти опрацьовано 17,3 тисяч подій безпеки та зафіксовано 730 кіберінцидентів різного рівня складності. Найбільшу частку серед них становили кіберінциденти, пов'язані з використанням шкідливого програмного забезпечення. Аналіз виявлених атак свідчить, що їх ключовою метою було встановлення прихованого контролю над інформаційними системами з подальшим використанням отриманого доступу для кіберрозвідки або незаконного заволодіння фінансовими ресурсами» [19]. Виходячи з того, що переважна більшість населення та суб'єктів господарювання не повідомляють про кіберінциденти, або не вся статистика доходить до Державної служби спеціального зв'язку та захисту інформації України, залишаючись на рівні Національної поліції чи прокуратури, 730 зафіксованих кіберінцидентів різного рівня складності можна множити більш, ніж на сто. Можливо у відповідь на загрози кібербезпеці держави постановою КМУ від 22 жовтня

2025 року було затверджено Порядок формування та ведення відкритого переліку забороненого до використання програмного забезпечення та комунікаційного (мережевого) обладнання [20]. Зрозуміло, що затвердження названого Порядку є хоча і важливою в умовах дії правового режиму воєнного стану, проте поточною подією. На нашу думку важливим інноваційним рішенням державного регулювання процесів боротьби із кіберзлочинами може стати утворення перших у світі Кіберсил у складі ЗСУ. Допоки таких сил немає в арміях держав світу. Так, 6 лютого 2024 року уперше в історії людства Сили безпілотних систем стали окремими силами у складі збройних сил держави. Сталося це в Україні через створення у структурі ЗСУ Сил безпілотних систем як окремого роду сил Указом Президента [21]. А 23 грудня 2024 року до Верховної Ради України було подано проєкт закону України «Про Кіберсили Збройних Сил України» [22], який станом на початок березня 2026 року очікує на друге читання. Проєкт складається лише із шести статей, якими буде закладено основу діяльності нових сил у складі ЗСУ. У випадку прийняття відповідного закону, останнім визначатиметься правовий статус, основні завдання, компетенція, структура, фінансування та матеріально-технічне забезпечення Кіберсил ЗСУ та інші аспекти діяльності нової складової ЗСУ [22].

У зв'язку із потребою забезпечення ефективної роботи цивільних і військових органів (сил), покликаних захищати український кіберпростір, особливо в умовах дії воєнного стану, а також із потребою обґрунтування напрямів формування збалансованої моделі сталого інвестування в інноваційно значущу сферу забезпечення кібербезпеки із наданням відсічі агресору в особливий період та убезпеченням кіберпростору у повоєнний час, важливе значення мають норми частин першої і другої статті 5 названого законопроєкту. У цих нормах фінансування діяльності Кіберсил ЗСУ пропонується покласти на Державний бюджет України на відповідний рік відповідно до статті 15 Закону України «Про Збройні Сили України» [23]. Але при цьому пропонується дозволити додаткове фінансування за рахунок субвенцій та благодійних пожертв фізичних та юридичних осіб у порядку, визначеному КМУ (частина перша статті 5 проєкту) [22]. Також пропонується дозволити фінансування окремих заходів діяльності Кіберсил ЗСУ за рахунок благодійних пожертв відповідно до Закону України «Про благодійну діяльність та благодійні організації» [24] або в рамках міжнародної технічної допомоги, залучення технічної і фінансової допомоги в рамках імплементаційних домовленостей, інших технічних угод про співробітництво та участі у наукових і практичних проєктах (програмах) кібероборони у порядку, визначеному КМУ (частина друга статті 5 проєкту) [22]. Враховуючи унікальний характер діяльності наявних і потенційних органів, які забезпечують (забезпечуватимуть) кібербезпеку в Україні, фінансування їх діяльності фізичними та юридичними особами, а також міжнародними організаціями є інвестиціями в інноваційну діяльність. Продукція, яку виготовляють суб'єкти із захисту кібербезпеки, у вигляді різноманітних антивірусних програм, алгоритмів дій, рішень технологічного характеру, способів шифрування та захисту інформації тощо, є інноваціями і відповідає визначенню, наданому у частині першій статті 1 «Визначення термінів» Закону України «Про інноваційну діяльність»: «інновації — новостворені (застосовані) і (або) вдосконалені конкурентоздатні технології, продукція або послуги, а також організаційно-технічні рішення виробничого, адміністративного, комерційного або іншого характеру, що істотно поліпшують структуру та якість виробництва і (або) соціальної сфери» [25].

