АДМІНІСТРАТИВНЕ ПРАВО І ПРОЦЕС; ФІНАНСОВЕ ПРАВО; ІНФОРМАЦІЙНЕ ПРАВО

УДК 349
DOI https://doi.org/10.32782/TNU-2707-0581/2022.4/05

Гнедюк В.Л.
Український науково-дослідний інститут спеціальної техніки та судових експертиз Служби безпеки України

ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ: ОРГАНІЗАЦІЙНО-ПРАВОВІ АСПЕКТИ

Статтю присвячено дослідженню сутності поняття «кібербезпека», розглянуто вектори досліджень в області забезпечення кібербезпеки. В дослідженні проаналізовані наслідки безконтрольного розповсюдження і використання інформаційного і кіберпросторів. Надано характеристику Стратегії кібербезпеки України, яка була прийнята в 2021 році указом Президента України. Перелічено можливості для забезпечення кібербезпеки в Україні, які виникнуть внаслідок реалізації Стратегії, на основі її результатів, за співробітництва з приватним сектором і міжнародними організаціями. В Стратегії, як у документі тривалого проектування, зазначені пріоритети національних інтересів нашої держави в області кібербезпеки, існуючі та ймовірно можливі кібернебезпеки життєво необхідним інтересам особи, громадянина, народу та країни в кіберпросторі, пріоритетні вектори, доктринальні підходи до створення та виконання політики держави стосовно безпечної діяльності кіберпростору, його застосування в інтересах людини, народу і країни, підвищення рівня продуктивності головних суб'єктів забезпечення кібербезпеки, в першу чергу суб'єктів сектору безпеки й оборони, з питань вирішення задач у кіберпросторі, а також необхідності фінансування з бюджету, достатнє для здійснення окреслених завдань і вирішення передбачених задач, та ключові вектори використання фінансового потенціалу.

Також окреслено організаційні, правові і технічні проблемні питання кібербезпеки. Зазначено рекомендації для забезпечення кібербезпеки України з метою гарантування інформаційного захисту. Основними з яких є інформаційна, організаційно-технічна та ресурсна допомога державі національним засобам масової інформації, що створюють у міжнародному інформаційному просторі гарну репутацію для України; підтримка формування і дотримання міжнаціональних норм поведінки країн в інформаційному полі; удосконалення міждержавного співробітництва в області забезпечення інформаційної безпеки на загальнонаціональному та відомчому рівнях. Найбільш багатообіцяючими векторами розвитку національної системи кібербезпеки є: покращення правового базису кіберохорони об'єктів критичної інфраструктури; запровадження порядку незалежної перевірки інформаційної безпеки на об'єктах критичної інфраструктури; формування галузевих пунктів реагування на інциденти кібербезпеки тощо.

Ключові слова: *кіберпростір, кібератаки, кібербезпека, стратегія, цифровізація, інформаційне поле, кіберфізичні системи.*

Постановка проблеми. Державна політика України в галузі національної безпеки й оборони направлена на забезпечення військової, зовнішньополітичної, економічної, інформаційної, екологічної безпеки, кібербезпеки і т.д. В рамках державного сегменту кіберпростору країни, в тому числі з ціллю захисту прав, свобод і законних інтересів людини та громадянина в області кібербезпеки, національна кібербезпекова політика як основа гарантування інформаційної безпеки України виступає наслідком досягнення інших соціальних та економічних цілей народу і держави у найбільш важливих сферах життєдіяльності. Ключовим механізмом забезпечення

і гарантування національної кібербезпеки виступає встановлення та укріплення національних, регіональних і міждержавних партнерських відносин в області кібербезпеки, забезпечення охорони від кібератак, мінімізація їх наслідків, розслідування останніх, відновлення після заподіяної ними шкоди, в тому числі за допомогою проведення колективних освітніх програм із використанням або формуванням належних інформаційних мереж зв'язку чи екстреного обміну інформаційних даних про такі загрози. Таким чином, в актуальному середовищі кібербезпека виступає домінантним об'єктом правового регулювання і потребує ретельного дослідження як явище, що пронизує усі найголовніші правові відносини в країні.

