УДК 342.95
DOI https://doi.org/10.32850/LB2414-4207.2021.22.17

СУЧАСНА КОНЦЕПЦІЯ ПРАВОВОГО РЕГУЛЮВАННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ

Мамедова Ельміра Алгаламівна,
ад'юнкт кафедри адміністративного права, процесу та адміністративної діяльності
(Дніпропетровський державний університет внутрішніх справ,
м. Дніпро, Україна)
https://orcid.org/0000-0001-9199-4431

Захист інформаційних систем державних органів та суб'єктів господарювання, які обробляють значну частину офіційної інформації та персональних даних громадян, не відповідають вимогам законодавства, що збільшує ризики втручання у такі системи, загрожує конфіденційності, недоторканності наявної інформації в реєстрах, базах даних, яка покликана задовольнити потреби та забезпечити гарантовані Конституцією інтереси громадян, суспільства та держави. У статті розкриваються проблеми формування сучасної концепції правового регулювання кібербезпеки в Україні. З'ясовано, що формування сучасної концепції правового регулювання кібербезпеки в Україні повинно здійснюватися з урахуванням потреб держави та прав громадян, дотримання верховенства права, засобів правового захисту, поваги до основних цінностей, прав людини та особи на свободу вираження поглядів, однаковий захист загальновизнаних основних прав. У статті було досліджено правову основу кібербезпеки, України котра визначає відповідальність, пріоритети та цілі забезпечення кібербезпеки України з метою формування умов безпечного функціонування кіберпростору, його використання в інтересах особистості, суспільства та держави. Кібербезпека є одним із найважливіших пріоритетів системи національної безпеки України. Цей пріоритет був досліджений та запропонований до реалізації шляхом посилення спроможності Національної системи кібербезпеки протидіяти кіберзагрозам у сучасному середовищі безпеки. Встановлено, що з причин складності кібернетичної сфери в умовах інформаційної глобалізації сучасних загроз кібербезпеці існує нагальна необхідність розвитку системи забезпечення кібербезпеки України, звернено увагу на потребу сформування відповідної правової, організаційної, технологічної моделі її функціонування та застосування, яка неможлива без ефективної взаємодії ключових суб'єктів національної системи кібербезпеки. Визначені пріоритети та шляхи підвищення якості сучасної недосконалої законодавчої бази у сфері кібербезпеки з урахуванням поточних вад: застарілість у сфері захисту інформації, повільна імплементація європейського законодавства у внутрішнє законодавство, недостатнє регулювання цифрового компоненту кримінальних розслідувань, а також низький рівень юридичної відповідальності за порушення законодавства у цій сфері.

Ключові слова: кібербезпека України, кібершпигунство, Національна поліція України, кібертероризм, кіберзагроза.

MODERN CONCEPT OF LEGAL REGULATION OF CYBERSECURITY IN UKRAINE

Mamedova Elmira Alhalamivna,
Adjunct at the Department
of Administrative Law, Process
and Administrative Activities
(Dnipropetrovsk State University
of Internal Affairs, Dnipro, Ukraine)

Protection of information systems of state bodies and economic entities that process a significant part of official information and personal data of citizens does not meet the requirements of legislation that increases the risk of interference in such systems, threatens confidentiality, inviolability of information in registers, databases needs and ensure the interests of citizens, society and the state guaranteed by the Constitution. The problems of formation of the modern concept of legal regulation of cybersecurity in Ukraine are revealed. It was found that the formation of a modern concept of legal regulation of cybersecurity in Ukraine should take into account the needs of the state and the rights of citizens, respect for the rule of law, remedies, respect for fundamental values, human and individual rights to freedom of expression, equal protection of universally recognized fundamental rights. The article examines the legal basis of cybersecurity in Ukraine, which defines the responsibilities, priorities and objectives of cybersecurity in Ukraine in order to create conditions for the safe functioning of cyberspace, its use in the interests of the individual, society and state. Cybersecurity is one of the most important priorities of Ukraine's national security system. This priority has been explored and proposed for implementation by strengthening the capacity of the National Cyber Security System to counter cyber threats in today's security environment. It is established that due to the complexity of the cyber sphere in the context of information globalization of modern cybersecurity threats there is an urgent need to develop a cybersecurity system in Ukraine. of the national cybersecurity system. Priorities and ways to improve the current imperfect legal framework in the field of cybersecurity, taking into account current shortcomings: obsolescence in the field of information protection, slow implementation of European legislation in domestic law, insufficient regulation of the digital component of criminal investigations, and low legal liability for violations.

