МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХЕРСОНСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ БІЗНЕСУ І ПРАВА
КАФЕДРА ПУБЛІЧНОГО ТА МІЖНАРОДНОГО ПРАВА І ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ

ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ: АДМІНІСТРАТИВНО-ПРАВОВІ ЗАСАДИ

Кваліфікаційна робота (проєкт)
на здобуття ступеня вищої освіти «магістр»

Виконала: студентка 2 курсу 12-283-Мз групи
Спеціальності 262 Правоохоронна діяльність
Освітньо-професійної програми
«Правоохоронна діяльність»

Лебедєва Ганна Юріївна
Керівник: к.ю.н., доцент Циганок С.В.
Рецензент: к.ю.н., доцент Проценко М.В.

Херсон – 2020

ЗМІСТ

ВСТУП

Актуальність теми дослідження. Одна із ключових задач політичного керівництва будь-якої держави – забезпечити та гарантувати відкрите, надійне та захищене функціонування кіберпростору. У зв'язку з тим, що у кіберпросторі відсутні кордони та враховуючи його відкритість, яка є основою для новітніх інтернет-технологій – значно збільшується ймовірність кібератак та кіберзагроз ззовні, що автоматично схиляє до потреби розроблення чіткої стратегічної концепції, яка буде слугувати тим фундаментом, щоб реалізувати пріоритети національної політики в кіберпросторі. Іншими словами, глобальний характер кіберпростору може збільшити ступінь ризику, впливаючи на сектори як державного, так і приватного рівня.

Сприятливість даної сфери для злочинної діяльності обумовлюється багатьма факторами, серед яких: розвиток комп'ютерних та інформаційно-комунікаційних технологій значно швидший за оновлення законодавчої бази, якою регулюються відносини в зазначеній сфері; необмеженість державних кордонів, що в свою чергу, надає досить сприятливі умови для того, щоб процвітала транснаціональна злочинність; проблематичність у виявленні суб'єкта злочинної діяльності та доведенні його винуватості. Тобто, сучасні реалії досить яскраво демонструють, що однією з найважливіших складових національної безпеки являється кібербезпека держави та механізм її забезпечення.

Зазначені аспекти змушують кожну цивілізовану державу приділяти серйозну увагу своїх кібернетичній безпеці. Україна також не є виключенням в зазначеному питанні, яка теж потребує суттєвих напрацювань та удосконалень стосовно національного механізму забезпечення кібербезпеки.

Ключовим етапом, щоб покращити якість та ефективність організації і функціонування зазначеного механізму є удосконалення адміністративно-правового забезпечення, який полягає в тому, щоб оновити відповідне законодавство та переглянути систему суб'єктів, на яких покладено обов'язок займатися сферою кібербезпеки. За останні роки у наукової спільноти все частіше мали місце бути думки стосовно необхідності зміцнити національну кібербезпеку, що є повністю логічно, оскільки ті кібернетичні загрози, які існують сьогодні – Україна ще не бачила на своєму шляху і як результат – немає відповідного досвіду, щоб оперативно та ефективно протистояти таким загрозам.

З огляду на це, теоретичним підґрунтям дослідження стали праці таких вчених як: І.В. Арістової, О.А. Баранова, Д.С. Бірюкова, С.О. Бондаря, В.М. Богуша, Ю.П. Бурила, Л.Є. Виноградова, М.В. Гайворонського, В.Д. Гавловського, Є.А. Гетьмана, О.Д. Довганя, Д.В. Дубова, А.А. Демцова, А.В. Кірмача, О.М. Клюєва, Н.В. Коваленка, Т.М. Кравцової, Р.О. Куйбіди, О.С. Лагоди, В.А. Ліпкана, Д.М. Лук'янця, П.С. Лютікова, В.В. Маркова, А.В. Мовчана, О.М. Музичука, В.Я. Настюка, Ю.В. Нестеряка, В.В. Пахомова, Т.О. Проценка, Д.М. Притики, В.В. Петрова, В.В. Сухоноса, І.М. Сопілко, О.О. Черногора, В.П. Шеломенцева та інших.

Проте, незважаючи на існуючі наукові праці, які присвячені становленню кібернетичного простору загалом, та забезпеченню кібербезпеки, зокрема, спеціальних комплексних досліджень, які б визначали особливості адміністративно-правового забезпечення кібербезпеки в Україні у зв'язку з оновленням законодавства – не є достатніми.

Отже, потреба удосконалення кібербезпеки в Україні, а також недосконале правове регулювання зазначеної сфери, з однієї сторони, та відсутність відповідних напрацювань в зазначеному питанні – з іншої, зумовлюють своєчасність та актуальність дослідження щодо розгляду

адміністративно-правових засад стосовно забезпечення кібербезпеки в Україні з ціллю виокремити прогалини, які існують в даному механізмі та визначити перспективні напрями для подальшого розвитку, враховуючи сьогоднішні реалії та виклики.

Зв'язок роботи з науковими програмами, планами, темами. Кваліфікаційна робота ґрунтується на положеннях Закону України «Про Загальнодержавну програму адаптації законодавства України до законодавства Європейського Союзу» від 18 березня 2004 року № 1629-IV, Указу Президента України «Про Стратегію сталого розвитку «Україна – 2020» від 12 січня 2015 року № 5/2015, Указу Президента України «Про невідкладні заходи з проведення реформ та зміцнення держави» від 8 листопада 2019 року № 837, Указу Президента України «Про Концепцію Загальнодержавної програми адаптації законодавства України до законодавства Європейського Союзу» від 21 листопада 2002 року № 228-IV.

Кваліфікаційна робота виконана згідно напрямів наукових досліджень кафедри публічного та міжнародного права і правоохоронної діяльності факультету бізнесу і права Херсонського державного університету на тему: «Адміністративно-правове регулювання суспільних відносин у соціально-економічній, адміністративно-політичній сферах та правоохоронній діяльності» (номер державної реєстрації 0117U001733). Тему кваліфікаційної роботи затверджено Вченою радою Херсонського державного університету (наказ від 30.10.2020 № 1059-Д).

Мета та завдання дослідження. Мета кваліфікаційної роботи полягає в теоретичному обґрунтуванні адміністративно-правових засад щодо забезпечення кібербезпеки в Україні, встановленні проблемних питань, визначенні шляхів їх вирішення, а також формулюванні можливих напрямів удосконалення зазначеної сфери, враховуючи міжнародний досвід.

Для досягнення вказаної мети у процесі дослідження було поставлено та вирішено такі **завдання:**

– визначити поняття та розглянути зміст кібербезпеки в аспекті адміністративно-правової охорони;

– виокремити об’єктний склад кібербезпеки та кіберзахисту як складової частини;

– охарактеризувати правові засади забезпечення кібербезпеки;

– дослідити адміністративно-правовий статус суб’єктів, які забезпечують кібербезпеку України;

– з’ясувати адміністративно-правові форми та методи щодо забезпечення кібербезпеки в Україні;

– встановити юридичну відповідальність за порушення законодавства у сфері кібербезпеки України;

– узагальнити міжнародний досвід забезпечення кібербезпеки та визначити можливості його імплементації у вітчизняне законодавство;

– встановити недоліки законодавства щодо забезпечення кібербезпеки в Україні, визначити шляхи їх вирішення та розглянути можливі напрями удосконалення.

Об’єкт дослідження – суспільні відносини, які формуються у сфері забезпечення кібербезпеки в Україні.

Предмет дослідження – теоретичні напрацювання та адміністративно-правові засади, які забезпечують кібербезпеку в Україні.

Методи дослідження. Методи дослідження обрано з урахуванням мети і завдань теми кваліфікаційної роботи. Під час доведення основних теоретичних положень було використано загальнонаукові та спеціальні методи. За допомогою діалектичного методу було визначено поняття та розглянуто зміст кібербезпеки; логіко-семантичний метод дозволив надати характеристику адміністративно-правовим формам та методам щодо забезпечення кібербезпеки в Україні; формально-юридичний

метод дав змогу окреслити правові засади забезпечення кібербезпеки; застосування системно-структурного методу уможливило здійснити розгляд об’єктів кібербезпеки та кіберзахисту, визначити адміністративно-правовий статус суб’єктів, які забезпечують кібербезпеку України та встановити юридичну відповідальність в зазначеному питанні; порівняльний метод застосовувався під час вивчення міжнародного досвіду в сфері забезпечення кібербезпеки; метод структурного аналізу та моделювання надали можливість виявити проблемні питання та розглянути можливі напрями удосконалення в сфері забезпечення кібербезпеки в Україні.

Наукова новизна одержаних результатів. Кваліфікаційна робота є комплексним дослідженням, в процесі якого було здійснено спробу теоретичного аналізу забезпечення кібербезпеки в Україні, враховуючи адміністративно-правові засади. У межах дослідження одержано наступні результати, які мають наукову новизну, а саме:

– обґрунтовано, що розмежування адміністративно-правового забезпечення кібербезпеки та кіберзахисту являється дуже важливим моментом, оскільки воно безпосередньо пов'язується з процесом їх реалізації, тому що при неправильному підході може бути завдано шкоди правам та інтересам громадян, які спеціалізуються на проведенні різних операцій з інформацією у кіберпросторі;

– виокремлено позицію, за якою суб’єкти, які забезпечують кібербезпеку являються учасниками не інформаційних, а адміністративних правовідносин, тому що, по-перше, в основу їх відносин покладену принцип влади та підпорядкування, а по-друге, останні реалізують механізм кіберзахисту, використовуючи засіб примусу, який надається їм у встановленому законом порядку. Між іншим, розглядати адміністративно-правовий статус суб’єктів, які забезпечують кібербезпеку, не являється можливим, якщо виходити за межі галузі адміністративного права;

– визначено, що кібербезпека виступає як складне правове явище, в межах якого функціонує механізм кіберзахисту, який представлено комплексом заходів організаційного, нормативно-правового, воєнного, технічного та іншого характеру;

– встановлено, що після прийняття Закону України «Про основні засади забезпечення кібербезпеки України» вперше на законодавчому рівні було закріплено поняття «кібербезпека», тим самим, надавши змогу розробити стратегію захисту кібербезпеки в адміністративно-правовому порядку та закріпити правові засади, систему суб'єктів, щоб визначити механізм забезпечення зазначеної категорії, що в сукупності характеризує означене позитивною новелою у сфері забезпечення кіберпростору загалом, та в процесі використання інноваційних технологій, зокрема;

– аргументовано, що питання юридичної відповідальності за порушення законодавства у сфері кібербезпеки України недостатньо врегульовано, що, без сумніву, вважається як суттєва прогалина, яка сприяє лише процвітанню кіберзлочинності в Україні. Перш за все, мова йде про питання притягнення правопорушників до цивільної та адміністративної відповідальності, яке регламентується багатьма нормативно-правовими актами, кожен з яких по-різному визначає підстави притягнення винних осіб до відповідальності. Як наслідок – таке розгалуження лише ускладнює застосування стягнень до правопорушників компетентними органами.