Аналіз останніх досліджень і публікацій. Проблемі забезпечення кібербезпеки в Україні присвячено праці багатьох дослідників, таких як: Бурячок В. Л., Богуш В. М., Гаращенко Ю. В., Лахтадир С. Л., Лісовська Ю. П., Марущак А. І., Сліпченко Т. О., Федченко Д. І. та багато інших. Разом з цим питання організаційно-правових аспектів забезпечення кібербезпеки в Україні потребує детальнішого аналізу.

Цілі статті. Завданнями наукового дослідження є:

– розтлумачити термін «кібербезпека»;

– розглянути вектори досліджень в області забезпечення кібербезпеки;

– проаналізувати наслідки безконтрольного розповсюдження і використання інформаційного і кіберпросторів;

– дати характеристику Стратегії кібербезпеки України;

– окреслити організаційні, правові і технічні проблемні питання кібербезпеки;

– вказати рекомендації для забезпечення кібербезпеки України з метою гарантування інформаційного захисту.

Виклад основного матеріалу. В процесі стрімких, динамічних видозмін і вдосконалень інформаційного суспільства в країні та глобального інформаційного поля, прослідковується активізація застосування інформаційних і комунікаційних технологій в усіх сферах життєдіяльності, приймають небезпечних наслідків для держави проблеми інформаційної безпеки.

Внаслідок відсутності ефективного механізму дотримання і гарантування інформаційної безпеки у національному інформаційному просторі нашої держави прослідковується багато негативних фактів, що провокують появу реальних та прихованих небезпек інформаційній безпеці індивіда, народу та країни.

Це має місце на фоні потужного й агресивного інформаційного наступу російської пропаганди, яка наперекір європейським шаблонам у галузі ЗМІ активізує в нашій державі міжнаціональне протистояння і сепаратистські погляди, посягає на суверенітет і територіальну цілісність нашої країни [3, с. 140].

Нині існує велика кількість визначень терміну «кібербезпека», наприклад:

– кібербезпека – це комплекс належних відповідних способів стосовно зменшення рівня мінімізація ризиків;

– кібербезпека – це охорона кіберфізичних систем від шкідливого та невірного їх застосування, а також від інших руйнівних форсувань;

– кібербезпека – це метод охорони від великої кількості кібернебезпек (до яких відносяться заходи з ушкодження інформаційних ресурсів, вилучення чужих інформаційних даних і т.д.);

– кібербезпека – це охорона інформаційних систем, що відносяться до складу кіберпростору, від нападів, гарантування конфіденційності, цілісності, а також доступності інформаційних даних, які форматуються в цьому просторі, запобігання та боротьба з атаками і кіберзлочинами;

– кібербезпека – охорона кіберфізичних систем від шкідливого невірного застосування і реалізації, а також від інших злочинів [8, с. 77–78].

– Закон України «Про основні засади забезпечення кібербезпеки України» окреслює організаційно-правові засади гарантування охорони життєво необхідних інтересів особистості і громадянина, народу і країни, національних інтересів нашої держави в кіберпросторі, головні задачі, вектори та стандарти політики країни в області кібербезпеки, повноваження органів державної влади, підприємств, установ, організацій, осіб та громадян в цій галузі, ключові базиси координування їх діяльності із забезпечення комп'ютерної безпеки [1].

Звертаючи увагу на вирішення проблемних питань кібербезпеки, потрібно зважати на достатньо серйозний її аспект, а саме на взаємозалежність учасників, іншими словами користувачів, який може породити синергетичний ефект. Потрібні скрупульозні, систематичні дослідження якостей кіберпростору, динаміки його вдосконалення, способів регулювання цієї динаміки. Надзвичайно тяжко, майже неможливо конструювати справді результативну систему кібербезпеки без її системного дослідження, саме тому необхідно

додати в сукупність досліджень у сфері кібербезпеки такі вектори як:

– формування комплексу показників діяльності інформаційного простору та його охорони від можливих небезпек і атак;

– конструювання моделей інформаційного віртуального простору і чинників, які здійснюють вплив на його діяльність;

– розробка спеціальних способів дотримання і гарантування стійкості кіберпростору при наявності небезпек і атак;

– розробка інтелектуальних способів гарантування комп'ютерної безпеки (метод ситуативного дослідження стану).

