Міжнародне приватне право

УДК 341.171

Косінова Дарина Станіславівна
доктор філософії в галузі права,
асистент кафедри права Європейського Союзу
Національний юридичний університет імені Ярослава Мудрого
Косинова Дарина Станиславовна
доктор философии в области права,
ассистент кафедры права Европейского Союза
Национальный юридический университет имени Ярослава Мудрого
Kosinova Daryna
Philosophy Doctor in the Field of Law,
Assistant at the Department of European Union Law
Yaroslav Mudryi National Law University

Івчук Катерина Іванівна
студентка
Національного юридичного університету імені Ярослава Мудрого
Ивчук Екатерина Ивановна
студентка
Национального юридического университета имени Ярослава Мудрого
Ivchuk Kateryna
Student of the
Yaroslav Mudryi National Law University

Чернявський Олександр Владиславович
студент
Національного юридичного університету імені Ярослава Мудрого
Чернявский Александр Владиславович
студент
Национального юридического университета имени Ярослава Мудрого

Cherniavskyi Oleksandr
Student of the
Yaroslav Mudryi National Law University

ПРАВОВИЙ АНАЛІЗ СУЧАСНОГО СТАНУ ТА ТЕНДЕНЦІЙ РОЗВИТКУ ЗАКОНОДАВСТВА ЄС ТА УКРАЇНИ У СФЕРІ КІБЕРБЕЗПЕКИ
ПРАВОВОЙ АНАЛИЗ СОВРЕМЕННОГО СОСТОЯНИЯ И ТЕНДЕНЦИЙ РАЗВИТИЯ ЗАКОНОДАТЕЛЬСТВА ЕС И УКРАИНА В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ
LEGAL ANALYSIS OF THE CURRENT SITUATION AND TRENDS IN THE DEVELOPMENT OF EU AND UKRAINE LEGISLATION IN THE FIELD OF CYBER SECURITY

Анотація. *Статтю присвячено питанню врегулювання відносин реалізації політики кібернетичної безпеки у Європейському Союзі та Україні. Досліджується керівна роль ЄС у процесі визначення ключових напрямів кіберполітики у державах-членах ЄС, а також кроки України у даній сфері в ході проведення євроінтеграційних реформ. Автори аналізують систему нормативних актів інституцій ЄС у сфері кібербезпеки, серед яких, зокрема, стратегічні документи, що містять загальні відправні засади реалізації політики, а також загальнобов`язкові регламенти та директиви, положення яких конкретизують механізми втілення кіберполітики у державах-членах ЄС. Визначено основні нормативні документи ЄС у сфері забезпечення кіберзахисту як держав, такі приватних осіб-споживачів цифрових послуг в мережі Інтернет. Аналізуються становлення безпечного цифрового ринку ЄС у контексті впровадження схем сертифікації цифрових продуктів та послуг, а також нормативна та інституційна основа боротьби з шахрайством в мережі Інтернет. Досліджуються основні можливості, засоби реалізації та*

установи ЄС, відповідальні за функціонування безпечного кібернетичного європейського простору, зокрема Агентство ЄС з кібербезпеки (ENISA). У контексті прийняття нової Стратегії кібербезпеки ЄС на найближчі 10 років визначаються майбутні кроки ЄС у сфері кіберзахисту, наприклад прискорення впровадження ключових стандартів безпеки в Інтернеті, застосування і швидке завершення реалізації технологій 5G, кіберрозвідувальна діяльність тощо. Автори аналізують систему нормативно-правових актів України у сфері забезпечення національної кібербезпеки. Визначаються недоліки нормативно-правового регулювання кібербезпеки та виконання нормативних положень національного законодавства. Крім того, автори відзначають позитивні зрушення у питаннях реалізації кіберполітики в Україні, пов'язані у тому числі з розробленням Стратегії кібербезпеки України на 2021-2025 роки.

Ключові слова: *право ЄС, кібербезпека ЄС, кібератаки, кіберполітика, інформаційно-телекомунікайні технології, сертифікація.*

Аннотация. *Статья посвящена вопросу урегулирования отношений реализации политики кибернетической безопасности в Европейском Союзе и Украине. Исследуется руководящая роль ЕС в процессе определения ключевых направлений киберполитики в государствах-членах ЕС, а также шаги Украины в данной сфере в ходе проведения евроинтеграционных реформ. Авторы анализируют систему нормативных актов институтов ЕС в сфере кибербезопасности, среди которых, в частности, стратегические документы, содержащие общие отправные принципы реализации политики, а также общеобязательные регламенты и директивы, положения которых конкретизируют механизмы воплощения киберполитики в государствах-членах ЕС. Определены основные нормативные документы ЕС в сфере обеспечения киберзащиты как государств, так и частных лиц-потребителей цифровых услуг в сети Интернет. Анализируются становление*

безопасного цифрового рынка ЕС в контексте внедрения схем сертификации цифровых продуктов и услуг, а также нормативная и институциональная основа борьбы с мошенничеством в сети Интернет. Исследуются основные возможности, средства реализации и учреждения ЕС, ответственные за функционирование безопасного кибернетического европейского пространства, в частности Агентство ЕС по кибербезопасности (ENISA). В контексте принятия новой Стратегии кибербезопасности ЕС на ближайшие 10 лет определяются будущие шаги ЕС в сфере киберзащиты, например ускорение внедрения ключевых стандартов безопасности в Интернете, применение и быстрое завершение реализации технологий 5G, кибершпионская деятельность и тому подобное. Авторы анализируют систему нормативно-правовых актов Украины в сфере обеспечения национальной кибербезопасности. Определяются недостатки нормативно-правового регулирования кибербезопасности и выполнения нормативных положений национального законодательства. Кроме этого, авторы отмечают положительные сдвиги в вопросах реализации киберполитики в Украине, связанные в том числе с разработкой Стратегии кибербезопасности Украины на 2021-2025 года.