Практичне значення одержаних результатів полягає в тому, що сформульовані й викладені в роботі висновки та пропозиції становлять теоретичний інтерес та можуть бути використані в різних галузях діяльності, а саме:

– у правотворчій – для вдосконалення чинного законодавства України в частині забезпечення кібербезпеки в Україні;

– у правозастосовній – під час вирішення проблем та недоліків в зазначеній сфері;

– у навчально–методичній – при викладанні навчальних дисциплін з адміністративного права, адміністративного процесу та кримінального права, а також під час підготовки підрозділів підручників і навчальних посібників із відповідних навчальних дисциплін, монографій тощо.

Апробація результатів дослідження. Теоретичні висновки, сформульовані в роботі, обговорювалися на засіданнях кафедри публічного та міжнародного права і правоохоронної діяльності.

Публікації. Основні теоретичні положення та висновки кваліфікаційної роботи знайшли відображення в наступних публікаціях:

– Лебедєва Г.Ю. Юридична відповідальність за порушення законодавства у сфері кібербезпеки України. *Актуальні дослідження правової та історичної науки (випуск 25): матеріали міжнародної науково-практичної інтернет-конференції* / Збірник тез доповідей: випуск 25 (м. Тернопіль, 17 вересня 2020 р.). Тернопіль, 2020. 84 с. С. 18–20.

– Лебедєва Г.Ю. Міжнародний досвід забезпечення кібербезпеки та можливості його імплементації у вітчизняне законодавство. *Магістерські студії. Альманах*. Вип. 20. Херсон. ХДУ, 2020.

Структура роботи обумовлена метою, задачами, об’єктом та предметом дослідження й складається зі вступу, трьох розділів, висновків, списку використаних джерел.

Повний обсяг роботи становить 96 сторінок: основний текст – 88 сторінок, обсяг, що займає список використаних джерел і літератури (70 найменувань) – 8 сторінок.

РОЗДІЛ 1
ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ КІБЕРПЕЗПЕКИ В УКРАЇНІ

1.1. Поняття, зміст кібербезпеки в аспекті адміністративно-правової охорони

Після здобуття Україною незалежності, державний розвиток було направлено на технологічний процес та адаптацію у повсякденне життя інформаційних технологій, які сьогодні значно спрощують процеси пошуку та обміну інформацією. Вагому роль процес «електронного» розвитку відіграє на державному рівні, тому що впровадження сучасних технологій слугує підґрунтям для відкриття великих можливостей у сфері державного будівництва. Однак «цифрова революція», яка відбувається сьогодні – має багато негативних моментів, одним з яких є незадовільний рівень кібербезпеки. Аналіз зазначеного питання є пріоритетним в науковій доктрині, оскільки кібербезпека як об’єкт правової охорони становить беззаперечний інтерес для держави.

Найбільш коректним та ефективним «буфером» правової охорони вказаного об’єта є адміністративно-правовий, тому що він є похідним в юридичній галузі, в межах якої функціонує державний примус. Тобто, дослідження кібербезпеки в контексті об’єкта адміністративно-правової охорони дає змогу окреслити рівень правової регламентації її захищеності.

Перш за все необхідно визначити поняття та основоположні аспекти адміністративно-правової охорони як ключового та функціонального механізму, який забезпечує кібербезпеку.

Як і будь-які інші правові явища в державі, основоположні засади забезпечення кібербезпеки відображені в положеннях Конституції України, оскільки цей нормативний акт є ключовим джерелом в

національній правовій системі. Так, відповідно до ст. 3 Конституції зазначається: «Людина, її життя і здоров'я, честь і гідність, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю. Права і свободи людини та їх гарантії визначають зміст і спрямованість діяльності держави. Держава відповідає перед людиною за свою діяльність. Утвердження і забезпечення прав і свобод людини є головним обов'язком держави» [1]. Із зазначеного положення випливає, що наявний адміністративно-правовий механізм охорони кібербезпеки слугує як прояв виконання покладених на державу обов’язків щодо забезпечення життєдіяльності населення країни.

Взагалі сутність адміністративно-правової охорони розглядається через те благо, на яке спрямовується дія механізму. На сьогодні вже напрацьована величезна кількість поглядів науковців стосовно проблематики визначення терміну «адміністративно-правова охорона», по причині того, що фактично вона не закріплена в нормативно-правових актах. Так, на думку В.В. Галунько: «адміністративно-правова охорона – це система впорядкованої адміністративно-правовими нормами діяльності публічної адміністрації, що спрямована на попередження правопорушень (профілактику злочинів) та відновлення порушених прав, свобод та законних інтересів фізичних і юридичних осіб, що здійснюються засобами адміністративного права з можливістю застосування заходів адміністративного примусу та притягнення винних до адміністративної відповідальності» [2, с. 242-247]. Іншою, не менш цікавою є думка О.І. Харитонової, яка акцентує увагу на тому, що «явище адміністративно-правової охорони являє собою окремий правовий інститут. Вона доводить свій погляд тим, що порушення встановлених законодавством правил поведінки тягне за собою припинення дії регулятивних правовідносин, замість яких виникають охоронні (регулятивні трансформуються в охоронні), підставою до чого є припис норми права та вчинення адміністративного делікту. В цьому

випадку йдеться вже не про реалізацію встановлених адміністративно-правових регулятивних норм, якими були визначені вимоги до поведінки зобов'язального суб'єкта, а про реалізацію положень охоронних адміністративно-правових норм, які передбачають встановлення нових прав і обов'язків» [3, с. 38]. Отже, враховуючи зазначені погляди науковців, можна дійти висновку про те, що адміністративно-правова охорона є системним явищем адміністративного права, суть якого проявляється у діяльності публічних органів, яка спрямована на те, щоб забезпечити права громадян.

Повертаючись до мети підрозділу, а саме розгляду кібербезпеки, необхідно відмітити, що кібербезпека становить системну проблему кожної держави і перш за все по відношенню економіки країни, в особливості електронної промисловості, а також в аспекті питань, які стосуються розвитку інфраструктури електронних комунікацій, технологій кіберзахисту, інформаційних ресурсів державного зразка, заходів по боротьбі з кіберзлочинністю та кібертероризмом тощо.

З юридичної точки зору, кібербезпека – це стан захищеності інтересів суспільства, держави та особи від можливих кіберзагроз, бо правильне розуміння кіберзагроз дає можливість опанувати не тільки суть кібербезпеки, але і організаційно-правову основу її забезпечення [4, с. 133].

В науковій доктрині на сьогоднішній день, тлумачення кібербезпеки обговорюється досить жваво. Це і дає можливість звернути свою увагу до відповідних напрацювань науковців, які вже аналізували зазначений об'єкт та виокремлювали його особливості. Кібербезпека являється абстрактним поняттям, яке з'явилося у сфері експлуатації комп'ютерної техніки з ціллю обмінюватися інформацією у віртуальному світі. Більш того, «віртуальний світ» не встановлений якимись межами або кордонами, тобто в ньому абсолютно кожна

людина набуває широкі можливості в сфері його використання. Цей момент і визначає «віртуальний світ» (кіберпростір), як зручне середовище для того, щоб здійснювати протиправну діяльність у вигляді правопорушень, різних злочинів (хакерські атаки на сайти, банківські бази тощо) [5, с. 97]. Отже, серед наукової спільноти, наприклад Д.В. Дубов визначає кібербезпеку як «стан захищеності інтересів людини і громадянина, суспільства та держави в кіберпросторі» [6, с. 73]. Тобто, його думка має вираз в тому, що політика забезпечення кіберебезпеки є вкрай важливою та пріоритетною для будь-якої держави, являючись складовою національної безпеки. В свою чергу, А.В. Тонконогов вважає, що з філософського погляду «кібербезпека – це властивість або стан системи зберігати надійність та функціональну стабільність в умовах сучасного інформаційного протиборства. При цьому кібербезпека, як і сфера, яка нею регулюється, – кіберпростір має дві змістові складові – інформаційну і технічну, завдяки чому кардинально розширяються сфера її дії» [7, с. 42-43]. Отже, кібербезпека як вид національної безпеки держави демонструє собою стан захищеності від внутрішніх та зовнішніх загроз в кіберпросторі.

На думку І.В. Діордіца: «кібербезпека – це стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі, що досягається комплексним застосуванням сукупності правових, організаційних, інформаційних заходів» [8, с. 110]. Схожа позиція відмічається О.А. Барановим, який зазначає, що «кібербезпека – це деякий стан систем, за якого нейтралізуються загрози доступності, цілісності або конфіденційності даних, що циркулюють в інформаційних системах» [9, с. 5]. На нашу думку, останні позиції вчених не до кінця характеризують суть явища, яке досліджується, тому що не дуже зрозуміло, про які інтереси людини і громадянина та системи йде мова.