– вдосконалення процесу кібербезпеки, новітні способи криптографічної охорони, інтелектуальні способи запобігання системних атак, способи інтелектуальної ідентифікації користувачів в процесі кібератаки) [7, с. 130].

Безконтрольне розповсюдження і невичерпне використання інформаційного і кіберпросторів на протязі останніх років:

– спричинило підвищення рівня уразливості інформаційної сфери майже у всіх державах для чужого, невідомого кібернетичного впливу;

– означило політичну потребу у нагляді і майбутній регламентації відносин у цій сфері;

– надало підвалини для засвідчення винятковості актуальності: процесів розшукування, збору і добування інформаційних даних у відкритих, відносно відкритих і закритих електронних джерелах; методів гарантування конфіденційності, цілісності та доступності власної IP-адреси, а також запобігання ціле направленому впливу зі сторони ймовірно можливих кібернетичних небезпек, інцидентів і загроз.

Беручи це до уваги та зважаючи на безперервно зростаючі ресурси для застосування мережі Internet з оборонно-воєнною метою, передові держави світу, такі як Китай, Франція, США, Японія, Велика Британія та багато інших на протязі останніх десятиріч динамічно модифікують власні сегменти сфери безпеки, в першу чергу кібербезпеки, надаючи при цьому першість проблемному питанню отримання інформаційної переваги в управлінні військовими збройними силами, а також модернізації нормативно-правової бази [9, с. 654].

Стратегія кібербезпеки України – це документ тривалого проектування, що характеризує загрози кібербезпеці країни, пріоритети та вектори дотримання і гарантування кібербезпеки держави з ціллю формування середовища для безпечної діяльності кіберполя, його застосування в інтересах індивіда, народу і країни.

В Стратегії, як у документі тривалого проектування, зазначені пріоритети національних інтересів нашої держави в області кібербезпеки, існуючі та ймовірно можливі кібернебезпеки життєво необхідним інтересам особи, громадянина, народу та країни в кіберпросторі, пріоритетні вектори, доктринальні підходи до створення та виконання політики держави стосовно безпечної діяльності кіберпростору, його застосування в інтересах людини, народу і країни, підвищення рівня продуктивності головних суб'єктів забезпечення кібербезпеки, в першу чергу суб'єктів сектору безпеки й оборони, з питань вирішення задач у кіберпросторі, а також необхідності фінансування з бюджету, достатнє для здійснення окреслених завдань і вирішення передбачених задач, та ключові вектори використання фінансового потенціалу. Процес проектування Стратегії кібербезпеки країни відбувається за дорученням Президента України Національним координаційним центром кібербезпеки після того як затверджується Стратегія національної безпеки України. Стратегія кібербезпеки України ухвалюється рішенням РНБО України та затверджується указом Президента України. Цей нормативний акт слугує базисом для створення державних програм, проектів та нормативно-правових актів, що стосуються забезпечення кібербезпеки України [5, с. 237].

В 2021 році була прийнята Стратегія кібербезпеки України. У вказаному правовому акті президент України Володимир Олександрович Зеленський визнав такою, що втратила чинність попередня Стратегія кібербезпеки, що була затверджена екс-Президентом України Петром Олексійовичем Порошенко в 2016 році.

В опублікованому тексті Стратегії зазначається, що забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки України і здійснення вказаного пріоритету буде виконуватися завдяки посиленню можливостей національної системи кібербезпеки для боротьби з кібернебезпеками у нинішньому безпековому середовищі.

В Стратегії зазначено, що Росія була і залишається однією з ключових осередків загроз національній та міжнаціональній кібербезпеці, стрімко виконує концепцію інформаційної боротьби, засновану на симбіозі руйнуючих дій у кіберпросторі і інформаційно-психологічних дій, інструменти якої динамічно використовуються у гібрид-

ній інформаційній війні проти нашої країни. Така руйнуюча активізація формує справжню, серйозну небезпеку здійснення актів кібертероризму та кібердиверсій щодо національної інформаційної інфраструктури.