Слід вказати на те, що акти чинного законодавства, прийняті у межах визначеної парадигми державного регулювання процесів кіберзахисту і покликані сприяти підвищенню рівня кібербезпеки, не забороняють здійснення інноваційного інвестування у діяльність відповідних суб'єктів, проте і не стимулюють його. Так, пунктом 54 статті 14 «Обов'язки Державної служби спеціального зв'язку та захисту інформації України» передбачено забезпечення в межах своїх повноважень формування та реалізації інноваційної та інвестиційної політики [12].

Серед стратегічних завдань Стратегії кібербезпеки України 2021 року серед іншого вказано, що Україна сформує систему дієвої кібероборони шляхом удосконалення аналітичного і криміналістичного забезпечення контррозвідувального захисту кібербезпеки держави за рахунок впровадження інноваційних методик обробки та оцінки цифрових даних, формування електронних доказів, а також утворення центрів, що будуть здійснювати узагальнення та обмін досвідом у сфері кібербезпеки, підтримку інновацій та вітчизняних розробок у цій сфері. Одним із вимірів успіху у досліджуваній сфері визначено розвиток кадрового потенціалу та інноваційного ринку кібербезпеки, що сприятиме створенню національних розробок на рівні кращих світових практик для забезпечення можливості протидіяти майбутнім кіберзагрозам [14]. Статтею 15–4 «Ініціативи щодо тестування інноваційних схем, засобів і технологій електронної ідентифікації» Закону України «Про електронну ідентифікацію та електронні довірчі послуги» передбачено можливість КМУ приймати рішення про реалізацію ініціатив щодо тестування інноваційних схем, засобів і технологій електронної ідентифікації, а також визначено порядок і строки [15]. Проте обов'язкового припису щодо цього названа стаття не містить.

Стаття 13 Закону України «Про основні засади забезпечення кібербезпеки України» проголошує, що «джерелами фінансування робіт і заходів із забезпечення кібербезпеки та кіберзахисту є кошти дер-

жавного і місцевих бюджетів, власні кошти суб'єктів господарювання, кредити банків, кошти міжнародної технічної допомоги та інші джерела, не заборонені законодавством» [16]. Законом України «Про електронні комунікації» передбачено сприяння інвестуванню та реалізації інновацій, забезпечення розвитку науково-технічного та інноваційного потенціалу, врахування технологічних інновацій, сприяння конкуренції та інноваціям та ін. [17], проте засоби і механізми цього не наведено, а отже, віднесено до актів підзаконного законодавства або правозастосовної практики. Законом України «Про національну програму інформатизації» допускається інноваційне інвестування та фінансування з різних джерел заходів програми інформатизації. Серед іншого заслуговують на увагу положення статті 92 «Заходи із сприяння спільному інвестуванню елементів мереж надвисокої пропускної здатності» [18].

