УДК 004.056.5:343.326 (045)
DOI: https://doi.org/10.31359/1993-0941-2022-44-391

А. В. Науменко, аспірантка НДІ державного будівництва та місцевого самоврядування НАПрН України
ORCIDID: 0000-0001-5002-7365

КІБЕРБЕЗПЕКА, ЯК НЕВІД’ЄМНИЙ ЕЛЕМЕНТ СУЧАСНОЇ ДЕРЖАВНОЇ ПОЛІТИКИ УКРАЇНИ

Анотація. *У статті проаналізовано поняття «кібербезпека» та досліджено національне та міжнародно-правове регулювання цієї сфери. Вказано основні напрями та цілі розвитку кіберсфери в Україні. Досліджено внутрішньодержавні інституції та міжнародні організації, що здійснюють та допомають в реалізації політики кібербезпеки. Наведено міжнародний досвід, а саме досвід Естонії з реалізації та функціонування кіберзахисту, виділено корисні для України рекомендації. З’ясовано проблемні питання, що потребують вирішення для ефективного функціонування політики кібербезпеки в Україні.*

Ключові *слова: кібербезпека, кіберзахист, кіберзлочин, інформаційно-комунікаційні технології, інформаційне суспільство.*

Постановка проблеми. Світ не стоїть на місці, він є динамічним і розвивається. З урахуванням науково-технічного прогресу та впровадження інформаційно-комунікаційних систем до функціонування інститутів державної та місцевої влади виникає потреба у вдосконаленні заходів безпеки.

З появою електронної демократії та електронного урядування у населення з’явилось більше можливостей для реалізації своїх прав та інтересів більш ефективним способом, разом з тим з’явилося більше загроз. До таких загроз відносять і кібератаки. Багато країн світу вже мають досвід вчинення кіберзлочинів, в тому числі й Україна. Водночас, можливості попередження та запобігання таким злочинам та притягнення до відповідальності винних потребують вдосконалення в нашій державі.

В умовах гібридної війни кіберзігрози є не потенційними, а реальними. Хакерські атаки з боку російської федерації вже були здійснені щодо комп’ютерних і телекомунікаційних мереж. Одним з найпоширеніших об’єктів враження залишаються вебсайти органів державної та місцевої влад. Це дестабілізує їх безперебійну роботу, унеможливлює надання населенню необхідної інформації та забезпечення реалізації послуг.

Таким чином, наразі для нашої держави актуальним є покращення кібербезпеки. Для України в цьому питанні може бути корисним міжнародний досвід.

Аналіз останніх досліджень і публікацій. Дослідженням певних аспектів кібербезпеки, формуванням ефективного механізму правового регулювання протидії кіберзагрозам та вивченню їх інших аспектів у своїх працях займались Безуглий Д. С., Аристов І. В., Березовська І. Р., Дзьобань О. П., Калюжний Р. А., Кормич Б. А., Ліпкан В. А., Марущак А. І., Цимбалюк В. С., Юдін О. К., Сопілко І. В., Куцаєв В. В., Живило Є. О., Мінін Д. С., Шеломенцев В .П., Бурячок В. Л., Гнатюк С. О. та інші. Вищезазначені науковці розглядали певні проблемні аспекти кібербезпеки, досліджували правове регулювання та вказували на необхідності формування системи інформаційної безпеки України.

Водночас, **метою цієї статті** є застосування комплексного підходу до аналізу даної проблематики, дослідження міжнародного досвіду, сучасного стану впровадження заходів інформаційної та комп’ютерної безпеки в Україні та її перспектив і проблемних питань. Це дасть можливість сформувати загальне уявлення про стан кібербезпеки в Україні та світі на даний час та встановити можливості її поліпшення.