Необхідно зазначити, що в Стратегії передбачений факт того, що пандемія COVID-19 буде мати довгостроковий вплив на світову організованість та системність, підвищуючи роль електронних комунікацій у щоденній комунікації та роботі, що збільшує рівень вразливості процесів обробки інформаційних даних, в першу чергу персональних даних. Це потребує гарантування відповідного рівня їх захищеності та примушує країну і бізнес вводити додаткові інструменти щодо якісного функціонування і охорони усіх потрібних для життя інформаційних ресурсів і систем.

В документі сказано, що Україна повинна бути спроможною забезпечити свій соціальний та економічний розвиток у світі тотальної цифровізації, що потребує набуття можливості продуктивно вдержувати руйнуючі дії в кіберпросторі, досягнення кіберстійкості на всіх рівнях та взаємодії всіх суб'єктів забезпечення кібербезпеки, яка засновується на довірі. В цьому випадку доцільним є затвердження цієї Стратегії кібербезпеки України» [10].

Координатором виконання цієї Стратегії є робочий орган РНБО України – Національний координаційний центр кібербезпеки.

Виконання Стратегії безпосередньо здійснюється головними суб'єктами національної системи кібербезпеки, Міністерством закордонних справ України, Міністерством цифрової трансформації України, Міністерством освіти і науки України та іншими суб'єктами гарантування кібербезпеки в рамках їх повноважень.

Результативність виконання Стратегії буде визначатися через систематичний аналіз її реалізації та спиратися на конкретний комплекс показників стану кібербезпеки, які буде розроблено на протязі першого року виконання Стратегії.

На основі результатів виконання Стратегії кібербезпеки України, країна у співробітництві з приватним сектором, а також за участю міжнародних партнерів забезпечить:

– витримку кібератак, збільшивши рівень можливості органів державної влади і місцевого самоврядування, бізнес-структур і народу охороняти себе та реагувати на кіберзагрози;

– можливість результативного попередження загрозливим діям у інформаційному просторі, забезпечивши їх стрімке виявлення та розслідування, формування продуктивного комплексу запобігаючих заходів щодо недопущення загрозливих дій, а також можливість здійснення наступальних дій у кіберпросторі;

– вдосконалення кадрових ресурсів та інноваційного ринку кібербезпеки, що впливатиме на пришвидшення формування державних розроблень на рівні кращих міжнародних прикладів для забезпечення можливості протистояти ймовірним кібератакам [2].

Наявні проблемні питання кібербезпеки, які є в країні розподіляються на види: організаційні, технічні (апаратні, інструментальні), правові, інформаційно-технологічні (програмні, алгоритмічні, тощо).

Поміж організаційних проблемних питань комп'ютерної безпеки виділити в першу чергу потрібно:

– відсутність належної налагодженої діяльності з підготовки підприємств, установ та організацій до кібератак;

– недостатній рівень здійснення операцій по запобіганню, превенції, реагуванню на кіберзагрози та зменшення рівня їх негативних наслідків;

– брак результативних інструментів по видаленню порушників інформаційної безпеки з локальних мереж організацій та глобальних міждержавних (міжнародних) мереж;

– неналежний рівень координування державою дій стосовно управління кібербезпекою як в країні, так і на окремих установах, підприємствах, організаціях.

Поміж технічних проблемних питань кібербезпеки необхідно в першу чергу вказати на:

– відсутність точної реєстрації апаратного і технічного обладнання (підприємств і мереж);

– відсутність підтримки технічними способами процесу управління змінами і реалізації безпекової політики;

– недостатній рівень можливості апаратного аудиту становищ підприємства та мереж;

– недостатній рівень апаратного і технічного забезпечення попередженню проникнення до мережі (підприємств, установ, організацій тощо) кіберзлочинців [8, с. 79–80].

Кібербезпека є невіддільною частиною кожної із галузей національної безпеки. Кібербезпека – серйозна самостійна область гарантування національної безпеки, що дає розуміння актуального стану охорони національних інтересів в інформаційній сфері від зовнішніх та внутрішніх загроз, а також є комплексом психолого-інформаційної і технологічно-інформаційної безпеки країни.