Key words: cybersecurity of Ukraine, cyber espionage, National Police of Ukraine, cyberterrorism, cyber threat.

Постановка проблеми. З 2014 року Росія активно використовує кіберпростір у гібридній агресії проти України, надаючи руйнівний вплив на органи державної влади, оборону та системи контролю над озброєннями сил оборони, а також на критичну інфраструктуру. Держава-агресор постійно збільшує арсенал кіберзброї для наступальних, розвідувальних та диверсійних цілей, застосування якої може спричинити непоправні, незворотні руйнівні наслідки. Ці фактори вимагають постійного збільшення можливостей кібербезпеки з боку сектору безпеки та оборони. Як зазначала Г.О. Блінова, держава має виступити ініціатором та гарантом ефективного розвитку і використання інформаційного простору України, особливо в оборонній сфері. Захист повинен бути багаторівневий, що забезпечує розмежування допуску суб'єктів, з різними правами щодо інформації з обмеженим доступом, а також передбачає алгоритми дій військовослужбовців з відомостями військового характеру, що складають державну таємницю, дотримання яких дасть змогу не допустити незаконного розголошення державної таємниці чи втрати її носіїв, навіть під час активних військових дій [1, с. 85; 2, с. 161].

Надзвичайно актуальною загрозою сьогодні є розвідувальна та диверсійна діяльність у кіберпросторі проти України, яка пов'язана з розвідувальними службами іноземних держав, насамперед Російської Федерації, розвідувальною діяльністю з викрадення інформації (кібершпигунством) та диверсійними діями, що порушують регулярну роботу критично важливих об'єктів інформаційної інфраструктури, насамперед урядові системи, електроенергетика, транспорт, ядерна та хімічна промисловість, банківська справа, також загрозою є відсутність правового регулювання забезпечення кібербезпеки в державі. Крім того, більшого поширення набуває використання кіберпростору для інших злочинів проти основ національної безпеки, відмивання грошей, торгівлі людьми, незаконного обігу зброї, наркотиків та інших предметів і речовин, що загрожують життю та здоров'ю людей. Ситуація ускладнюється низьким рівнем кіберграмотності населення, зокрема звичайних користувачів електронних послуг.

Приймаючи рішення щодо автоматизації процесів державного управління, органи державної влади не завжди оцінюють ризики, що виникають у кіберзахисті публічних інформаційних ресурсів. Захист інформаційно-комунікаційних систем державних органів та суб'єктів господарювання, які обробляють значну частину офіційної інформації та персональних даних громадян, не відповідає вимогам законодавства, що збільшує ризики втручання у такі системи, загрожує конфіденційності, недоторканності та наявність інформації (реєстри, бази даних), яка покликана задовольнити потреби та забезпечити гарантовані Конституцією інтереси громадян, суспільства та держави.

Аналіз публікацій, у яких започатковано вирішення цієї проблеми. Дослідженням питань правового регулювання забезпечення кібербезпеки в Україні займались такі вчені, як Є.Д. Бондаренко, В.В. Бухарев, В.О. Єльцов, Д.П. Кисленко, Н.В. Рудевіч, Г.М. Шорохова та інші науковці. Проте натепер відсутня сучасна узгоджена концепція правового регулювання кібербезпеки в Україні.