Ключевые слова: *право ЕС, кибербезопасность ЕС, кибератаки, киберполитика, информационно-телекомуникационные технологии, сертификация.*

Summary. *The article is devoted to the issue of settling relations on the implementation of cyber security policy in the European Union and Ukraine. The leading role of the EU in the process of determining the key directions of cyber policy in the EU member states, as well as the steps of Ukraine in this area in the course of European integration reforms are studied. The authors analyze the system of normative acts of EU institutions in the field of cybersecurity, including, in particular, strategic documents containing general*

guidelines for policy implementation, as well as binding regulations and directives, the provisions of which specify mechanisms for implementing cyber policy in EU member states. The main normative documents of the EU in the field of cyber security of both states and private consumers of digital services on the Internet have been identified. The formation of a secure digital market in the EU in the context of the implementation of certification schemes for digital products and services, as well as the regulatory and institutional framework for combating fraud on the Internet are analyzed. The main opportunities, means of implementation and EU institutions responsible for the functioning of the secure European cyberspace, in particular the EU Cyber Security Agency (ENISA), are explored. In the context of the adoption of the new EU Cyber Security Strategy for the next 10 years, future EU steps in the field of cyber security are identified, such as accelerating the implementation of key Internet security standards, application and rapid completion of 5G technologies, cyber intelligence, etc. The authors analyze the system of legal acts of Ukraine in the field of national cybersecurity. The shortcomings of the regulatory and legal regulation of cybersecurity and the implementation of regulations of national legislation are identified. In addition, the authors note the positive developments in the implementation of cyber policy in Ukraine, including the development of the Cyber Security Strategy of Ukraine for 2021-2025.

Keywords: *EU law, EU cybersecurity, cyberattacks, cyber policy, information and telecommunication technologies, certification.*

Постановка проблеми. Цифрова ера відкрила нові можливості та позитивні перспективи для спілкування, торгівлі та бізнесу. Водночас, прискорена цифровізація сфер діяльності та послуг обумовлює тенденції розвитку суспільства, уразливого до кібернетичних небезпек. Очевидно, що з використанням та розширенням кіберпростору, забезпечення кібернетичної безпеки стало надзвичайно актуальним питанням як для національних органів держав-членів ЄС, так і для приватних суб'єктів.

Європейським Союзом були відзначені постійно зростаючі загрози, що походять від природи цифрового світу протягом останніх років. З метою попередження та відвернення кібератак Європейський Союз формує всеосяжну та цілісну стратегію кібербезпеки для своїх держав-членів, намагаючись посилити стійкість кіберпростору, пом'якшити кіберзагрози та дослідити переваги цифрової трансформації. Кібертаки на енергетичні компанії України у 2015 році, а також наслідки глобальної атаки програмою NotPetyay 2017 році обумовили необхідність модернізації існуючої системи кіберзахисту в Україні. У цьому контексті, в рамках укладеної Угоди про асоціацію з ЄС до сих пір залишаються актуальними питання приведення національного законодавства Українидо стандартів, вироблених у праві ЄС та пошук шляхів поглибленої співпраці України та ЄС у цифровій сфері, у тому числі кібербезпеці.

Аналіз останніх досліджень і публікацій.Питанням нормативно-правового регулювання та реалізації політики кібербезпеки у ЄС та Україні приділяли увагу такі зарубіжні та вітчизняні науковці як Крістоу Г. (Christou, G.) [1], Пернік П. (Pernik, P.) [2], Ренард Т. (Renard, T.) [3], Корніш П. (Cornish, P.) [4], Бакалінський О., Бакалінська О. [5], Трофименко О. Ю. Прокоп, Н. Логінова, О. Задерейко [6], Живило Є. [7], Забара І.М. [8].

Метою наукової роботи є дослідження нормативно-правової основи забезпечення кібербезпеки та механізму функціонування безпечного цифрового простору у Європейському Союзі, аналіз законодавства України у сфері кіберзахисту, а також виявлення проблем, які існують під час управління кібербезпекою на національному рівні.

Виклад основного матеріалу. У зв'язку з потужним розвитком інформаційних технологій, стрімкою цифровізацією сфер діяльності та послуг, кібератаки стали реальною загрозою для державного суверенітету, яка не обмежується кордонами та має значний економічний і політичний

вплив на стабільне функціонування та розвиток держав-членів ЄС. Шкідливе програмне забезпечення (файлові віруси, троянські програми («Trojans»), програми-вимагачі («ransomwares»), атаки на відмову в обслуговуванні («DoS-атаки»), фішинг («phishing») на сьогоднішній день стали звичними таефективними інструментами втручання як у приватне життя особи, так й у сферу національної безпеки конкретної держави. Наслідки останніх глобальних атак програмами Wannacry та NotPetya у 2017 році підтвердили недостатню спроможність низки європейських країн, у тому числі України, протистояти загрозам кіберпростору та створили нові імпульси для поглибленої співпраці держав у сфері кібербезпеки в рамках спільної зовнішньої та безпекової політики Європейського Союзу.