У зв'язку з цим розвиток нашої країни (як демократичної, суверенної, правової і економічно стабільної країни) припустимий тільки у випадку гарантування відповідного ступеня її інформаційної безпеки, надання повної, абсолютної підтримки держави національним виробникам інформаційного матеріалу та телекомунікаційного обладнання, розробка фінансово-економічних, нормативно-правових та інших передумов, потрібних для вдалого суперництва на міжнародному і національному ринках інформаційних та телекомунікаційних послуг.

Національна інформаційна безпека це сукупний термін, що по-різному проявляється в тих чи інших державних документах, навчальних підручниках, статтях експертів та фахівців. Національна інформаційна безпека не обмежується тільки інформаційною безпекою країни, її структур, галузей захисту і внутрішньої політики. Концепція інформаційної безпеки об'єктом охорони розглядає збалансовані інтереси індивіда, народу і країни. Без охорони інформаційних інтересів індивіда і громадянина не вважається можливим сприймання країни як суб'єкта суспільного договору й носія суверенітету, і відповідно без цього неможлива охорона громадян держави. Суть терміну передбачає також охорону інформаційної інфраструктури, яка забезпечується програмними, фізико-технічними способами дотримання охорони наукових розроблень і ноу-хау. Отже, під національною безпекою у цифровому вимірі, що включає гарантування і реалізацію інформаційної безпеки індивіда, народу, країни, а також інфраструктури, розуміється стан охорони інформаційного простору, що забезпечує дотримання прав і законних інтересів індивіда, народу і країни в інформаційній сфері, коли забезпечуються їх охорона, виконання й можливості вдосконалення незалежно від наявності внутрішніх і зовнішніх небезпек [5, с. 237].

З метою забезпечення кібербезпеки наша країна повинна виконати коло заходів у зовнішньополітичній області:

– підвищення освітньої та освітньо-інформаційної роботи щодо плюсів для країни інтеграції та вступу до Європейського Союзу, вдосконалення прикладної взаємодії з Північноатлантичним альянсом, іншими міжнародними організаціями та країнами-партнерами у сфері безпеки, а також щодо результативних векторів покращення національної безпеки країни, беручи до уваги ймовірні можливості повноправного членства в Північноатлантичному альянсі;

– інтегрування в світові інформаційно-комунікаційні системи економічної раціональності та організації на підвалинах рівноправності, кіберохорони та збереження інформаційного суверенітету;

– забезпечення вчасного виявлення зовнішніх небезпек державному інформаційному суверенітету та знешкодження, в першу чергу із застосуванням технологій кібербезпеки;

– розповсюдження у міжнародному інформаційному просторі інформаційних даних, що формують позитивну репутацію нашої країни як перевіреного партнера для міждержавних відносин, а також популяризація позитивних здобутків країни;

– допомога діючим навчальним курсам із запобігання інформаційним небезпекам щодо державної і приватної інформаційної інфраструктури, а також впровадження новітніх типів таких навчальних курсів і т.д. [3, с. 141–142].

Оскільки кіберзагрози ніяк не можна лімітувати якоюсь однією сферою, це потребує від всіх зацікавлених сторін різносторонніх знань з чинниками ризику, вмінь та навичок для їх розв'язання та належних заходів для попередження кібератак ще до їх початку. Наша держава динамічно залучає головні організації до підвищення рівня знань діяльності комерційних підприємств і неприбуткових організацій інформаційної безпеки на всіх рівнях. Налагоджено діяльність підрозділу CERT-UA – Державного центру захисту інформаційно-телекомунікаційних систем (ДЦЗ ІТС) ДССЗЗІ, який здійснює виявлення кіберінцидентів та реагує на них. CERT-UA на своєму сайті https://cert.gov.ua/ презентує сприйнятливі до зламу місця стандартного периметру захисту інформаційних даних, надає поради по зменшенню ризиків, а також надає технічну допомогу в знищенні результатів кібератак. Команда CERT-UA у кооперації з іншими групами країн-членів CERT не тільки здійснює заходи з виявлення чинників та обставин кіберінцидентів у критичній інформаційній інфраструктурі, а й надає можливість мінімізувати та знешкодити загрози для приватного та іноземного секторів. Також необхідно зазначити, що Закон України «Про основні засади кібербезпеки України», серед іншого, окреслює задачі CERT-UA на рівні законодавства. Згідно норм цього Закону, CERT-UA та Центр реагування на кіберзагрози відіграватимуть координаційну роль у заходах, направлених на максимально швидку (кризову) реакцію на кібератаки та кіберінциденти, а також у введенні