Виклад основного матеріалу дослідження. Для початку необхідно дійти розуміння, що собою уявляє кібербезпека. Міжнародний телекомунікаційний союз визначає кібербезпеку як набір інструментів, політик, концепцій безпеки, заходи безпеки, керівні принципи, підходи до управління ризиками, дії, навчання, передовий досвід, гарантії та технології, які можуть бути використані, щоб захистити кіберсередовище, організацію й активи користувачів. Організація й активи користувачів включають підключені обчислювальні пристрої, персонал, інфраструктуру, додатки, послуги, телекомунікаційні системи та всі передані та/або збережені дані у кіберсередовищі. [1]

Іноді кібербезпеку також визначають крізь призму діяльності, спрямованої на захист систем, мереж і комп'ютерних програм від цифрових атак. Метою таких кібератак зазвичай є отримання доступу до конфіденційної інформації, її зміна або знищення, вимагання грошей у користувачів або порушення нормального бізнес-процесу підприємства. На шляху забезпечення кібербезпеки постає таке явище, як кібероборона. Остання визначається як сукупність політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються у державі та кіберпросторі та спрямовані на забезпечення захисту її суверенітету й обороноздатності, запобігання виникненню збройного конфлікту та відсіч збройній агресії. З урахуванням широкого застосування сучасних інформаційних технологій у секторі безпеки й оборони створення єдиної автоматизованої системи управління Збройних Сил України оборона нашої держави стає більш уразливою до кіберзагроз. Кібероборона має стати одним із пріоритетних напрямів державної політики у сфері оборони.

На думку Павленка В. С. кібербезпека є станом захищеності інформаційного середовища, що гарантує дотримання прав і законних інтересів особистості, суспільства та держави в інформаційній сфері. До основних елементів кібербезпеки він відносить безпеку додатків, інформацію або безпеку даних, безпеку мережі, відновлення після кібератак, планування кіберзахисту, операційну безпеку, хмарну безпеку, критичну безпеку

інфраструктури, фізичну безпеку, підготовку кінцевих користувачів [2, с. 31].

На рівні національного законодавства поняття «кібербезпека» визначено у Законі України «Про основні засади забезпечення кібербезпеки України» і означаєзахищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.

Правове регулювання кібербезпеки в Україні здійснюється Конституцією України, Кримінальним кодексом України, Законами України «Про основні засади забезпечення кібербезпеки України», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основи національної безпеки», Доктриною інформаційної безпеки України, Конвенцією Ради Європи про кіберзлочинність.

Крім того, указом Президента України від 26 серпня 2021 року № 447/2021 затверджено Стратегію кібербезпеки України (далі – Стратегія). Її текст починається з тези «Безпечний кіберпростір – запорука успішного розвитку країни».

За результатами реалізації Стратегії Україна у співпраці з приватним сектором та із залученням міжнародних партнерів забезпечить:

1. стійкість до кіберзагроз, підвищивши здатність державних органів, бізнесу і громадян захищати себе та реагувати на кіберзагрози;

2. спроможність до ефективної протидії недружнім діям у кіберпросторі, забезпечивши їх швидке виявлення та розслідування, створення ефективної системи превентивних заходів щодо недопущення таких дій, а також можливість проведення наступальних операцій у кіберпросторі;

3. розвиток кадрового потенціалу та інноваційного ринку кібербезпеки, що сприятиме створенню національних розробок на рівні кращих світових практик для забезпечення можливості протидіяти майбутнім кіберзагрозам [3].

Таким чином, було визначено такі засади розбудови національної системи кібербезпеки, як стримування, кіберстійкість, взаємодія.

Для реалізації цілей Стратегії було створено Національний координаційний центр кібербезпеки (далі – НКЦК), який є робочим органом Ради національної безпеки і оборони України, діяльність якого регулюється Положенням про Національний координаційний центр кібербезпеки, затвердженим Указом Президента України від 7 червня 2016 року № 242/2016. [4]

Реалізація Стратегії безпосередньо здійснюється основними суб'єктами національної системи кібербезпеки, Міністерством закордонних справ України, Міністерством цифрової трансформації України, Міністерством освіти і науки України та іншими суб'єктами забезпечення кібербезпеки в межах їх компетенції.

На офіційній сторінці НКЦК на Фейсбук керівник управління забезпечення діяльності НКЦК Апарату РНБО України Сергій Прокопенко за результатами XV засідання Національного кластера кібербезпеки на тему «Поточний стан, виклики та перспективи реалізації Стратегії кібербезпеки на місцевому рівні», що відбулося 27 жовтня 2022 року у місті Вінниця, повідомив, що через війну цьогорічний показник виконання Стратегії становить 49%. При цьому основні суб'єкти забезпечення кібербезпеки виконують завдання приблизно на 80%, а показник їх виконання на регіональному рівні і з-поміж інших суб'єктів кібербезпеки становить близько 40%, – сказав він. – Тож основна мета заходу – обговорення проблемних питань, які виникають при реалізації Стратегії на регіональному рівні». [5]