Наріжним каменем політики ЄС стала Стратегія кібербезпеки 2013 року, яка передбачила п'ять основних цілей: 1) підвищення кіберстійкості; 2) зменшення кіберзлочинності; 3) розробка політики та можливостей кіберзахисту; 4) розвиток промислових та технологічних ресурсів кібербезпеки; та 5) встановлення міжнародної політики у галузі кіберпростору, узгодженої з основними цінностями ЄС [9]. Цілі даної Стратегії сутнісно взаємопов'язані з трьома прийнятими згодом стратегічними документами:

1) Європейським порядком денним з питань безпеки (2015), мета якого полягала у: 1) вдосконаленні правоохоронної діяльності та реагуванні судової системи на кіберзлочинність, головним чином шляхом оновлення існуючої політики та законодавства; 2) виявленні перешкод у розслідуванні кримінальних справ щодо кіберзлочинності та посиленні кібернетичного потенціалу [10];

2) Стратегією єдиного цифрового ринку (2015), яка має на меті створити кращий доступ до цифрових товарів та послуг шляхом створення

належних умов для максимізації потенціалу зростання цифрової економіки [11].

3) Глобальною стратегією (2016), положення якої передбачають посилення ролі ЄС на міжнародній арені шляхом співпраці з ключовими партнерами у процесі вирішення кіберпроблем [12].

На розвиток цілей Стратегії 2013 року була прийнята Директива про мережеву та інформаційну безпеку (NetworkandInformationSecurity (NIS) Directive 2016), по суті перший загальноєвропейський «закон про кібербезпеку», який встановив мінімальні стандарти кібербезпеки, зобов'язуючи держав-членів ЄС прийняти національні стратегії мережевої та інформаційної безпеки та створити єдині контактні пункти та групи реагування на надзвичайні комп'ютерні випадки(CSIRT) [13]. У грудні 2020 року Європейська комісія запропонувала оновлену Директиву NIS (NIS2) [14] замість Директиви 2016 року. Новий проект, який наразі розглядається Радою, є реакцією на мінливі загрози і враховує цифрову трансформацію суспільства, яка прискорилася у зв'язку з кризою COVID-19. Окрім цього, у 2017 році Європейською Комісією був розроблений План швидкого реагування на надзвичайні ситуації у разі великомасштабного транскордонного кіберінцідента або кризи [15], в якому визначаються завдання і способи співпраці між державами-членами та інституціями ЄС під час реагування на такі інциденти, а також пояснюється, як існуючі механізми антикризового управління можуть в повній мірі використовувати відповідні суб'єкти кібербезпеки на рівні ЄС.

Разом з Директивою NIS у 2016 році набув чинності також Загальний регламент про захист даних (General Data Protection Regulation (GDPR), нормативні положення якого спрямовані на захист персональних даних європейських громадян шляхом встановлення правил щодо їх обробки та розповсюдження. Регламент надає суб'єктам даних певні права, покладає на постачальників цифрових послуг обов'язки щодо використання та

передачі інформації, встановлює вимоги щодо сповіщення у разі виявлених порушень та відповідальність у вигляді адміністративних штрафів за порушення норм Регламенту [16].

За останні декілька років ЄС також посилив боротьбу з шахрайством із використанням безготівкових коштів. У квітні 2019 року шляхом модернізації існуючих правил, Рада ЄС прийняла Директиву про боротьбу з шахрайством і підробкою безготівкових платіжних засобів [17]. Нормативні положення Директиви стосуються не тільки традиційних безготівковихзасобів платежу, таких як банківські картки або чеки, а й нових способів здійснення платежів, що з'явилися за останні роки, серед яких, зокрема, електронні гаманці, мобільні платежі і віртуальні валюти. Директива узгоджує визначення деяких видів злочинів в Інтернеті, таких як злом комп'ютера жертви або «фішинг»; види покарань для фізичних осіб; уточнюємежі юрисдикцій для більш ефективної протидії транскордонному шахрайству тощо. Загалом, кіберзлочинність може приймати різноманітні форми: крадіжка або компрометація особистих даних або інтелектуальної власності, використання інтернет-платформ для поширення незаконного контенту, використання «тіньової мережі» (DarkNet) для продажу незаконних товарів і хакерських послуг тощо. Тому з метою захисту громадян, підприємств та урядів держав-членів ЄС від злочинів в мережі Інтернет та посилення реакції правоохоронних органів на кіберзлочинність при Європолі був заснований Європейський центр боротьби з кіберзлочинністю (ЕС3), який надає підтримку державам-членам ЄС у розслідуванні кіберзлочинів, у тому числі у ліквідації злочинних мереж [18].

Суттєвим кроком вдосконалення нормативно-правової основи безпечного функціонування кібернетичного простору ЄС стало прийняття та набуття чинності у 2019 році Закону ЄС про кібербезпеку (CyberSecurityAct) [19], що запровадив загальноєвропейську схему

сертифікації та оновлений постійний мандат Агентства ЄС з кібербезпеки (ENISA). Система сертифікації передбачає схеми сертифікації у вигляді вичерпного набору правил, технічних вимог, стандартів і процедур для продуктів та послуг інформаційно-телекомунікаційних технологій (ІКТ). Запроваджені спільні засади сертифікації в ЄС можуть поступово покласти край роздрібненості законодавчих актів та політик між країнами-членами ЄС, оскільки передбачають простір для уніфікації стандартів та процедур щодо продуктів та послуг ІКТ, загальнообов'язкових для всіх країн-членів ЄС.