Найбільш аргументованим, на нашу думку, є погляд щодо визначення кібербезпеки О.Г. Корченка, адже ним розкривається суть кібербезпеки через основоположні ознаки, які йому властиві як явищу. На його погляд, «кібербезпекою є сукупність активних захисних і розвідувальних дій, що в процесі інформаційного протиборства зусиллями поодиноких інсайдерів або організованих кіберугрупувань розгортаються навколо інформаційного ресурсу, інформаційно-комунікаційних технологій та інформаційно-телекомунікаційних систем та які спрямовані на досягнення і утримання потенційними протиборчими сторонами переваги у протидії новим загрозам безпеці для власних об'єктів критично важливої інформаційної і кіберінфраструктури» [10, с. 41].

Вказані погляди науковців знайшли своє відображення у не так давно прийнятому, основоположному Законі України нашого дослідження «Про основні засади забезпечення кібербезпеки України» № 2163-VIII від 5 жовтня 2017 року. Згідно до п. 5 ст. 1 зазначеного Закону вказується, що «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» [11]. Вважаємо, що означене трактування хоч і лаконічне, проте, не демонструє в повній мірі усю суть кібербезпеки як явища. Однак, якби там не було, закріплення цього поняття на законодавчому рівні є позитивним моментом для правової системи України.

Отже, проаналізувавши поняття «адміністративно-правова охорона» та «кібербезпека», можна зазначити, що адміністративно-правовою охороною у сфері забезпечення кібербезпеки можна розуміти діяльність відповідних органів державної влади, яка виконується

відповідно до засад імперативності та ієрархічності та направлена на те, щоб підтримувати та забезпечувати належний стан захищеності прав, інтересів та інформації конкретних суб'єктів у кіберпросторі.

Ключова особливість адміністративно-правового забезпечення кібербезпеки полягає в тому, що вона виконується в аспекті адміністративно-правових відносин. Окрім цього, суть зазначеного інституту є досить широкою і не обмежується виключно нормами захисту та спеціальними процедурами. Зокрема, досить часто адміністративно-правова охорона якогось об'єкта може сприйматись як інститут «карального» характеру, який складається з норм Кодексу України про адміністративні правопорушення (далі – КУпАП). Проте, норми КупАП містять в собі адміністративні стягнення для суб'єктів, якими порушується легальний стан конкретного об'єкта (кібербезпеки). У зв'язку з чим, щодо правопорушень, які здійснюються цим суб'єктом застосовуються норми юридичної відповідальності, ціль яких полягає в тому, щоб обмежити права і свободи. Застосовуючи подібні юридичні механізми, вони являються крайнім заходом, який має місце тільки по факту вчиненого правопорушення, об'єктом яких виступають правовідносини в розглядуваній сфері. Тобто, інститут адміністративно-правової охорони кібербезпеки в цьому випадку має куди більшу сферу дію, оскільки, щоб забезпечити ті чи інші правовідносини в адміністративному порядку, потрібно не тільки карати винних осіб, але і належно виконувати функціональні обов'язки органами державної влади з цілю не допускати виникнення подібних ситуацій та інших несприятливих моментів.

Насамкінець, слід також зазначити, що кібербезпеці притаманні особливості, які мають як негативне, так і позитивне забарвлення. Особливість негативного характеру цього інституту проявляється в недосконалому понятійному апараті. Відсутність чіткого визначення змісту кібербезпеки говорить про неоднозначність його розуміння, а

також про те, що її застосування дає змогу в окремо взятих випадках правопорушнику уникати відповідальності.

Інша особливість розглядуваного інституту виражається в тому, що з появою та закріплення на законодавчому рівні поняття «кібербезпека», про що вже йшла мова вище, в подальшому дасть змогу розробити ефективну та надійну стратегію захисту кібербезпеки в адміністративно-правовому порядку. З-поміж іншого, за Законом України «Про основні засади забезпечення кібербезпеки України» також визначено основні засади та суб'єктний склад механізму забезпечення зазначеного інституту, що без сумніву вважається юридичним проривом в зазначеній сфері та в процесі використання інноваційних технологій. Про зазначене вище більш детально буде йти мова під час подальшого дослідження.

Таким чином, після прийняття Закону України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року вперше було закріплено поняття кібербезпеки, яке означає «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».

Встановлено, що адміністративно-правова охорона у сфері забезпечення кібербезпеки – це діяльність відповідних органів державної влади, яка виконується відповідно до засад імперативності та ієрархічності та направлена на те, щоб підтримувати та забезпечувати належний стан захищеності прав, інтересів та інформації конкретних суб'єктів у кіберпросторі.

Ключовими особливостями кібербезпеки як об'єкта адміністративно-правової охорони є наступні: 1) відсутність чіткого

визначення змісту кібербезпеки, що говорить про неоднозначність його розуміння, а також про те, що її застосування дає змогу в окремо взятих випадках правопорушнику уникати відповідальності;
2) адміністративно-правова охорона кібербезпеки хоч і виконується в аспекті адміністративно-правових відносин, однак, суть зазначеного інституту є досить широкою і не обмежується виключно нормами захисту та спеціальними процедурами.

1.2. Об’єктний склад кібербезпеки та кіберзахисту як складової частини

Визначившись в попередньому підрозділі, що собою становить кібербезпека як об’єкт адміністративно-правової охорони – це дало змогу зрозуміти його суть як правового інституту. Відсутність його законодавчого виразу у національній системі права можна компенсувати нормами міжнародного права, за якими визначаються основні положення, напрямки дії, суб’єктний склад та завдання кібербезпеки, враховуючи сьогоднішні реалії. Окрім цього, за останні роки була активізована діяльність, яка направлена на те, щоб розробити та імплементувати норми, які регулюють цей інститут в державну законодавчу систему. Зазначений факт підтверджує суттєве розширення сфери дії кібербезпеки, що відображається на появі великої кількості пов’язаних із цим інститутом явищ та окремого об’єктного складу.

Розглядаючи усі аспекти кібербезпеки в межах дослідження, питання об’єктного складу не можна лишити уваги. Наукова розробка з зазначеного питання, враховуючи сучасну нормативну базу у сфері регулювання кібербезпеки дасть можливість більш точніше виявити сферу її безпосередньої дії. Проте, необхідно відмітити, що протягом довгого періоду становлення інституту, а також неоднозначність регулюючого законодавства стало підґрунтям для появи багатьох, які

також потребують певної уваги та визначення їх «змісту» діяльності. А тому, необхідно проаналізувати та співвіднести кібербезпеку та кіберзахист, тому що доволі часті зазначені явища можна сприймати як абсолютно ідентичні, що є не досить правильно. Забігаючи наперед, потрібно зазначити, що кібербезпеці властива більш змістовніша дефініція та суть ніж кіберзахисту. З іншої сторони, кіберзахист як явище характеризується наявним окремим об'єктним складом.

На сьогоднішній день термін «кіберзахист» належним чином не відображено ні серед наукової спільноти, ні на законодавчому рівні. Більша частина науковців зазвичай ототожнюють його із кібербезпекою, що з нашого погляду являється невірним. За положеннями чинного законодавства термін «фігурує» доволі часто, але в той же час його дефініція за жодним офіційним документам не представлена. Як приклад, відповідно до Указу Президента України Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» [12], поняття кіберзахисту можна зустріти неодноразово. Зокрема, згідно до загальних положень Стратегії зазначається, що для того, щоб досягнути мету документа, тобто «створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави» [12], потрібно забезпечити кіберзахист державних електронних інформаційних ресурсів та інформації, яка в них міститься. Серед іншого, зазначений термін можна опосередковано побачити в іншому аналогічному нормативно-правовому акті, а саме: в Указі Президента України «Про рішення Ради національної безпеки і оборони України від 2 вересня 2015 року «Про нову редакцію Воєнної доктрини України» [13]. Згідно до положень зазначеного документу зазначається, що ключова роль під час забезпечення воєнної безпеки України покладається на Збройні сили України, водночас, виходячи зі своєї компетенції, інші суб'єкти сектору безпеки теж здійснюють важливі

функції. Так, Державна служба спеціального зв’язку та захисту інформації України направляє свої повноваження на «забезпечення функціонування урядового зв'язку Верховного Головнокомандувача Збройних Сил України з посадовими особами Збройних Сил України, інших військових формувань, правоохоронних органів спеціального призначення під час їх перебування у пунктах управління, забезпечення кіберзахисту об'єктів критичної інфраструктури» [13]. Не дивлячись на те, що означений термін відбивається за цими нормативно-правовими актами, однак, суть та інші властивості цього явища взагалі не розкриваються. Саме тому, враховуючи відсутність дефініції поняття кіберзахисту на законодавчому рівні, за доцільно буде проаналізувати його, спираючись на його тлумачення з лінгвістичної точки зору.

Поняття «кіберзахисту» можна розуміти як захисні дії, які направляються на те, щоб забезпечити безпеку у сфері отримання, обробки, зберігання та передачі інформації за сприянням складних систем управління. Основним проблемним аспектом зазначеного трактування є те, що воно не відображає особливості кіберзахисту як явища та в цілому створює тільки плутаність, тим самим не дає змогу розмежувати його з кібербезпекою як правовим інститутом. Проте, в працях науковців ці терміни мають синонімічний відбиток, однак деякими науковцями наводяться інші точки зору. Наприклад, О.В. Коломієць стверджує, що «поняття кіберзахисту доречно трактувати як сукупність методів і заходів організаційного, нормативно-правового та технічного характеру, спрямованих на забезпечення кібербезпеки» [14, с. 548]. Хоч це визначення в певній мірі дає пояснення природи цього явища, однак воно не відображає його внутрішнє змістовне наповнення. Тому, більш ширше розуміння наводить В.П. Шеломенцев, який під кіберзахистом розуміє «систему заходів правового, організаційного, ресурсно-фінансового, програмно-технічного та іншого характеру, спрямовану на створення умов, за яких

виключаються або суттєво утрудняються протиправні посягання на об’єкти такого захисту (певні інформаційні об’єкти кіберпростору). Іншими словами, це діяльність у кіберпросторі з охорони певних його об’єктів від протиправних посягань (наприклад, кіберзлочинів) і створення перешкод у реалізації загроз кримінального характеру» [15, с. 347]. На нашу думку, це визначення є більш ніж коректним науковим поглядом, тому що воно майже в повній мірі відповідає тому поняттю кіберзахисту, яке представлено в п. 7 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України», за яким: «кіберзахист – сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем» [11]. Цим поняттям законодавцем було закріплено на нормативному рівні напрями, які регулюють поточний стан кібербезпеки в Україні. Окрім цього, це визначення представлено дуже грамотно, оскільки воно передбачає існування заходів забезпечення «іншого характеру», тим самим значно поширює дію правового інституту, задля підтримки якого вони створювалися.