Отже, видається що організувати безпечне функціонування кіберпростору в Україні можливо за посередництва інноваційного інвестування у програми кібербезпеки, розроблені цивільними і військовими державними органами із забезпечення кібербезпеки та кіберзахисту, а також недержавними суб'єктами господарювання, зокрема стартапами у сфері диджиталізованої економіки. Найкращі варіанти реалізації можна імлементувати із європейських програм — Нового інноваційного порядку денного Європи (The New European Innovation Agenda), а також Цифрового порядку денного для Європи (Digital Agenda for Europe). Загальновідомо, що перший спирається на п'ять «китів», зокрема: 1) інвестування інституційними інвесторами в об'єднання із багатьох технологічних стартапів (у нашому випадку мається на увазі інвестування у приватні ІТ-компанії і навіть окремих фахівців у сфері ІТ-технологій у зв'язці із державними органами, покликаними своїми розробками забезпечувати кібербезпеку та кіберзахист); 2) підтримку експериментальних досліджень через новітні підходи до цього — використання «регуляторних пісочниць», «випробувальних стендів», «живих лабораторій» тощо (у нашому випадку це є цілком можливим у межах України, навіть в умовах дії правового режиму воєнного стану); 3) поглиблену співпрацю інноваторів у межах ЄС із державним інвестуванням в інновації у розмірі, не меншому 10 млрд. євро на міждержавні і міжрегіональні програми, потрібні ЄС (у нашому випадку українські воєнні інновації уже сьогодні затребувані у світі, що підтвердили військові дії на Близькому Сході; українські цивільні і військові інновації із захисту кіберпростору уже завтра будуть не менш затребуваними у ЄС та світі); 4) підтримку місцевих (європейських) талантів у межах стартапів, пошук талантів за межами ЄС, зокрема через економічні способи стимулювання (у нашому випадку інвестиційні інновації в українські компанії та державні органи, що розробляють інноваційні програми захисту кібербезпеки, можуть надходити із ЄС уже сьогодні); 5) удосконалення механізмів співпраці і розробки єдиної державної політики розвитку і підтримки інновацій, зокрема і через координацію на рівні усього ЄС (у нашому випадку український кіберпростір, а також засоби його захисту, розроблені і запроваджені найкращими фахівцями, зокрема й українськими, мають бути інтегровані із відповідним кіберпростором ЄС із спільним застосуванням засобів його захисту).

Останній «кит» тісно переплітається із Цифровим порядком денним для Європи (Digital agenda for Europe). Цей Порядок спирається на сім «китів», які визначатимуть важливі для нашого дослідження напрями розвитку, зокрема створення єдиного цифрового простору у межах Європи, підвищення швидкості і якості інтернету, підвищення енергоефективності програм та обладнання, спільну боротьбу із кіберзагрозами, підвищення ступеня захисту персональних даних, скооперване інвестування у розвиток інноваційних цифрових технологій, підвищення загальної комп'ютерної грамотності населення та ін.

Отже, наведене вказує на потребу в оновленні концептуальних актів українського законодавства у бік розширення напрямів і способів інвестування інноваційної діяльності, покликаної забезпечити кібербезпеку із наданням відсічі агресору в особливий період та убезпеченням кіберпростору у повоєнний час. Принципи оптимальності і раціональності законотворчої діяльності вказують на недоцільність неконтрольованого множення актів законодавства і на пріоритетність доповнення чинних актів, аніж розробку і прийняття нових. Тому видається доцільним продовжити роботу з досліджуваної проблематики, щоб розробити положення і доповнити ними Розділ ІІІ «Формування та виконання Національної програми інформатизації» чинного Закону України «Про національну програму інформатизації». Імплементація, навіть у переробленій формі, загальних положень про поширення диджиталізації та забезпечення кібербезпеки двох названих «порядків» для Європи сприятиме об'єднанню українського та європейського кіберпросторів і відбуватиметься у загальній канві імплементації Acquis communautaire до українського законодавства. Складові збалансованої моделі сталого інвестування в інноваційно значущу сферу забезпечення кібербезпеки із наданням відсічі агресору в особливий період та убезпеченням кіберпростору у повоєнний час мають бути взяті із обох названих «порядків» та знайти місце у розвитку Розділу IV «Фінансове забезпечення Національної програми інформатизації» чинного Закону України «Про національну програму інформатизації» [18], який складається лише із однієї статті 16 із назвою, однотипною із назвою Розділу. Видається раціональним додання кількох норм, в яких визначатимуться основи фінансового забезпечення кібербезпеки в Україні, інвестування в інноваційні дослідження державних органів,

суб'єктів господарювання та окремих розробників програм із протидії кіберінцидентам. Також виглядає доречною підтримка прийняття проєкту закону України «Про Кіберсили Збройних Сил України» [22], завдяки чому буде підтверджено першість України в утворенні нових сил у складі ЗСУ, а також підвищено спеціалізацію у протидії ворожим кібератакам в умовах дії правового режиму воєнного стану та ефективній роботі в часи повоєнного відновлення.