Мета статті – визначення ознак, особливостей правового регулювання захисту кіберпростору в Україні для оборони суверенітету держави та захисту суспільства від шкідливої інформації, забезпечення правового захисту прав, свобод та законних інтересів громадян України у кіберпросторі, реалізації цілей Європейської та євроатлантичної інтеграції України у сфері кібербезпеки.

Виклад основного матеріалу. XXI століття відзначається активним формуванням шостої технологічної сфери (біо-, нано-, інфо-, когнотехнології, їх конвергенція) та ризиками, з якими стикається цивілізація через впровадження нових технологій, зокрема їх використання в кіберпросторі. Роль кіберзагроз у спектрі загроз національній безпеці зростає, і ця тенденція буде посилюватися в міру розвитку інформаційних технологій та їхнього зближення з технологіями штучного інтелекту протягом наступного десятиліття. Зростання такого впливу на функціонування управлінських структур, як національних, так і транснаціональних, формує абсолютно нову ситуацію безпеки з викликами нового технологічного рівня. У кіберпросторі існує поділ сфер впливу між світовими центрами сили, і їхнє бажання забезпечити реалізацію власних геополітичних інтересів зростає.

Кіберпростір поряд з іншими фізичними областями визнається одним із можливих областей військової операції, тому здатність держави захищати національні інтереси в ньому розглядається як важлива складова кібербезпеки [3]. Тенденція створення нового виду сил – кіберсил, метою яких є не тільки захист критичної інформаційної інфраструктури від кібератак, а й проведення профілактичних наступальних операцій у кіберпросторі, спрямованих на знищення комп'ютерних мереж та інформаційних систем ворожих сил, а також виведення з системи критичних об'єктів противника шляхом знищення інформаційних систем, які керують такими об'єктами.

Як зазначив українські вчені В.М. Брижко, В.М. Фурашев у своєму дослідженні: «інформаційно-комп'ютерні технології сумісно з машиною-комп'ютером уже давно використовується не стільки як засіб, винайдений для прискорення розрахунків, а як електронно-інформаційний інструмент, який розширює можливості людини в обробці великої й різноманітної кількості даних, відборі інформації та прийнятті рішень на основі безлічі різних відомостей» [4, с. 62].

Насамперед прогнозується зростання інтенсивності міждержавного протистояння та розвідувально-диверсійної діяльності у кіберпросторі, що проявиться перш за все в розширенні кола держав, які намагатимуться формувати власний кібер-інтелект, освоювати сучасні технології розвідувальної та диверсійної діяльності в кіберпросторі та посилити державний контроль над Інтернетом. Водночас набуде поширення розробка інструментів, які ґрунтуються на накопиченні великої кількості даних про поведінку людей, соціальних групах та на використанні сучасних досягнень у галузі штучного інтелекту.

Негативною ознакою правового розвитку, пов'язаного з широким розповсюдженням цифрових технологій, розширенням Інтернет -середовища, є критично зростаючий технічний рівень інструментів реалізації кіберзагроз, а ландшафт таких загроз охоплює все більше сфер життя як результат. Кібератаки, їхні різновиди стають усе більш розумними та небезпечними, створюючи реальну загрозу критичним інфраструктурам. Зловмисники зосереджуються на пошуку вразливостей в активах (системах управління) та розробці унікальних функцій: багатофункціональних шкідливих програм, програм-вимагачів, ботнетів, які виконують розподілені атаки (DDoS) на операційні мережі, виробничі системи, що використовують хмарні послуги, атаки на ланцюжки поставок. Враховуючи розвиток технологій штучного інтелекту в найближчі 5–10 років, масштаби та наслідки таких втручань збільшаться [5].