Отже, зазначене вище дає змогу встановити, що під кіберзахистом необхідно розуміти механізм засобів різного характеру, які забезпечують підтримку інституту кібербезпеки. Тобто розмежування кібербезпеки та кіберзахисту є принциповим та важливим моментом, адже воно так чи інакше пов’язується із процесом під час їх реалізації, який при некоректному підході може надати шкоди інтересам та правам людей, які охороняються законом та які виконують спеціальні операції з інформацією в кіберпросторі.

Аналізуючи та проводячи границю між суттю інститутів кібербезпеки та механізму кіберзахисту також являється ключовим

значенням для того, щоб висвітлити їх об’єктний склад, який є дуже різноманітним. Несхожа природа, а також цільове призначення цих явищ прямо вказують на те, об’єкти їх правового впливу є різними. Слід відзначити, що цей аспект відображено за чинним законодавством України.

Враховуючи надані наукові позиції, можна побачити, що об’єктний склад кібербезпеки представлений у вигляді суспільних відносин щодо використання кіберпростору та організації безпечного пошуку, обробки та передачі інформації в розглядуваній сфері. Об’єктами ж механізму кіберзахисту є матеріальні та нематеріальні блага, на які спрямовуються заходи щодо забезпечення кібербезпеки, які складають цей механізм.

Щоб більш детальніше зрозуміти об’єктний склад кібербезпеки, його потрібно проаналізувати через призму напрямків його забезпечення. Так, відповідно до положень Закону України «Про основні засади забезпечення кібербезпеки України», зазначається, що основними напрямами забезпечення кібербезпеки України є:

– «розвиток інформаційної інфраструктури держави, забезпечення безпечного функціонування об’єктів критичної інформаційної інфраструктури;

– розвиток міжнародного співробітництва у сфері кібербезпеки;

– зосередження ресурсів і посилення координації діяльності правоохоронних, розвідувальних і контррозвідувальних органів України для боротьби з проявами кіберзлочинності та кібертероризму;

– забезпечення ефективного застосування Збройних Сил України для адекватної відповіді реальним та потенційним кіберзагрозам національному сегменту кіберпростору;

– розвиток пріоритетних напрямів науки і техніки як основи створення високих інформаційних технологій;

– підтримка виробників продукції та послуг у сфері кібербезпеки на засадах стимулювання вітчизняних виробників;

– адаптація законодавства України до норм ЄС, створення нормативно-правових та економічних передумов для розвитку інформаційної інфраструктури держави, підвищення її стійкості до кібератак, спроможності держави більш ефективно захищати національні інтереси у кіберпросторі;

– забезпечення неухильного дотримання власниками об’єктів критичної інформаційної інфраструктури вимог законодавства у сфері захисту державних інформаційних ресурсів, криптографічного та технічного захисту інформації, захисту персональних даних;

– підвищення рівня обізнаності суспільства щодо ризиків, викликів і загроз у кіберпросторі» [11].

Враховуючи наведені напрями забезпечення кібербезпеки, можна зробити висновок про те, що до об’єктів кібербезпеки відносяться:

1) правовідносини у сфері розвитку державної інформаційної інфраструктури;

2) правовідносини у сфері знаходження міжнародних зв’язків з ціллю обмінюватися необхідним досвідом при розбудові сфери кібербезпеки;

3) правовідносини щодо регулювання, координування та контролю діяльності правоохоронних органів та інших суб’єктів, які забезпечують кібербезпеку під час виконання своїх обов’язків;

4) правовідносини, які стосуються сфери запровадження інформаційних технологій в ключових галузях життєдіяльності суспільства та приведення в належний стан процесу під час їх безпечного використання;

5) правовідносини, які стосуються сфери розвитку науки та техніки з ціллю побудувати предметну основу інституту кібербезпеки,

мається на увазі розробити новітні технології, які допоможуть підвищити безпеку під час роботи у кіберпросторі;

6) правовідносини, які стосуються сфери адаптації у чинне законодавство України правових механізмів, які дозволять забезпечити кібербезпеку, враховуючи міжнародний досвід у цій галузі;

7) правовідносини, які стосуються сфери підвищення інформаційної освіченості суспільства під час роботи з відповідною інформацією у кіберпросторі, тощо.

Окрім цього переліку існують ще об’єкти, які закріплені за ст. 4 Закону України «Про основні засади забезпечення кібербезпеки України», за яким встановлено: «1) конституційні права і свободи людини і громадянина; 2) суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища; 3) держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність; 4) національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави; 5) об’єкти критичної інфраструктури» [11].

Звичайне, перелік об’єктів, який представлено не є сталим, тому що суспільні відносини у сфері кібербезпеки сьогодні невпинно розвиваються. Вектор становлення зазначеного правового інституту направлений євроінтеграційним процесом, саме тому його особливості загалом та об’єктний склад, зокрема, в найближчому майбутньому будуть відповідати європейським стандартам.

Продовжуючи, зазначимо, що кіберзахист, як вже було визначено, має впливову дію не на конкретні групи правовідносин, а на матеріальні та нематеріальні блага. Тобто, можна стверджувати, що об’єкти кіберзахисту виділяються значним ступенем конкретики. Зазначена позиція закріплена на законодавчому рівні. Згідно до ст. 2 Рішення Ради Національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації»

підкреслюється, що на Кабінет Міністрів України, Службу Безпеки України та Національну поліцію України покладається обов'язок забезпечувати регулювання та охорону окремих об'єктів кіберзахисту, до яких відносяться:

– об'єкти критичної інформаційної інфраструктури;

– інформаційно-телекомунікаційні системи фінансового сектору держави, тощо [16].

В зазначеному нормативно-правовому акті окреслені об'єкти кіберзахисту тільки згадуються в окремих положеннях, а повністю весь перелік не виділяється. Однак, відповідно до ст. 4 Закону України «Про основні засади забезпечення кібербезпеки України» визначено чіткий перелік об'єктного складу кіберзахисту, до якого входять: «комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону; об'єкти критичної інформаційної інфраструктури; комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу» [11]. Охарактеризуємо кожен із видів змістовніше.

1. Першою ланкою вважаються інформаційно-телекомунікаційні системи, відповідно до яких обробляється інформація, яка охороняється законом, тобто це такі відомості, які не призначаються для загального користування. Виходячи з положень законодавства, зазвичай виділяють певні види такої інформації. Одним із таких видів виступає державна таємниця, яка відповідно до Закону України «Про державну таємницю», означає «вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та

охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому цим Законом, державною таємницею і підлягають охороні державою» [17]. В даному разі штучне порушення роботи інформаційно-телекомунікаційних систем, в яких зберігаються такі відомості, можуть нанести значної шкоди не тільки приватним, але й інтересам держави в окремих галузях діяльності України.

З-поміж державної таємниці, в зазначеній сфері може оброблятися і інша інформація, яка охороняється законом, зокрема: 1) інформація, якою володіють засоби масової інформації або журналісти та яка надається їм на підставі нерозголошення авторства чи джерела походження такої інформації; 2) відомості, які становлять лікарську таємницю; 3) відомості, які становлять таємницю вчинення нотаріальних дій; 4) відомості, які становлять банківську таємницю; 5) інформація, яка може знаходитись у операторів та провайдерів телекомунікацій щодо (зв'язку, абонентів, під час надання телекомунікаційний послуг) тощо [18, с. 456-457].

Розголошення чи викрадення відомостей, які були перераховані під час здійснення кібератаки, звісно ж не будуть мати такої шкоди, як під час здійснення подібної атаки на відомості, які містять державну таємницю. Однак, уся інформація, згідно з якою є законодавча вимога стосовно охорони, в автоматичному порядку стає об'єктом кіберзахисту в тих випадках, якщо під час її обробки використовуються комп'ютерні технології.

2. Другою ланкою виступають об'єкти критичної інформаційної інфраструктури. Відповідно їх перелік визначено у постанові Кабінету Міністрів України № 563 від 23 серпня 2016 року «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави», в якій виділяють наступні об'єкти: «підприємства та установи (незалежно від форми

власності) таких галузей, як енергетика, хімічна промисловість, транспорт, банки та фінанси, інформаційні технології та телекомунікації (електронні комунікації), продовольство, охорона здоров’я, комунальне господарство, що є стратегічно важливими для функціонування економіки і безпеки держави, суспільства та населення» [19].

Забезпечення охорони перелічених об'єктів є однією із основних задач. Головна загроза, яка порушує цілісність останніх визнається як законом, так і іншими нормативно-правовими актами. Зокрема, відповідно до цієї ж постанови встановлюється, що «кібератака – несанкціоновані дії, що здійснюються з використанням інформаційно-комунікаційних технологій та спрямовані на порушення конфіденційності, цілісності і доступності інформації, яка обробляється в інформаційно-телекомунікаційній системі, або порушення сталого функціонування такої системи» [19].

3. До третьої групи об’єктів кіберзахисту відносяться інформаційно-телекомунікаційні системи, за якими відбувається обробка державних інформаційних ресурсів. Останні фактично визнаються головною ціллю державної охорони від можливих кібератак. З цього приводу, О.Д. Довгань визначає, що «інформаційні ресурси – це документи і масиви документів в інформаційних системах: бібліотеках, архівах, фондах, банках даних, депозитаріях, музейних сховищах і т. ін. Існують інформаційні ресурси спільного користування – сукупність інформаційних ресурсів державних органів науково-технічної інформації, наукових, науково-технічних бібліотек, а також комерційних центрів, фірм, організацій, які займаються науково-технічною діяльністю і з власниками яких укладено договори про їх спільне використання» [20, с. 86-87].

