МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ МІЖНАРОДНИХ ВІДНОСИН
Кафедра міжнародного права та порівняльного правознавства

ДОПУСТИТИ ДО ЗАХИСТУ

Завідувач кафедри

_____ Т. Р. Короткий

«____»_____2021 р.

ДИПЛОМНА РОБОТА

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ

«БАКАЛАВР»

спеціальності 293 «Міжнародне право»

Тема: **ПРАВОВІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В ЄВРОПЕЙСЬКОМУ СОЮЗІ ТА НАТО**

Виконавець: Пазюк Валерій Андрійович

Науковий керівник: к.ю.н. , доцент Невара Л.М.,

Нормоконтролер: викладач Головатенко Марина Юріївна

Київ, 2021

ЗМІСТ

ВСТУП

Актуальність обраної теми дослідження. Стрімкий розвиток інформаційних технологій, комп'ютеризація, створення глобального кіберпростору сформували принципово нові реалії – інформаційне суспільство і цифровий ринок – які мають невичерпний потенціал і відіграють головну роль в економічному і соціальному розвитку країн світу. Однак, створення інформаційного суспільства призвело до виникнення багатьох кіберзагроз, а одним із головних завдань для забезпечення сталого розвитку сучасного інформаційного суспільства та цифрової економіки є кібербезпека.

23 грудня 2015 року в Україні внаслідок кібератаки на «Прикарпаттяобленерго» в Івано-Франківській області залишилися без електроенергії 80 тисяч споживачів [1] Через 2 місяці, 16 січня 2016 року в київському аеропорту «Бориспіль» заявили про хакерську атаку із застосуванням вірусу Black Energy, який було виявлено також після атаки на системи «Прикарпаттяобленерго» [2].

27 червня 2017 року, велика кількість українських компаній та державних установ піддалась атакам хакерів. Атака була здійснена за допомогою вірусу-здирникаWin32/Petya. Постраждали «Укренерго», ДТЕК, «Нова пошта», аеропорт Бориспіль, «Укрпошта» і київський метрополітен. Про проблеми в роботі комп'ютерної мережі повідомили і в Кабміні.

Попередньо експерти Департаменту кіберполіції України встановили, що вірусна атака на українські компанії виникла через оновлення програми «M.E.doc.» [3]. За даними експертів Cybersecurity Ventures, загальні збитки від глобальної кіберзлочинності сягатимуть $10,5 трлн. щорічно вже до 2025 року [4].

Протидія загрозам національній безпеці, що надходять з кіберпростору, сьогодні, набула нового значення. Кіберінциденти стають дедалі частішими, більш організованими і збитковішими для державних установ, підприємств, економіки та операторів критичної інфраструктури; вони можуть досягти критичного рівня, який загрожує національному і євроатлантичному процвітанню, безпеці і стабільності. Джерелом таких загроз можуть бути іноземні військові і розвідувальні служби, організовані злочинні угруповання, терористичні та екстремістські групи.

Актуальність даної роботи обумовлена передусім якісно новими викликами та загрозами кіберпростору, які постали перед Україною у сфері національної безпеки. На тлі сучасної інформаційної революції та розвитку інформаційно-комунікаційних застосувань можливостей кіберпростору перетворилося на елемент міждержавного протиборства, що використовується спецслужбами іноземних держав для здійснення розвідувально-підривної діяльності, організації спеціальних операцій, акцій кібершпигунства, встановлення віддаленого доступу та контролю над об’єктами критичної інформаційної інфраструктури тощо направлених на отримання інформаційних переваг та забезпечення інтересів власної держави у військовій, економічній, політичній та інших сферах.

Кібербезпека є важливою складовою національної безпеки будь-якої держави. Не випадково, що країни ЄС приділяють значну увагу становленню спільних правил і запровадженню механізмів протидії кіберзагрозам. Україна наразі лише приступила до імплементації в національне законодавство положень актів права ЄС щодо кібербезпеки та захисту об’єктів критичної інфраструктури.

У 2018 році Верховна Рада України закликала інституції Європейського Союзу сприяти максимальному використанню можливостей інтеграції України до внутрішнього ринку Європейського Союзу, включаючи питання

формування оновленого порядку денного співробітництва між Україною та Європейським Союзом у сферах юстиції, свободи та безпеки, зокрема сформувати спільне бачення шляхів інтеграції України до Єдиного цифрового ринку ЄС та безпекового простору Північноатлантичного Договору.

Тема кібербезпекової політики ЄС є цікавою та важливою для вивчення та дослідження. В українських академічних працях розглядаються окремі аспекти цієї тематики в контексті інтеграції України до Європейського Союзу, а також наближення законодавства України до права ЄС і стандартів НАТО.

Предметом дослідження є основні засади (принципи) забезпечення кібербезпеки в ЄС та тенденції розвитку як напрямку євроатлантичної інтеграції України. Що ж стосується об'єкту дослідження, то ним є політико-правові, інституційні та нормативно-правові засади кібербезпекової політики ЄС і НАТО.

Мета і завдання дослідження. Мета дослідження – з'ясувати основні принципи та тенденції розвитку кібербезпекової політики та її нормативно-правового забезпечення в Європейському Союзі та НАТО.

Для досягнення поставленої мети, визначено наступні завдання:

надати визначення та сформулювати сутнісні характеристики кібербезпеки;

визначити основні етапи розвитку кібербезпекової політики ЄС;

надати характеристику сучасної кібербезпекової стратегії ЄС;

дослідити інституційні засади кібербезпекової політики ЄС, функції Агентства ЄС з кібербезпеки (ENISA);

дослідити вплив кібербезпекової політики ЄС та НАТО на Україну та стан імплементації положень законодавства ЄС та стандартів НАТО у сфері кібербезпеки в Україні.

Методологічну основу роботи склали діалектичні, історичні, компаративні та формально-логічні методи, які у своєму органічному поєднанні допомогли досягти виконання поставлених завдань.

У вітчизняній науковій літературі на сьогодні бракує досліджень щодо міжнародно-правового співробітництва з питань забезпечення кібербезпеки України та її євроатлантичної інтеграції. З огляду на це тема дипломного дослідження є актуальною як з теоретичної, так і з практичної точки зору.

Теоретичною основою бакалаврського дослідження стали наукові праці, в яких досліджувались лише окремі аспекти цієї теми, зокрема, що пов'язані з боротьбою проти кіберзлочинності та засадами міжнародно-правового співробітництва держав у боротьбі з транскордонною злочинністю в цілому, таких вчених, як: В.Ф. Антипенко, І.П. Бліщенко, Н.А. Зелінська, Г.В. Ігнатенко, Р.А. Каламкарян, І.І. Лукашук, А.С. Мацко, Л.Д. Тимченко, Л.О. Тимченко, С.В. Саяпін, О.О. Шибаєва та ін. Серед вітчизняних вчених, які безпосередньо вивчали різні аспекти інформаційної сфери та кібербезпеки назвати таких як О.А. Баранов, А.А. Васильєв, І.М. Доронін, І.М. Забара, В.В. Коваленко, О.О. Мережко В.А. Мінаєв, В.Б. Наумов, Т.Л. Тропіна, А.С. Юрасов.

Окремі питання розвитку міжнародного співробітництва щодо протидії кіберзлочинності розглядались у роботах закордонних вчених, серед яких слід виділити таких як: К. Браун (K. Brown), Д. Вол (D. Wall), С. Гудман (S. Goodman), У. Зібер (U. Sieber), Г. Касперсен (H. Kaspersen), А. Софаер (A. Sofaer), Ш. Шольберг (S. Schjolberg) та М. Яр (M. Yar).

Віддаючи належне академічному доробку вчених і попри досить високий рівень політичного дискурсу навколо питань євроатлантичної інтеграції України, аналізу саме кібербезпекового напрямку міжнародно-правового співробітництва приділено недостатню увагу, хоча актуальність такого дослідження постійно зростає.

Методологія і методи дослідження. Наукову обґрунтованість сформульованих висновків визначено сукупністю методів наукового пізнання.

Структура роботи обумовлена її метою, завданнями та предметом дослідження. Дипломна робота складається із переліку умовних скорочень, вступу, трьох розділів, якими охоплюються сім підрозділів, висновків та списку використаних джерел (66 найменувань). Загальний обсяг дипломної роботи –72 сторінки, у тому числі список використаних джерел – 9 сторінок.

РОЗДІЛ 1
ДОКТРИНА ТА ПРАВОВА РЕГЛАМЕНТАЦІЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В ЄС

1.1. Теоретико-правові підходи до визначення кібербезпеки

Поняття «безпеки» в сучасному світі відіграє чи не найголовнішу роль у всіх життєвих процесах: біологічних, політичних, економічних, соціальних, технічних, територіальних та багатьох інших [5]. Забезпечення безпеки є базовою потребою і важливим завданням кожної держави, як і міжнародної спільноти в широкому розумінні цього поняття. В цьому випадку постає питання щодо визначення кібербезпеки (англ. cybersecurity), поняття якої все частіше і частіше з'являється як в національних, так і в міжнародних правових джерелах.

В сучасних визначеннях міжнародних та українських джерелах, безпека переважно окреслюється як: стан відсутності загроз та інструментарій захисту перед небезпеками. В цьому випадку застосування слова-приставки «кібер» пов'язано із кібернетикою (з грец. kybernetike – мистецтво управління) – наукою про управління, зв'язок та перероблення інформації, започатковану Норбертом Віннером (Norbert Wiener) у 1948 р.

На думку М.С. Соколова, використання термінів, похідних від терміну «кібернетика», наприклад, таких як «кібернетична атака», «кібернетична безпека», «кіберпростір», «кіберсфера», «кіберзлочинність», «кібервійна», «кібероборона», є виправданим у разі опису явищ або фактів, безпосередньо пов'язаних із системами і процесами управління [6].

Перш ніж визначати термін "кібербезпека" варто вказати наступне: велика частина звітів, рекомендацій і публікацій в цій сфері починаються з

визначення термінів “комп’ютерна злочинність” і “кіберзлочинність”. Що стосується терміну “кіберзлочинність”, то воно має вужче значення, ніж “злочини, пов’язані із застосуванням комп’ютерів”, оскільки має на увазі використання комп’ютерної мережі. Під злочинами, пов’язаними із застосуванням комп’ютерів, розуміються навіть ті правопорушення, які не мають ніякого відношення до мережі, а лише торкаються окремо стоять комп’ютерні системи.

На 10-му Конгресі ООН з запобігання злочинності та поводження з правопорушниками в ході семінару на відповідну тематику були вироблені два визначення. Кіберзлочинність в вузькому сенсі (комп’ютерна злочинність) – це будь-яка протизаконна поведінка у формі електронних операцій, спрямована проти безпеки комп’ютерних систем і оброблюваних ними даних.

Кіберзлочинність в ширшому сенсі (злочини, пов’язані із застосуванням комп’ютерів) – це будь-яка протизаконна поведінка, здійснювана за допомогою або в зв’язку з комп’ютерною системою або мережею, включаючи такі злочини, як незаконне володіння, пропозиція або поширення інформації за допомогою комп’ютерної системи або мережі [7].

Термін “кіберзлочинність” використовується відповідно до найрізноманітнішої злочинної поведінки. Оскільки визначення злочину включає широкий спектр різних правопорушень, це ускладнює розробку системи типології або класифікації для кіберзлочинності.

Один з підходів наводиться в Конвенції Ради Європи про кіберзлочинність, яка розрізняє чотири типи правопорушень:

1) злочини проти конфіденційності, цілісності та доступності комп’ютерних даних і систем;

2) злочини, пов’язані із застосуванням комп’ютерів;

3) злочини, пов’язані з контентом (змістом інформації);

4) злочини, пов’язані з правами інтелектуальної власності на об’єкти інформаційної діяльності [8].

Ця типологія не є повністю послідовною, оскільки вона не базується на єдиному базовому критерії, який би визначав відмінності між категоріями. Проте, ці чотири категорії можуть служити корисною основою для обговорення як явища кіберзлочинності, так функцій кібербезпеки щодо запобігання, реагування, протидії і відновлення від зловмисних втручань у роботу інформаційно-комунікаційних мереж, систем та інформацію.

Публікація Першої стратегії кібербезпеки Європейського Союзу (ЄС) у 2013 році ознаменувала офіційне визнання “кібербезпеки” як нового напряму політики в ЄС. Це визнання було довгоочікуваним розвитком, який визнав розмиття ліній у трьох спочатку окремих, але збіжних сферах політики мережевих та інформаційних заходів безпеки, які націлені на операторів основних послуг та постачальників критичних та цифрових інфраструктур; електронні комунікації, включаючи питання конфіденційності та захисту даних; та кіберзлочинність.

Знадобилось понад 20 років, щоб поступово зростаюча кількість розпорошених ініціатив, що стосуються цифрового середовища – від цифрових підписів та електронної комерції до кіберзлочинів та критичної інфраструктури – була визнана загальним терміном «кібербезпека» в Європейському Союзі.

Для визначення кібербезпеки доцільно порівняти її крізь призму з інформаційною безпекою. Ці поняття часто межують між собою, але не є тотожними, що часто викликає, в свою чергу, проблеми з визначенням джерел при регулюванні міжнародно-правового співробітництва в цих сферах. Основна відмінність полягає в тому, що інформаційна безпека та кібербезпека різняться за сферою своєї дії. Захист інформації пов’язаний із забезпеченням

.