Використання кіберпростору терористичними організаціями (кібертероризм) набуває глобального масштабу. Цьому сприятиме всебічна цифрова трансформація систем управління та засобів до існування, яка спричинює постійне розширення цільової аудиторії кібертероризму та кола потенційних цілей кібератак. Пріоритетними об'єктами кібератак терористів є об'єкти ядерної енергетики, потужні сховища для стратегічної сировини, системи управління електропостачанням, повітряний та залізничний транспорт, системи водопостачання, хімічні та біологічні об'єкти. Нові виклики несуть перехід до мереж 5G, робота яких залежить від правильної роботи програмного забезпечення, яке через новизну технологій може мати нові, не повністю передбачені загрози. Такі технології, як «Інтернет речей», «доповнена реальність», «розумне місто», активно доповнюються новими – «гіперавтоматизація», «розумно організований бізнес», «мережа кібербезпеки», «розподілена хмара», «поведінка в Інтернеті» тощо.

Докорінно змінивши світовий порядок, пандемія коронавірусу COVID-19 матиме довгостроковий вплив на нього. Зростає залежність від цифрових комунікацій, що робить процес обміну інформацією, захисту інформації та персональних даних уразливим. Кіберзлочинці, максимально використовуючи пандемію, з моменту її заснування все частіше застосовували нові методи кібератак, змушуючи національні уряди впроваджувати додаткові заходи протидії, підтримувати доступ до необхідних пристроїв та забезпечувати належне функціонування всіх електронних ресурсів та систем.

На нашу думку, правове регулювання забезпечення кібербезпеки в Україні є дуже складним етапом сталого розвитку у кіберпросторі. Документами, що місять принципи формування та реалізації державної інформаційної політики, зокрема пов'язані з протидією деструктивному зовнішньому інформаційному впливу, є Концепції

розвитку цифрової економіки та суспільства України на 2018–2020 роки та плану заходів щодо її реалізації Розпорядженнями Кабінету Міністрів України від 20 вересня 2017 року [6], від 8 листопада 2017 року № 797-р [7] та від 17 січня 2018 року № 67-р [8], а також Укази Президента України від 14 вересня 2020 року № 392/2020 «Про Стратегію національної безпеки України», від 15 березня 2016 року № 96/2016 «Про рішення Ради національної безпеки і оборони України», від 27 січня 2016 року «Про Стратегію кібербезпеки України» [9; 10; 5] тощо.

Ми вважаємо, що стратегія кібербезпеки України, котра була прийнята у 2016 році [10], стала важливим кроком у впровадженні підходів довгострокового планування в цій сфері, а отже, сам факт її прийняття став позитивним результатом. З роками були докладені зусилля для створення та розвитку національної системи кібербезпеки. Важливим етапом її інституціоналізації стало прийняття Закону України «Про основні засади кібербезпеки України» [11], що є правовою основою створення національної системи кібербезпеки та її основних суб'єктів у сфері кібербезпеки.

Наразі також покращено нормативне забезпечення кібербезпеки критично важливої інформаційної інфраструктури, прийнято процедуру її визначення та загальні вимоги до її кібербезпеки. Центри (підрозділи) з кібербезпеки або кіберзахисту створені в Державній службі спеціального зв'язку та захисту інформації України, Службі безпеки України, Національному банку України, Міністерстві інфраструктури України та Міністерстві оборони Україна. Розвивається Національна телекомунікаційна мережа, функціонують захищені центри обробки даних, формується Національний центр резервування державних інформаційних ресурсів, запускається система виявлення вразливих місць та реагування на кіберінциденти та кібератаки. Водночас діяльність суб'єктів національної системи кібербезпеки залишається недостатньо скоординованою та спрямованою на виконання лише поточних завдань.