Крім того, в Україні створено Команду реагування на комп'ютерні надзвичайні події України – CERT-UA. Цеурядова команда, яка функціонує в складі Державної служби спеціального зв'язку та захисту інформації України з 2007 року. Її завданнями є накопичення та проведення аналізу даних про кіберінциденти, ведення державного реєстру кіберінцидентів; надання власникам об'єктів кіберзахисту практичної допомоги з питань запобігання, виявлення та усунення наслідків кіберінцидентів щодо цих об'єктів; організація та проведення практичних семінарів з питань кіберзахисту для суб'єктів національної

системи кібербезпеки та власників об’єктів кіберзахисту; підготовка та розміщення на своєму офіційному веб-сайті рекомендацій щодо протидії сучасним видам кібератак та кіберзагроз; взаємодія з правоохоронними органами, забезпечення їх своєчасного інформування про кібератаки; взаємодія з іноземними та міжнародними організаціями з питань реагування на кіберінциденти, зокрема в рамках участі у Форумі команд реагування на інциденти безпеки FIRST із сплатою щорічних членських внесків; взаємодія з українськими командами реагування на комп’ютерні надзвичайні події, а також іншими підприємствами, установами та організаціями незалежно від форми власності, які провадять діяльність, пов’язану із забезпеченням безпеки кіберпростору; опрацювання отриманої від громадян інформації про кіберінциденти щодо об’єктів кіберзахисту; сприяння державним органам, органам місцевого самоврядування, військовим формуванням, утвореним відповідно до закону, підприємствам, установам та організаціям незалежно від форми власності, а також громадянам України у вирішенні питань кіберзахисту та протидії кіберзагрозам [6].

З урахуванням вищенаведеного важливо розуміти який рівень кібербезпеки в Україні в порівнянні з іншими країнами. Так, Україна посіла 24 місце в рейтингу Державного індексу кібербезпеки (NCSI), який щорічно складає Фонд електронного урядування Естонії. Індекс України в рейтингу становить 75,32 зі 100 можливих балів. Серед критеріїв, які впливають на оцінку, – здатність держави визначати кіберзагрози, створювати системи захисту від них і розвивати в державі відповідний освітній напрямок. У списку Україна випередила Австрію, Ірландію й Норвегію. Усього в рейтингу 160 країн. Найвищі оцінки в рейтингу отримали Греція (96), Бельгія (93), Литва (93), Естонія (90), Чехія (92), Німеччина (90). [7]

Кібербезпека тісно пов’язана з кіберзлочинністю. Саме заради унеможливлення вчинення кіберзлочинів й з’явилась інформаційна та цифрова безпека. Від яких саме загроз ми маємо захищати інформаційно-цифрове поле визначено в Конвенції Ради Європи про кіберзлочинність, яка була ратифікована Україною у 2005 році.

Відповідно до її норм кіберзлочини умовно поділяються на чотири види. До першого виду належать правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем. До цього виду кіберзлочинів можна віднести всі злочини, спрямовані проти комп'ютерних систем і даних (наприклад, навмисний доступ до комп'ютерної системи або її частини; навмисне пошкодження, знищення, погіршення, зміна або приховування комп'ютерної інформації; навмисне вчинення, не маючи на це права, виготовлення, продажу, придбання для використання, розповсюдження або надання для використання іншим чином пристроїв, включаючи комп'ютерні програми).

До другого виду кіберзлочинів належать правопорушення, пов'язані з комп'ютерами. Такі злочини характеризуються умисним діянням, що призводить до втрати майна іншої особи шляхом будь-якого введення, зміни, знищення чи приховування комп'ютерних даних або будь-якого втручання у функціонування комп'ютерної системи, з шахрайською або нечесною метою набуття, не маючи на це права, економічних переваг для себе чи іншої особи.

Третій вид кіберзлочинів охоплює правопорушення, пов'язані зі змістом (контентом), що полягає у здійсненні умисних незаконних дій щодо вироблення, пропонування або надання доступу, розповсюдження дитячої порнографії, а також володіння такими файлами у своїй системі.