безпеки даних в будь-якій формі і є трохи ширшим, ніж кібербезпека. Цей висновок виходить з визначень, які наведені в міжнародних та національних джерелах.

Для прикладу, відповідно до Закону України “Про основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки” інформаційна безпека визначається як «певний стан захищеності життєво важливих інтересів особистості, суспільства і держави, за якого запобігається завдання шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання і порушення цілісності, конфіденційності та доступності інформації» [9].

А у Законі України «Про основні засади забезпечення кібербезпеки» подається таке визначення кібербезпеки: «кібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі» [10].

Європейський Союз не є безпековим альянсом, хоча й має власну спільну політику безпеки та оборони, адже створювався як економічний союз. Безпека для нього має переважно внутрішній і невійськовий вимір, і протидія гібридним загрозам набуває там особливої актуальності. Тому кібербезпека поміщена на одне з перших місць сьогоднішньої безпекової політики ЄС й була виведена в пріоритетні сфери набагато раніше, ніж у термінології ЄС з’явилось визначення «протидія гібридним загрозам», особливо враховуючи

активний розвиток цифрового ринку та перспективи створення, так званого, «Цифрового союзу ЄС».

Стратегія кібербезпеки ЄС 2013 року передбачила визначення, згідно з яким кібербезпека зводиться до гарантій та дій, які можуть бути використані для захисту кібердоменів як у цивільному, так і у військовому секторах від тих загроз, які пов'язані або можуть зашкодити взаємозалежним мережам та інформаційній інфраструктурі. У такому контексті, основними цілями кібербезпеки вважалося забезпечення доступності та цілісності мереж та інфраструктури та конфіденційності інформація, що міститься в ній.

Хоча дві Стратегії кібербезпеки ЄС слідували за прийняттям численних законодавчих заходів, що стосуються кібербезпеки, вони висунули цілі політики, що згодом призвели до законодавства, а саме Директиву про мережеву та інформаційну безпеку та Закон про кібербезпеку, що додатково уточнює роль та мандат Агентства Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA). Політичні заходи з різних областей політики зрештою призвели до змін та коригувань у різних правових рамках ЄС і навпаки.

Як уже згадувалося, було прийнято численні політичні та регуляторні заходи для підвищення безпеки громадян, підприємств та державних адміністрацій у сферах заходів мережевої та інформаційної безпеки, електронних комунікацій та кіберзлочинності. Насправді ЄС лише нещодавно почав використовувати термін «кібербезпека» у своїх політичних документах. Можна вважати, що прийняття всеосяжної стратегії кібербезпеки ЄС у 2013 році стало критичним моментом, який спричинив збільшення використання цього терміну в політичних документах ЄС, що можна побачити на прикладі Повідомлення Європейської Комісії і Ради «Зміцнення системи кіберстійкості

Європи та сприяння конкурентоспроможній та інноваційній кібербезпеці» 2016 року [11].

Отже, різні актори політики, включаючи інституції ЄС, часто вибирають визначення розроблені організаціями зі стандартизації, такими як Європейський комітет з питань стандартизації (ESTI), Міжнародна організація стандартизації (ISO), або міжурядові організації, такі як Міжнародний Союз електрозв'язку (МСЕ).

Не дивно, що на сьогодні численні визначення співіснують, зосереджуючись на різних аспектах кібербезпеки.

Згідно стандарту ETSI, функції кібербезпеки складаються з постійного циклу структурованих дій:

визначити (зрозуміти стан та ризики для систем, активів, даних і можливостей);

захистити (впровадити відповідні гарантії);

виявити (реалізувати здатність ідентифікувати кібербезпеку);

відреагувати (реалізувати здатність вживати заходів у відповідь на загрозу кібербезпеці);

відновлювати (забезпечити стійкість і відновлення порушених можливостей).

Цей самий стандарт визначає кібербезпеку як «сукупність інструментів, політик, концепцій безпеки, гарантій безпеки, настанов, підходів до управління ризиками, дій, навчання, найкращих практик, гарантій та технологій, які можна використовувати для захисту кіберсередовища і організації та активів користувача» [12].

Кібербезпека може розглядатися з різних сторін: як проблема, що викликає занепокоєння через ризики, що існують в Інтернеті (кіберпросторі);

її можна розуміти як захист лише віртуальних активів; або вона може бути націлена лишень на захист від зловмисних дій.

Такі вузькі визначення несуть за собою ризик не врахування наслідків для людей та їх прав. Визначення, що використовуються для позначення кібербезпеки різними суб'єктами, включаючи держави-члени ЄС, як правило, представляють різні точки зору, які потенційно можуть суперечити один одному. ENISA часто розглядає кібербезпеку як лише технічну проблему; деякі держави-члени у своїх стратегіях національної безпеки розглядають кібербезпеку як питання національної безпеки.

У контексті Директиви з безпеки мережевих та інформаційних систем («Директива NIS»), кібербезпека розуміється як «здатність мережевих та інформаційних систем протистояти будь-якій дії, яка порушує доступність, автентичність, цілісність або конфіденційність збережених, переданих або оброблених даних або пов'язаних з ними послугами» [13].

Тим не менше, Директива NIS формально стосується "безпеки мережевих та інформаційних систем", а не кібербезпеки. Неоднозначність, яка закладена та підтримувана терміном «кібербезпека» дозволяє використовувати цей термін у різних сферах політики, згаданих вище. Що ще важливе, тут виникає питання, чи є кібербезпека ЄС автономним поняттям, що має специфічний характер у політиці ЄС на відміну від інших рівнів політики.

У 2004 році Європейська Комісія схвалила рішення про створення дорадчого органу ENISA, яке вже перетворилось в Агентство кібербезпеки ЄС для надавання оперативної допомоги державам-членам ЄС в протидії кібератакам. Відповідну пропозицію 13 вересня 2017 року озвучив Президент Єврокомісії Жан-Клод Юнкер: «Європа все ще не оснащена належним чином, коли мова йде про кібератаки. Ось чому сьогодні Комісія пропонує нові

інструменти, включаючи Європейське агентство кібербезпеки, щоб допомогти нашому захисту проти таких атак» [14].

Агентство проводитиме щорічні пан-європейські навчання з кібербезпеки та обмін розвідувальною інформацією щодо кіберзагроз шляхом створення центрів обміну інформацією та аналізу. Ще однією важливою функцією Агентства визначено сертифікацію програмних продуктів на відповідність вимогам кібербезпеки в ЄС. Одночасно, Єврокомісія запропонувала створити Фонд реагування на надзвичайні ситуації з кібербезпеки, до якого можуть приєднатися держави-члени ЄС за бажанням.

Однак, започаткований наприкінці 2017 року в рамках безпекової ініціативи PESCO Європейський оборонний фонд, який серед іншого акумулював фінансові засоби й для проектів з кібероборони, фактично відсунув на другий план потребу створення окремого кібер-фонду ЄС.

Можна виділити п’ять стратегічних пріоритетів кібербезпеки ЄС:

- досягнення «кіберстійкості» шляхом встановлення мінімальних вимог до співробітництва та координації національних компетентних органів з питань безпеки мереж та інформаційних систем;

- зменшення кіберзлочинності шляхом забезпечення швидкого впровадження вимог Директиви NIS, заохочення ратифікації положень Будапештської конвенції Ради Європи про кіберзлочинність та фінансування програми для розгортання оперативних інструментів кіберзахисту;

- розробка спільної політики та розвиток можливостей кібероборони, пов’язаних із загальною безпекою та оборонною політикою в контексті кіберзахисту ЄС, розробка політики ЄС щодо кіберзахисту, стимулювання діалогу та координації між цивільними та військовими суб’єктами в ЄС, та сприяння діалогу з міжнародними партнерами;

- розвиток промислових та технологічних ресурсів для кібербезпеки шляхом створення державно-приватної платформи з питань мережевої та інформаційної безпеки, надання технічних вказівок та рекомендацій для прийняття стандартів та практики й заохочення розвитку стандартів безпеки;

- встановлення послідовної міжнародної політики щодо кіберпростору для ЄС та сприяння включення основних цінностей ЄС у спільну зовнішню політику та політику безпеки. ЄС повинен забезпечити проведення своїх консультацій з міжнародними партнерами з кіберпитань, що покликані доповнити існуючий порядок денний двостороннього діалогу між державами-членами та третіми країнами.

Ці консультації керуватимуться основними цінностями ЄС – людською гідністю, свободою, демократією, рівністю, верховенством права та повагою до основних свобод. Дотримуючись цілей цього пріоритету, ЄС прагне досягти високого рівня захисту даних, включаючи захист персональних даних, переданих третім країн.

Підсумовуючи вищезазначене, термін «кібербезпека», з точки зору ЄС, передбачає поєднання державної кіберстійкості, протидію кіберзлочинності, кіберзахисту та глобальні проблеми безпеки кіберпростору. В умовах зростаючих гібридних загроз, головним завданням європейських, та й інших країн світу є вжиття заходів, що дозволять принципово зменшити негативні наслідки від кіберінцидентів, гарантуючи безпеку цифрового розвитку.

Можливість надати різне значення терміну «кібербезпека» має як переваги, так і недоліки. Це вказує на гнучкість терміну, який може адаптуватися до мінливих обставин.

У той же час постійне розширення терміну може стати надмірно інклюзивним або широким таким чином, що перешкоджатиме узгодженому регулюванню в цій галузі та таким чином перешкоджатиме розробці регуляторних заходів. Це також відкриває простір для неоднозначності у

розумінні між ЄС та державами-членами, що спираються на поняття національної безпеки. Отже, таке змінне значення цього терміну може досягти прогресу в цій конкретній сфері політики важко досягти або, принаймні, менш помітним.

За декілька останніх десятиліть відбулася потужна технологічна революція в галузі використання комп'ютерів та телекомунікацій, яка привела до принципових змін та збільшення апаратного парку, суттєвого прискорення швидкості передачі інформації. Водночас саме стрімкий інформаційний прогрес спричинив проблему захищеності персональних даних через виникнення глобальних лідерів, що призвело до концентрації інформації в руках «великих гравців мережі» та централізації загальної інфраструктури.

Це зробило можливими великомасштабні атаки та створило великі ризики значних збитків при критичних пошкодженнях інфраструктури таких систем.

1.2. Концептуалізація кібербезпеки як сфери політики та правового регулювання в ЄС

Розглядаючи питання регулювання кібербезпеки в ЄС, необхідно враховувати принцип делегування, що є наскрізним для багатьох сфер спільної політики. ЄС може приймати законодавчі акти у сферах, що потребують колективного вирішення між державами-учасницями, зокрема й у сфері кібербезпеки, проте це вимагає надання юридичного обґрунтування, тобто правового підґрунтя [15]. Зокрема, пропозиція щодо законодавчого заходу повинна відповідати критеріям, викладеним у статті 5 Договору про ЄС (ДЕС).

Це означає, що для встановлення компетенції в певній галузі законодавча пропозиція повинна підпадати під одну з таких двох ситуацій:

1) запропоновані дії не можуть бути в достатній мірі досягнуті державами-членами ні на центральному рівні, ні регіональному та місцевому рівнях;

2) з точки зору масштабу або наслідків запропонованої дії краще її досягати на рівні Союзу (ДЕС; стаття 5).

Визначити потребу у запровадженні правового регулювання кібербезпеки на рівні ЄС намагались науковці, політики та представники приватного сектору. Щоб полегшити це завдання, Європейська Рахункова Палата, установа, яка опікується інтересами платників податків ЄС, опублікувала звіт, що забезпечує чудовий огляд складної політики ЄС щодо кібербезпеки.

Звіт визначає багато викликів ефективному здійсненню політики, таких як: змістовна оцінка та підзвітність політики та законодавчої бази; усунення прогалин у законодавстві ЄС та нерівномірності його упровадження; узгодження рівнів інвестицій в кібербезпеку з відповідними цілями; адекватне фінансування агентств ЄС; та посилення управління інформаційною безпекою, а також оцінки загроз та ризиків.[16]

Більшість правових заходів, що стосуються кібербезпеки, містяться в директивах, які є мінімальними заходами гармонізації (наприклад, Директива NIS та Директива про напади на інформаційні системи). На практиці це означає, що держави-члени вільні у виборі форми та методів реалізації вимог, що випливають з таких директив. Ця гнучкість може розглядатися як слабкість інструментів мінімальної гармонізації. Однак директиви вважаються найкращим інструментом при впровадженні складних законодавчих змін, таких як запровадження нової регуляторної сфери.[17, 106]

У деяких сферах, які є традиційно регламентовані більш суворо, таких як захист персональних даних та охорона здоров’я, спостерігається тенденція

до прийняття більш гармонізованого регулювання. Приклади включають Загальний регламент про захист даних (GDPR), що скасовує Директиву про захист даних 95/46 / ЕС та Регламент про медичні вироби (MDR), що скасовує Директиву про медичні вироби [18].

Європейському Союзу знадобилось понад 20 років для розгортання кібербезпекових ініціатив та вирішення питань, що стосуються цифрового середовища – від цифрових підписів до електронної комерції, протидії кіберзлочинності та захисту критичної інфраструктури. До того ж, кібербезпека, зовсім недавно охопила питання кібероборони.