Правові основи сьогодення дають змогу виявляти низку юридичних проблем, які або ускладнюють, або перешкоджають ефективній реалізації кібербезпеки в Україні. На думку української вченої Н.І. Логінової, правові основи кібербезпеки закладені в національне законодавство України, але необхідно внести істотні зміни до чинних нормативно-правових актів та розробити нові, також однією з проблем була відсутність чіткості у визначених пріоритетах та сферах кібербезпеки в Україні, більшість із яких не мала чіткої кінцевої мети та не була конкретною [12, с. 576]. Ця проблема була вирішена у Стратегії кібербезпеки України 2021 року. Окрім того, показники реалізації Стратегії кібербезпеки України 2016 року не розроблені, що ускладнило процес оцінки її ефективності та виявлення невиконаних завдань. Представники сектору безпеки та оборони в основному брали участь у реалізації Стратегії кібербезпеки України 2016 року, інші міністерства та відомства, наукові установи та громадськість були залучені недостатньо. Навчальні та науково-дослідні установи не проводили достатню роботу з реалізації завдань, пов'язаних з розвитком наукового потенціалу та поширенням кіберграмотності. Ці недоліки необхідно врахувати та усунути під час реалізації Стратегії кібербезпеки України 2021 року.

У преамбулі Закону України «Про основні засади забезпечення кібербезпеки України» визначено, що він закріплює основні цілі державної політики у сфері кібербезпеки, проте окремої статті, яка б їх закріплювала, немає. Таким чином, це стало однією з виявлених і закріплених у Стратегії кібербезпеки України проблем, яка полягає в недостатній чіткості визначених пріоритетів та напрямів забезпечення кібербезпеки України, значна частина яких не мала зрозумілої кінцевої мети та не була конкретною [3]. На наш погляд, це зумовлює й відсутність конкретизованої мети і завдань державної політики у сфері кібербезпеки.

У статті 31 «Стратегія кібербезпеки України» Закону України «Про національну безпеку України» визначено, що Стратегія кібербезпеки України є документом довгострокового планування, у якому визначаються пріоритети національних інтересів України у сфері кібербезпеки, наявні та потенційно можливі кіберзагрози життєво важливим інтересам людини і громадянина, суспільства та держави в кіберпросторі, пріоритетні напрями, концептуальні підходи до формування та реалізації державної політики щодо безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави, підвищення ефективності основних суб'єктів забезпечення кібербезпеки, насамперед суб'єктів сектору безпеки і оборони, щодо виконання завдань у кіберпросторі, а також потреби бюджетного фінансування, достатні для досягнення визначених цілей і виконання передбачених завдань, та основні напрями використання фінансових ресурсів. Також Стратегія кібербезпеки України є основою для підготовки державних програм та нормативно-правових актів, що стосуються забезпечення кібербезпеки України [13]. Таким чином, Стратегія кібербезпеки України є тим документом, який розкриває цілі, задачі та зміст державної політики у сфері кібербезпеки України.

У законодавстві визначена мета Стратегії кібербезпеки України – створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави, а також визначено стратегічні завдання, які, на наш погляд, і відображають завдання державної політки у сфері кібербезпеки в Україні: 1) формування системи дієвої кібероборони; 2) ефективної протидії розвідувально-підривній діяльності у кіберпросторі та кібертероризму; 3) посилення спроможності у протидії кіберзлочинності; 4) запровадження асиметричних інструментів стримування; 5) убезпечення кіберпростору задля захисту суверенітету держави та розвитку суспільства; 6) захист прав, свобод і законних інтересів громадян України у кіберпросторі; 7) європейська і євроатлантична інтеграція у сфері кібербезпеки [3].

На наш погляд, посилюється висока технологічна залежність України від іноземних виробників продуктів програмного забезпечення для управління, відсутність сучасних національних стандартів щодо вимог безпеки для ланцюга поставок відповідного обладнання, розробка програмного забезпечення та інформаційно-комунікаційних систем, сертифікація чи системи оцінки відповідності для безпеки таких продуктів, ступінь вразливості військової, політичної, фінансової, економічної та промислової інфраструктури держави від шкідливих та незадекларованих функцій у такому обладнанні та звуження внутрішнього потенціалу для протидії кіберзагрозам.