Висновки. Проведене дослідження дозволило комплексно проаналізувати правові та інституційні передумови інноваційного інвестування у сферу забезпечення кібербезпеки держави в умовах воєнного стану та повоєнного відновлення. З урахуванням підходів, що реалізуються у державах-членах ЄС відповідно до Нового інноваційного порядку денного Європи (The New European Innovation Agenda) та Цифрового порядку денного для Європи (Digital Agenda for Europe), обґрунтовано необхідність формування комплексної моделі інноваційного інвестування у сферу кібербезпеки як складової державної політики розвитку цифрової економіки та забезпечення національної безпеки.

У результаті дослідження встановлено, що сучасна система забезпечення кібербезпеки держави потребує інтеграції безпекової, інноваційної та інвестиційної політики. У цьому контексті інвестиції у розвиток цифрових технологій та засобів кіберзахисту мають розглядатися не лише як інструмент протидії кіберзагрозам, але і як важливий чинник технологічного розвитку, модернізації економіки та підвищення міжнародної конкурентоспроможності держави.

Обґрунтовано доцільність формування моделі сталого інвестування у сферу забезпечення кібербезпеки, яка передбачає поєднання державного фінансування, залучення приватних інвестицій, міжнародної технічної допомоги, інноваційних стартапів та оборонно-технологічних розробок у межах єдиної системи державного регулювання розвитку цифрової економіки. Така модель має забезпечувати підтримку наукових досліджень, стимулювання інноваційної діяльності у сфері кіберзахисту та формування національного ринку кібербезпекових технологій.

Доведено, що ефективне функціонування національної системи кібербезпеки значною мірою залежить від розвитку інноваційної екосистеми, до якої мають бути залучені наукові установи, IT-компанії, стартапи, підприємства оборонно-промислового комплексу та міжнародні партнери України. Формування такого інноваційного середовища сприятиме створенню конкурентоспроможних технологічних рішень у сфері кіберзахисту та зміцненню цифрового суверенітету держави.

Запропоновано напрями вдосконалення законодавства України у сфері інноваційного інвестування кібербезпеки, зокрема шляхом доповнення положень Закону України «Про національну програму інформатизації» нормами, що передбачають стимулювання інвестицій у розвиток технологій кіберзахисту, підтримку державних і приватних розробників інноваційних програмних рішень у сфері кібербезпеки, а також розвиток механізмів публічно-приватного партнерства у сфері цифрової безпеки.

Окрему увагу приділено інституційним аспектам розвитку системи кібербезпеки держави. Підтримано доцільність створення Кіберсил Збройних Сил України як спеціалізованого елементу системи оборони, що поєднуватиме військові, технологічні та інноваційні ресурси держави для протидії сучасним кіберзагрозам та забезпечуватиму ефективне функціонування кіберпростору держави в умовах воєнного стану та повоєнного відновлення.

З урахуванням євроінтеграційного курсу України доведено доцільність подальшої імплементації положень стратегічних документів ЄС у сфері розвитку інноваційної економіки та цифрових технологій до національного законодавства України. Реалізація таких підходів сприятиме інтеграції українського кіберпростору до європейського цифрового середовища, розвитку спільних інноваційних програм та посиленню міжнародної співпраці у сфері забезпечення кібербезпеки.