Окремо варто звернути увагу на оновлений посилений постійний мандат Агентства ЄС з кібербезпеки (ENISA), яке до набрання чинності Законом про кібербезпеку ЄС у силу відсутності належних ресурсів та повноважень відігравало досить обмежену роль у здійснення політики кібербезпеки в європейському просторі. Відтепер ENISA грає ключову роль у створенні і підтримці європейської системи сертифікації кібербезпеки шляхом підготовки технічної основи для конкретних схем сертифікації, а також відповідає за інформування громадськості про схеми сертифікації та видані сертифікати через спеціальний веб-сайт. Окрім цього, ENISA доручено розширювати оперативне співробітництво на рівні ЄС, допомагаючи державам-членам ЄС, і підтримувати координацію ЄС в разі великомасштабних транскордонних кібератак. Зокрема, у вересні 2020 року за підтримки ENISA були проведені вже другі командні навчання Blueprint (BlueOLEx) 2020, у яких взяли участь керівники національних органів кібербезпеки держав-членів ЄС, представники Європейської Комісії та ENISA. Метою проведення таких навчань є перевірка готовності Європейського Союзу у разі виникнення кібер-криз. Крім того, на виконання Плану Європейської комісії зі швидкого реагування на надзвичайні ситуації в разі великомасштабного транскордонного кіберінцідента або кризи (2017) було утворено CyCLONe (Cyber

CrisisLiaisonOrganisationNetwork) – Комунікаційну мережу організацій з протидії кібернетичним кризамдля держав-членів ЄС, функцію секретаріату у якій виконує ENISA [20].

У грудні 2020 року Європейська комісія та Європейська служба зовнішніх справ (EEAS) представили нову Стратегію кібербезпеки ЄС [21] на найближчі 10 років. Метою цієї стратегії є підвищення стійкості Європи до кіберзагроз і забезпечення громадян та підприємств ЄС безпечними та надійними цифровими послугами та технологіями. У кінці березня 2021 року Рада ЄС прийняла висновки щодо оновленої Стратегії, у яких виділила ряд напрямків для дій в найближчі роки, серед яких зокрема: 1) створення мережі операційних центрів безпеки по всьому ЄС для відстеження та запобігання сигналів про атаки на мережі; 2) визначення спільного підрозділу кібербезпеки, який забезпечить чітку спрямованість дій ЄС з управління кризами в області кібербезпеки; 3) застосування і швидке завершення реалізації технологій 5G у ЄС, забезпечення безпеки мереж 5G і розвиток майбутніх поколінь мереж; 4) прискорення впровадження ключових стандартів безпеки в Інтернеті; 5)розвиток надійного шифрування як засобу захисту основних прав і цифрової безпеки; 6) підвищення ефективності та дієвості інструментарію кібердипломатії; 7) створення робочої групи з кіберрозвідки для посилення спеціального потенціалу Розвідувального і ситуаційного центру Європейського союзу (EU INTCEN) в цій сфері тощо [22]. Для забезпечення розробки, впровадження та моніторингу пропозицій, передбачених Стратегією, Рада ЄС закликала Комісію та Верховного представника ЄС з питань закордонних справ та політики безпеки розробити детальний план їх реалізації.

Україна в останні роки намагається відповідати новим викликам у сфері кібербезпеки, але спеціалісти та статистика кажуть нам про слабкість нашої держави в цій сфері. За статистичними даними Україна посідає одні

з найнижчих місць у сфері кібербезпеки, адже вона займає 54 місце у рейтингу GlobalCybersecurityIndex, 51 місце за рейтингом дослідницької компанії Comparitech, а також займає найнижчі позиції на рівні регіону Центрально-Східної Європи. У 2017 році через вірус NonPetya Україна втратила 0,5 % ВВП, що в грошовому еквіваленті – 14,914 мільярдів гривень [23].

Співзасновник української спільноти етичних хакерів Hacken, співзасновник школи «білих» хакерів Cyber School Є.Аушев так коментує сучасний стан кібербезпеки в Україні: «В Україні немає закону про кібербезпеку – тільки закон про її засади. А в ньому не прописані практично ніякі правила гри. В Україні у сфері кібербезпеки панує не стільки демократія, скільки анархія. Правил практично немає, а ті, які є, кожен може інтерпретувати як хоче» [24].

Так О. Янковський вказує на неефективність нормативної бази та системи управління: «Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" та серія нормативних документів про технічний захист інформації безнадійно застарілі. Більше того, вони зобов'язують органи державної влади, об'єкти критичної інфраструктури та приватні компанії, які хочуть надавати послуги державним органам (наприклад, Інтернет-провайдери), впроваджувати так звану Комплексну систему захисту інформації (КСЗІ). Вона, окрім того, що морально застаріла, впродовж багатьох років довела свою неефективність» [25].

У своїй статті «Кібербезпека України: Аналіз сучасного стану» О. Трофименко, Ю. Прокоп, Н. Логінова, О. Задерейко вказують на те, що «проблема ефективного забезпечення кібербезпеки потребує комплексного вирішення і вимагає скоординованих дій на національному, регіональному та міжнародному рівнях для запобігання, підготовки, реагування та

відновлення інцидентів з боку органів влади, приватного сектора і громадянського суспільства» [6, с. 156].