Загалом, можна сказати, що охорона об’єктів кібербезпеки є одним із стратегічно важливих питань для сучасного стану національної

безпеки України, в якій кіберзахисту відводиться не менш важливе – тактичне значення.

На підставі вищевикладеного, слід зазначити про те, що кібербезпека являється складним правовим явищем, в межах якого діє механізм кіберзахисту, який представлено у вигляді засобів різного характеру (організаційного, нормативно-правового, воєнного, технічного тощо), що забезпечують підтримку інституту кібербезпеки та який є невід'ємною складовою частиною під час визначення об'єктного складу в зазначеній сфері.

Встановлено, що об'єктний склад кібербезпеки представлений у вигляді суспільних відносин щодо використання кіберпростору та організації безпечного пошуку, обробки та передачі інформації в розглядуваній сфері. Об'єктами ж механізму кіберзахисту є матеріальні та нематеріальні блага, на які спрямовуються заходи щодо забезпечення кібербезпеки, які складають цей механізм.

1.3. Правові засади забезпечення кібербезпеки

За Стратегією сталого розвитку «Україна – 2020», яка була схвалена Указом Президента України від 12 січня 2015 р. № 5 [21], визначено, що в Україні було розпочато та триває по сей день реформування системи державного управління, основна мета якого полягає у тому, щоб забезпечити її прозорість, яка спрямовується на приведення суспільного сталого розвитку та на ефективне і чітке реагування сьогоднішніх внутрішніх та зовнішніх викликів.

З огляду на це, в межах кваліфікаційної роботи та складових елементів державного управління в розглядуваній сфері, виникає потреба проаналізувати базові ідеї, категорії та фундаментальні засади, на яких функціонує означена система, тобто – основоположних принципів.

Не менш цікавою є структура кібербезпеки, до складу якої входить, як вже було визначено – механізм кіберзахисту. Сучасна нормативно-правова база дає змогу виділяти значний масив правових засад, які забезпечують цей інститут, однак, враховуючи специфіку дослідження, потрібно також звернути увагу та розглянути місце адміністративно-правового регулювання в системі принципів зазначеного механізму.

Слід зазначити, що правові засади будь-якої юридичної галузі беруть свій початок згідно до положень Конституції України. Тому, якщо розглянути адміністративно-правові засади забезпечення кібербезпеки, потрібно мати на увазі і особливості правової системи, яка формується за Конституцією України. Отже, відповідно до ст. 8 Конституції України закріплено, що «Конституція України має найвищу юридичну силу. Закони та інші нормативно-правові акти приймаються на основі Конституції України і повинні відповідати їй» [1].

Тобто, за цією нормою можна побачити, що право проголошується як єдиний та головний регулятор суспільних відносин. Цей аспект дає змогу стверджувати, що механізм, який забезпечує інститут кібербезпеки має підґрунтя юридичного характеру, а саме – основну частину правових засад (принципів), які формують адміністративно-правові відносини.

Юридичні засади взагалі представляють собою досить цікаву теоретичну конструкцію. В науковій літературі їх загальноприйнято виокремлювати в поняття «правові принципи». Найпростіша дефініція виглядає наступним чином: «це керівні ідеї, основи певної правової галузі, інституту чи окремого механізму» [22, с. 44].

Зазначене є достатнім для того, щоб запропонувати під правовими засадами забезпечення кібербезпеки розуміти керівні ідеї, засади та положення, які закріплені за нормами нормативно-правових актів, що

мають різну юридичну силу та визначають механізм правового регулювання щодо забезпечення кібербезпеки.

Вагоме місце в системі правових засад щодо забезпечення кібербезпеки займають принципи правового регулювання, які відображені в Законі України «Про основні засади забезпечення кібербезпеки України». Згідно до п.1 ст. 3 зазначеного Закону: «Правову основу забезпечення кібербезпеки України становлять Конституція України, закони України щодо основ національної безпеки, засад внутрішньої і зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, цей та інші закони України, Конвенція про кіберзлочинність, інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, укази Президента України, акти Кабінету Міністрів України, а також інші нормативно-правові акти, що приймаються на виконання законів України» [11]. Однак, необхідно відмітити, що вказана норма не містить перелік актів, положення яких встановлюють механізм забезпечення кібербезпеки. Цілком логічно, що цими актами є Кримінальний кодекс України (далі – КК України) та КУпАП. Важливість цих документів полягає у тому, що вони виступають своєрідним «буфером», який протидіє правопорушенням у сфері кібербезпеки. В цих кодексах закріплено норми, за якими дозволяється застосовувати до винних осіб більш суворі заходи примусу, в тому числі запобігати та припиняти правопорушення.

Продовжуючи, зазначимо, що на сьогоднішній день правові засади, які забезпечують механізм кібербезпеки України, ґрунтуються на основних принципах, які закріплені у ст. 7 Закону України «Про основні засади забезпечення кібербезпеки України»:

– «верховенства права, законності, поваги до прав людини і основоположних свобод та їх захисту в порядку, визначеному законом;

– забезпечення національних інтересів України;

– відкритості, доступності, стабільності та захищеності кіберпростору, розвитку мережі Інтернет та відповідальних дій у кіберпросторі;

– державно-приватної взаємодії, широкої співпраці з громадянським суспільством у сфері кібербезпеки та кіберзахисту, зокрема шляхом обміну інформацією про інциденти кібербезпеки, реалізації спільних наукових та дослідницьких проектів, навчання та підвищення кваліфікації кадрів у цій сфері;

– пропорційності та адекватності заходів кіберзахисту реальним та потенційним ризикам, реалізації невід'ємного права держави на самозахист відповідно до норм міжнародного права у разі вчинення агресивних дій у кіберпросторі;

– пріоритетності запобіжних заходів;

– невідворотності покарання за вчинення кіберзлочинів;

– пріоритетного розвитку та підтримки вітчизняного наукового, науково-технічного та виробничого потенціалу;

– міжнародного співробітництва з метою зміцнення взаємної довіри у сфері кібербезпеки та вироблення спільних підходів у протидії кіберзагрозам, консолідації зусиль у розслідуванні та запобіганні кіберзлочинам, недопущення використання кіберпростору в терористичних, воєнних, інших протиправних цілях;

– забезпечення демократичного цивільного контролю за утвореними відповідно до законів України військовими формуваннями та правоохоронними органами, що провадять діяльність у сфері кібербезпеки» [11].

Розглядати усі принципи не будемо, щоб не виходити за межі дослідження, проте надамо характеристику тим, які на нашу думку, викликають найбільший інтерес.

1. Принцип пріоритетності запобіжних заходів означає, що держава здійснює першочергові заходи, які спрямовані на те, щоб

запобігати зловживанню та корупції зі сторони посадових осіб компетентних органів, які займаються питаннями кібербезпеки, удосконаленням системи державного контролю, які забезпечують стан кібербезпеки та посилюють обороноздатність держави в кіберпросторі.

Сьогодні практично безмежні можливості використання мережі Інтернет свідчать про глобальну загрозу віртуальних злочинів, кібертероризму та ведення кібервійни.

Україна до сих пір залишається тією державою, яка уразлива в сфері щодо використання сучасних ІТ і не останнє місце у цьому відіграє надмірно велике використання іноземних програмних продуктів, а також впровадження матеріально-технічної бази іноземного виробництва. У зв'язку з цим, існують питання, які становлять проблеми стосовно реалізації національної операційної системи (хоча б для того, щоб використовувати її в системі органів державної влади, однак для цього переходу до програмного забезпечення з відкритим кодом існують значні зауваження зі сторони вітчизняних організацій, які займаються безпекою) [23, с. 123–124]. При таких умовах обов'язки держави повинні спрямовуватися, перш за все, на те, щоб розробляти вітчизняну інноваційну продукцію, яка в подальшому може використовуватися з ціллю посилення кібербезпеки та під час запобігання правопорушення у сфері державної безпеки вітчизняного кіберпростору, тощо.

Переходячи безпосередньо до суті цього принципу, необхідно вказати, що запобіжні заходи закріплюються саме за нормами адміністративного законодавства, тому що вони реалізуються органами державної влади та використовуються, як вже неодноразово наголошувалося, з ціллю попередження правопорушень в кіберпросторі та їх недопущення в подальшому. Окрім цього, в межах механізму забезпечення кібербезпеки адміністративно-правове регулювання становить вагоме значення.

Роль адміністративно-правового регулювання в розглядуваній сфері проявляється в тому, що згідно до діючих норм адміністративного законодавства відбувається правове регулювання діяльності суб'єктів, які забезпечують кібербезпеку в Україні. До речі, щодо суб'єктів, то про них мова буде йти вже в наступному розділі дослідження.

Яскравий приклад, який відображає роль адміністративно-правового регулювання у системі забезпечення кібербезпеки є сформована урядова команда, яка здійснює реагування на комп'ютерні надзвичайні події України «CERT-UA». Відповідно до ст. 9 Закону України «Про основні засади забезпечення кібербезпеки України», основними завданнями цієї команди є наступні:

– «накопичення та проведення аналізу даних про кіберінциденти, ведення державного реєстру кіберінцидентів;

– надання власникам об'єктів кіберзахисту практичної допомоги з питань запобігання, виявлення та усунення наслідків кіберінцидентів щодо цих об'єктів;

– організація та проведення практичних семінарів з питань кіберзахисту для суб'єктів національної системи кібербезпеки та власників об'єктів кіберзахисту;

– підготовка та розміщення на своєму офіційному веб-сайті рекомендацій щодо протидії сучасним видам кібератак та кіберзагроз;

– взаємодія з правоохоронними органами, забезпечення їх своєчасного інформування про кібератаки» [11] тощо.

Отже, адміністративно-правове регулювання можна вважати як одну із ключових засад, яка забезпечує кібербезпеку України. Більш того, заходам, які формують систему управлінського регулювання, надається пріоритетний характер, оскільки їх дія направляється на те, щоб попереджати порушення прав і законних інтересів суб'єктів у сфері обробки інформації, яка знаходиться в кіберпросторі.