Отже, забезпечення ефективного функціонування кіберпростору держави в умовах сучасних глобальних викликів потребує формування комплексної системи інноваційного інвестування у сферу кібербезпеки, що поєднуватиме правові, економічні, технологічні та інституційні механізми розвитку цифрової економіки та захисту національних інтересів держави.

ДОДАТКОВА ІНФОРМАЦІЯ

ВНЕСОК АВТОРІВ: Усі автори зробили внесок порівну.

ФІНАНСУВАННЯ: Статтю підготовлено у межах теми НДР «Комплексне наукове дослідження інвестиційно-інноваційної детермінанти сталого економічного розвитку України» (номер державної реєстрації 0125U003540) на підставі договору № БФ/С22–2025 про виконання наукового дослідження, укладеного з МОН України, за рахунок бюджетних коштів, спрямованих на забезпечення проведення державними науковими установами наукових досліджень і науково-технічних (експериментальних) розробок за результатами державної атестації.

ЗАЯВА ПРО ДОСТУПНІСТЬ ДАНИХ: Не застосовується.

КОНФЛІКТ ІНТЕРЕСІВ: Автори заявляють про відсутність конфлікту інтересів.

Література

1. Левкун Т. В., Гамалюк Б. М., Лис А. Б. Диджиталізація в територіальних громадах: громада в смартфоні. *Успіхи й досягнення в науці.* 2024. № 8(8). С. 420–432.

2. Васиньова Н.С Диджиталізація публічного управління в Україні: тренд чи вимога часу? *Вчені записки ТНУ імені В. І. Вернадського. Серія: Публічне управління та адміністрування.* 2022. Том 33 (72). № 6. С. 48–52. DOI: https://doi.org/10.32782/TNU-2663-6468/2022.6/08

3. Шминдрук О. Ф., Балагур Ю. С. Забезпечення права на доступ до правосуддя в умовах диджиталізації цивільного судочинства. *Часопис Національного університету «Острозька академія». Серія «Право».* 2025. № 2. С. 43–47. DOI: https://doi.org/10.32782/2223-9995.2024.26.10

4. Рудюк В. С. Диджиталізація в сучасному судочинстві. *Філософські та методологічні проблеми права.* 2020. № 2 (20). С. 82–85.

5. Барабаш О. Диджиталізація вітчизняної освіти: проблеми і перспективи розвитку в умовах глобалізації. *Право України.* 2022. № 12. С. 109–121. DOI: https://doi.org/10.33498/louu-2022-12-109

6. Вінник О. М., Попович Т. Г., Деревянко Б. В. Регулювання відносин цифрової економіки: окремі аспекти. *Вісник Національної академії правових наук України*. 2022. Том 29. № 3. С. 181–204. URL: https://repository.ndippp.gov.ua/handle/765432198/527 (дата звернення: 08.01.2026).

7. Дешко Л. М., Бондарєва К. Д. Кібербезпека в Україні: національна стратегія та міжнародне співробітництво. *Порівняльно-аналітичне право.* 2018. № 2. С. 379–382.

8. Поліщук В. П., Панасевич Л. А. Міжнародне право і кібербезпека: визначення правового статусу кібератак та кібервійськових операцій. *Юридичний науковий електронний журнал.* 2024. № 2. С. 503–506.

9. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 5 липня 1994 року № 80/94-ВР. *Відомості Верховної Ради України.* 1994. № 31. Ст. 286.

10. Про ратифікацію Конвенції про кіберзлочинність: Закон України від 7 вересня 2005 року № 2824-IV. *Відомості Верховної Ради України.* 2006. № 5–6. Ст. 71.

11. Деревянко Б. В. Ризики здійснення операцій з криптовалютою (біткойнами) громадян і суб'єктів господарювання України. *Форум права.* 2017. № 3. С. 33–39. URL: https://repository.ndippp.gov.ua/handle/765432198/269 (дата звернення: 08.01.2026).

12. Про Державну службу спеціального зв'язку та захисту інформації України : Закон України від 23 лютого 2006 року № 3475-IV. *Відомості Верховної Ради України.* 2006. № 30. Ст. 258.

13. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : Указ Президента України від 15 березня 2016 року № 96/2016 (втратив чинність). *Офіційний портал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/96/2016#n11 (дата звернення: 08.01.2026).

14. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26 серпня 2021 року № 447/2021. *Офіційний портал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/447/2021#n7 (дата звернення: 08.01.2026).

15. Про електронну ідентифікацію та електронні довірчі послуги : Закон України від 5 жовтня 2017 року № 2155-VIII. *Відомості Верховної Ради України.* 2017. № 45. Ст. 400.

16. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 року № 2163-VIII. *Відомості Верховної Ради України.* 2017. № 45. Ст. 403.

17. Про електронні комунікації : Закон України від 16 грудня 2020 року № 1089-IX. *Офіційний портал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/1089–20#Text (дата звернення: 08.01.2026).

18. Про національну програму інформатизації : Закон України від 1 грудня 2022 року № 2807-IX. *Відомості Верховної Ради України.* 2023. № 51. Ст. 127.

19. Аналітичний звіт про стан виконання Плану реалізації Стратегії кібербезпеки України за 2025 рік. *Офіційний портал Державної служби спеціального зв'язку та захисту інформації України.* URL: https://cip.gov.ua/services/cm/api/attachment/download?id=73801 (дата звернення: 08.01.2026).

20. Про затвердження Порядку формування та ведення відкритого переліку забороненого до використання програмного забезпечення та комунікаційного (мережевого) обладнання : постанова Кабінету Міністрів України від 22 жовтня 2025 року № 1335. *Офіційний портал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/1335-2025-%D0%BF#n8 (дата звернення: 08.01.2026).

21. Про нарощування спроможностей сил оборони : Указ Президента України від 6 лютого 2024 року № 51/2024. *Офіційний портал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/51/2024?lang=en#Text (дата звернення: 08.01.2026).

22. Про Кіберсили Збройних Сил України: проект закону України від 23 грудня 2024 року. *Офіційний портал Верховної Ради України.* URL: https://itd.rada.gov.ua/billinfo/Bills/Card/45453 (дата звернення: 08.01.2026).

23. Про Збройні Сили України : Закон України від 6 грудня 1991 року № 1934-XII. *Відомості Верховної Ради України.* 1992. № 9. Ст. 108.

24. Про благодійну діяльність та благодійні організації : Закон України від 5 липня 2012 року № 5073-VI. *Відомості Верховної Ради України.* 2013. № 25. Ст. 252.

25. Про інноваційну діяльність : Закон України від 4 липня 2002 року № 40-IV. *Відомості Верховної Ради України.* 2002. № 36. Ст. 266.

References

1. Levkun, T.V., Hamaliuk, B.M., & Lys, A.B. (2024). Dydzhytalizatsiia v terytorialnykh hromadakh: Hromada v smartfoni [Digitalization in territorial communities: Community in a smartphone]. *Uspikhy y dosiahnennia v nautsi*, 8(8), 420–432 [in Ukrainian].

2. Vasynova, N.S. (2022). Dydzhytalizatsiia publichnoho upravlinnia v Ukraini: Trend chy vymoha chasu? [Digitalization of public administration in Ukraine: A trend or a demand of time?]. *Vcheni zapysky TNU imeni V.I. Vernadskoho. Seriia: Publichne upravlinnia ta administruvannia*, 33(72), 6, 48–52. https://doi.org/10.32782/TNU-2663-6468/2022.6/08 [in Ukrainian].

3. Shmyndruk, O.F., & Balahur, Yu.S. (2025). Zabezpechennia prava na dostup do pravosuddia v umovakh dydzhytalizatsii tsyvilnoho sudochynstva [Ensuring the right to access to justice under digitalization of civil proceedings]. *Chasopys Natsionalnoho universytetu "Ostrozka akademiia". Seriia "Pravo"*, 2, 43–47. https://doi.org/10.32782/2223-9995.2024.26.10 [in Ukrainian].