контрзаходів, направлених на зменшення рівня вразливості систем зв'язку [4, с. 153].

Крокуючи до перспективного інформаційного майбутнього, на сьогоднішній день, для нашої країни актуальним буде формування єдиної гнучкої стрімкої політики держави щодо кібербезпеки, яка братиме до уваги багатоаспектність факту кібербезпеки, багатообіцяючі перспективи трансформацій інформаційного простору, особливості геополітичного становища, політико-економічного стану держави і знайде своє відображення в суспільній свідомості, а також на правовому концептуально-доктринальному рівні та на рівні результативного інформаційного законодавства, що має комплексний, упорядкований характер.

Аналізуючи вищевикладене, з точки зору науки, розумним і логічним є виокремлення дисциплінарних аспектів розуміння (політико-правового, соціологічно-психологічного, ідеологічного, технічного і т.д.) в межах цілісного широкого підходу до кібербезпеки як до складного соціально-технічного явища, як актуального глобального дослідження [6, с. 25].

Інформаційні технології стрімко увійшли в буденне життя народу, тому саме формування нової законодавчої бази актуальне для покращення регламентації і цієї сфери. Нині одним з ключових векторів такої діяльності є війна з інтернет-піратством. Тому для кібербезпеки Україна (з ціллю гарантування інформаційної охорони та супроводу) має здійснювати наступні рекомендації:

– покращення роботи національних громадських організацій та підприємців за межами країни як інформаційного супроводу політики держави;

– інформаційна, організаційно-технічна та ресурсна допомога державі національним ЗМІ, що створюють у міжнародному інформаційному просторі гарну репутацію для України;

– підтримка формування і дотримання міжнаціональних норм поведінки країн в інформаційному полі;

– удосконалення міждержавного співробітництва в області забезпечення інформаційної безпеки на загальнонаціональному та відомчому рівнях і т.д. [3, с. 144].

Висновки. Отже, одним з ключових сегментів національної безпеки держави є кібербезпека. Її забезпечення із застосуванням належно сформованої державної інформаційної політики в великій мірі сприяло б появі результативних досягнень у вирішенні задач в соціально-економічній, політичній, військово-політичній, військовій, та інших галузях діяльності держави. Наприклад, запровадження правильної інформаційної політики в країні може суттєво сприяти зменшенню рівня соціальної напруги і вирішення зовнішньополітичних та військових конфліктів.

Задля формування максимально відкритого інформаційного простору в нашій державі, в першу чергу, необхідно впровадити інструменти прикладного виконання конституційного права на свободу отримання достовірної, повної інформації. Правовим базисом такого інструментарію повинні стати закріплені в законодавстві України конкретні норми, умови і регламент отримання громадянами країни та інституційними структурами суспільства інформації в державновладних органах і органах місцевого самоврядування, від інших державних і недержавних юридичних осіб. Також вкрай необхідним є забезпечення прямого доступу до державних і недержавних інформаційних ресурсів.

Найбільш багатообіцяючими векторами розвитку національної системи кібербезпеки є: покращення правового базису кіберохорони об'єктів критичної інфраструктури; запровадження порядку незалежної перевірки інформаційної безпеки на об'єктах критичної інфраструктури; формування галузевих пунктів реагування на інциденти кібербезпеки; вдосконалення міжнаціональної взаємодії в галузі забезпечення кібербезпеки; вдосконалення порядку підготовки кадрових ресурсів в галузі кібербезпеки; підвищення рівня цифровізації громадян та культури безпечного поводження в кіберполі, запровадження систем інформаційної відповідності нормам і, в першу чергу, формування довірливих відносин між країною і народом, для якого країна є головним об'єктом надання сервісних послуг.