Є. Живило у своїй роботі «Шляхи врегулювання нормативно-правової бази із захисту інформації, кібербезпеки і кібероборони України» зазначає те, що на сьогодні нормативно-правова база України не дозволяє нашим Збройним Силам України та іншим військовим формуванням здійснювати ефективну підготовку держави до відбиття воєнної агресії у кіберпросторі (кібероборони), а також виконувати заходи з кібероборони (що стосується не тільки мирного часу, а й в умовах кризових ситуацій, особливий період і воєнного стану). «Зокрема, це пов'язано із відсутністю дієвих вимог та механізмів щодо виконання операторами і провайдерами телекомунікацій усіх форм власності завдань Генерального штабу Збройних Сил України з кібероборони, контролю і блокування трафіка в телекомунікаційних мережах» [7, с. 7].

О. Бакалінська та О. Бакалінський в роботі «Правове забезпечення кіберзахисту в Україні» вказують на те, що «Найбільш перспективними напрямами розвитку національної системи кіберзахисту є:

1) Вдосконалення правової основи кіберзахисту об'єктів критичної інфраструктури;

2) Впровадження системи незалежного аудиту інформаційної безпекина об'єктах критичної інфраструктури;

3) Створення галузевих центрів реагування на кіберінциденти;

4) Розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки;

5) Розвиток системи підготовки кадрів у сфері кібербезпеки;

6) Підвищення цифровоїг рамотності (правил кібергігієни) громадян та культури безпекового поводження в кіберпросторі;

7) Впровадження систем інформаційного комплаєнсу;

8) Створення довірчих відносин між державою та суспільством, для якого держава повинна грати сервісну роль» [5, с. 106].

На підставі аналізу зазначених вище наукових праць, варто відзначити схожість поглядів авторів щодо недосконалості, а також застарілості тих нормативно-правових актів, які повинні забезпечувати нашу кібербезпеку, що виражається у неспроможності таких актів відповідати умовам сьогодення і виконувати своє завдання, з чим складно не погодитись.

Важливо зазначити, що основними нормативно-правовими актами у сфері кібербезпеки є Закон України «Про основні засади забезпечення кібербезпеки України», Закон України «Про національну безпеку», Закон України «Про інформацію», Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», Конвенція Ради Європи про кіберзлочинність, а також Доктрина інформаційної безпеки України і Конституція України. Крім того Указом Президента України №121/2021 введено в дію рішення Ради національної безпеки і оборони України від 25 березня 2021 року «Про Стратегію воєнної безпеки України» [26]. Відповідно до цієї стратегії пріоритетами досягнення цілей державної політики у воєнній сфері, сфері оборони і військового будівництва є розвиток спроможностей щодо забезпечення кібербезпеки, кіберзахисту та кібероборони під час підготовки та ведення всеохоплюючої оборони України.

Так, у попередньому аналітичному звіті про контроль за виконанням Закону України «Про основні засади кібербезпеки в Україні» Л. Олексюк виокремлює такі основні проблеми цього Закону:

1) Відсутність у ньому формулювання власне його цілей;

2) Закон містить численні завдання для державного сектора, тоді як більшість об'єктів критичної інфраструктури знаходяться у приватному секторі;

3) Питання взаємодії суб'єктів сфери безпеки і оборони, органів, що формують і реалізують політику у сфері кібербезпеки та приватного сектора на сьогодні взагалі не порушується;

4) Неврегульованими є питання пошуку вразливостей як об'єктів критичної інфраструктури, так і інших інформаційно-телекомунікаційних систем державного і приватного сектора;

5) Закон не вимагає створення та використання інформаційно-аналітичних систем підтримки прийняття управлінських рішень, зокрема в умовах криз та кризового реагування. У ньому відсутні механізми реалізації багатьох поставлених перед органами завдань [27, с. 27-29].

Тобто авторка виділяє велику кількість недоліків цього Закону, а він є основним для регуляції питання в цій сфері в Україні. Також нею рекомендовано заміщення закону з розробкою повного пакету документів, включно з фінансовими розрахунками, аналізом регуляторного впливу, визначенням заінтересованих осіб, підготовкою і розповсюдженням серед них опитувальника, що, на нашу думку, було б також доречним.

Все ж позитивні зрушення в сфері кібербезпеки є. 4 березня 2021 року Робочагрупа при НКЦК РНБО України схвалила проект Стратегії кібербезпеки України на 2021-2025 роки. Проєкт цього нормативно-правового акту вказує нам на ті цілі, а також основні напрямки в якому буде розвиватись українське законодавство у сфері кібербезпеки, а також проаналізовано певні проблеми минулих років. Так в цій Стратегії вказується на «недосконаліть нормативно-правової бази у сфері кібербезпеки, а також її застарілість у сфері захисту інформації, повільна імплементація положень європейського права у вітчизняне законодавство, недостатня врегульованість цифрової складової частини розслідування

злочинів, а також низький рівень правової відповідальності за порушення вимог законодавства у цій сфері». Крім того зазначено, що в Україні відсутня значна частина міністерств і відомств відповідних структурних підрозділів, необхідного кадрового забезпечення та належного контролю за кіберзахистом, а фінансування цієї сфери здійснюється за залишковим принципом. Ще й досі не урегульоване питання щодо відсутності законодавчого акта про критичну інфраструктуру України та її захист, що значно ускладнює формування системи кіберзахисту такої інфраструктури. [28, с. 3-4, 10]. Подальше затвердження такої стратегії, а також дотримання тих цілей та завдань, які вказані в тексті цього акту, можуть наблизити Україну до відповідності європейським стандартам в сфері кібербезпеки.