Ще у 2001 році Європейська Комісія випустила повідомлення «Безпека мереж та інформації» [19]. Хоча в Європейській стратегії безпеки 2003 року кіберзагрози не увійшли до переліку загроз безпеці ЄС, але у звітах про її імплементацію кібербезпеці приділяється все більше уваги.

В якості концептуального документу ЄС у 2006 році була схвалена Стратегія безпечного інформаційного суспільства [20]. В подальшому кібербезпека стає невід'ємною складовою безпекових документів Євросоюзу. У 2009 році була схвалена нова стратегічна комунікація «Захист критичної інформаційної інфраструктури». У 2012 році в ЄС була створена Група з питань реагування на інциденти в галузі комп'ютерної безпеки, відповідальна за безпеку інформаційних систем інституцій ЄС. А у лютому 2013 року – схвалена перша стратегія кібербезпеки ЄС. Публікація першої стратегії кібербезпеки Європейського Союзу у 2013 році ознаменувала офіційне визнання «кібербезпеки» як нового напряму політики ЄС.

Глобальна стратегія із зовнішньої і безпекової політики ЄС, схвалена в червні 2016 року, стала основою для розробки інших секторальних та операційних документів. У ній кібербезпека виведена в окрему безпекову

сферу, яка включає розвиток технологічних можливостей для протидії кіберзагрозам, скорочення кіберзлочинності, посилення стійкості критичної інфраструктури, мереж і сервісів [21].

Пізніше, в липні 2016 року, ЄС схвалив Директиву з безпеки мережевих та інформаційних систем (Директива NIS). Відповідно до неї, держави-члени ЄС повинні були схвалити відповідні національні закони до 9 травня 2018 року і визначити операторів основних послуг (“essential services providers”) у цій сфері до 9 листопада 2018 року. Директивою була створена Група співробітництва NIS, на яку покладені функції забезпечення стратегічного співробітництва та обміну інформацією між державами-членами з питань кібербезпеки. Група здійснює безпосередню координацію мережі Груп реагування на інциденти комп’ютерної безпеки.

Кібер-стратегія ЄС “Відкритий, надійний і безпечний кіберпростір” [22] визначає такі стратегічні пріоритети ЄС: кіберстійкість, зменшення кіберзлочинності, розвиток можливостей і політики кіберзахисту, індустріальних і технологічних ресурсів кібербезпеки, послідовної міжнародної політики з кіберпростору.

У вересні 2017 року ЄС доповнив цю Стратегію, схваливши Спільну комунікацію Європейської служби зовнішньої дії і Єврокомісії з розбудови належної кібербезпеки ЄС [23]. Цей документ визначив пакет додаткових заходів, спрямованих, перш за все, на посилення Агентства кібербезпеки ЄС (ENISA), створення загальної для ЄС схеми сертифікації з кібербезпеки, розвиток Плану відповіді на масштабні кібератаки і кризи, посилення досліджень.

Наприкінці 2017 року в ЄС було запущено Постійне Структуроване Співробітництво, до якого приєднались 25 із 29 держав-членів Євросоюзу.

Одним із напрямків цієї співпраці стала кібербезпека, зокрема, розпочалось створення Груп швидкого реагування на кіберзагрози. Позитивним для України рішенням є те, що треті країни можуть запрошуватись до участі в окремих проектах PESCO, включаючи сферу кіберзахисту.

Восени 2017 року Європейська Комісія та Верховний представник Союзу із закордонних справ та політики безпеки опублікували спільне повідомлення до Європейського Парламенту та Ради Європейського Союзу під назвою "Стійкість, стримування та захист: побудова міцної кібербезпеки для ЄС" (Стратегія ЄС з кібербезпеки 2017 року) [24], яке базувалося на попередніх ініціативах та галузевій структурі.

Друга стратегія передбачила правові рамки для телекомунікацій, електронної комерції та електронних підписів, політичні та регуляторні заходи. Ця стратегія кібербезпеки наголосила на необхідності заходів, які дозволять підвищити стійкість ЄС до кібератак, вона допоможе виявляти кібератаки та посилити міжнародне співробітництво у галузі кібербезпеки. Стратегія наголошує на необхідності аналізу наслідків нових технологій та застосування заходів для усунення ризиків, які вони створюють. ЄК обіцяє переглянути існуючий закон основи для розгляду «нових технологічних розробок (включаючи робототехніку, Штучний інтелект та 3D-друк)». Потреба усунення відповідальності в цьому контексті знову з'являється в 2018 році.

В грудні 2018 року Європейський Парламент, Європейська Рада і Європейська Комісія досягли політичної згоди щодо Акту з кібербезпеки [25], який також посилює мандат ENISA, встановлює рамки для сертифікації з кібербезпеки, прискорює розвиток онлайн сервісів з кібербезпеки. Слід окреслити інституційний вимір кібербезпеки ЄС.

У вересні 2018 року Єврокомісія схвалила рішення про створення мережі центрів компетентності в державах-членах за координації Європейського центру досліджень і компетентності з кібербезпеки, яка сприятиме розвитку знарядь і технологій для протидії кіберзагрозам. З метою більшого залучення приватного сектору до протидії кіберзагрозам, в ЄС була створена Європейська платформа публічно-приватного партнерства стійкості. В рамках агентства Європол діє Європейський Центр протидії кібер-злочинності [26].

Як зазначає Р. Вессель, кібербезпека формує «чудовий приклад сфери, в якій необхідна комбінація різних напрямків політики (вимога щодо горизонтальної узгодженості), а також заходи на рівні ЄС, так і держав-членів (вимагаючи вертикальної узгодженості)» [27, 405].

Правова база ЄС в сфері кібербезпеки розвивається з урахуванням потреб цифрового ринку ЄС. Важливим є стратегічне бачення та заклик до більш всеохоплюючого, перехресного політичного підходу до формування кіберстійкості в рамках спільного цифрового ринку ЄС. Незважаючи на те, що стратегії не є юридично обов'язковими інструментами політики, в них уточняється роль різних агенцій ЄС, що формують спільну кібербезпекову політику.

Концептуалізація кібербезпеки як сфери політики та правового регулювання відбувається поступово та фрагментарно. У Європейському Союзі були прийняті численні регуляторні акти, які сприяють забезпеченню кібербезпеки громадян, підприємств та державних інституцій, що стосуються конкретних заходів мережевої та інформаційної безпеки, електронних комунікацій та протидії кіберзлочинності.

Підводячи підсумок, процес становлення кіберзаконодавства в державах-членах ЄС розпочався у 2001 році й досі набирає оберти, створюючи

нове законодавство в цій галузі. Однак з позиції системного підходу більшість проблем кібербезпеки виникає через відставання сучасної законодавчої бази від науково-технічного прогресу.

Незважаючи на існуючу сучасну низку документів щодо кібербезпеки, остання досі залишається досить вразливою, незалежно від ступеня розробки і стану законодавства, виявляючи випереджаючі проблемні науково-технічні прогалини щодо підвищення якості та стану кібербезпеки в ЄС загалом.

В праві Європейського Союзу виділяють п’ять стратегічних пріоритетів кібербезпеки ЄС:

- досягнення «кіберстійкості» шляхом встановлення мінімальних вимог до функціонування співробітництва та координації національних компетентних органів з питань безпеки мереж та інформаційних систем;

- зменшення кіберзлочинності шляхом забезпечення швидкого впровадження вимог директиви ЄС, заохочення ратифікації положень Будапештської конвенції Ради Європи про кіберзлочинність та фінансування програми для розгортання оперативних інструментів;

- розробка політики та можливостей кібедорони, пов’язаних із загальною безпекою та оборонною політикою шляхом оперативної оцінки кіберзахисту ЄС, розробка політики ЄС щодо кіберзахисту, стимулювання діалогу та координації між цивільними та військовими суб’єктами в ЄС, та сприяння діалогу з міжнародними партнерами;

- розвиток промислових та технологічних ресурсів для кібербезпеки шляхом створення державно-приватної платформи з питань мережевої та інформаційної безпеки, надання технічних вказівок та рекомендацій для прийняття стандартів та практики та заохочення розвитку стандартів безпеки;

- встановлення послідовної міжнародної політики щодо кіберпростору для ЄС та сприяння включення основних цінностей ЄС у спільну зовнішню політику та політику безпеки.

РОЗДІЛ 2
ІНСТИТУЦІЙНО-ПРАВОВІ ОСНОВИ СИСТЕМИ КІБЕРЗАХИСТУ У ЄС

2.1. Нормативно-правове забезпечення кібербезпеки в ЄС

У Європейському Союзі під безпекою мережевих та інформаційних систем розуміють здатність цих систем протистояти суперечливим випадковим подіям або незаконним чи зловмисним діям, що несуть загрозу для доступності, автентичності, цілісності та конфіденційності збережених або переданих даних і відповідних послуг, пропонованих або доступних через ці мережі та системи [28]. Для організації взаємодії країн ЄС у питаннях забезпечення безпеки спеціально створене Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA).

Також ENISA має аналізувати стратегії мережевої та інформаційної безпеки, сприяти представленню їх у форматі, що надається до порівняння, забезпечувати за допомогою електронних засобів доступність для громадськості стратегій та результатів їх аналізу, оприлюднених інституцією, органом, офісом або агентством Союзу чи державою-членом і наданих ENISA для отримання інформації та уникнення дублювання.

Директива з безпеки мережевих та інформаційних систем (Директива NIS) становить першу частину законодавства ЄС щодо кібербезпеки. Вона забезпечує правові заходи, спрямовані на підвищення загального рівня кібербезпеки в ЄС.

Документ ухвалений Європейським Парламентом 6 липня 2016 року і набрав чинності в серпні 2016 року, але держави-члени мали 21 місяць, щоб

транспонувати Директиву до своїх національних законів і понад 6 місяців, щоб визначити операторів основних послуг.

Директива NIS передбачає юридичні заходи для підвищення загального рівня кібербезпеки в ЄС. Для цього вона вимагає забезпечити: готовність держав-членів, їхнє належне оснащення, наприклад наявність групи з реагування на інциденти в галузі комп'ютерної безпеки (CSIRT) та компетентного національного органу (або органів); співробітництво між усіма державами-членами шляхом створення групи співпраці з метою підтримки та сприяння стратегічній взаємодії та обміну інформацією між державами-членами.

Крім того, їм необхідно було розбудувати мережу CSIRT, щоб сприяти швидкому та ефективному оперативному співробітництву щодо конкретних випадків кібербезпеки та обміну інформацією про ризики; культуру безпеки між секторами, що є життєво важливими для економіки та суспільства і, крім того, сильно залежать від ІКТ, наприклад: енергетика, транспорт, водопостачання, банківська справа, інфраструктура фінансового ринку, охорона здоров'я та цифрова інфраструктура.

Підприємства в цих секторах, що визначені державами-членами як оператори основних послуг, мають вживати відповідних заходів безпеки та повідомляти відповідним національним органам про серйозні інциденти. Крім того, основні цифрові постачальники послуг (пошукові системи, служби хмарних обчислень та інтернет-магазини) повинні відповідати вимогам безпеки та інформування відповідно до положень Директиви.

Сьомий пріоритет Східного партнерства до 2020 року «Зосередження уваги на ключових пріоритетах та відчутних результатах»[29] також підтверджує необхідність узгодження безпекових стратегій для досягнення єдиного цифрового ринку як в ЄС, так і з третіми країнами. 7 червня 2019 року

в Офіційному журналі ЄС опубліковано Регламент про кібербезпеку Європейського Союзу (Регламент (ЄС) 2019/881 Європейського Парламенту та Ради від 17 квітня 2019 року про ENISA (Агентство Європейського Союзу з питань кібербезпеки) та про сертифікацію кібербезпеки в галузі інформаційних та комунікаційних технологій та скасування Регламенту (ЄС) №526/2013) (далі — Регламент про кібербезпеку). Документ набрав чинності 27 червня 2019 року.

Право ЄС має на меті зміцнити спроможність Агентства Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) допомагати державам-членам подолати загрози кібербезпеки. Право ЄС про кібербезпеку має дві основні цілі:

1) посилення мандата ENISA як наглядового органу ЄС у сфері кібербезпеки, задля підтримки держав-членів ЄС у подоланні загроз та атак у цій сфері;

2) створення загальноєвропейської системи сертифікації кібербезпеки (Рамки), в якій ENISA відіграватиме ключову роль.

Відповідно до Регламенту про кібербезпеку, ENISA має координувати підготовку запропонованих схем сертифікації кібербезпеки, що подаються для ухвалення до Європейської Комісії. Регламент дасть можливість видавати європейські сертифікати кібербезпеки та акти про відповідність продукції, послуг та процесів ІКТ у всіх державах-членах ЄС.

Законодавство про кібербезпеку пропонує індустрії можливість засвідчити, що їхня продукція відповідає стандартам кібербезпеки ЄС. Сертифікація з питань кібербезпеки буде добровільною, якщо інше не встановлено законодавством ЄС або держав-членів.

Комісія ЄС регулярно оцінюватиме необхідність впровадження обов’язкових сертифікацій. Схема сертифікації може визначати один або кілька рівнів забезпечення безпеки: базовий, значний або високий. На

базовому рівні виробники ІКТ або постачальники послуг зможуть самі здійснювати оцінку відповідності. У випадку значного чи високого рівня ризиків, оцінювання здійснюватимуть національні органи з сертифікації кібербезпеки.