2. Інший, досить цікавий принцип стосується засади невідворотності покарання за вчинення кіберзлочинів. Він є похідним від основоположного завдання кримінального права, яке полягає у тому, щоб забезпечити охорону прав і свобод людини і громадянина, громадський порядок та безпеку, конституційний устрій України від злочинних посягань, мир і безпеку людства, а також запобігати злочинам.

Світова спільнота наголошує, що якогось одного єдиного підходу, який би узагальнював норми кримінального законодавства держав у сфері боротьби з кіберзлочинністю – не існує, в тому числі є вагомі відмінності під час формування кримінальної статистики правоохоронними органами тощо. Специфічна особливість кіберзлочинності полягає в тому, що кіберзлочини можуть відноситись і до міжнародної категорії, тому що злочинці здійснюють протиправні дії в одній країні, а їх жертви знаходиться зовсім в іншій, саме тому, з ціллю боротися з такими кримінальними правопорушеннями необхідно об’єднувати зусилля в межах міжнародного співробітництва та міжнародних організацій. Тобто, цей принцип означає, що особа, вчинивши кіберзлочин, повинна бути покарана в рамках кримінального закону, що в свою чергу передбачає своєчасність у притягненні цієї особи до відповідальності, а також те, що ні у кого не повинно бути привілеїв перед законом і що найголовніше – така особи не може бути двічі покарана за одне і теж кримінальне правопорушення. В цьому і відмічається посил невідворотності відповідальності як ефективний засіб запобігати правопорушенням.

3. Принцип пріоритетності розвитку та підтримки вітчизняного наукового, науково-технічного та виробничого потенціалу являється декларативним та спрямовується на те, що створювати належні умови і слугувати стимулом для розбудови, в першу чергу, науково-технічного

потенціалу країни, що в комплексі становить сукупність усіх її наукових засобів і ресурсів.

Інформаційне суспільство – це без сумніву якісний та новий етап еволюції суспільства, головним напрямком якого під час його формування є побудова інформаційного простору, який буде динамічний, структурований, високотехнологічним та завжди захищеним [24, с. 168].

Як вказує О.Ф. Гіда, «залежність Української держави від іноземного інформаційного продукту набула загрозливих масштабів для національної безпеки і робить малоефективною систему державного регулювання національного медіапростору» [25, с. 276]. Однак, це не завжди відображає реальний стан справ у зазначеній сфері, тому що, не дивлячись на те, що проводиться антитерористична операції на Сході України, держава активно направляє зусилля в напрямі розвитку та підтримки вітчизняного наукового, науково-технічного та виробничого потенціалу, враховуючи аналіз положень Концепції Державної цільової програми реформування та розвитку оборонно-промислового комплексу України на період до 2020 року [26], за якою передбачено реалізувати заходи, які спрямовані на те, щоб залучати інвестиції в оборонно-промисловий комплекс з використанням державних, приватних та іноземних фінансових ресурсів; створювати системи науково-технічної і виробничої кооперації; впроваджувати у виробництво нову техніку та наукоємні технології і матеріали, створення яких передбачено державними цільовими оборонними програмами; вдосконалювати системи науково-технічної і виробничої кооперації на внутрішньому та зовнішньому ринках; упроваджувати сучасний ринковий механізм господарювання; розвивати державно-приватне партнерство [26].

4. Принцип забезпечення демократичного цивільного контролю над утвореними відповідно до законів України військовими формуваннями та правоохоронними органами держави, що діють у сфері

кібербезпеки. Вагомою задачею держави у цьому напрямі залишається вдосконалення системи демократичного цивільного контролю у секторі безпеки і оборони та посилення парламентського контролю у цій сфері.

Основна складова, яка дає змогу формувати системи цивільно-військових відносин є реалізація демократичного цивільного контролю щодо суб'єктів, які забезпечують кібербезпеку та яка визнана як одна із ключових ознак, за якою забезпечується стабільний політичний режим в країні, в тому числі існує демократична зрілість самого громадянського суспільства. Серед іншого, одне із фундаментальних досягнень України в аспекті забезпечення такого контролю є сформована принципово нова законодавча та нормативно-правова база з військових та оборонних питань, завдяки якій і забезпечується відповідна координація зусиль суб'єктів органів державної влади загалом та суспільства, зокрема, що в сукупності дає можливість вдосконалювати заходи стосовно забезпечення кібербезпеки [27, с. 119–120].

Підсумовуючи, зазначимо, що під правовими засадами забезпечення кібербезпеки слід розуміти керівні ідеї, засади та положення, які закріплені за нормами нормативно-правових актів, що мають різну юридичну силу та визначають механізм правового регулювання щодо забезпечення кібербезпеки.

На сьогоднішній день правові засади, які забезпечують механізм кібербезпеки України, ґрунтуються на основних принципах, які закріплені у Законі України «Про основні засади забезпечення кібербезпеки України».

РОЗДІЛ 2
АДМІНІСТРАТИВНО-ПРАВОВИЙ МЕХАНІЗМ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ

2.1. Адміністративно-правовий статус суб'єктів, які забезпечують кібербезпеку України

Розглядаючи явище кібербезпеки, було виявлено, що на сьогоднішній день воно містить в собі законодавчу основу, яка є досить структурованою. Інститут та усі явища, які для нього є супутніми, цілком і повністю узаконені на території нашої держави. Окрім цього, визначна перевага законодавчої база, яка здійснює регулювання кібербезпеки полягає в тому, що в ній досить чітко конкретизовано перелік суб'єктів, які забезпечують даний інститут та визначено їх повноваження. У зв'язку з чим, враховуючи цю особливість, потрібно охарактеризувати систему суб'єктів, які забезпечують кібербезпеку та визначити їх адміністративно-правовий статус (повноваження) під час реалізації механізму кіберзахисту, який стосується окремих об'єктів.

Необхідно пам'ятати, що якщо мова йде про суб'єктів, які забезпечують кібербезпеку, то в цьому контексті це має відношення до учасників правових відносин відповідного типу. З цього випливає, що для аналізу їх адміністративно-правового статусу потрібно враховувати класичний погляд на суб'єктів правовідносин. В загальній правовій теорії, «суб'єктами правових відносин є учасники суспільних відносин, які виступають носіями юридичних прав та обов'язків» [28, с. 229].

Відмітимо, що суб'єкти, які забезпечують кібербезпеку – окремими науковцями розглядаються як учасники інформаційних відносин. Наприклад, подібна думка висловлюється І.В. Діордициною. Аргументуючи свою позицію, вона спирається на трактування учасників інформаційних відносин, яке представлене у Словнику стратегічних

комунікацій В.А. Ліпкана, в якому зазначається, що «суб'єкт інформаційної діяльності – це юридична або фізична особа, задіяна в інформаційному процесі» [29, с. 161]. Зазначений погляд має місце бути, проте, на нашу думку, він є не зовсім вірним. Суб'єкти, які забезпечують кібербезпеку являються учасниками не інформаційних, а адміністративних правовідносин, тому що: 1) їх відносини базуються на засадах влади і підпорядкування; 2) реалізація механізму кіберзахисту здійснюється за рахунок використання примусу, який надається їм згідно до чинного законодавства; 3) їх діяльність спрямовується на те, щоб припиняти правопорушення у цій сфері. Необхідно також додати, що для того, щоб аналізувати адміністративно-правовий статус зазначеної категорії, апріорі неможливо виходити за межі адміністративної галузі права.

Отже, суб'єкти, які забезпечують кібербезпеку являються учасниками правовідносин управлінського характеру, який зумовлено їх правовим статусом. З ціллю максимально змістовно проаналізувати зазначене питання, потрібно звернутися до нормативно-правових актів, в яких зазначено перелік цих суб'єктів, їх права та обов'язки.

Слід зазначити, що на законодавчому рівні, перелік зазначених суб'єктів є не однорідним. Один із перших офіційних документів, положення якого згадують систему суб'єктів, які забезпечують кібербезпеку, є Указ Президента України «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» [12]. За цим нормативним документом вперше було впроваджено трактування «національна система кібербезпеки». За цією системою і визначено головних учасників процесу, які займаються захистом прав і свобод осіб у відносинах, що стосуються обробки та обміну інформацією, яка знаходиться у кіберпросторі. Отже, відповідно до глави 3 Стратегії зазначається, що «основу національної системи кібербезпеки становитимуть Міністерство

оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, Національний банк України, розвідувальні органи» [12]. В свою чергу, згідно до положень ч. 4 ст. 5 Закону України «Про основні засади забезпечення кібербезпеки України», «суб'єктами, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, є:

1) міністерства та інші центральні органи виконавчої влади;

2) місцеві державні адміністрації;

3) органи місцевого самоврядування;

4) правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності;

5) Збройні Сили України, інші військові формування, утворені відповідно до закону;

6) Національний банк України;

7) підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури;

8) суб'єкти господарювання, громадяни України та об'єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом» [11].

Отже, можна побачити, що в Законі України «Про основні засади забезпечення кібербезпеки України» окреслюється загальна система суб'єктів, які забезпечують кібербезпеку України. Звісно, за кожним учасником правовідносин в зазначеній сфері закріплюються повноваження, які дають змогу йому реалізувати напрями діяльності та забезпечувати необхідні заходи з ціллю підтримувати належний стан зазначеного інституту. Іншими словами, адміністративно-правовий

статус кожного із суб'єктів, які забезпечують кібербезпеку є суто індивідуальним та характеризується деякими особливостями, які більш яскраво відображаються саме в правах та обов'язках цих суб'єктів.

Окрім цього, відповідно до п. 5 ст. 5 Закону України «Про основні засади забезпечення кібербезпеки України» вказується, що «суб'єкти забезпечення кібербезпеки у межах своєї компетенції: здійснюють заходи щодо запобігання використанню кіберпростору у воєнних, розвідувально-підривних, терористичних та інших протиправних і злочинних цілях; здійснюють виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків; здійснюють інформаційний обмін щодо реалізованих та потенційних кіберзагроз; розробляють і реалізують запобіжні, організаційні, освітні та інші заходи у сфері кібербезпеки, кібероборони та кіберзахисту; забезпечують проведення аудиту інформаційної безпеки, у тому числі на підпорядкованих об'єктах та об'єктах, що належать до сфери їх управління; здійснюють інші заходи із забезпечення розвитку та безпеки кіберпростору» [11].