Четвертим видом є умисні дії, пов'язані з порушенням авторських та суміжних прав, відповідно до вимог Бернської Конвенції про захист літературних і художніх творів, Угоди про торговельні аспекти прав інтелектуальної власності та Угоди ВОІВ про авторське право, а також національного законодавства України.

Існують також інші класифікації кіберзлочинів, проте запропонована Конвенцією про кіберзлочинність є найбільш популярною.[8]

Необхідність зміцнення спроможності захищатись від кібератак була вперше визнана лідерами країн Північноатлантичного альянсу (далі – Альянс, НАТО) на саміті в Празі 2002 року.

З того часу кіберпитання стають дедалі більш важливими елементами порядку денного самітів НАТО. У 2008 році була прийнята перша політика кіберзахисту НАТО. У 2014 році члени Альянсу зробили кіберзахист важливим елементом колективної оборони, оголосивши, що кібератака може призвести до застосування положення про колективну оборону (Article 5) Основоположного договору НАТО. Більше того, в 2016 році члени Альянсу визнали кіберпростір сферою військових операцій і взяли на себе додаткові зобов'язання надати пріоритетність посиленню кіберзахисту своїх національних мереж та інфраструктури. [9]

14 травня 2008 року було засновано Об'єднаний центр передових технологій з кібероборони НАТО (далі – Центр), як один з центрів НАТО, що забезпечує боротьбу з кібератаками й кіберзахист інформаційних систем, а також навчання та підготовку фахівців з кіберзахисту НАТО. Його створено за ініціативи Естонії разом із шістьма іншими країнами – Німеччиною, Італією, Латвією, Литвою, Словаччиною та Іспанією. Північноатлантична рада вирішила надати Центру повну акредитацію та статус Міжнародної військової організації в жовтні того ж року. Естонія запропонувала НАТО концепцію передового центру кіберзахисту ще в 2004 році, після приєднання до Альянсу. Хоча цю концепцію було схвалено Верховним головнокомандувачем ОЗС НАТО з питань трансформації у 2006 році, перші політично вмотивовані кібератаки проти Естонії у 2007 році послужили тривожним дзвіночком для інших країн та Альянсу, насторожившись всіх щодо зростаючої актуальності потенційних загроз у кіберсфері.

Одним із найвідоміших і всесвітньо визнаних дослідницьких досягнень Центру став процес Талліннського посібника, започаткований у 2009 році. У цьому процесі брали участь експерти Центрк, всесвітньо відомі вчені-юристи з різних країн, юридичні радники майже 50 держав та інші партнери. Опублікований у 2017 році «Талліннський посібник 2.0 з міжнародного права, застосовного до кібероперацій», створений дев'ятнадцятьма експертами з міжнародного права, доповнив перше видання, опубліковане в 2013 році, юридичним аналізом більш поширених кіберінцидентів, з якими держави стикаються щодня, і які

є нижчими порогами застосування сили чи збройного конфлікту. Tallinn Manual 2.0 – це найповніший аналіз того, як чинне міжнародне право застосовується до кіберпростору.

Крім того, Центр відповідає за визначення та координацію освітніх і навчальних рішень у сфері кіберзахисту для всіх органів НАТО. [10]

Таким чином, НАТО об'єднало передовий досвід країн-членів і партнерів-однодумців, створює теоретичні та практичні напрацювання і продовжує вдосконалювати сферу кіберзахисту.

Наразі для України це є визначальним, так як 30 вересня 2022 року Україна подала заявку на пришвидшений вступ до НАТО. Тому в найближчій перспективі з партнера-однодумця Альянсу наша держава може перейти у статус країни-члена НАТО, що розширить можливості у співпраці, зокрема, стосовно кібербезпеки. При цьому, варто відмітити, що обмін досвідом у кіберсфері потрібен не лише Україні, а й чинним країнам-членам Альянсу, бо маючи досвід гібридної війни, боротьби з масованими кібератаками, запобігання та усунення наслідків міжнародної кіберзлочинності маємо власні досягнення та напрацювання на цьому «фронті».

На сьогодні кіберпростір повинен розглядатись як п'ята сфера ведення бойових дій, поряд з наземною, повітряною, морською та космічною. Кібератаки є одним із шляхів та засобів вирішення державних і недержавних проблем. [11]

Варто відмітити й досвід Естонії у кіберсфері.Зараз Естонія входить в топ-5 країн за рівнем кіберзахисту, згідно з Національним індексом кібербезпеки 2020 року. Поштовхом для серйозних змін стала скоординована кібератака російських хакерів на комп'ютерні системи державних установ Естонії в квітні 2007 року.