Держави-члени ЄС мають розробити законодавчі норми щодо відповідальності за порушення вимог Регламенту та за порушення схем сертифікації кібербезпеки ЄС. Законодавство про кібербезпеку є частиною загальної кіберекосистеми Європейського Союзу, мета якої — підвищення безпеки цифрового середовища Європейського Союзу та безпечне використання інформаційних послуг на Єдиному цифровому ринку.

Таким чином, до законодавства ЄС в сфері кібербезпеки можна віднести такі акти:

Директива (ЄС) 2016/1148 Європейського Парламенту та Ради від 6 липня 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу (Директива NIS), що встановлює вимоги щодо сповіщення та безпеки для операторів основних послуг та постачальників цифрових, наприклад хмарних, послуг [30];

Регламент (ЄС) 2016/679 Європейського парламенту та Ради від 27 квітня 2016 року про захист фізичних осіб щодо обробки персональних даних та про вільний рух таких даних та про скасування Директиви 95/46/ЄС [31];

Директива (ЄС) 2016/680 Європейського Парламенту та Ради від 27 квітня 2016 року про захист фізичних осіб щодо обробки персональних даних компетентними органами з метою запобігання, розслідування, виявлення або притягнення до відповідальності за кримінальні злочини чи виконання кримінальних покарань, а також про вільний рух таких даних та скасування Рамкового рішення Ради 2008/977/ПВР [32];

Директива 2002/58/ЄС Європейського Парламенту та Ради від 12 липня 2002 року щодо обробки персональних даних та захисту конфіденційності в секторі електронних комунікацій (Директива про конфіденційність та електронні комунікації)[33] і розроблений на її заміну Проєкт Регламенту електронної конфіденційності, спрямований на захист прав на приватність та конфіденційність комунікацій, а також на просування надійного та безпечного «Інтернету речей» на єдиному цифровому ринку [34];

Директива 2014/24/ЄС Європейського Парламенту та Ради від 26 лютого 2014 року щодо державних закупівель та скасування Директиви 2004/18/ЄС [35];

Регламент (ЄС) №593/2008 Європейського Парламенту та Ради від 17 червня 2008 року «Про право, що застосовується до договірних зобов'язань (Рим I)» [36];

Директива (ЄС) 2015/1535 Європейського Парламенту та Ради від 9 вересня 2015 року, що встановлює порядок надання інформації у сфері технічних регламентів та правил щодо послуг інформаційного суспільства [37];

Рамкове рішення Ради 2006/960/JHA від 18 грудня 2006 року «Про спрощення обміну інформацією та розвідувальних данних між правоохоронними органами держав-членів Європейського Союзу» [38];

Директива 2014/41/ЄС Європейського Парламенту та Ради від 3 квітня 2014 року щодо Європейського наказу про розслідування у кримінальних справах [39];

Конвенція Ради Європи про кіберзлочинність, CETS №185[40];

Регламент Ради (ЄС) №1206/2001 від 28 травня 2001 року про співпрацю між судами держав-членів у справі отримання доказів у цивільних чи господарських справах [41];

Директива 2008/114/ЄС від 8 грудня 2008 року Європейського Парламенту та Ради про ідентифікацію та призначення європейських критичних інфраструктур та оцінку необхідності вдосконалення їх захисту [42];

Регламент (ЄС) 2018/1807 Європейського Парламенту та Ради від 14 листопада 2018 р. про рамки для вільного обміну неособистими даними в Європейському Союзі [43].

Право Європейського Союзу про кібербезпеку не розглядає окремо заходи з кібербезпеки, захист конфіденційності й захист мереж та / або інформаційних систем, а має на меті узгоджені дії щодо захисту засобів, інформації та конфіденційності як частину екосистеми кібербезпеки.

Директива NIS є першим інструментом внутрішнього ринку, спрямованим на підвищення опірності ЄС до ризиків у сфері кібербезпеки. Вона орієнтована на забезпечення безперервності послуг, що дають економіці та суспільству ЄС змогу функціонувати належним чином. З цією метою Директива NIS запроваджує конкретні заходи з розбудови можливостей кібербезпеки в ЄС та зменшення зростаючих загроз для мережевих та інформаційних систем, які використовуються для надання основних послуг у ключових секторах.

Директива NIS:

«(а) встановлює обов’язки всіх держав-членів щодо ухвалення національної стратегії з безпеки мережевих та інформаційних систем;

(b) створює Групу з питань співробітництва з метою підтримки та сприяння стратегічному співробітництву й обміну інформацією між державами-членами та розвитку довіри між ними;

(c) створює мережу команд реагування на комп'ютерну безпеку («мережа CSIRT»), щоб сприяти розвитку довіри між державами-членами й швидкій та ефективній оперативній співпраці;

(г) встановлює вимоги щодо безпеки та оповіщення для операторів основних послуг та для постачальників цифрових послуг;

(e) встановлює обов'язки держав-членів щодо призначення національних компетентних органів, єдиних контактних пунктів та CSIRT із завданнями, пов'язаними з безпекою мережевих та інформаційних систем» 44.

Після набрання Директивою NIS чинності, тобто з серпня 2016 року, держави-члени мали до 9 травня 2018 року імплементувати у національне законодавство інструменти й заходи, необхідні для виконання її положень.

Отже, проведений аналіз дозволяє стверджувати, що метою Директиви NIS є гарантування високого загального рівня безпеки мережевих та інформаційних систем в рамках ЄС. Для того, щоб цього домогтися, було вирішено зобов'язати держави-учасники підвищити свою готовність і поліпшити співпрацю один з одним, а також зобов'язати операторів, які надають критично важливі послуги, пов'язані з певними об'єктами інфраструктури, і провайдерів окремих цифрових послуг вжити відповідних заходів з управління ризиками безпеки і повідомляти про серйозні інциденти компетентним національним органам.

2.2 Стратегія кібербезпеки ЄС: загальна характеристика

“Стратегія кібербезпеки ЄС на цифрове десятиліття” (2020) [45] спрямована на захист глобального та відкритого Інтернету, одночасно пропонуючи захисні заходи не лише для забезпечення безпеки, але й для захисту європейських цінностей та основних прав кожного.

Спираючись на досягнення минулих місяців та років, він містить конкретні пропозиції щодо регуляторних, інвестиційних та політичних ініціатив у трьох сферах дій ЄС:

Відповідно до цього напряму, комісія з кібербезпеки пропонує реформувати правила безпеки мережевих та інформаційних систем відповідно до директиви про заходи щодо високого загального рівня кібербезпеки в усьому Союзі з метою збільшення рівня кіберстійкості критично важливого державного та приватного секторів: лікарні, енергосистеми, залізниці, а також центри обробки даних, державні адміністрації, дослідницькі лабораторії та виробництво критично важливих медичних виробів та ліків, а також іншої критичної інфраструктури та послуг.

Комісія також пропонує запустити мережу операційних центрів безпеки по всьому ЄС, що працюють на основі штучного інтелекту, що буде справжнім “щитом кібербезпеки” для ЄС, здатного досить рано виявляти ознаки кібератаки та забезпечувати активність дії до виникнення пошкодження.

Додаткові заходи включатимуть спеціальну підтримку малого та середнього бізнесу в рамках центрів цифрових інновацій, а також посилення зусиль для підвищення кваліфікації робочої сили, залучення та збереження найкращих талантів у галузі кібербезпеки та інвестування у відкриті наукові дослідження та інновації, конкурентоспроможні та засновані на досконалості.

ЄС активізує роботу з міжнародними партнерами з метою зміцнення глобального порядку, заснованого на правилах, сприяння міжнародній безпеці та стабільності в кіберпросторі та захисту прав людини та основних свобод в

Інтернеті. Він сприятиме розвитку міжнародних норм та стандартів, що відображають основні цінності ЄС, співпрацюючи зі своїми міжнародними партнерами в ООН.

ЄС і надалі зміцнюватиме свій набір інструментів кібердипломатії ЄС та збільшуватиме зусилля з розбудови кібернетичного потенціалу для країн третього світу шляхом розробки порядку денного розбудови зовнішнього кіберпотенціалу ЄС. Буде активізований кібердіалог регіональними та міжнародними організаціями, а також спільнотою із багатьма зацікавленими сторонами. ЄС також сформує мережу кібердипломатії у всьому світі для просування свого бачення кіберпростору.

ЄС прагне підтримувати нову стратегію кібербезпеки, щоб перейти на новий рівень кібербезпеки протягом наступних семи років через наступний довгостроковий бюджет, зокрема програму цифрової Європи та Horizon Europe. Таким чином, державам рекомендується повною мірою використовувати механізм відновлення та стійкості для посилення кібербезпеки та відповідності інвестиціям на рівні ЄС.

Мета полягає в тому, щоб досягти до 4,5 млрд. євро спільних інвестицій з державами, зокрема в рамках центру компетенції з питань кібербезпеки та мережі координаційних центрів.

Стратегія також спрямована на зміцнення промислового та технологічного потенціалу ЄС у галузі кібербезпеки, в тому числі за допомогою проектів, що підтримуються спільно з ЄС та національними бюджетами. ЄС має унікальну можливість об’єднати свої активи для підвищення своєї стратегічної автономії та просування свого лідерства в галузі кібербезпеки у цифровому ланцюжку поставок (включаючи дані та хмари, процесорні технології наступного покоління, надзахищені підключення та мережі 5G) відповідно до своїх цінностей та пріоритетів.

Існуючі заходи на рівні ЄС, спрямовані на захист ключових послуг та інфраструктур як від кібер-, так і від фізичних ризиків, потребують оновлення. Ризики кібербезпеки продовжують розвиватися із зростанням цифровізації та взаємозв'язку. Фізичні ризики також ускладнились після прийняття у 2008 р. правил ЄС щодо критичної інфраструктури, які наразі охоплюють лише енергетичний та транспортний сектори. Ці перегляди мають на меті оновити правила, дотримуючись логіки стратегії Європейського Союзу Безпеки, подолати хибну дихотомію між Інтернетом та Інтернетом та зламати підхід до силосу.

Щоб відповісти на зростаючі загрози внаслідок оцифровування та взаємозв'язку, запропонована директива NIS-2 про заходи щодо високого загального рівня кібербезпеки в усьому Союзі, охоплюватиме середні та великі організації з більшої кількості секторів на основі їхньої критичності економіки та суспільства.

NIS-2 посилює вимоги безпеки, що накладаються на компанії, вирішує питання безпеки ланцюгів поставок та відносин з постачальниками, впорядковує зобов'язання щодо звітності, запроваджує більш жорсткі наглядові заходи для національних органів влади, жорсткіші вимоги до виконання та спрямований на гармонізацію режимів санкцій у державах-членах. Пропозиція NIS-2 допоможе розширити обмін інформацією та співпрацю щодо управління кіберкризами на національному рівні та на рівні ЄС.

Запропонована директива щодо стійкості критичних суб'єктів (CER) розширює сферу дії Європейської директиви про критичну інфраструктуру 2008 року. Зараз охоплено десять секторів: енергетика, транспорт, банківська справа, інфраструктура фінансового ринку, охорона здоров'я, питна вода, стічні води, цифрова інфраструктура, державне управління та космос.

Відповідно до запропонованої директиви, держави-члени повинні прийняти національну стратегію забезпечення стійкості критично важливих структур та проводити регулярні оцінки ризиків. Ці оцінки також допоможуть визначити меншу підгрупу критично важливих суб'єктів, на яких покладатимуться зобов'язання, спрямовані на підвищення їх стійкості до некібернетичних ризиків, включаючи оцінки ризиків на рівні суб'єктів господарювання, вживання технічних та організаційних заходів та повідомлення про події. Комісія, в свою чергу, надаватиме додаткову підтримку державам-членам та критично важливим структурам,

Тепер Європейському Парламенту та Раді слід вивчити та прийняти запропоновану директиву NIS 2 та директиву про стійкість критичних суб'єктів. Після узгодження та, відповідно, прийняття пропозицій, держави повинні будуть їх впровадити протягом 18 місяців з моменту набрання ними чинності.

Нова Стратегія кібербезпеки пропонує інтегрувати кібербезпеку у всі елементи поставок та зблизити діяльність та ресурси ЄС у чотирьох колонах кібербезпеки – внутрішньому ринку, правоохоронних органах, дипломатії та обороні. Вона базується на формуванні «цифрового майбутнього Європи» та «Стратегії безпеки ЄС», а також спирається на низку законодавчих актів, дій та ініціатив, які ЄС запровадив для зміцнення потенціалу кібербезпеки та забезпечення більш стійкого кіберзахисту.

Таким чином, можна запропонувати такі основні етапи та здобутки розвитку кібербезпекової політики ЄС:

- до 2001 року – зародження кібербезпекової політики ЄС;
- 2001 – 2004 роки – прийняття та реалізація першої стратегії «Безпека мережі та інформації»;
- 2004 – 2012 рік – утворення і розвиток Агентства ENISA;
- 2013 – 2016 рік – друга стратегія кібербезпеки;

- 2017 – 2019 рік – стратегія «Стійкість, стримування та захист: побудова міцної кібербезпеки для ЄС»;
- з 2020 року – «Стратегія кібербезпеки ЄС на цифрове десятиліття».