Крім того позитивним «дзвіночком» може слугувати те, що в березні 2021 року в Україні запрацював Центр протидії дезінформації, який працюватиме на базі РНБО. Цей центр об'єднає спеціалістів з різних відомств та приватних компаній, які будуть перевіряти інформацію, яка з'являється в публічному просторі [29].

Тому в українському законодавстві необхідно провести велику роботу, щоб забезпечити ефективну дієвість як нормативних актів, так і державних органів і приватного сектору в цій сфері. Необхідність оновлення законодавства, а також приведення його до європейських стандартів надасть змогу в найближчі роки захистити як і державу, так і громадян, що надасть більше можливостей для інвестицій, захисту осіб, а також наблизить нашу державу до європейської інтеграції.

Висновок. Законодавство Європейського Союзу, яке постійно оновлюється, а також ті тенденції, які зараз розвиваються в сфері кібербезпеки, є передовими та на своєму рівні здійснюють ефективну реалізацію кіберзахисту, регулювання та реагування на сучасні виклики та зміни у цій сфері.

Українське ж законодавство у сфері кібербезпеки є недостатньо розвинутим, про що кажуть і правники, і спеціалісти. Невідповідність європейським стандартам, недостатня врегульованість багатьох законодавчих питань, слабка заінтересованість суспільства, а також залишкове фінансування, яке не дає змоги для створення належної системи з боку держави – основні чинники,що обумовлюють уразливе до кіберзагроз становище нашої держави, особливо у часи ведення гібридної інформаційної війни. Оновлення законодавства України, а також приведення його до європейських стандартів наблизить державу до європейської інтеграції, надасть дієві способи та засоби захисту фізичних та юридичних осіб, що в свою чергу сприятиме залученню іноземних інвестицій, а також створить ефективні механізми протидії кіберзагрозам.

Література

1. Christou G. Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy: New Security Challenges. Hampshire. Palgrave Macmillan, 2016. 222 p.
2. Pernik P. Improving Cyber Security: NATO and the EU. Tallinn: International Centre for Defence Studies, 2014. 18 p. URL: https://icds.ee/wp-content/uploads/2010/02/Piret_Pernik_-_Improving_Cyber_Security.pdf (date of access: 15.03.2021).
3. Renard T. EU cyber partnerships: assessing the EU strategic partnerships with third countries in the cyber domain. *European Politics and Society*. 19 (3). P. 1–17. URL: https://www.researchgate.net/publication/322782485_EU_cyber_partnerships_assessing_the_EU_strategic_partnerships_with_third_countries_in_the_cyber_domain (date of access: 25.03.2021).
4. Cornish P. Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks. Brussels : European Parliament, 2009. 32 p. URL:

https://www.europarl.europa.eu/RegData/etudes/etudes/join/2009/406997/EXPO-AFET_ET(2009)406997_EN.pdf (date of access: 18.03.2021).

5. Бакалінський О., Бакалінська О. Правове забезпечення кібербезпеки в Україні. *Підприємництво, господарство і право*. № 9. С. 100–108. URL: https://doi.org/10.32849/2663-5313/2019.9.17 (дата звернення: 01.04.2021).
6. Кібербезпека України: аналіз сучасного стану / О. Трофименко та ін. *Захист інформації*. Т. 21, № 3. С. 150–157. URL: http://dspace.onua.edu.ua/bitstream/handle/11300/12213/statya_Trofymenko_Prokop_Loginova_Zadereyko_CYBERSECURITY%20OF%20UKRAINE.pdf?sequence=1&isAllowed=y (дата звернення: 01.04.2021).
7. Живило Є. О. Шляхи врегулювання нормативно-правової бази із захистуінформації, кібербезпеки та кібероборони України. *Electronic scientific publication "Public Administration and National Security"*. URL: https://www.inter-nauka.com/uploads/public/15658573148870.pdf (датазвернення: 26.03.2021).
8. Забара І. М. Формування сучасних правових засад кібернетичної безпеки Європейського Союзу в умовах поширення нових інноваційних технологій. Журнал європейського і порівняльного права. 2017. Вип. 3. С. 2-13.
9. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace : of 07.02.2013 no. 52013JC0001. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52013JC0001 (date of access: 01.04.2021).
10. The European Agenda on Security : of 28.04.2015. URL: https://ec.europa.eu/home-affairs/sites/default/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf (date of access: 01.04.2021).