Важливий складник кібербезпеки – це освіта. В університетах Естонії є сучасні програми з кібербезпеки, у школах курси для початківців. Також є військовий навчальний кіберна-прям. Протягом 3–4 років молоді люди повинні пройти кіберпідготовку. Цей курс обов'язковий для всіх.

Звичайно ж, важливу роль в системі кіберзахисту Естонії відіграє Центр. Це гарне місце, щоб навчати й утримувати фа-

хівців. Він працює не тільки для естонців, а й для представників країн-членів НАТО. Там проводиться багато різних безкоштовних курсів і масштабні навчання для фахівців із кібербезпеки.

Загалом, системний підхід до підготовки кіберфахівців і тренінги, на яких учасники отримують практичні навички з розпізнавання кібератак, реагування та усунення наслідків, а також навчання взаємодії з фахівцями з інших країн – це невід'ємна частина підготовки кадрового потенціалу.17–19 травня 2021 року подібні навчання вперше пройшли в Україні. Їх проводила естонська компанія CybExer Technologies OÜ під керуванням Естонської академії електронного управління за фінансової підтримки Євросоюзу (проект EU4DigitalUA) у співпраці з Держспецзв'язку.У навчанні взяли участь 30 співробітників суб'єктів кібербезпеки України.Основною метою кібернавчань було підвищення потенціалу та навичок учасників. Полювання на кіберзагрози дозволяє фахівцям розвинути всебічні навички технічної точки зору, керівництву – розвинути обізнаність про наслідки, які можуть спричинити кіберінциденти.

І ще один аспект, який Естонії вдається робити дуже добре – це підтримка кібербезпечної спільноти, враховуючи як державний, так і приватний сектор.Підтримка полягає як в офіційних заходах з обговорення стратегії, тренінгах, так і неофіційних, а також їх комбінації. Естонці підтримують єдність в цьому співтоваристві, залучають до активного діалогу, розвивають довіру між державним і приватним сектором, розуміючи, що 85% критичної інформаційної інфраструктури належить приватному сектору, який постачає електроенергію, воду, газ та інші життєво необхідні для суспільства елементи.Уряд Естонії підтримує взаємини, а не тільки ставить вимоги. Він допомагає дотримуватися правил, виконувати вимоги, пропонує тренінги, залучає до діалогу, щоб приватний сектор бачив цілісну картину. В цьому аспекті Естонія також може слугувати прикладом для України.[12]

Враховуючи стан розвитку кібербезпеки в Україні, досвід Естонії та міжнародно-правове регулювання цієї сфери можемо виділити основні проблемні питання, що мають бути вирішені для подальшого ефективного функціонування безпечного інформаційно-цифрового середовища в Україні.

Перш за все відзначимо проблему кадрового голоду. Для ефективного функціонування системи кіберзахисту держави необхідно максимальне заповнення відповідних посад.

За словами керівниці служби з питань інформаційної безпеки та кібербезпеки Апарату РНБО України Наталії Ткачук головна проблема національної системи кібербезпеки – відсутність кадрів у кожному органі, який відповідає за цю сферу. Це питання слід вирішити шляхом побудови кіберрезерву фахівців – молодих хлопців і дівчат, які проходитимуть, у тому числі, строкову службу. Це буде такий своєрідний пул кадрів, який потім зможуть використовувати всі суб'єкти сектору безпеки й оборони, задіяні у завданнях кібербезпеки. Україна має для цього величезний потенціал, у жодній країні немає такої кількості молодих, талановитих айтішників, які при цьому є справжніми патріотами своєї країни й готові боронити кіберпростір.

Для реалізації цієї мети державою створено спеціальність «Кібербезпека» у вищих навчальних закладах. Але для вирішення цього питання необхідно популяризувати цей напрям, інформувати громадськість про його важливість, престижність та високо оплачуваність праці. Стосовно популяризації в нагоді стане досвід Естонії, яка впроваджує обов'язкове навчання основам кібербезпеки починаючи з молодшої школи. При цьому, необхідно періодично поширювати необхідну інформацію і серед населення, для підняття рівня інформованості та персональної кібербезпеки. Це зумовлено тим, що зараз часто на електронну пошту громадянам приходять листи з загрозливими програмами, що в кращому випадку може нанести шкоду пристрою, а в гіршому отримати доступ до інформації з обмеженим доступом. Тому, інформування населення є важливою складовою кіберзахисту.