Популярні вебсайти, соціальні мережі, реєстри збирають велику кількість ідентифікаційних даних користувачів та особистих даних. Витоки інформації з належних їм баз даних становлять загрозу для використання цих даних для атаки на інші ресурси та інформаційні системи. Ми вважаємо, що недосконала законодавча база у сфері кібербезпеки, а також її застарілість у сфері захисту інформації, повільна імплементація європейського законодавства у внутрішнє законодавство, недостатнє регулювання цифрового компоненту кримінальних розслідувань, а також низький рівень юридичної відповідальності за порушення законодавства в цій сфері, відсутність відповідних міністерств та відомств (немає відповідних структурних підрозділів, необхідного персоналу та належного контролю за кібербезпекою) становить загрозу для кібербезпеки України. Фінансування роботи з кібербезпеки, що здійснюється за залишковою ознакою з технологічними помилками, недотримання сучасних вимог до рівня підготовки та підвищення кваліфікації фахівців у галузі кібербезпеки та кіберзахисту, відсутність системи підвищення цифрової грамотності громадян та культури безпечної поведінки в кіберпросторі – це лише деякі проблеми, з якими сьогодні стикається Україна.

Європейський парламент для протидії таким негативним сучасним викликам ухвалив низку документів, серед яких Резолюція «Стратегічні комунікації Європейського Союзу як протидія пропаганді третіх сторін» [14], Директива Європейського Парламенту і Ради «Про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу» [15], Регламент Європейського парламенту і Ради «Про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних)» тощо [16].

Слід погодитись із Г.М. Шорохом, що сьогодні важко уявити роботу будь-якого з підрозділів Національної поліції України без інформаційної підтримки та інформаційного забезпечення, накопичення та систематизації інформації в базах даних [18, с. 246]. Г.О. Блінова наголошує, що для виконання покладених на правоохоронні органи функцій, відповідно до положень про їх правовий статус, вони мають право одержувати від державних органів та органів місцевого самоврядування, підприємств, установ, організацій усіх форм власності, інших юридичних осіб та їх посадових осіб, фізичних осіб-підприємців інформацію, документи і матеріали, необхідні для виконання покладених на них завдань, а також користуватися відповідними інформаційними базами даних державних органів, державними, зокрема урядовими, системами зв'язку і комунікацій, мережами спеціального зв'язку та іншими технічними засобами. Це свідчить про провідну роль інформаційної складової в роботі цих органів. Значний масив інформації, що використовується ними в процесі роботи, носить конкретизований характер, зумовлений використанням персональних даних окремих фізичних осіб, що потрапляють до правоохоронних органів шляхом реалізації адміністративних правовідносин [1, с. 62]. Практика використання засобів інформаційного забезпечення працівниками поліції свідчить про труднощі організаційного, правового та технічного характеру, що супроводжують цей процес. Унаслідок реалізації ризиків зниження рівня інформаційного забезпечення, інформаційної безпеки та кібербезпеки підрозділів та працівників Національної поліції значно знижується їхня ефективність.

З точки зору розробки стандартів у галузях нових технологій (включаючи штучний інтелект, хмарні технології, квантові обчислення та квантові комунікації), Інтернет повинен залишатися глобальним та відкритим, технології повинні бути людськими, забезпечувати його основні свободи, гарантувати користувачеві невтручання в його особисте життя, забезпечити його конфіденційність у кіберпросторі, і будь-які обмеження в цій частині повинні виконуватися лише відповідно до законодавства. Використання технологій має бути законним, безпечним та етичним. Водночас через складність міжнародної безпеки в кіберпросторі Україна займе більш активну позицію в дискусіях в ООН та на інших міжнародних форумах із метою просування, координації та закріплення української правової позиції у кіберпросторі, зменшення небезпеки кібервійни.