4. Rudiuk, V.S. (2020). Dydzhytalizatsiia v suchasnomu sudochynstvi [Digitalization in modern judicial proceedings]. *Filosofski ta metodolohichni problemy prava*, 2(20), 82–85 [in Ukrainian].

5. Barabash, O. (2022). Dydzhytalizatsiia vitchyznianoi osvity: Problemy i perspektyvy rozvytku v umovakh hlobalizatsii [Digitalization of domestic education: Problems and prospects of development under globalization]. *Pravo Ukrainy*, 12, 109–121. https://doi.org/10.33498/louu-2022-12-109 [in Ukrainian].

6. Vinnyk, O.M., Popovych, T.H., & Derevianko, B.V. (2022). Rehuliuvannia vidnosyn tsyfrovoi ekonomiky: Okremi aspekty [Regulation of digital economy relations: Certain aspects]. *Visnyk Natsionalnoi akademii pravovykh nauk Ukrainy*, 29(3), 181–204. https://doi.org/10.31359/1993-0909-2022-29-3-181 [in Ukrainian].

7. Deshko, L.M., & Bondarieva, K.D. (2018). Kiberbezpeka v Ukraini: Natsionalna stratehiia ta mizhnarodne spivrobitnytstvo [Cybersecurity in Ukraine: National strategy and international cooperation]. *Porivnialno-analitychne pravo*, 2, 379-382 [in Ukrainian].

8. Polishchuk, V.P., & Panasevych, L.A. (2024). Mizhnarodne pravo i kiberbezpeka: Vyznachennia pravovoho statusu kiberatak ta kiberviiskovykh operatsii [International law and cybersecurity: Determining the legal status of cyberattacks and cyber military operations]. *Yurydychnyi naukovyi elektronnyi zhurnal*, 2, 503–506 [in Ukrainian].

9. Verkhovna Rada of Ukraine. (1994). *Pro zakhyst informatsii v informatsiino-komunikatsiinykh systemakh: Law of Ukraine dated July 5, 1994 No. 80/94-VR* [On protection of information in information and communication systems]. *Vidomosti Verkhovnoi Rady Ukrainy*, 31, Art. 286 [in Ukrainian].

10. Verkhovna Rada of Ukraine. (2005). *Pro ratyfikatsiiu Konventsii pro kiberzlochynnist: Law of Ukraine dated September 7, 2005 No. 2824-IV* [On ratification of the Convention on Cybercrime]. *Vidomosti Verkhovnoi Rady Ukrainy*, 5–6, Art. 71 [in Ukrainian].

11. Derevianko, B.V. (2017). Ryzyky zdiisnennia operatsii z kryptovaliutoiu (bitkoinamy) hromadian i subiektiv hospodariuvannia Ukrainy [Risks of cryptocurrency (bitcoin) transactions by citizens and business entities of Ukraine]. *Forum prava*, 3, 33–39. Retrieved from https://repository.ndippp.gov.ua/handle/765432198/269 [in Ukrainian].

12. Verkhovna Rada of Ukraine. (2006). *Pro Derzhavnu sluzhbu spetsialnoho zviazku ta zakhystu informatsii Ukrainy: Law of Ukraine dated February 23, 2006 No. 3475-IV* [On the State Service of Special Communications and Information Protection of Ukraine]. *Vidomosti Verkhovnoi Rady Ukrainy*, 30, Art. 258 [in Ukrainian].

13. President of Ukraine. (2016). *Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid January 27, 2016 "Pro Stratehiiu kiberbezpeky Ukrainy": Decree of the President of Ukraine No. 96/2016* (expired). Retrieved from https://zakon.rada.gov.ua/laws/show/96/2016#n11 [in Ukrainian].

14. President of Ukraine. (2021). *Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid May 14, 2021 "Pro Stratehiiu kiberbezpeky Ukrainy": Decree of the President of Ukraine No. 447/2021*. Retrieved from https://zakon.rada.gov.ua/laws/show/447/2021#n7 [in Ukrainian].