Стратегія кібербезпеки ЄС 2020 року визначає такі пріоритети:

- захисні заходи не лише для забезпечення безпеки, але й для захисту європейських цінностей та основних прав кожного;
- ЄС прагне підтримувати нову стратегію кібербезпеки, щоб перейти на новий рівень кібербезпеки протягом наступних семи років;
- державам рекомендується повною мірою використовувати механізм відновлення та стійкості для посилення кібербезпеки.

2.3 Європейське агентство з питань інформаційної та мережевої безпеки (ENISA)

Агентство Європейського Союзу з кібербезпеки, ENISA, є агентством Союзу, що займається досягненням високого загального рівня кібербезпеки в Європі.

Створене в 2004 році та посилене Законом ЄС про кібербезпеку, Агентство Європейського Союзу з кібербезпеки вносить свій внесок у кіберполітику ЄС, підвищує надійність продуктів, послуг та процесів ІКТ за допомогою схем сертифікації кібербезпеки, співпрацює з державами-членами та органами ЄС та допомагає Європі підготуватися для кібервикликів. Шляхом обміну знаннями, розбудови спроможності та підвищення обізнаності Агентство працює разом зі своїми ключовими зацікавленими сторонами, щоб зміцнити довіру до пов’язаної економіки, підвищити стійкість інфраструктури Союзу та, зрештою, зберегти європейське суспільство та громадян у цифровій безпеці.

ENISA доручається активізувати оперативну співпрацю на рівні ЄС, допомагаючи державам-членам ЄС, які бажають звернутися з ним, для вирішення їхніх інцидентів в галузі кібербезпеки, а також підтримуючи координацію діяльності ЄС у разі масштабних транскордонних кібератак та криз. Це завдання ґрунтується на ролі ENISA як секретаріату національної мережі команд реагування на інциденти комп'ютерної безпеки (CSIRT), створеної Директивою про безпеку мережі та інформаційних систем (Директива NIS).

Європейська система сертифікації кібербезпеки. Закон ЄС про кібербезпеку запроваджує загальноєвропейську систему сертифікації кібербезпеки для продуктів, послуг та процесів ІКТ. Компанії, що ведуть бізнес в ЄС, виграють від необхідності сертифікувати свої ІКТ-продукти, процеси та послуги лише один раз і бачити їх сертифікати визнаними в Європейському Союзі.

Кібербезпека має досягти високого загального рівня кібербезпеки в ЄС у співпраці з широкою спільнотою. Місією ENISA є вдосконалення мережевої та інформаційної безпеки в Європейському Союзі. Агентство має сприяти розвитку культури мережевої та інформаційної безпеки на користь громадян, споживачів, підприємств та громадських організацій Європейського Союзу, сприяючи безперебійному функціонуванню внутрішнього ринку ЄС.

ENISA допомагає Європейській Комісії, державам-членам ЄС та індустрії виконувати вимоги мережевої та інформаційної безпеки. ENISA стає центром експертизи як для держав-членів, так й для інституцій ЄС з отримання консультацій з питань, пов'язаних із мережевою та інформаційною безпекою.

Посилені та розширені завдання Агентства у галузі оперативної співпраці були перевірені в 2020 році протягом коронавірусної кризи. Діючи в контексті статті 7 Регламенту, ENISA взяла на себе вжиття низки заходів, які зіграли важливу роль у допомозі органам ЄС координувати свою діяльність

протягом початкових фаз пандемії та у підвищенні стійкості ЄС. Управління ENISA здійснюється виконавчим директором та підтримується персоналом, який складається з фахівців, що представляють галузь інформаційних та комунікаційних технологій, груп споживачів та наукових експертів.

Агентство контролює правління, яке складається з представників держав-членів ЄС, Європейської комісії та інших зацікавлених сторін. Була також створена постійна група зацікавлених сторін, яка надає консультації Виконавчому директору.

Агентству потрібно буде передбачити і бути готовим зробити свій внесок у розвиток та імплементація законів та політики ЄС в різні сектори, у тому числі щодо європейського кодексу електронних комунікацій (EECC), шляхом надання досвіду та технічного внеску у кібербезпеку.

З огляду на вище зазначене, функціями Агентства ENISA є надання допомоги Європейській Комісії, державам-членам ЄС та бізнесу виконувати вимоги мережевої та інформаційної безпеки, включаючи чинне та майбутнє право ЄС; ENISA є центром експертизи як для держав-членів, так й для інституцій ЄС з отримання консультацій з питань, пов’язаних із мережевою та інформаційною безпекою; Агентство вносить в розвиток свій внесок та імплементації законів та політики ЄС в різні сектори в сфері кібербезпеки тощо.

РОЗДІЛ 3
КІБЕРБЕЗПЕКА УКРАЇНИ В КОНТЕКСТІ ЄВРОАТЛАНТИЧНОЇ ІНТЕГРАЦІЇ

3.1. Наближення законодавства України до стандартів ЄС і НАТО

Україна перебуває на начальному етапі імплементації до національного законодавства положень права ЄС щодо кібербезпеки та захисту об'єктів критичної інфраструктури. Законодавство щодо державного регулювання в зазначених сферах потребує суттєвого доопрацювання і корекції з огляду на необхідність тіснішої співпраці і взаємодії із ЄС та НАТО, а в частині захисту об'єктів критичної інфраструктури — розробки повноцінної державної політики.

Узгодження процедур і протоколів взаємодії між Україною та ЄС може посилити загальну спільну безпеку кіберпростору не тільки в геополітичному вимірі, але й практичному – для уможливлення інтеграції України до цифрового ринку ЄС. Відповідно до Національного індексу кібербезпеки, за яким Естонська академія електронного врядування вимірює готовність країн до запобігання кіберзагрозам та управління кіберінцидентами, Україна посідає в рейтингу 28 місце з-поміж 152 країн [46].

Аналіз складових Національного індексу кібербезпеки показує недостатність заходів, застарілість інформації. Рейтинг складався на підставі офіційних даних органів влади, але їхня оцінка відрізняється від оцінки, наданої громадянським суспільством і експертами в цій сфері[47][48]. На підставі Національного індексу кібербезпеки слід зазначити, що в Україні зафіксовано нерозвинутість деяких складових кібербезпеки:

- відсутній підрозділ аналізу кіберзагроз;
- відсутні опубліковані щорічні громадські звіти;
- відсутні вимоги до компетенцій з кібербезпеки у молодшій та середній школі; країна не входить до регіональної чи міжнародної організації з кібербезпеки;
- за останні 3 роки країна не (спів)фінансувала або (спільно) не організувала принаймні один проект з нарощування потенціалу для іншої країни;
- відсутній стандарт кібербезпеки для державного сектора;
- уряд не має компетентного органу в галузі кібер/інформаційної безпеки, уповноваженого контролювати державних та приватних постачальників цифрових послуг щодо виконання вимог кібер/інформаційної безпеки;
- відсутній регулярний моніторинг заходів кібербезпеки;
- не встановлено регулювання для відмітки часу при наданні електронних довірчих послуг; уряд не призначив єдиний контактний пункт для міжнародної координації кібербезпеки;
- відсутні механізми врегулювання кіберкризових ситуацій;
- відсутній підрозділ із військових кібероперацій;
- не впроваджено відповідне тренування з моделюванням сценаріїв інцидентів у реальному часі, яке має важливе значення для перевірки готовності й співпраці держав-членів у питаннях безпеки мережевих та інформаційних систем.

Згідно з дослідженнями науковців [49], індекс розвитку цифрової економіки DESI [50] для України становить 0,18, що значно нижче за середнє значення в ЄС. З метою розвитку цифрової економіки та забезпечення національної безпеки в кіберпросторі необхідно здійснити низку узгоджених

із ЄС дій, які можуть слугувати базою для Єдиного цифрового ринку[51] між Україною і ЄС. У Спільній декларації саміту Східного партнерства у листопаді 2017 року учасники саміту погодилися співпрацювати у сфері гармонізації цифрових ринків, щоб поширити вигоди ЄЦР ЄС для країн-партнерів. Відповідний пріоритет зазначений серед 20 очікуваних досягнень до 2020 року [52].

Ключовими завданнями в рамках наближення законодавства України до законодавства ЄС задля поширення режиму внутрішнього ринку ЄС на базову для цифрової економіки сферу телекомунікацій є імплементація актів ЄС у законодавство України. Інтеграція України до Єдиного цифрового ринку ЄС є одним із пріоритетних завдань для України.

Угода про асоціацію між Україною та ЄС закладає чітке юридичне підґрунтя для досягнення цієї мети. Угода про асоціацію передбачає перспективу взаємного надання режиму внутрішнього ринку в секторі телекомунікаційних послуг. Відповідно до статті 4 Додатку XVII до Угоди про асоціацію, такий режим означає, що в цьому секторі не має бути обмежень щодо надання послуг українською юридичною особою на території ЄС і навпаки. Режим можна отримати за умови позитивного оцінювання Європейським Союзом кроків України з наближення нормативно-правових актів України до права ЄС.

Зближення ринків можливе за умови: 1) наближення нормативно-правового регулювання; 2) наявності тотожних регуляторів ринку та чіткого розподілу повноважень між органами, якщо регуляторів сфери, що належить до певного ринку, більш ніж один; 3) однакового або зрозумілого технічного регулювання й стандартизації сфери. Таким чином, інтеграція України до Єдиного цифрового ринку ЄС можлива за умови наближення усіх трьох складових до європейських норм, правил і стандартів.

У рамках виконання завдань забезпечення кібербезпеки України та створення можливостей для участі в Єдиному цифровому ринку ЄС Верховна Рада України ухвалила Закон України “Про основні засади забезпечення кібербезпеки України”, яким, зокрема, визначено сферу застосування закону, понятійний апарат, базові принципи, об’єкти та суб’єкти кібербезпеки й кіберзахисту, їхні завдання, способи державно-приватного партнерства, у тому числі й щодо формування і розвитку системи кіберзахисту об’єктів критичної інфраструктури.

На підставі зазначеного закону суб’єкти кібербезпеки та кіберзахисту розробили низку підзаконних актів, якими затверджено порядок формування переліку об’єктів критичної інформаційної інфраструктури, порядок внесення об’єктів критичної інформаційної інфраструктури до державного реєстру об’єктів критичної інформаційної інфраструктури, його формування та забезпечення функціонування; загальні вимоги щодо кіберзахисту об’єктів критичної інфраструктури, критеріїв та порядку віднесення об’єктів до об’єктів критичної інфраструктури; критерії формування переліку об’єктів критично інформаційної інфраструктури. Але більшість із них досі залишаються у статусі проєктів.

З огляду на важливість та актуальність завдань щодо захисту об’єктів критичної інфраструктури, зокрема критичної інформаційної інфраструктури, уряд ухвалив Концепцію створення державної системи захисту критичної інфраструктури [53], якою визначено шляхи і способи розв’язання проблем забезпечення захисту критичної інфраструктури.

Серед них — розробка проекту закону про критичну інфраструктуру та її захист, яким має бути визначено основні напрями, принципи, механізми й строки комплексного правового врегулювання питання захисту критичної інфраструктури та створення системи державного управління у сфері захисту

критичної інфраструктури, комплекс заходів на загальнодержавному, регіональному, галузевому, а також на місцевому та об'єктовому рівнях, критерії, за сукупністю яких об'єкти мають відноситися до критичної інфраструктури, порядок категоризації та паспортизації таких об'єктів, складання та ведення їх реєстру, а також завдання з кіберзахисту суб'єктів державної системи захисту критичної інфраструктури та загальні вимоги з кіберзахисту до операторів критичної інфраструктури.

Угодою про асоціацію прямо не передбачено зобов'язань щодо імплементації актів ЄС з кібербезпеки та захисту об'єктів критичної інфраструктури. Але оскільки вони є фундаментальними засадами Єдиного цифрового ринку ЄС, а Україна має на меті приєднатися до нього, постала необхідність визначити механізми й процедури імплементації актів, що не увійшли до числа Додатків до Угоди про асоціацію.

У грудні 2019 року було оновлено План заходів з виконання Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони, затверджений Постановою Кабінету Міністрів України №1106 від 25 жовтня 2017 р. «Про виконання Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони».

У квітні 2018 року Україна надала для розгляду ЄС звернення про розширення сфери дії Угоди про асоціацію та оновлення Додатку XVII до Угоди про асоціацію — внесення до нього 18 актів законодавства ЄС. Документ було проаналізовано місією ЄС, оскільки більшість цих матеріалів також були перелічені в Плані заходів, що теж подавався для аналізу.

Більшість із законодавчих актів, перелічених у документі, безпосередньо не стосуються телекомунікаційних послуг. Через специфічні положення

Додатку про телекомунікації включення цих актів розширило б саме сферу телекомунікацій, хоча ці акти є лише дотичними і формально до цієї царини не належать. При цьому деякі інші сфери, що підлягають імплементації зазначені в інших розділах чи додатках Угоди про асоціацію.

Влітку 2018 року в контексті обговорень запиту ЄС повідомив Україні, що неофіційний документ не є достатньою основою для подальшої співпраці, адже Угода про асоціацію чітко передбачає формальні підстави для співробітництва в галузях, на які поширюється Додаток XVII.