Забезпечення кібербезпеки України як стану захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі, що досягається комплексним застосуванням сукупності правових, організаційних, інформаційних заходів, як вважає Г.О. Блінова, має базуватися на принципах: 1) верховенства права і поваги до прав та свобод людини і громадянина; 2) забезпечення національних інтересів України; 3) відкритості, доступності, стабільності та захищеності кіберпростору; 4) державно-приватного партнерства, широкої співпраці з громадянським суспільством у сфері забезпечення кібербезпеки та кіберзахисту; 5) пропорційності та адекватності заходів кіберзахисту реальним та потенційним ризикам; 6) пріоритетності

запобіжних заходів; 7) невідворотності покарання за вчинення кіберзлочинів; 8) пріоритетного розвитку та підтримки вітчизняного наукового, науково-технічного та виробничого потенціалу; 9) міжнародного співробітництва з метою зміцнення взаємної довіри у сфері кібербезпеки та вироблення спільних підходів у протидії кіберзагрозам, консолідації зусиль у розслідуванні та запобіганні кіберзлочинам, недопущенні використання кіберпростору в протиправних та воєнних цілях; 10) забезпечення демократичного цивільного контролю над утвореними відповідно до законів України військовими формуваннями та правоохоронними органами держави, що діють у сфері кібербезпеки [10]. Усі зазначені принципи, на думку Г.О. Бліновой, повинні знайти своє відображення у Законі України «Про інформаційне забезпечення органів публічної адміністрації» [1, с. 85]. Водночас ми вважаємо, що ці принципи повинні бути відображені й у Законі України «Про основні засади кібербезпеки України».

Враховуючи взаємопов'язаність сучасного кіберпростору та з метою розвитку співпраці між державою, приватним сектором, науковими колами та громадянським суспільством у сфері кібербезпеки, сьогодні Україна намагається розвивати національний кіберпростір як глобальний, відкритий, вільний, правовий і насамперед безпечний, що є запорукою успішного розвитку країни.

Висновки та пропозиції. Отже, ми робимо висновки, що Україна не тільки повинна створювати та розвивати ефективні (правові, кадрові та технологічні сили), які мають повноваження вести збройний конфлікт у кіберпросторі, а й сформувати відповідну правову, організаційну, технологічну модель їхнього функціонування та застосування, яка неможлива без ефективної взаємодії ключових суб'єктів національної системи кібербезпеки та сил оборони під час діяльності з кіберзахисту, належної підготовки та фінансової підтримки таких структур, систематичної підготовки з кібербезпеки, оцінки можливостей та ефективності підрозділів, розробки та впровадження показників для оцінки їхньої ефективності.

Спираючись на зазначене вище, вважаємо, що формування сучасної концепції правового регулювання кібербезпеки в Україні повинно здійснюватися з урахуванням таких аспектів: 1) збалансоване забезпечення потреб держави та прав громадян, дотримання верховенства права, процесуальних гарантій та засобів правового захисту, повага до основних цінностей, прав людини та особи на свободу вираження поглядів, однаковий захист загальновизнаних основних прав онлайн та офлайн; засудження практики перевищення встановлених меж необхідності обмеження прав громадян та юридичних осіб при використанні кіберпростору та технологій інформаційно-комунікаційних технологій; 2) посилення можливості національної системи кібербезпеки для запобігання збройній агресії проти України у кіберпросторі або з її використанням, нейтралізація розвідувальної та підривної діяльності, мінімізація загроз кіберзлочинності та кібертероризму (стримування); 3) забезпечення розвитку комунікації, координації та партнерства між суб'єктами кібербезпеки на національному рівні, в нормативно-правовому аспекті, розвиток стратегічних відносин у сфері кібербезпеки з ключовими іноземними партнерами, особливо з Європейським Союзом та НАТО та їхніми державами-членами, співпраця в цій сфері з іншими державами та міжнародними організаціями на основі національних інтересів України (взаємодія); 4) проведення щорічних кібернавчань на стратегічному рівні за участю представників державного та приватного секторів для корегування та закріплення правових позицій держави.