15. Verkhovna Rada of Ukraine. (2017). *Pro elektronnu identyfikatsiiu ta elektronni dovirchi posluhy: Law of Ukraine dated October 5, 2017 No. 2155-VIII* [On electronic identification and electronic trust services]. *Vidomosti Verkhovnoi Rady Ukrainy*, 45, Art. 400 [in Ukrainian].

16. Verkhovna Rada of Ukraine. (2017). *Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Law of Ukraine dated October 5, 2017 No. 2163-VIII* [On the basic principles of ensuring cybersecurity of Ukraine]. *Vidomosti Verkhovnoi Rady Ukrainy*, 45, Art. 403 [in Ukrainian].

17. Verkhovna Rada of Ukraine. (2020). *Pro elektronni komunikatsii: Law of Ukraine dated December 16, 2020 No. 1089-IX* [On electronic communications]. Retrieved from https://zakon.rada.gov.ua/laws/show/1089-20#Text [in Ukrainian].

18. Verkhovna Rada of Ukraine. (2022). *Pro natsionalnu prohramu informatyzatsii: Law of Ukraine dated December 1, 2022 No. 2807-IX* [On the national informatization program]. *Vidomosti Verkhovnoi Rady Ukrainy*, 51, Art. 127 [in Ukrainian].

19. State Service of Special Communications and Information Protection of Ukraine. (2025). *Analitychnyy zvit pro stan vykonannia Planu realizatsii Stratehii kiberbezpeky Ukrainy za 2025 rik* [Analytical report on the implementation of the Cybersecurity Strategy of Ukraine for 2025]. Retrieved from https://cip.gov.ua/services/cm/api/attachment/download?id=73801 [in Ukrainian].

20. Cabinet of Ministers of Ukraine. (2025). *Pro zatverdzhennia Poriadku formuvannia ta vedennia vidkrytoho pereliku zaboronenoho do vykorystannia prohramnoho zabezpechennia ta komunikatsiinoho (merezhevoho) obladnannia: Resolution dated October 22, 2025 No. 1335*. Retrieved from https://zakon.rada.gov.ua/laws/show/1335-2025-%D0%BF#n8 [in Ukrainian].

21. President of Ukraine. (2024). *Pro naroshchuvannia spromozhnostei syl oborony: Decree of the President of Ukraine dated February 6, 2024 No. 51/2024*. Retrieved from https://zakon.rada.gov.ua/laws/show/51/2024 [in Ukrainian].

22. Verkhovna Rada of Ukraine. (2024). *Pro Kibersyly Zbroinykh Syl Ukrainy: Draft law dated December 23, 2024*. Retrieved from https://itd.rada.gov.ua/billinfo/Bills/Card/45453 [in Ukrainian].

23. Verkhovna Rada of Ukraine. (1991). *Pro Zbroini Syly Ukrainy: Law of Ukraine dated December 6, 1991 No. 1934-XII* [On the Armed Forces of Ukraine]. *Vidomosti Verkhovnoi Rady Ukrainy*, 9, Art. 108 [in Ukrainian].

24. Verkhovna Rada of Ukraine. (2012). *Pro blahodiinu diialnist ta blahodiini orhanizatsii: Law of Ukraine dated July 5, 2012 No. 5073-VI* [On charitable activities and charitable organizations]. *Vidomosti Verkhovnoi Rady Ukrainy*, 25, Art. 252 [in Ukrainian].

25. Verkhovna Rada of Ukraine. (2002). *Pro innovatsiinu diialnist: Law of Ukraine dated July 4, 2002 No. 40-IV* [On innovation activity]. *Vidomosti Verkhovnoi Rady Ukrainy*, 36, Art. 266 [in Ukrainian].

Дата першого надходження статті до видання: 27.01.2026
Дата прийняття статті до друку після рецензування: 28.02.2026
Дата публікації: 05.03.2026