Таким формальним кроком є подання дорожньої карти, вимоги до якої викладені у статті 2 Додатку XVII-6 до Угоди про асоціацію. У серпні 2018 року Україна подала Цифрову дорожню карту, розроблену на підставі Концепції розвитку цифрової економіки та суспільства України на 2018–2020 роки та плану заходів щодо її реалізації, де окреслено заходи з імплементації правових актів, що містяться в Додатку про телекомунікації. Крім того, ця дорожня карта також містить заходи з впровадження ширшого переліку нормативно-правових актів, зокрема попередніх, поданих у квітні 2018 року. З огляду на важливість цього документу та визначені юридичні питання ЄК запропонувала багатоетапний процес оцінки цифрової дорожньої карти. У межах виконання наявних зобов'язань передбачено три фази процесу:

Фаза 1: внутрішній глибокий аналіз кожного акту, зазначеного в Дорожній карті.

Фаза 2: оцінка виконання наявних зобов'язань, адміністративної спроможності та законодавства на практиці (зокрема оцінка на місці).

Фаза 3: робочий план виконання зобов'язань відповідно до Додатку XVII до Угоди про асоціацію із зазначенням пріоритетів, термінів та орієнтирів виконання.

Європейська Комісія запропонувала цей багатоступеневий процес, прагнучі надати Україні конструктивну та прагматичну допомогу у виконанні

зобов’язань за Угодою про асоціацію. При цьому багатоетапний процес не замінює інші формальні кроки, передбачені в Угоді про асоціацію.

Режим внутрішнього ринку у секторі не надається автоматично. Щойно Україна переконається, що умови фази завершення, прийняття та впровадження, зокрема забезпечення належного регуляторного потенціалу та нагляду в певному секторі, а також усі домовленості виконано, вона має повідомити ЄС про необхідність комплексної оцінки в цьому секторі. Тільки після успішного проходження оцінки ЄС та Україна можуть вирішити надати одне одному режим внутрішнього ринку в секторі.

Наразі Україна за результатами перемовин із ЄС узгодила інший механізм внесення змін до Угоди та оновлення додатків, який стане в пригоді для вирішення питання імплементації актів ЄС, що не увійшли до Угоди про асоціацію або були змінені з часу її підписання.

Отже, ключовими завданнями в рамках наближення законодавства України до законодавства ЄС задля поширення режиму внутрішнього ринку ЄС на базову для цифрової економіки сферу телекомунікацій є імплементація актів ЄС у законодавство України. Інтеграція України до Єдиного цифрового ринку ЄС є одним із пріоритетних завдань для України.

З огляду на необхідність впровадження європейського законодавства та гармонізації різних підходів до кібербезпеки, необхідно розробити нову Стратегію кібербезпеки з окремим розділом, присвяченим мережевої та інформаційної безпеки і, відповідно, етапам, цілям і показниками ефективності, запропонованим ENISA. Оновлена Стратегія кібербезпеки України повинна встановити основні принципи планування, бюджетування, реалізації та аналізу ефективності заходів щодо реалізації Стратегії кібербезпеки України, які не повинні суперечити заходам і принципам, визначеним законом.

Повноцінний розвиток України неможливий без створення належного державно-правового забезпечення кіберзахисту на національному рівні, а також єдиної стійкої і функціональної системи внутрішніх справ, як частини сектора національної безпеки, а також громадську безпеку, враховуючи останні тенденції і нововведення у вітчизняній нормативно-правовій базі. Сучасні загрози національній безпеці України з'явились на фоні впливу соціально-демографічних, економічних, політичних, правових, психологічних і технологічних чинників.

Ці фактори потребують системного реагування, належної та прогресивної трансформації сектора безпеки і системи внутрішніх справ. Тому для повноцінного розвитку держави і забезпечення належної національної безпеки необхідно якісне і результативне державно-правове забезпечення.

3.2. Співробітництво між Україною та НАТО в сфері кібербезпеки

Запорукою розбудови України як суверенної незалежної держави є формування національної системи кібербезпеки, що включає створення ефективних механізмів протидії кіберзагрозам, серед яких найсуттєвішу загрозу становлять кібервійна та кіберзлочинність. Актуальність проблеми міжнародного співробітництва обумовлена проблемами зростання кількості, видів та рівнів кіберзагроз та кіберінцидентів в кіберпросторі, масштабним та динамічним впровадженням ІКТ в усі сфери суспільного життя, розбудовою цифрового суспільства та держави, неможливістю ні однієї з країн самостійно розв'язати ці проблеми, а для України додатково – веденням проти неї РФ гібридної війни.

Розбудова національної системи кібербезпеки, здатної забезпечити належну протидію кіберзагрозам національній безпеці держави, є нагальним завданням, що постало сьогодні перед Україною. У цьому контексті, з

урахуванням транснаціонального та транскордонного характеру кіберзагроз набуває особливого значення міжнародне співробітництво в ці сфері. Насамперед йдеться про співробітництво з Північноатлантичним Альянсом, який з самого початку агресії РФ надає нам практичну допомогу зі зміцнення обороноздатності України.

Кіберзахист є частиною основного завдання колективної оборони НАТО. Кіберзагрози безпеці Альянсу стають все більш частими, складними, руйнівними та нагальними. НАТО продовжуватиме пристосовуватися до мінливого ландшафту кіберзагроз, а члени Альянсу покладаються на надійну та стійку кіберзахист для виконання основних завдань щодо колективної оборони, врегулювання криз та кооперативної безпеки. Щоб не відставати від швидкоплинних змін і підтримувати надійний кіберзахист, Північноатлантичний альянс прийняв посилену політику та план дій, які були схвалені союзниками на саміті в Уельсі у вересні 2014 р.[54].

Однією з фаз розвитку та вдосконалення інформаційної безпеки України в контексті кризи, було створення цільового фонду Україна-НАТО з питань кібероборони (NATO-Ukraine Trust Fund on Cyber Defense / TF CD) [55]. Цільовий фонд Україна-НАТО з кіберзахисту (NATO-UKRAINE TF CD) був узгоджений Альянсом та Україною під час саміту в Уельсі в НАТО в 2014 році [56].

На вищезгаданому саміті союзники по НАТО розробили комплексний і адаптований пакет заходів, щоб Україна могла краще забезпечувати свою безпеку. Першою фазою, було зосередження на кіберзахисті, основною метою якого, було надати допомогу Україні для розвинення технічних можливостей для протидії кіберзагрозам. З метою формування правової бази для процесу нарощування потенціалу та можливостей національної кібербезпеки України

були зроблені кроки щодо формулюванню законодавства кіберзахисту. Для забезпечення успішного розвитку потенціалу кібербезпеки України також необхідне ефективне міжвідомче і міжнародне співробітництво в сфері кіберзахисту, а для цього потрібен конкретний і ефективний механізм такої співпраці.

Розвиток оборонних кіберможливостей України здійснювався шляхом впровадження передових технічних рішень і систем кіберзахисту на об'єкти критичної інфраструктури України з метою забезпечення належного рівня кібербезпеки, навчання персоналу з обслуговування та управління встановленими системами і створення лабораторій комп'ютерної та мережевої криміналістики з їх стаціонарними і мобільними компонентами.

Проєкт НАТО-УКРАЇНА TF CD був спрямований на надання Україні необхідної підтримки для розвитку її оборонних технічних можливостей типу CSIRT, лабораторій з розслідування інцидентів кібербезпеки і центрів управління інцидентами, а також для забезпечення безпеки однієї або декількох критичних інформаційних інфраструктур (Critical Information Infrastructures / CII) [57]. Проєкт також включав навчальний і консультативний аспекти з адаптивним підходом, заснованим на інтересах як союзників, так і України. Такий підхід забезпечив конкретні і значимі результати в короткостроковій перспективі. Для виконання мети проекту його основними характеристиками були:

виключно оборонний характер;

аспект навчання і консультування;

масштабований підхід в залежності від наявних коштів.

З самого початку передбачалося, що проект буде змінюватися в розмірах, відповідно до внесків, отриманих від країн, і з можливістю розширення. Обладнання, програмне забезпечення та навчання, необхідні для

реалізації НАТО-Україна TF CD, були підтримані з бюджету Фонду. Всі апаратні засоби і програмне забезпечення, необхідні для його реалізації, були придбані на міжнародному ринку.

Друга фаза проєкту була спрямована на подальше зміцнення виключно захисних кібертехнічних можливостей України на основі масштабованого технічного проекту. Основні задачі фази:

залучити нові внески для подальшого розвитку української кібербезпеки та оборонної спроможності;

забезпечити захист більшої кількості об'єктів критичної інфраструктури відповідно до потреб України;

провести навчальні курси для українських бенефіціарів відповідно до потреб, виявлених після роботи з інтегрованою системою кібербезпеки та оборони, впровадженою на першій фазі проєкту.

На саміті у Варшаві у 2016 році союзники підтвердили оборонний мандат НАТО і визнали кіберпростір сферою операцій, в рамках яких НАТО повинна захищати себе так само ефективно, як у повітрі, на суші та на морі. Оскільки більшість конфліктів сьогодні мають кібервиміри, розгляд кіберпростору як домену дозволяє НАТО краще захищати та виконувати свої місії та операції [58]. У Варшаві, члени Альянсу, також пообіцяли посилити кіберзахист національних мереж та інфраструктур, як першочергове завдання.

Кіберзахист також був інтегрований в ініціативі НАТО «Розумна оборона» [59]. Розумна оборона – це концепція, яка спонукає союзників до співпраці у розробці, придбанні та підтримці військового потенціалу для вирішення поточних проблем безпеки відповідно до нової стратегічної концепції НАТО.

Оскільки кіберзагрози кидають виклик державним кордонам та організаційним кордонам, НАТО взаємодіє з низкою країн-партнерів та

іншими міжнародними організаціями для посилення міжнародної безпеки. Взаємодія з країнами-партнерами базується на спільних цінностях та загальних підходах до кіберзахисту. Запити про співпрацю з Альянсом розглядаються в кожному конкретному випадку на основі взаємних інтересів.

Кіберзахист є одним із напрямків посиленої співпраці між НАТО та ЄС, як частина все більш скоординованих зусиль двох організацій щодо протидії гібридним загрозам. НАТО та ЄС обмінюються інформацією між групами реагування на кіберкризи та обмінюються передовим досвідом.

Політика НАТО щодо кіберзахисту реалізується політичними, військовими та технічними органами НАТО, а також окремими членами Альянсу. Північноатлантична рада (НАК) забезпечує політичний нагляд на високому рівні за всіма аспектами впровадження[60]. НАК поінформований про великі кіберінциденти та виконує основну владу в галузі управління кризовими ситуаціями, пов'язаної з кіберзахистом. Комітет з кіберзахисту, підпорядкований НАК, є провідним комітетом з питань політичного управління та політики кіберзахисту загалом. На робочому рівні Комісія з управління кіберзахистом НАТО (CDMB) відповідає за координацію кіберзахисту у цивільних та військових органах НАТО. CDMB включає керівників політичних, військових, оперативних та технічних органів НАТО, відповідальних за кіберзахист [61].

Співпраця між НАТО і країнами-партнерами, в тому числі з Україною, відбувається в рамках Ради євроатлантичного партнерства (РЄАП) та програми «Партнерство заради миру» (ПЗМ).

На сьогодні вступ України в НАТО чітко визначено як один з ключових чинників державної політики. З метою отримання членства в Альянсі Україна активізує зусилля по всьому комплексу реформ, в тому числі в сфері оборони і безпеки. З огляду на, що саме кібербезпека зараз є одним з найважливіших

аспектів забезпечення національної, регіональної та міжнародної безпеки в цілому, наша країна повинна ввести досить запобіжних заходів і процедур для її забезпечення відповідно до положень політики НАТО в цій сфері, а також дотримати умови, які були запропоновані в плані дій Україна – НАТО.

Це передбачає, зокрема:

забезпечення реалізації гарантій доступу до інформації;

імплементації відповідного законодавства для усунення перешкод діяльності ЗМІ;

поглиблення інформаційного виміру співробітництва Україна-НАТО, включаючи парламентське співробітництво;

створення прозорої і гнучкої структури електронного урядування; забезпечення розвитку здібностей військових частин і підрозділів в сфері кібероперацій;

підвищення рівня обізнаності громадськості про діяльність НАТО, підвищення рівня забезпечення кібербезпеки тощо.

Перелік поточних заходів з виконання Річної національної програми під егідою Комісії Україна — НАТО на 2021 рік передбачає досягнення низки цілей. В рамках Стратегічної мети "4.1. Удосконалена система безпеки інформації забезпечує захищеність, цілісність інформації та належний порядок доступу до неї" визначена ціль 4.1.2. "Інформація з обмеженим доступом захищена за визначеними законодавством критеріями та згідно з міжнародними стандартами". Реалізація цієї мети потребує виконання таких завдань:

- Завдання 441.Забезпечення гармонізації законодавства у сфері безпеки інформації, її криптографічного та технічного захисту з урахуванням директив і стандартів НАТО та ЄС;
- Завдання 442. Набуття Адміністрацією Державної служби спеціального зв’язку та захисту інформації України повноважень безпекового

акредитаційного органу щодо комунікаційно-інформаційних систем, призначених для обробки, зберігання та обміну інформацією НАТО з обмеженим доступом;

- Завдання 443. Підвищення рівня професійної компетентності спеціалістів з інформаційної безпеки відповідно до вимог нормативно-правових актів у сфері захисту інформації та безпеки комунікаційно-інформаційних систем;

- Завдання 444. Створення навчальних/тренінгових центрів з підвищення та оцінки рівня професійної компетентності спеціалістів з інформаційної безпеки.