11. A Digital Single Market Strategy for Europe : of 06.05.2015 no. 52015DC0192. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:52015DC0192 (date of access: 01.04.2021).
12. EEAS Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy. URL: https://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf (date of access: 01.04.2021).
13. Network and Information Security (NIS) : Directive (EU) of 06.07.2016 no. 2016/1148. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC (date of access: 01.04.2021).
14. Directive on Security of Network and Information Systems (NIS 2 Directive): Revised. URL: https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union (date of access: 01.04.2021).
15. Recommendation on coordinated response to large-scale cybersecurity incidents and crises : Recommendation (EU) of 13.09.2017 no. 2017/1584. URL: https://eur-lex.europa.eu/eli/reco/2017/1584/oj (date of access: 01.04.2021).
16. General Data Protection Regulation (GDPR) : Regulation of 27.04.2016 no. 2016/679. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj (date of access: 01.04.2021).
17. Directive (EU) of the European Parliament and of the Councilon combating fraud and counterfeiting of non-cash means of payment and replacing : of 17.04.2019 no. 2019/713. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.123.01.0018.01.ENG (date of access: 01.04.2021).

18. European Cybercrime Centre (EC3). *Europol*. URL: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (date of access: 01.04.2021).
19. REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act") : of 13.09.2017 no. 2017/0225. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017PC0477&from=EN (date of access: 01.04.2021).
20. Blue OLEx 2020: the European Union Member States launch the Cyber Crisis Liaison Organisation Network (CyCLONe). The European Union Agency for Cybersecurity. URL: https://www.enisa.europa.eu/news/enisa-news/blue-olex-2020-the-european-union-member-states-launch-the-cyber-crisis-liaison-organisation-network-cyclone (date of access: 01.04.2021).
21. The EU's Cybersecurity Strategy for the Digital Decade : JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL of 16.12.2020. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2020:18:FIN (date of access: 01.04.2021).
22. Council conclusions on the EU's Cybersecurity Strategy for the Digital Decade: of 09.03.2021 no. 6722/21. URL: https://data.consilium.europa.eu/doc/document/ST-6722-2021-INIT/en/pdf (date of access: 01.04.2021).
23. Кібербезпека. Новий підхід в Україні | Український інститут майбутнього. Український інститут майбутнього | Кадровий резерв майбутнього. URL: https://uifuture.org/publications/kiberbezpechna-ukrayina-novyj-pidhid/ (дата звернення: 07.04.2021).
24. В Україні у сфері кібербезпеки панує не стільки демократія, скільки анархія, - Аушев. znaj.ua. URL: https://life.znaj.ua/375670-v-ukrajini-u-

sferi-kiberbezpeki-panuye-ne-stilki-demokratiya-skilki-anarhiya-aushev (дата звернення: 07.04.2021).

25. Украинская правда. Кибербезопасность Украины: проблемы и пути их решения. Украинская правда. URL: https://www.pravda.com.ua/rus/columns/2019/09/14/7226291/ (дата звернення: 07.04.2021).
26. Указ Президента України №121/2021 – Офіційне інтернет-представництво Президента України. Офіційне інтернет-представництво Президента України. URL: https://www.president.gov.ua/documents/1212021-37661 (дата звернення: 07.04.2021).
27. Олексюк Л. Попередній аналітичний звіт про контроль за виконанням Закону України «Про основні засади кібербезпеки в Україні». www.ua.undp.org. URL: https://www.ua.undp.org/content/dam/ukraine/img/demgov/Rada%20for%20Europe/Report_on_Cybersecurity_02.pdf (дата звернення: 07.04.2021).
28. Проєкт стратегії кібербезпеки України на 2021-2025 роки. Рада національної безпеки і оборони України. URL: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf (дата звернення: 07.04.2021).
29. Указ Президента України №106/2021 – Офіційне інтернет-представництво Президента України. Офіційне інтернет-представництво Президента України. URL: https://www.president.gov.ua/documents/1062021-37421 (дата звернення: 07.04.2021).

References

1. Christou G. Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy: New Security Challenges. Hampshire. Palgrave Macmillan, 2016. 222 p.

2. Pernik P. Improving Cyber Security: NATO and the EU. Tallinn : International Centre for Defence Studies, 2014. 18 p. URL: https://icds.ee/wp-content/uploads/2010/02/Piret_Pernik_-_Improving_Cyber_Security.pdf (date of access: 15.03.2021).
3. Renard T. EU cyber partnerships: assessing the EU strategic partnerships with third countries in the cyber domain. European Politics and Society. 19 (3). P. 1–17. URL: https://www.researchgate.net/publication/322782485_EU_cyber_partnerships_assessing_the_EU_strategic_partnerships_with_third_countries_in_the_cyber_domain (date of access: 25.03.2021).
4. Cornish P. Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks. Brussels : European Parliament, 2009. 32 p. URL: https://www.europarl.europa.eu/RegData/etudes/etudes/join/2009/406997/EXPO-AFET_ET(2009)406997_EN.pdf (date of access: 18.03.2021).
5. Bakalinsjkyj O., Bakalinsjka O. Pravove zabezpechennja kiberbezpeky v Ukrajini. Pidpryjemnyctvo, ghospodarstvo i pravo. # 9. S. 100–108. URL: https://doi.org/10.32849/2663-5313/2019.9.17 (data zvernennja: 01.04.2021).
6. Kiberbezpeka Ukrajiny: analiz suchasnogho stanu / O. Trofymenko ta in. Zakhyst informaciji. T. 21, # 3. S. 150–157. URL: http://dspace.onua.edu.ua/bitstream/handle/11300/12213/statya_Trofymenko_Prokop_Loginova_Zadereyko_CYBERSECURITY%20OF%20UKRAINE.pdf?sequence=1&isAllowed=y (data zvernennja: 01.04.2021).
7. Zhyvylo Je. O. Shljakhy vreghuljuvannja normatyvno-pravovoji bazy iz zakhystuinformaciji, kiberbezpeky ta kiberoborony Ukrajiny. Electronic scientific publication "Public Administration and National Security". URL: https://www.inter-nauka.com/uploads/public/15658573148870.pdf (datazvernennja: 26.03.2021).