Серед зазначених загальних повноважень, якими володіють суб'єкти, що забезпечують кібербезпеку, їм ще притаманні спеціальні права і обов'язки, які зумовлюють їх особливий адміністративно-правовий статус. На нашу думку, ключовими суб'єктами, які забезпечують кібербезпеку, відображено в ст. 8 Закону України «Про основні засади забезпечення кібербезпеки України», серед яких: 1) Державна служба спеціального зв'язку та захисту інформації України; 2) Національна поліція України; 3) Служба безпеки України; 4) Міністерство оборони України; 5) Генеральний штаб Збройних Сил України; 6) розвідувальні органи; 7) Національний банк України [11].

Роль перелічених відомств, з-поміж інших суб'єктів, які забезпечують кібербезпеку, характеризується особливими напрямками їх діяльності та змогою використовувати спеціальні заходи стосовно

підтримки законного та належного рівня кібербезпеки, які фактично інші органи в своєму розпорядженні не мають.

Перед більш ґрунтовним розглядом основних повноважень зазначених суб'єктів, необхідно відмітити з нашої думки, що представлений перелік не є повним, оскільки до нього чомусь не було включено Кабінету Міністрів України (далі – КМУ). Згідно до положень законодавства, «Кабінет Міністрів України є вищим органом у системі органів виконавчої влади. Кабінет Міністрів України здійснює виконавчу владу безпосередньо та через міністерства, інші центральні органи виконавчої влади» [30]. Повноваження КМУ у сфері забезпечення кібербезпеки є беззаперечними, оскільки саме Урядом формується та реалізується державна політика в зазначеній сфері, в тому числі щодо захисту національних інтересів України у кіберпросторі, боротьби з кіберзлочинністю, а також під час організації та забезпечення відповідними засобами і ресурсами функціонування національної системи кібербезпеки тощо. Враховуючи зазначене, КМУ не тільки повинен входити до національної системи забезпечення кібербезпеки, а й фактично очолювати її. Проте, положеннями чинної нормативної бази, КМУ до цієї системи не відноситься, а просто слугує як суб'єкт із загальним статусом, що підтримує цей інститут. Тож, сподіваємось, що у найближчому майбутньому цю нормативну прогалину буде виправлено.

Продовжуючи розгляд основоположних суб'єктів, які забезпечують кібербезпеку та виокремлення особливостей їх адміністративно-правового статусу, відмітимо:

1) Державну служба спеціального зв'язку та захисту інформації України, бо цей орган більш за все переймається проблемами щодо регулювання правовідносин, об'єктом яких виступає інформація в усіх її проявах. Відповідно до п. 2. ст. 2 Закону України «Про Державну службу спеціального зв'язку та захисту інформації України» від

23 лютого 2006 року, «Державна служба спеціального зв'язку та захисту інформації України спрямовує свою діяльність на забезпечення національної безпеки України від зовнішніх і внутрішніх загроз та є складовою сектору безпеки і оборони України» [31].

У сфері забезпечення кібербезпеки «Державна служба спеціального зв'язку та захисту інформації України забезпечує формування та реалізацію державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту об'єктів критичної інформаційної інфраструктури, здійснює державний контроль у цих сферах; координує діяльність інших суб'єктів забезпечення кібербезпеки щодо кіберзахисту; забезпечує створення та функціонування Національної телекомунікаційної мережі, впровадження організаційно-технічної моделі кіберзахисту; здійснює організаційно-технічні заходи із запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків; інформує про кіберзагрози та відповідні методи захисту від них; забезпечує впровадження аудиту інформаційної безпеки на об'єктах критичної інфраструктури, встановлює вимоги до аудиторів інформаційної безпеки, визначає порядок їх атестації (переатестації)» [11];

2) досить специфічний адміністративно-правовий статус належить Національній поліції України (далі – НПУ) та Службі безпеки України (далі – СБУ) у сфері забезпечення кібербезпеки. Ці правоохоронні органи наділяються повноваженнями, які стосуються припинення правопорушень та притягнення злочинців до відповідальності.

Безпосередньо у галузі забезпечення кібербезпеки «Національна поліція України забезпечує захист прав і свобод людини і громадянина, інтересів суспільства і держави від злочинних посягань у кіберпросторі; здійснює заходи із запобігання, виявлення, припинення та розкриття

кіберзлочинів, підвищення поінформованості громадян про безпеку в кіберпросторі» [11];

3) повноваження СБУ у сфері забезпечення кібербезпеки дещо відрізняються. Так, у своїй діяльності СБУ наділяється повноваженнями, які направлені на протидію правопорушень та припинення злочинів, проте, її можливості є більш ширшими, враховуючи функціональну направленість відомства. Отже, «Служба безпеки України здійснює запобігання, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, які вчиняються у кіберпросторі; здійснює контррозвідувальні та оперативно-розшукові заходи, спрямовані на боротьбу з кібертероризмом та кібершпигунством, негласно перевіряє готовність об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів; протидіє кіберзлочинності, наслідки якої можуть створити загрозу життєво важливим інтересам держави; розслідує кіберінциденти та кібератаки щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечує реагування на кіберінциденти у сфері державної безпеки» [11];

4) суб'єктами, які забезпечують кібернетичну безпеку є Міністерство оборони України (далі – Міноборони) та Генеральний штаб Збройних Силу України (далі – Генеральний штаб). Повноваження цих органів абсолютно ідентичні. Вони «відповідно до компетенції здійснюють заходи з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони); здійснюють військову співпрацю з НАТО та іншими суб'єктами оборонної сфери щодо забезпечення безпеки кіберпростору та спільного захисту від кіберзагроз; впроваджують заходи із забезпечення кіберзахисту критичної інформаційної інфраструктури в умовах надзвичайного і воєнного стану» [11];

5) Досить близькі повноваження із Мінобороною та Генеральним штабом належать розвідувальним органам. У сфері забезпечення кібербезпеки «розвідувальні органи України здійснюють розвідувальну діяльність щодо загроз національній безпеці України у кіберпросторі, інших подій і обставин, що стосуються сфери кібербезпеки» [11]. З-поміж цього, необхідно зазначити, що до розвідувальних органів необхідно відносити відомства, які існують в незначній кількості. Цим же правовим статусом наділяються: «Служба зовнішньої розвідки України, розвідувальні органи Міноборони, розвідувальні органи спеціально уповноваженого центрального органу виконавчої влади у справах охорони державного кордону» [32];

6) важливе місце в зазначеній сфері займає Національний банк України, оскільки він «визначає порядок, вимоги та заходи із забезпечення кіберзахисту та інформаційної безпеки у банківській системі України та для суб’єктів переказу коштів, здійснює контроль за їх виконанням; створює центр кіберзахисту Національного банку України, забезпечує функціонування системи кіберзахисту у банківській системі України; забезпечує проведення оцінювання стану кіберзахисту та аудиту інформаційної безпеки на об’єктах критичної інфраструктури у банківській системі України» [11].

Повноваження Національного банку України, якщо порівнювати їх з іншими органами, є десь простіші, тому що він являється центральним банком України, головна мета якого – забезпечувати фінансову стабільність у державі. Виходячи з цього, можна сказати, що так і формується його роль у механізмі підтримки інституту кібербезпеки.

Враховуючи зазначене вище, слід вказати про те, що всі суб’єкти, які забезпечують кібербезпеку наділяються як загальними, так і специфічними повноваженнями.

Підсумовуючи, робимо висновок про те, що суб’єкти, які забезпечують кібербезпеку являються учасниками не інформаційних, а

адміністративних правовідносин, тому що: 1) їх відносини базуються на засадах влади і підпорядкування; 2) реалізація механізму кіберзахисту здійснюється за рахунок використання примусу, який надається їм згідно до чинного законодавства; 3) їх діяльність спрямовується на те, щоб припиняти правопорушення у цій сфері. Необхідно також додати, що для того, щоб аналізувати адміністративно-правовий статус зазначеної категорії, апріорі неможливо виходити за межі адміністративної галузі права.

Суб'єктів, які забезпечують кібербезпеку, потрібно поділяти на дві групи: загальну та спеціальну. До суб'єктів цих груп відносяться органи, перелік яких закріплено в Законі України «Про основні засади забезпечення кібербезпеки України».

2.2. Характеристика адміністративно-правових форм та методів щодо забезпечення кібербезпеки в Україні

Потреба забезпечення кібербезпеки в усьому світі та Україні є беззаперечною, адже сьогодні уявити життя без інформаційних технологій неможливо, в тому числі це стосується і діяльність органів державної влади, суб'єктів господарювання, тощо. А відтак, головний обов'язок держави – забезпечувати конфіденційність, цілісність та доступність даних. Проте, доводиться констатувати, що той стан, в якому знаходиться реалізація заходів, які забезпечують кібербезпеку в Україні, м'яко кажучи, бажає кращого, а це, в свою чергу, зумовлює потребу досліджувати та удосконалювати багато аспектів такої діяльності, одним із яких є розгляд адміністративно-правових форм та методів, які забезпечують кібербезпеку України. Саме ця категорія в комплексі створює так званий інструмент, завдяки якому суб'єкти, що забезпечують кібербезпеку мають можливість вирішувати складні завдання, які стоять перед ними в зазначеній сфері.

Розпочинаючи розгляд, зазначимо, що за загальним розумінням форма являє собою об’єктивне відображення змісту того чи іншого явища або процесу. За лінгвістичним тлумаченням, «форма – це типова будова, спосіб організації чого-небудь, структура, спосіб побудови думки» [33, с. 1328].