Наступним проблемним питанням є фінансування. Не дивлячись на те, що держава звертає вагому увагу на кібербезпеку, фінансування кіберсфери продовжує здійснюватись за залишковим принципом. Це є однією з причин недостатності кадрів. Зараз, в умовах повномасштабного вторгнення екстренно було зібрано 400-тисячне кібервійсько на громадських засадах. Але

маємо розуміти, що це не постійні працівники, при чому це все одно не вирішило питання заповнення усіх необхідних кадрів.

Достатнє фінансування дозволить реалізовувати всі прогресивні проєкти як на державному, так і місцевому рівнях. Фінансове забезпечення кібербезпеки є прерогативою місцевої влади. Місцеві бюджети мають враховувати надважливу роль кібербезпеки та закладати більший обсяг фінансів, ніж є наразі, для реалізації ефективної політики кіберзахисту.

Ще одним моментом, на який варто звернути увагу, є недостатня врегульованість цифрової складової розслідування кримінальних правопорушень, а також низький рівень правової відповідальності за порушення вимог законодавства у цій сфері.

Основними причинами цього є специфіка кіберзлочинів. А саме, анонімність і неперсоніфікованість кіберзлочинів (механізми ідентифікації глобальної мережі дозволяють особі здійснювати операції анонімно або видавати себе за іншу особу, змінювати біографічні дані або соціальний статус); віддаленість кіберзлочинів;їх транснаціональність (більше половини злочинів вчиняється у складі організованих груп, що знаходяться на території декількох країн); швидке зростання кіберзлочинності, що пов’язане із дедалі більшим розповсюдженням та здешевленням Інтернет-послуг [13].

У Кримінальному кодексі України міститься низка статтей стосовно кіберзлочинів, за які передбачено санкції у вигляді штрафу, обмеження волі, позбавлення волі з позбавленням права обіймати певні посади чи займатися певною діяльністю. Водночас, виходячи з вищенаведених підстав, більшість статтей є декларативними і потребують практичного вдосконалення механізмів розслідування цих злочинів. А на це впливає як кадрове, так і фінансове забезпечення кібербезпеки.

Висновки. Сучасний стан розвитку кібербезпеки в Україні є доволі прогресивним в порівнянні з більшістю країн світу. Водночас, рівень розвитку кіберзахищеності держави ще не дає можливостей запобігти кібератакам та притягнути до відповідальності усіх винних за вже вчинені кіберзлочини. Це говорить про те, що є напрями і поставлені цілі, яких ми маємо досягти. Стратегією визначено орієнтири для подальших дій держави.

Крім того, враховуючи транснаціональний характер кіберзлочинів, ця проблема є важливою для усього світу, а не виключно якоїсь країни. Тому для її вирішення необхідний комплексний підхід на рівні міжнародних організацій. Однією з них є Центр, з яким Україна вже співпрацює і має спільні проєкти.

Але для досягнення того рівня кібербезпеки, якого ми прагнемо, необхідно вирішити питання з кадровим голодом, фінансовим забезпеченням, інформуванням та навчанням населення, підвищенням рівня та покращенням методик розслідування кіберзлочинів і досягненням ефективності кримінальної відповідальності за них. У нас є весь необхідний потенціал та ресурси для досягнення поставлених цілей, тому сподіваємось, що в найближчому майбутньому Україна стане передовою державою з реалізації політики кібербезпеки.

Список використаних джерел:

1. Understanding the concept of cyber security. Policy competition and economic analysis department. URL: https://www.ncc.gov.ng/docman-main/industry-statistics/policies-reports/682-understanding-theconcept-of-cyber-security/file.
2. Павленко В. С. Сутність кібербезпеки у теорії інформаційного права. Право та державне управління. Запоріжжя. 2021. Вип. 2. С. 28–33.
3. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України від 26.08.2021 р. № 447/2021. URL: https://www.president.gov.ua/documents/4472021–40013
4. Про Національний координаційний центр кібербезпеки: Указ Президента України від 07.06.2016 р. № 242/2016. URL: https://zakon.rada.gov.ua/laws/show/242/2016#Text
5. Відбулося XV засідання Національного кластера кібербезпеки на тему «Поточний стан, виклики та перспективи реалізації Стратегії кібербезпеки на місцевому рівні». Національний координаційний центр кібербезпеки.URL :https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjd277f0JH7AhUilYsKHZj5AUAQFnoECA4QAQ&url=https%3A%2F%2Fwww.facebook.com%2FncsccUA%2F&usg=AOvVaw3QbmwOlpK2csAeNP-Ro-Zb
6. Про CERT-UA. URL: https://cert.gov.ua/about-us.
7. Липська Д. Україна увійшла в ТОП-25 країн за рейтингом кібербезпеки. 2022. URL: https://glavcom.ua/country/society/ukrajina-uviyshla-v-top-25-krajin-za-reytingom-kiberbezpeki-–853804.html

8. Що таке кібербезпека і чому це важливо? URL: https://enigma.ua/articles/shcho-take-kiberbezpeka-i-chomu-tse-vazhlivo
9. Брент Л. Роль НАТО в кіберпросторі. 2019. URL: https://www.nato.int/docu/review/uk/articles/2019/02/12/rol-nato-v-kberprostor/index.html
10. Об'єднаний центр передових технологій з кібероборони НАТО: Про нас. URL: https://ccdcoe.org/about-us/
11. Даник Ю. Основні тренди трансформації і розвитку кібербезпеки і кібероборони в світі, що змінюється. URL: https://metod.suitt.edu.ua/download/686file.
12. Майгре М. Віртуальний фронт. Як Естонія стала гуру з кіберзахисту і чому може повчитися в неї Україна? 2021. URL: https://focus.ua/uk/opinions/484496-virtualnyy-front-kak-estoniya-stala-guru-po-kiberzashchite-i-chemu-mozhet-pouchitsya-u-nee-ukraina.
13. Лекція. Тема V. Кіберзлочинність та кібертероризм.URL : https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiok4rZ0ZH7AhVJiIsKHaXnA0AQFnoECBUQAQ&url=https%3A%2F%2Fmoodle.znu.edu.ua%2Fmod%2Fresource%2Fview.php%3Fid%3D242191&usg=AOvVaw0JKM-eHc9WMg5D5M7Vz85k

References :

1. Understanding the concept of cyber security. Policy competition and economic analysis department. URL: https://www.ncc.gov. ng/docman-main/industry-statistics/policies-reports/682-understanding-theconcept-of-cyber-security/file.
2. Pavlenko V. S. (2021).Sutnist kiberbezpeky u teorii informatsiinoho prava. Pravo ta derzhavne upravlinnia. Zaporizhzhia. Issuer. 2. pp. 28–33.
3. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14/05/2021 r. «Pro Stratehiiu kiberbezpeky Ukrainy»: Ukaz Prezydenta Ukrainy vid 26.08.2021 r. № 447/2021. URL: https://www.president.gov.ua/documents/4472021–40013
4. Pro Natsionalnyi koordynatsiinyi tsentr kiberbezpeky: Ukaz Prezydenta Ukrainy vid 07.06.2016 r. № 242/2016. URL: https://zakon.rada.gov.ua/laws/show/242/2016#Text
5. Vidbulosia KhV zasidannia Natsionalnoho klastera kiberbezpeky na temu «Potochnyi stan, vyklyky ta perspektyvy realizatsii Stratehii kiberbezpeky na mistsevomu rivni». Natsionalnyi koordynatsiinyi tsentr kiberbezpeky. URL :https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjd277f0JH7AhUilYsKHZj5AUAQFnoECA4QAQ&url=https%3A%2F%2Fwww.facebook.com%2FncsccUA%2F&usg=AOvVaw3QbmwOlpK2csAeNP-Ro-Zb
6. Pro CERT-UA. URL: https://cert.gov.ua/about-us.