Пов'язана з попередньою, Стратегічна мета 4.2. "Створено умови для безпечного функціонування кіберпростору та його використання в інтересах особи, суспільства і держави", визначає досягнення цілі 4.2.1. "Національна система кібербезпеки відповідає сучасним вимогам і викликам". Досягнення результату передбачається шляхом виконання наступних завдань:

- Завдання 445. Розроблення та впровадження цілісної системи нормативно-правових актів у сфері виявлення кібератак та протидії кіберзагрозам щодо державних інформаційних ресурсів та об’єктів критичної інфраструктури;

- Завдання 446. Упровадження сучасної системи підготовки та підвищення рівня професійної компетентності фахівців у сфері кіберзахисту та кібербезпеки за міжнародними стандартами;

- Завдання 448. Упровадження системи дієвого багатостороннього співробітництва між основними суб’єктами забезпечення кібербезпеки для вирішення проблеми завчасного виявлення і попередження кібератак на об’єкти критичної інформаційної інфраструктури;

- Завдання 449. Розроблення та впровадження автоматизованої системи обміну інформацією (взаємооповіщення) щодо кібератак, кіберінцидентів та їх джерел між суб'єктами системи кібербезпеки;

- Завдання 450. Впровадження системи інформаційної взаємодії між державним та приватним сектором;

- Завдання 452. Створення законодавчих та організаційних умов для підвищення спроможності операторів критичної інформаційної інфраструктури щодо виявлення кібератак і кіберінцидентів, зокрема для диверсифікації джерел інформації про зовнішні та внутрішні кіберзагрози;

- Завдання 453. Удосконалення взаємодії з відповідними (спеціальними) органами держав–членів НАТО та ЄС з метою обміну інформацією про проведені кібератаки для ефективного та своєчасного реагування;

- Завдання 455. Упровадження системи класифікації кіберзагроз та кіберінцидентів, сумісної з NATO Computer Incident Response Capability.

Ціль 4.2.2. "Створена єдина мережа галузевих ситуаційних центрів кібербезпеки, що здатна забезпечити оперативне реагування на кіберзагрози на рівні, який відповідає стандартам НАТО" передбачає такі завдання:

- Завдання 456. Визначення сфери відповідальності державних органів, залучених до створення єдиної мережі галузевих ситуаційних центрів кібербезпеки, та затверджено Концепцію створення такої мережі;

- Завдання 457. Запровадження механізмів взаємодії та координації дій між основними суб'єктами забезпечення кібербезпеки держави та приватного ІТ-сектору, а також іноземними партнерами у сфері протидії кіберзагрозам та забезпечення безпеки у кіберпросторі;

З 2019 року євроатлантична інтеграція й надалі позиціонується як ключовий пріоритет зовнішньої політики України (разом з європейською), а процес впровадження стандартів Альянсу є безперервним. Зокрема, за цей час

було зроблено низку як практичних, так і нормативно-правових кроків у процесі впровадження стандартів НАТО.

Україна сумарно запровадила 292 стандарти та керівні документи НАТО шляхом розроблення 317 національних документів (оперативних — 205, матеріальних — 86, адміністративних — 26) [62]. У відсотковому співвідношенні Україна впровадила вже близько 19% угод зі стандартизації НАТО. Альянсом розробляються нові стандарти, і від зміни їх кількості може відбуватись певне викривлення у цифрах, що позначають відсоток впроваджених стандартів в Україні.

Серед конкретних та зрозумілих не лише фахівцям прикладів впровадження стандартів НАТО можна назвати впровадження операційних умовних позначок та кольорів, які використовуються при розробці графічних частин документів з оперативної та бойової підготовки НАТО. Наразі синім кольором позначаються свої і дружні війська, червоним — вороги. Раніше усе було навпаки, що вносило елементи непорозуміння. Також в Україні було впроваджено еквівалентний званням армій держав-членів НАТО перелік військових звань офіцерського та сержантського складу з введенням військового звання «бригадний генерал». Уніфіковано військову форму одягу, розширено її перелік для усіх можливих умов проходження військової служби. Водночас, Україною було також опрацьовано декілька десятків Доктрин, настанов та інших інструкцій із утримання, навчання і підготовки, логістичного забезпечення, планування та застосування військ [63].

Інший важливий аспект: впровадження стандартів НАТО, тобто введення в українську нормативно-правову базу відповідних документів, це радше бюрократична процедура на рівні Міністерства оборони. Найважливіше питання стосується саме застосування стандартів, тобто їх практичної імплементації. Згідно з Положенням, військові стандарти не лише

впроваджують, але й застосовують на добровільній основі [64]. Це означає, що впровадження стандартів у нормативно-правову базу не гарантує того, що вони будуть застосовуватись на практиці.

Технічно оцінка Альянсом впровадження стандартів НАТО відбувається в рамках Процесу планування та оцінки сил (ППОС) — фахівці Альянсу готують щорічні закриті звіти про виконання Цілей партнерства та стан реформ у секторі безпеки і оборони, які передаються Міністерству оборони України та іншим органам влади, відповідальним за їх впровадження. Остання така оцінка відбулась у 2019 році. Зазначено, що в цілому прогрес досягнуто у багатьох сферах, проте жодна з Цілей партнерства повністю не досягнута [65]. У 2020 році сталася технічна перерва у наданні оцінок Альянсу, пов'язана з пандемією COVID, втім у поточному році планується відновити цей процес.

Інші завдання, які ставить перед собою Україна щодо стандартів Альянсу на 2021 рік, включають створення координаційного центру з питань впровадження стандартів НАТО, згідно з Річною національною програмою Україна-НАТО 2020. Це сприятиме досягненню цілі 5.1.1. РНП 2020 «Законодавство України гармонізовано із законодавством держав-членів НАТО для забезпечення набуття повноправного членства України в НАТО» [66].

Планується підписання Річної національної програми на 2022 рік та нового пакету Цілей партнерства Україна-НАТО до 2023 року. Очікується, що останній буде ухвалено протягом кількох місяців, приблизно у травні-червні цього року, та буде містити більш ніж 50 цілей партнерства, що стосуватимуться не тільки Міністерства оборони і Генерального Штабу, але і ширшого кола органів із сектору безпеки та оборони України. Йдеться про Міністерство внутрішніх справ, Національну гвардію, СБУ тощо.

Практична діяльність щодо впровадження стандартів Альянсу буде здійснюватися у рамках нової програми Міністерства оборони України з військової стандартизації на 2021-2023 роки [67], у якій спланова опрацювання 62 стандартів НАТО.

Цей перелік містить як стандарти, заплановані до опрацювання в межах Цілей партнерства, так і поза ними (втім, кількість стандартів може бути збільшеною після схвалення нового пакету Цілей партнерства). Нова Програма поширюватиметься не лише на Міністерство оборони, а й на Національну гвардію України.

Отже, вступ України в НАТО є одним з визначальних чинників державної політики. Для отримання усіх переваг від членства в Альянсі, потрібно активізувати зусилля по всьому комплексу реформ, в тому числі в сфері оборони і безпеки. Як один з найважливіших аспектів забезпечення національної, регіональної та міжнародної безпеки в цілому, кібербезпека повинна забезпечуватися шляхом запровадження запобіжних заходів і процедур відповідно до положень політики НАТО в цій сфері з дотриманням заходів, передбачених Планом дій Україна – НАТО.

ВИСНОВКИ

1. Підсумовуючи, термін «кібербезпека», з точки зору ЄС, передбачає поєднання кіберстійкості, кіберзлочинності, кіберзахисту, кібербезпеки та глобальних проблем кіберпростору. Визначивши ці п’ять чітких пріоритетних областей, стратегія 2013 року ставила за мету зробити онлайн-середовище ЄС найбезпечнішим у світі. За декілька останніх десятиліть відбулася потужна технологічна революція в галузі використання комп’ютерів та телекомунікацій, яка привела до принципових змін та збільшення апаратного парку, суттєвого прискорення швидкості передачі інформації. Водночас саме стрімкий інформаційний прогрес спричинив проблему захищеності персональних даних через виникнення глобальних лідерів, що призвело до концентрації інформації в руках «великих гравців мережі» та централізації загальної інфраструктури. Це зробило можливими великомасштабні атаки та створило великі ризики значних збитків при критичних пошкодженнях інфраструктури таких систем.

2. Процес становлення кіберзаконодавства в державах-членах ЄС розпочався у 2001 році й досі набирає оберти, створюючи нове законодавство в цій галузі. Однак з позиції системного підходу більшість проблем кібербезпеки виникає через відставання сучасної законодавчої бази від науково-технічного прогресу. Незважаючи на існуючу сучасну низку документів щодо кібербезпеки, остання досі залишається досить вразливою, незалежно від ступеня розробки і стану законодавства, виявляючи випереджаючі проблемні науково-технічні прогалини щодо підвищення якості та стану кібербезпеки в ЄС загалом.

3. В праві Європейського Союзу виділяють п’ять стратегічних пріоритетів кібербезпеки ЄС:

- досягнення «кіберстійкості» шляхом встановлення мінімальних вимог до функціонування співробітництва та координації національних компетентних органів з питань безпеки мереж та інформаційних систем;

- зменшення кіберзлочинності шляхом забезпечення швидкого впровадження вимог директиви ЄС, заохочення ратифікації положень Будапештської конвенції Ради Європи про кіберзлочинність та фінансування програми для розгортання оперативних інструментів;

- розробка політики та можливостей кібедорони, пов'язаних із загальною безпекою та оборонною політикою шляхом оперативної оцінки кіберзахисту ЄС, розробка політики ЄС щодо кіберзахисту, стимулювання діалогу та координації між цивільними та військовими суб'єктами в ЄС, та сприяння діалогу з міжнародними партнерами;

- розвиток промислових та технологічних ресурсів для кібербезпеки шляхом створення державно-приватної платформи з питань мережевої та інформаційної безпеки, надання технічних вказівок та рекомендацій для прийняття стандартів та практики та заохочення розвитку стандартів безпеки;

- встановлення послідовної міжнародної політики щодо кіберпростору для ЄС та сприяння включення основних цінностей ЄС у спільну зовнішню політику та політику безпеки.

4. Метою Директиви NIS є гарантування високого загального рівня безпеки мережевих та інформаційних систем в рамках ЄС. Для того, щоб цього домогтися, було вирішено зобов'язати держави-учасники підвищити свою готовність і поліпшити співпрацю один з одним, а також зобов'язати операторів, які надають критично важливі послуги, пов'язані з певними об'єктами інфраструктури, і провайдерів окремих цифрових послуг вжити відповідних заходів з управління ризиками безпеки і повідомляти про серйозні інциденти компетентним національним органам.

5. Визначені основні етапи та здобутки розвитку кібербезпекової політики ЄС:

- до 2001 року – зародження кібербезпекової політики ЭС;
- 2001 – 2004 роки – прийняття та реалізація першої стратегії «Безпека мережі та інформації»;
- 2004 – 2012 рік – утворення і розвиток Агентства ENISA;
- 2013 – 2016 рік – друга стратегія кібербезпеки;
- 2017 – 2019 рік – стратегія «Стійкість, стримування та захист: побудова міцної кібербезпеки для ЄС»;
- з 2020 року – «Стратегія кібербезпеки ЄС на цифрове десятиліття».

6. Стратегія кібербезпеки ЄС 2020 року визначає такі пріоритети:

- захисні заходи не лише для забезпечення безпеки, але й для захисту європейських цінностей та основних прав кожного;
- ЄС прагне підтримувати нову стратегію кібербезпеки, щоб перейти на новий рівень кібербезпеки протягом наступних семи років;
- державам рекомендується повною мірою використовувати механізм відновлення та стійкості для посилення кібербезпеки.

7. Функціями Агентства ENISA є надання допомоги Європейській Комісії, державам-членам ЄС та бізнесу виконувати вимоги мережевої та інформаційної безпеки, включаючи чинне та майбутнє право ЄС; ENISA є центром експертизи як для держав-членів, так й для інституцій ЄС з отримання консультацій з питань, пов’язаних із мережевою та інформаційною безпекою; Агентство вносить в розвиток свій внесок та імплементації законів та політики ЄС в різні сектори в сфері кібербезпеки тощо.

8. Ключовими завданнями в рамках наближення законодавства України до законодавства ЄС задля поширення режиму внутрішнього ринку ЄС на базову для цифрової економіки сферу телекомунікацій є імплементація актів

ЄС у законодавство України. Інтеграція України до Єдиного цифрового ринку ЄС є одним із пріоритетних завдань для України.

9. З огляду на необхідність впровадження європейського законодавства та гармонізації різних підходів до кібербезпеки, необхідно розробити нову Стратегію кібербезпеки з окремим розділом, присвяченим мережевої та інформаційної безпеки і, відповідно, етапам, цілям і показниками ефективності, запропонованим ENISA. Сама Стратегія кібербезпеки України повинна встановити основні принципи планування, бюджетування, реалізації та аналізу ефективності заходів щодо реалізації Стратегії кібербезпеки України, які не повинні суперечити заходам і принципам, визначеним законом.