Список використаних джерел:

1. Блінова Г.О. Адміністративно-правові засади інформаційного забезпечення органів публічної адміністрації в Україні: актуальні питання теорії та практики : дис. … докт. юрид. наук. Запоріжжя. 2019. 458 с. С. 85.

2. Макушев П.В., Блінова Г.О. Розголошення відомостей військового характеру як загроза національній безпеці України. *Військові злочини: кримінально-правова, криміналістична та кримінологічна характеристика* : монографія. Херсон : Херсонський національний університет. 2015. С. 150–172.

3. Стратегія кібербезпеки України. Безпечний кіберпростір – запорука успішного розвитку країни : Указ Президента України від 26 серпня 2021 року № 447/2021. *База даних «Законодавство України».* URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text

4. Брижко В.М., Фурашев В.М. Конвергенція новітніх технологій: стан і перспективи змін у інформаційних відносинах. *Інформація і право.* 2017. № 1. С. 51–67. URL: http://nbuv.gov.ua/UJRN/Infpr_2017_1_8.

5. Draft of the Cybersecurity Strategy of Ukraine (2021-2025) (Unofficial English translation) URL: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeka-Eng.docx.

6. Про схвалення Концепції розвитку електронного урядування в Україні : розпорядження Кабінету Міністрів України від 20 вересня 2017 р. № 649-р. *Урядовий кур'єр.* 2017. № 181.

7. Про схвалення Концепції розвитку електронної демократії в Україні та плану заходів щодо її реалізації : розпорядження Кабінету Міністрів України від 8 листопада 2017 р. № 797-р. *Урядовий кур'єр.* 2017. № 217.

8. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018–2020 роки та затвердження плану заходів щодо її реалізації: Розпорядження Кабінету Міністрів України від 17 січня 2018 р. № 67-р. *Урядовий кур'єр.* 2018. № 88.

9. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України» : Указ Президента України від 14 вересня 2020 р. № 392/2020. *База даних «Законодавство України».* URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text

10. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : Указ Президента України від 15 березня 2016 р. № 96/2016. *Урядовий кур'єр.* 2016. № 52.

11. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 року № 2163-VIII. *База даних «Законодавство України».* URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

12. Логінова Н.І. Правові основи кібербезпеки в Україні. *Правові та інституційні механізми забезпечення розвитку держави та права в умовах євроінтеграції* : матеріали Міжнародної науково-практичної конференції (20 травня 2016 р., м. Одеса) : у 2 т. Т. 1 / відп. ред. М.В. Афанасьєва. Одеса : Юридична література, 2016. С. 575–577.

13. Про національну безпеку України : Закон України від 21 червня 2018 р. № 2469-VIII. *База даних «Законодавство України».* URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text

14. Міжнародний досвід протидії гібридним загрозам: законодавче регулювання та організації з питань стратегічних комунікацій : інформаційна довідка, підготовлена Європейським інформаційно-дослідницьким центром на запит народного депутата України. URL: http://euinfocenter.rada.gov.ua/uploads/documents/29377.pdf.

15. Про заходи для високого спільного рівня безпеки мережевих та інформаційних систем Директива Європейського Парламенту і Ради : Наказ МВС № 73 на тери-

торії Союзу : від 6 липня 2016 р. № 2016/1148. *Офіційний вісник Європейського Союзу* від 19 липня 2016 р. 2016 р. L 194. С. 1.

16. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). URL: http://eurlex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32016R0679&from=ENм.

17. Інформаційне забезпечення та кібербезпека патрульної поліції: співвідношення понять. URL: https://er.dduvs.in.ua/xmlui/handle/123456789/6101.

18. Блінова Г.О., Мамедова Е.А. Інформаційне забезпечення та кібербезпека патрульної поліції: співвідношення понять. *Науковий вісник Дніпропетровського державного університету внутрішніх справ.* 2020. № 4. С. 15–24.