7. Lypska D. (2022). Ukraina uviishla v TOP-25 krain za reitynhom kiberbezpeky. URL: https://glavcom.ua/country/society/ukrajina-uviyshla-v-top-25-krajin-za-reytingom-kiberbezpeki-–853804.html
8. Shcho take kiberbezpeka i chomu tse vazhlyvo? URL: https://enigma.ua/articles/shcho-take-kiberbezpeka-i-chomu-tse-vazhlivo
9. Brent L.(2019). Rol NATO v kiberprostori.URL: https://www.nato.int/docu/ review/uk/articles/2019/02/12/rol-nato-v-kberprostor/index.html
10. Obiednanyi tsentr peredovykh tekhnolohii z kiberoborony NATO: Pro nas. URL: https://ccdcoe.org/about-us/
11. Danyk Yu. Osnovni trendy transformatsii i rozvytku kiberbezpeky i kiberoborony v sviti, shcho zminiuietsia. URL: https://metod.suitt.edu.ua/download/686file.
12. Maihre M. (2021). Virtualnyi front. Yak Estoniia stala huru z kiberzakhystu i chomu mozhe povchytysia v nei Ukraina? URL: https://focus.ua/uk/opinions/484496-virtualnyy-front-kak-estoniya-stala-guru-po-kiberzashchite-i-chemu-mozhet-pouchitsya-u-nee-ukraina.
13. Lektsiia. Tema V. Kiberzlochynnist ta kiberteroryzm. URL: https://www. google. com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiok4rZ0ZH7AhVJiIsKHaXnA0AQFnoECBUQAQ&url=https%3A%2F%2Fmoodle. znu. edu. ua%2Fmod%2Fresource%2Fview.php%3Fid%3D242191&usg=AOvVaw0JKM-eHc9WMg5D5M7Vz85k

V. Naumenko

Cyber security as an integral element of modern state policy of Ukraine

Summary. *Many countries of the world already have the experience of committing cybercrimes, including Ukraine. At the same time, the possibilities of prevention and prevention of such crimes and prosecution of the guilty need to be improved in our state.*

In the conditions of a hybrid war, cyber threats are not potential, but real. Thus, improving cyber security is currently relevant for our state.

The article analyzes the concept of «cyber security». The definition formed by the International Telecommunication Union is given. In addition, cyber security is considered through the prism of activities aimed at protecting systems, networks and computer programs from digital attacks, as well as as a state of security of the information environment. The concept of «cyber security» is defined in the Law of Ukraine «On Basic Principles of Ensuring Cyber Security of Ukraine».

The legal regulation of the cyber sphere at the national and international levels has been studied.

The main directions and goals of the development of the cyber sphere in Ukraine, which are outlined in the Cyber Security Strategy of Ukraine, are indicated. It is specified what exactly it will provide as a result of its implementation.

To implement the goals of the Strategy, the National Coordination Center for Cyber Security was created, which is a working body of the National Security and Defense Council of Ukraine. Certain aspects of his activity are given. The creation of the Computer Emergency Response Team of Ukraine – CERT-UA is described and its tasks are analyzed.

The rating of Ukraine on the implementation of cyber security in comparison with other countries of the world is outlined.

Since cyber security is closely related to cyber crime, the article examines the latter. There are four types of cybercrime outlined in the Council of Europe Convention on Cybercrime.

The experience of the North Atlantic Alliance in the policy of strengthening the ability to defend against cyber attacks is studied. The activities of the Joint Advanced Technologies Center for NATO Cyber Defense are analyzed. NATO has combined the best experience of member countries and like-minded partners, creates theoretical and practical developments and continues to improve the field of cyber defense.

International experience, namely the experience of Estonia in the implementation and functioning of cyber defense, is presented, and useful recommendations for Ukraine are highlighted.

Problematic issues that need to be solved for the effective functioning of the cyber security policy in Ukraine have been clarified.

Taking into account the state of development of cyber security in Ukraine, the experience of Estonia and the international legal regulation of this sphere, the main problematic issues that must be resolved for the further effective functioning of a secure information and digital environment in Ukraine are highlighted. It was noted that for the effective functioning of the state's cyber defense system, it is necessary to solve the issue of personnel shortage. The issue of insufficient financing of the cyber sphere has been identified. Sufficient funding will allow the implementation of all progressive projects both at the state and local levels. Another point to which attention has been drawn is the insufficient regulation of the digital component of the investigation of criminal offenses, as well as the low level of legal responsibility for violations of the requirements of legislation in this area.

We have all the necessary potential and resources to achieve our goals, so we hope that in the near future Ukraine will become a leading state in the implementation of cyber security policy.

Key words: *cyber security, cyber protection, cyber crime, information and communication technologies, information society.*