10. Повноцінний розвиток України неможливий без створення належного державно-правового забезпечення кіберзахисту на національному рівні, а також єдиної стійкої і функціональної системи внутрішніх справ, як частини сектора національної безпеки, а також громадську безпеку, враховуючи останні тенденції і нововведення у вітчизняній нормативно-правовій базі. Сучасні загрози національній безпеці України з'явились на фоні впливу соціально-демографічних, економічних, політичних, правових, психологічних і технологічних чинників. Ці фактори потребують системного реагування, належної та прогресивної трансформації сектора безпеки і системи внутрішніх справ. Тому для повноцінного розвитку держави і забезпечення належної національної безпеки необхідно якісне і результативне державно-правове забезпечення.

11. Євроатлантична інтеграція є одним з визначальних чинників державної політики. Для отримання усіх переваг від членства в НАТО, потрібно активізувати зусилля по всьому комплексу реформ, в тому числі в сфері оборони і безпеки. Як один з найважливіших аспектів забезпечення національної, регіональної та міжнародної безпеки в цілому, кібербезпека

повинна забезпечуватися шляхом запровадження запобіжних заходів і процедур відповідно до положень політики НАТО в цій сфері з дотриманням заходів, передбачених Планом дій Україна – НАТО.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Губенко Д.. Після кібератаки на «Прикарпаттяобленерго» в США переглянуть захист енергомереж (2016) [Електронний ресурс]. – Режим доступу: https://p.dw.com/p/1HZXJ
2. Прокопчук Д.. CERT-UA попереджає про нові спроби хакерських атак на українські мережі (2016) [Електронний ресурс]. – Режим доступу: https://p.dw.com/p/1HfCU
3. Дебет-Кредит. Кібератака, вірус Petya.A і до чого тут M.E.Doc: усе, що нам відомо на ранок 29 червня (ОНОВЛЕНО) (2017) [Електронний ресурс]. – Режим доступу: https://news.dtkt.ua/state/other/44158
4. Morgan S. Cybercrime To Cost The World $10.5 Trillion Annually By 2025 (2020) [Електронний ресурс]. – Режим доступу: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
5. Микитенко Д.О. Захист інформації та кібербезпека як складова частина національної безпеки України [Електронний ресурс] // Юридичний науковий електронний журнал. – 2020. - № 8. – Режим доступу: http://www.lsej.org.ua/8_2020/96.pdf
6. Соколов М.С. Кибернетическая безопасность – понятие, значение и эволюция от военных основ к самостоятельному виду безопасности [Електронний ресурс] // Военное право. - 2012. - № 1. – Режим доступу: http://db.inforeg.ru/eni/artList.asp?j=4&id=0220913464&idfull=0421200099
7. Crimes related to computer networks, Background paper for the workshop on crimes related to the computer network, 10th UN Congress on the Prevention of Crime and the Treatment of Offenders, [Електронний ресурс] 2000, A/CONF.187/10, p.5; - Режим доступу: www.uncjin.org/Documents/congr10/10e.pdf
8. Конвенція Ради Європи «Про кіберзлочинність» [Електронний ресурс] // Офіційний вісник України. – 2007. – № 65. – Стор. 107.

9. Баранов О.А. «Правова інформатика», № 2(42)/2014 54 УДК 340.13+007.51+165.12 Про тлумачення та визначення поняття «кібербезпека».

10. Закон України про основні засади забезпечення кібербезпеки України (2017), [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19#Text

11. Communication «Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry» (2016) [Електронний ресурс]. – Режим доступу: https://ec.europa.eu/digital-single-market/en/news/communication-strenghtening-europes-cyber-resilience-system-and-fostering-competitive-and

12. CYBER; Global Cyber Security Ecosystem. ETSI TR 103 306 V1.4.1 (2020-03) [Електронний ресурс]. – Режим доступу: https://www.etsi.org/deliver/etsi_tr/103300_103399/103306/01.04.01_60/tr_103306v010401.pdf

13. Директива Європейського Парламенту і Ради (ЄС) 2016/1148 від 6 липня 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/984_013-16#Text

14. State of the Union 2017 - Cybersecurity: Commission scales up EU's response to cyber-attacks (19 September 2017) [Електронний ресурс]. – Режим доступу: http://europa.eu/rapid/press-release_IP-17-3193_en.htm

15. Wessel RA (2015) Towards EU cybersecurity law: regulating a new policy field. In: Tsagourias N, Buchan R (eds) Research handbook on international law and cyberspace. Edward Elgar Publishing

16. European Court of Auditors (2019) Challenges to effective EU cybersecurity policy. [Електронний ресурс]. – Режим доступу: https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf Last access 7 July 2019

17. Craig P, de Burca G (2015) EU law: text, cases and materials. Oxford University Press. [Електронний ресурс]. – Режим доступу: https://global.oup.com/academic/product/eu-law-9780198856641?prevNumResPerPage=100&facet_narrowbytype_facet=Books%20for%20Courses&lang=en&cc=nz

18. European Union (2016) 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 (GDPR). Off J Eur Communities [Електронний ресурс]. – Режим доступу: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

19. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. (2006) [Електронний ресурс]. – Режим доступу: http://ec.europa.eu/information_society/doc/com2006251.pdf

20. Joint communication to the European parliament, the council, the European economic and social committee and the committee of the regions (2013) [Електронний ресурс]. – Режим доступу: http://ec.europa.eu/information_society/doc/com2006251.pdf

21. Joint communication to the European parliament and the council [Електронний ресурс]. – Режим доступу: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=EN

22. Cybersecurity package 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU' [Електронний ресурс]. – Режим доступу: https://digital-strategy.ec.europa.eu/en/library/cybersecurity-package-resilience-deterrence-and-defence-building-strong-cybersecurity-eu

23. EU. Joint Communication to the European Parliament and the council (2017) [Електронний ресурс]. – Режим доступу: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52017JC0450

24. Cybersecurity and Infrastructure Security Agency Act of 2018 [Електронний ресурс]. – Режим доступу: https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_en

25. Співробітництво Україна – ЄС – НАТО з протидії гібридним загрозам у кіберсфері. [Електронний ресурс]. – Режим доступу: https://www.kas.de/documents/270026/4625039/UA+Ukraine+-+EU+-+NATO+cooperation+to+counter+hybrid+threats+in+cyber+sphere.pdf/c970b17f-d9db-aba3-7990-bb4441a3e041?version=1.0&t=1554283399244

26. Wessel RA (2015) Towards EU cybersecurity law: regulating a new policy field. In: Tsagourias

27. N, Buchan R (eds) Research handbook on international law and cyberspace. Edward Elgar

28. Директива Європейського Парламенту і Ради (ЄС) 2016/1148 від 6 липня 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу [Електронний ресурс] // Веб-портал ВРУ. – Режим доступу: https://zakon.rada.gov.ua/laws/show/984_013-16#Text

29. Спільна декларація Саміту Східного партнерства: текст документа [Електронний ресурс] // Європейська правда. – 24 листопада 2017. – Режим доступу: https://www.eurointegration.com.ua/articles/2017/11/24/7074139/

30. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 [Електронний ресурс]. – Режим доступу: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0680

31. 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) [Електронний ресурс]. – Режим доступу: https://eur-lex.europa.eu/eli/reg/2016/679/oj

32. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 [Електронний ресурс]. – Режим доступу: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0680

33. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 [Електронний ресурс]. – Режим доступу: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0680

34. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 2016 [Електронний ресурс]. – Режим доступу: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058

35. Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 COUNCIL [Електронний ресурс]. – Режим доступу: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0024

36. Регламент (ЕС) N 593/2008 [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/go/994_905

37. Directive (EU) 2015/1535 of the European parliament and of the council [Електронний ресурс]. – Режим доступу: ttps://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015L1535&from=BG

38. Council Framework Decision 2006/960/JHA of 18 December 2006 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32006F0960

39. Directive 2014/41/EU of the European Parliament and of the Council [Електронний ресурс]. – Режим доступу: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0041Регламент (ЄС) N 593/2008 Європейського Парламенту та Ради «Про право, яке підлягає до застосування щодо договірних зобов'язань («Рим I»)» [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/go/994_905

40. Конвенція про кіберзлочинність (2005) [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/go/994_575

41. Council Regulation (EC) No 1206/2001 of 28 May 2001[Електронний ресурс]. – Режим доступу: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32001R1206

42. Council Directive 2008/114/EC of 8 December 2008[Електронний ресурс]. – Режим доступу: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32008L0114

43. Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018[Електронний ресурс]. – Режим доступу: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R1807#ntr3-L_2018303EN.01005901-E0003

44. Regulation (EU) 2019/881 of the European Parliament and of the Council [Електронний ресурс]. – Режим доступу: https://eur-lex.europa.eu/eli/reg/2019/881/oj

45. Спільне повідомлення Європейського Парламенту та Ради. [Електронний ресурс]. – Режим доступу: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72164

46. National Cyber Security Index [Електронний ресурс]. – Режим доступу: https://ncsi.ega.ee/ncsi-index/

47. Шипілова Ю. Правова база української кібербезпеки: загальний огляд і аналіз [Електронний ресурс]. – Режим доступу: https://ifesukraine.org/wp-content/uploads/2019/10/IFES-Ukraine-Ukrainian-Cybersecurity-Legal-Framework-Overview-and-Analysis-2019-10-07-Ukr.pdf

48. Янковський О. Україні потрібна нова кіберстратегія (2019) [Електронний ресурс]. – Режим доступу: https://www.pravda.com.ua/columns/2019/09/14/7226291/

49. The Digital Economy and Society Index (DESI) (2020) [Електронний ресурс]. – Режим доступу: https://ec.europa.eu/digital-single-market/en/desi

50. Communication from the commission to the European parliament, the council, the European economic and social committee and the committee of the regions (2015) [Електронний ресурс]. – Режим доступу: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52015DC0192

51. Joint Declaration of the Eastern Partnership Summit (2017) [Електронний ресурс]. – Режим доступу: https://www.consilium.europa.eu/media/31758/final-statement-st14821en17.pdf

52. Nochvai Vю, Oleksiuk L., Prykhodko O. Digital single market and the association agreement [Електронний ресурс]. – Режим доступу: http://eump.org/media/2019/Integrating%20Ukraine%20into%20the%20EU%E2%80%99s%20digital%20single%20market.pdf

53. Про схвалення Концепції створення державної системи захисту критичної інфраструктури (2017) [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80

54. «NATO-Ukraine Trust Funds», North Atlantic Treaty Organization website, [Електронний ресурс]. – Режим доступу: https://www.nato.int/cps/en/natolive/topics_153288.htm

55. Cocolan M-M., «International cooperation for Critical Information Infrastructure Protection: NATO-UKRAINE Trust Fund on Cyber Defence», 2018, [Електронний ресурс]. – Режим доступу: https://www.cipre-expo.com/wp-content/uploads/2018/10/Cocolan%20M%20NATO-UKRAINE%20Trust%20Fund%20on%20Cyber%20Defence.pdf

56. Cocolan M-M., «International cooperation for Critical Information Infrastructure Protection: NATO-UKRAINE Trust Fund on Cyber Defence», 2018, [Електронний ресурс]. – Режим доступу: https://www.cipre-expo.com/wp-

content/uploads/2018/10/Cocolan%20M%20NATO-UKRAINE%20Trust%20Fund%20on%20Cyber%20Defence.pdf

57. Wales Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales (2014) [Електронний ресурс]. – Режим доступу: https://www.nato.int/cps/en/natohq/official_texts_112964.htm

58. Warsaw Summit Communiqué Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016 Last updated: 29 Mar. 2017 10:55 [Електронний ресурс]. – Режим доступу: https://www.nato.int/cps/en/natohq/official_texts_133169.htm

59. Smart Defence (2017) [Електронний ресурс]. – Режим доступу: https://www.nato.int/cps/en/natolive/topics_84268.htm

60. North Atlantic Council (2017) [Електронний ресурс]. – Режим доступу: https://www.nato.int/cps/en/natolive/topics_49763.htm

61. Cyber defence (2021) [Електронний ресурс]. – Режим доступу: https://www.nato.int/cps/en/natohq/topics_78170.htm

62. «Інформаційний матеріал щодо запровадження стандартів та керівних документів НАТО», Міністерство оборони України, [Електронний ресурс]. – Режим доступу: https://www.mil.gov.ua/diyalnist/vprovadzhennya-standartiv-ta-inshih-kerivnih-dokumentiv-nato.html

63. Йдеться, зокрема, про Доктрину організації і проведення багатонаціональних навчань у ЗС України, Доктрину розвитку військового лідерства, Доктрину фінансового забезпечення, Доктрину з організації планування оборонних ресурсів, Доктрину з оборонного планування, Доктрину із стратегічних комунікацій, Доктрину з об'єднаної логістики, Доктрину з публічного спілкування, Доктрину участі у міжнародних операціях з підтримання миру і безпеки тощо

64. Інтерв'ю з представником НАТО, 1 березня 2021 року

65. Указ Президента України №203/2020 «Про Річну національну програму під егідою Комісії Україна-НАТО на 2020 рік», [Електронний ресурс]. – Режим доступу: https://www.president.gov.ua/documents/2032020-33861

66. «Інформаційний матеріал щодо запровадження стандартів та керівних документів НАТО», Міністерство оборони України, [Електронний ресурс]. – Режим доступу: https://www.mil.gov.ua/diyalnist/vprovadzhennya-standartiv-ta-inshih-kerivnih-dokumentiv-nato.html