Список літератури:

1. Про основні засади забезпечення кібербезпеки України: Закон України від 05 жовт. 2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/s-how/2163–19 (дата звернення: 05.02.2022).

2. Стратегія кібербезпеки України. Безпечний кіберпростір – запорука успішного розвитку країни: Указ Президента України від 26 серп. 2021 р. № 447 / 2021. URL: https://www.president.gov.ua/documents/4472021–40013 (дата звернення: 06.02.2022).

3. Гаращенко Ю. В. Державна політика у сфері кібербезпеки в Україні. *Вчені записки ТНУ імені В. І. Вернадського. Сер.: «Державне управління»*. Т. 30 (69). 2019. С. 140–145.

4. Кібербезпека України: аналіз сучасного стану / Трофіменко О. Г. та ін. *Захист інформації.* Т. 21. № 3. 2019. С. 150–157.

5. Лахтадир С. Л. Кібербезпека як елемент інформаційної безпеки держави. *Юридичний науковий електронний журнал.* №4. 2020. С. 236–239.

6. Лісовська Ю. П. Кібербезпека: ризики та заходи: навч. посібник. Київ: Видавничий дім «Кондор», 2019. 272 с.

7. Сліпченко Т. О. Кібербезпека як складова системи захисту національної безпеки: європейський досвід. *Актуальні проблеми правознавства*. 2020. № 1 (21). С. 128–133.

8. Ткаченко О., Ткаченко К. Кіберпростір і кібербезпека: проблеми, перспективи, технології. *Цифрова платформа: інформаційні технології в соціокультурній сфері.* Вип. 1. 2018. С. 75–86.

9. Федченко Д. І. Система забезпечення кібербезпеки: проблеми формування та ефективної діяльності. *Молодий вчений.* № 5 (2). 2018. С. 653–658.

10. Президент затвердив нову Стратегію кібербезпеки України: веб-сайт. URL: https://www.ukrinform.ua/rubric-polytics/3304775-prezident-zatverdiv-novu-strategiu-kiberbezpeki-ukraini.html (дата звернення: 06.02.2022).

Gnediuk V.L. ENSURING CYBER SECURITY IN UKRAINE: ORGANIZATIONAL AND LEGAL ASPECTS

The article is devoted to the study of the essence of the concept of "cybersecurity". The vectors of research in the field of cybersecurity are considered. The study analyzes the consequences of uncontrolled distribution and use of information and cyberspace. The description of the Cyber Security Strategy of Ukraine, which was adopted in 2021 by the decree of the President of Ukraine, is given. The opportunities for cybersecurity in Ukraine that will arise as a result of the implementation of the Strategy, based on its results, in cooperation with the private sector and international organizations are listed. The Strategy, as a long-term design document, identifies the priorities of our country's national interests in cybersecurity, existing and potential cyber threats to the vital interests of the individual, citizen, people and country in cyberspace, priority vectors, doctrinal approaches to creating and implementing state policy on security cyberspace activities, its use in the interests of human, people and country, increasing the level of productivity of the main actors in cybersecurity, especially the security and defense sector, in solving problems in cyberspace, as well as the need for budget funding sufficient for implementation of the outlined tasks and solution of the envisaged tasks, and key vectors of use of financial potential.

Organizational, legal and technical issues of cybersecurity are also outlined. Recommendations for ensuring cyber security of Ukraine in order to guarantee information protection are given. The main ones are informational, organizational-technical and resource assistance of the state to the national mass media, which create a good reputation for Ukraine in the international information space; support for the formation and observance of international norms of behavior of countries in the information field; improving interstate cooperation in the field of information security at the national and departmental levels. The most promising vectors for the development of the national cybersecurity system are improving the legal framework for cyber security of critical infrastructure; introduction of the procedure of independent verification of information security at critical infrastructure facilities; formation of sectoral cybersecurity incident response points, etc.

Key words: *cyberspace, cyber attacks, cybersecurity, strategy, digitalization, information field, cyberphysical systems.*