8. Zabara I.M. Formuvannja suchasnykh pravovykh zasad kibernetychnoji bezpeky Jevropejsjkogho Sojuzu v umovakh poshyrennja novykh innovacijnykh tekhnologhij. Zhurnal jevropejsjkogho i porivnjaljnogho prava. 2017. Vyp. 3. S. 2-13.
9. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace : of 07.02.2013 no. 52013JC0001. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52013JC0001 (date of access: 01.04.2021).
10. The European Agenda on Security : of 28.04.2015. URL: https://ec.europa.eu/home-affairs/sites/default/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf (date of access: 01.04.2021).
11. A Digital Single Market Strategy for Europe : of 06.05.2015 no. 52015DC0192. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:52015DC0192 (date of access: 01.04.2021).
12. EEAS Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy. URL: https://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf (date of access: 01.04.2021).
13. Network and Information Security (NIS) : Directive (EU) of 06.07.2016 no. 2016/1148. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC (date of access: 01.04.2021).
14. Directive on Security of Network and Information Systems (NIS 2 Directive): Revised. URL: https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union (date of access: 01.04.2021).
15. Recommendation on coordinated response to large-scale cybersecurity incidents and crises : Recommendation (EU) of 13.09.2017 no. 2017/1584.

URL: https://eur-lex.europa.eu/eli/reco/2017/1584/oj (date of access: 01.04.2021).

16. General Data Protection Regulation (GDPR) : Regulation of 27.04.2016 no. 2016/679. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj (date of access: 01.04.2021).
17. Directive (EU) of the European Parliament and of the Councilon combating fraud and counterfeiting of non-cash means of payment and replacing : of 17.04.2019 no. 2019/713. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.123.01.0018.01.ENG (date of access: 01.04.2021).
18. European Cybercrime Centre (EC3). Europol. URL: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (date of access: 01.04.2021).
19. REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act") : of 13.09.2017 no. 2017/0225. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017PC0477&from=EN (date of access: 01.04.2021).
20. Blue OLEx 2020: the European Union Member States launch the Cyber Crisis Liaison Organisation Network (CyCLONe). The European Union Agency for Cybersecurity. URL: https://www.enisa.europa.eu/news/enisa-news/blue-olex-2020-the-european-union-member-states-launch-the-cyber-crisis-liaison-organisation-network-cyclone (date of access: 01.04.2021).
21. The EU's Cybersecurity Strategy for the Digital Decade : JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL of 16.12.2020. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2020:18:FIN (date of access: 01.04.2021).

22. Council conclusions on the EU's Cybersecurity Strategy for the Digital Decade : of 09.03.2021 no. 6722/21. URL: https://data.consilium.europa.eu/doc/document/ST-6722-2021-INIT/en/pdf (date of access: 01.04.2021).
23. Kiberbezpeka. Novyy pidkhid v Ukraïni | Ukrajinsjkyj instytut majbutnjogho. Ukrajinsjkyj instytut majbutnjogho | Kadrovyj rezerv majbutnjogho. URL: https://uifuture.org/publications/kiberbezpechna-ukrayina-novyj-pidhid/ (data zvernennja: 07.04.2021).
24. V Ukrajini u sferi kiberbezpeky panuje ne stiljky demokratija, skiljky anarkhija, - Aushev. znaj.ua. URL: https://life.znaj.ua/375670-v-ukrajini-u-sferi-kiberbezpeki-panuye-ne-stilki-demokratiya-skilki-anarhiya-aushev (data zvernennja: 07.04.2021).
25. Ukraynskaja pravda. Kyberbezopasnostj Ukraynы: problemы y puty ykh reshenyja. Ukraynskaja pravda. URL: https://www.pravda.com.ua/rus/columns/2019/09/14/7226291/ (data zvernennja: 07.04.2021).
26. Ukaz Prezydenta Ukrajiny #121/2021 – Oficijne internet-predstavnyctvo Prezydenta Ukrajiny. Oficijne internet-predstavnyctvo Prezydenta Ukrajiny. URL: https://www.president.gov.ua/documents/1212021-37661 (data zvernennja: 07.04.2021).
27. Oleksjuk L. Poperednij analitychnyj zvit pro kontrolj za vykonannjam Zakonu Ukrajiny «Pro osnovni zasady kiberbezpeky v Ukrajini». www.ua.undp.org. URL: https://www.ua.undp.org/content/dam/ukraine/img/demgov/Rada%20for%20Europe/Report_on_Cybersecurity_02.pdf (data zvernennja: 07.04.2021).
28. Projekt strateghiji kiberbezpeky Ukrajiny na 2021-2025 roky. Rada nacionaljnoji bezpeky i oborony Ukrajiny. URL: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf (data zvernennja: 07.04.2021).

29. Ukaz Prezydenta Ukrajiny #106/2021 – Oficijne internet-predstavnyctvo Prezydenta Ukrajiny. Oficijne internet-predstavnyctvo Prezydenta Ukrajiny. URL: https://www.president.gov.ua/documents/1062021-37421 (data zvernennja: 07.04.2021).