Розглядаючи безпосередньо поняття адміністративно-правової форми, зазначимо, що в юридичній літературі єдиного підходу, щоб зрозуміти цей термін – не існує, тим самим це вказує на різноманітність думок з приводу його трактування, однак виділимо, на нашу думку, найактуальніші. Так, на думку Ю.П. Битяка, «адміністративно-правова форма – це зовнішній вияв конкретних дій, що здійснюються органами виконавчої влади для реалізації поставлених перед ними завдань» [34, с. 211]. В межах нашого дослідження, заслуговує на увагу позиція О.В. Логінова, який «під адміністративно-правовою формою забезпечення інформаційної безпеки розуміє здійснення передбачених нормативно-правовими актами, теорією та практикою державного управління однорідної діяльності посадовими та службовими особами органів виконавчої влади, за допомогою якої реалізується їх компетенція по забезпеченню інформаційної безпеки» [35, с. 128].

Узагальнюючи ці думки, вважаємо, що адміністративно-правові форми забезпечення кібербезпеки України – це зовнішній прояв діяльності уповноважених державних органів, який проявляється під час вчинення ними відповідних дій, що спрямовуються на реалізацію таких умов, згідно до яких буде забезпечуватися безпека комп’ютерних систем у всій країні загалом. Слід відмітити, що в юридичній літературі не визначається єдиний підхід стосовно конкретних форм в зазначеній сфері, а тому, акцентуючи увагу на наукову літературу та норми чинного законодавства України, запропонуємо власний погляд стосовно переліку відповідних форм.

Так, виділимо таку адміністративно-правову форму як нормотворчість (мається на увазі прийняття нормативно-правових актів у сфері забезпечення кібербезпеки).

Нормотворчість являється ключовою формою, яка забезпечує кібербезпеку в Україні, тому що завдяки їй існує можливість формувати таке правове поле, за яким будуть виключатися будь-які можливості для суб'єктів цих відносин вчиняти правопорушення в зазначеній сфері. Тобто, нормотворчість в процесі формування правового припису, дає змогу досягати певну поведінку людей за конкретною сферою суспільних правовідносин, що, в свою чергу, має позитивний ефект в соціальному, економічному та політичному аспекті [36, с. 79].

Інша форма, яка забезпечує кібербезпеку – це прийняття індивідуальних актів. Індивідуальні акти в зазначеній сфері дають змогу чітко вирішувати актуальні проблемні моменти. Їх перевагою є те, що вони спрямовуються на конкретного суб'єкта. Як приклад індивідуальних актів, В.В. Марков виділяє наступні: «протокол засідання Кабінету Міністрів України від 11.04.2012 р. № 27 та лист Державної служби спеціального зв'язку та захисту інформації України від 21.05.2012 р. № 16/1/1-1543 стосовно підготовки законопроекту щодо вдосконалення порядку отримання правоохоронними органами інформації про споживачів телекомунікаційних послуг та порядку придбання SIM-карт споживачами» [37, с. 44].

Наступна адміністративно-правова форма, яка забезпечує кібербезпеку в Україні – адміністративний договір. В.С. Стефанюк «визначає адміністративний договір як договір, побудований на публічно-правових нормах, який регулює добровільне погодження волі двох (або більше) суб'єктів права, один із яких є суб'єктом управління, про встановлення взаємних адміністративних правовідносин» [38, с. 154].

Отже, адміністративний договір як адміністративно-правову форму, яка забезпечує кібербезпеку, можна вважати добровільною угодою між двома (або більше) суб'єктами адміністративного права, які наділяються владними повноваженнями, з ціллю координації їх спільної діяльності, що як результат призводить до виникнення, зміни або припинення взаємних прав та обов'язки сторін відповідного договору [39, с. 62]. Тобто, адміністративний договір в розглядуваній сфері дає змогу координувати роботу різноманітних державних структур, але тільки за умови та у випадках, якщо це буде об'єктивно необхідно, а координація цих структур надасть позитивні плоди у вигляді бажаного кінцевого результату.

І останньою адміністративно-правовою формою, яка забезпечує кібербезпеку є правореалізація, яка втілює в собі вимоги правових норм у суспільні відносини. В контексті нашого дослідження правореалізацію можна охарактеризувати як безпосереднє втілення норм адміністративного права в діяльність суб'єктів, функціональне призначення яких – забезпечувати кібербезпеку в Україні. Слід відмітити і те, що кожен суб'єкт повинен дотримуватись визначених суб'єктивних прав та виконувати свої безпосередні зобов'язання.

Як підсумок по адміністративно-правовим формам, відзначимо, що вони об'єктивно та практично відображають дії, що вчиняють суб'єкти, які є уповноваженими для реалізації заходів, які забезпечують кібербезпеку в Україні.

Продовжуючи, необхідно звернути свою увагу на адміністративно-правові методи забезпечення кібербезпеки в Україні. За загальним розумінням, «метод – це шлях до мети, спосіб її досягнення» [33, с. 241]. З правої точки зору, В.О. Бурбика визначає, що «адміністративно-правові методи – це сукупність прийомів впливу, що містяться в адміністративно-правових нормах, за допомогою яких встановлюється

юридичне владне і юридичне підвладне становище сторін у правовідносинах» [40, с. 112].

Варто вказати на той факт, що як і з формами, в юридичній літературі не визначається єдиний підхід стосовно конкретних методів в зазначеній сфері, а тому, акцентуючи увагу на погляди науковців, запропонуємо наступні методи забезпечення кібербезпеки:

– адміністративний примус. Як вказується Р.С. Мельником: «адміністративний примус – це застосування до правозобов'язаних суб'єктів передбачених адміністративно-правовими нормами заходів впливу морального, особистісного, майнового, організаційного чи іншого характеру з метою попередження чи припинення протиправних дій, подолання їх шкідливих наслідків, покарання за вчинення правопорушення, а також забезпечення громадського порядку і громадської безпеки» [41, с. 5]. З цього випливає, що ключовим значенням цього методу є те, що він спрямовується на попередження виникнення правопорушення в зазначеній безпеці, а також забезпечує захист інформаційних, приватних, комп'ютерних ресурсів, тощо;

– метод дозволу та заборон. В рамках дослідження, метод дозволу можна охарактеризувати як такий, що надає суб'єктам відповідних правовідносин можливість (право) здійснювати активні дії та/або бездіяльність, тобто вони мають певну свободу під час вибору своєї поведінки. Проте, не потрібно забувати, що ця поведінка не повинна виходити за рамки, які визначаються нормами чинного законодавства. Що стосується методу заборон, то він «передбачає покладання на суб'єкта обов'язку певної пасивної поведінки, утримання від вчинення якихось дій під загрозою настання відповідальності» [42, с. 171];

– метод адміністративного контролю. Правознавець В.М. Кудрявцев характеризує адміністративний контроль як «перевірку якості адміністративної діяльності за допомогою співставлення фактично досягнутих результатів цієї діяльності з цілями, поставленими

в нормативних актах при вирішенні актуальних соціальних проблем, а також з рівнем вирішення цих проблем. Адміністративний контроль дає можливість не тільки виявляти відхилення, помилки і недоліки, але й запобігати їм, шукати нові резерви і можливості» [43, с. 140]. Отже, використання цього методу є дуже важливим в контексті забезпечення ефективного функціонування суб'єктів в зазначеній сфері, в тому числі, він прямо впливає на зазначену сферу суспільних відносин;

– метод контролю доступу. Цей метод виступає в ролі специфічного способу, який забезпечує кібербезпеку, але з іншого боку, є одним із найефективніших. Ним передбачається можливість встановлювати обмеження (заборону) до доступу окремих суб'єктів до тієї чи іншої інформації. Втім, справедливим буде відзначити, що для реалізації цього методу недостатньо належна матеріально-технічна база;

– метод ліцензування діяльності у сфері захисту відомостей, що становлять державну таємницю. Взагалі ліцензування – це «форма контролю за законністю передбачуваних дій громадянина чи організації дозволом робити тільки законні дії і відмовленням у здійсненні протиправних дій, що обумовлює вид і міру припустимої активності, а так само реалізацію нагляду за фактично здійснюваними діями» [34, с. 32]. А тому, ліцензування, без сумніву, вважається як один із найважливіших методів, що забезпечує інформаційну безпеку, тому що воно дає змогу: 1) здійснювати контроль за особами, у яких є доступ до конкретної інформації; 2) забезпечувати захист інформації, яка не повинна бути доступною для загального користування;

– метод сертифікації та стандартизації. Стандартизація та сертифікація є необхідними заходами, які мають відношення до встановлення мінімальних вимог до окремих засобів, які є небезпечними. В цілому, цей метод загальноприйнято використовувати з ціллю стандартизації та сертифікації системи телекомунікаційного обладнання й програмного забезпечення автоматизованих систем

обробки інформації, відповідно до вимог інформаційної безпеки [44, с. 60].

Таким чином, в завершення представленого підрозділу дослідження, констатуємо, що перелічені форми та методи забезпечення кібербезпеки в Україні не претендують на вичерпність, проте, на нашу думку, вони всебічно відображають зміст зазначеної діяльності. Окрім цього, відмітимо, що для забезпечення кібербезпеки в Україні, необхідно комплексно використовувати такі форми і методи. Суттєвим недоліком можна виділити те, що форми і методи на законодавчому рівні через інші нормативно-правові акти не закріплюються, що, беззаперечно говорить про нагальну потребу внести відповідні зміни в цьому питанні.

Як висновок, необхідно вказати, що в юридичній літературі не визначається єдиний підхід стосовно конкретних форм та методів в зазначеній сфері, а тому, акцентуючи увагу на наукову літературу та норми чинного законодавства України, було запропоновано власний погляд стосовно переліку відповідних форм та методів.

Надано характеристику наступним формам забезпечення кібербезпеки України: 1) нормотворчість; 2) прийняття індивідуальних актів; 3) адміністративний договір; 4) правореалізація. В свою чергу, серед основних методів було виділено та охарактеризовано наступні: 1) адміністративний примус; 2) метод дозволу та заборон; 3) метод адміністративного контролю; 4) метод контролю доступу; 5) метод ліцензування діяльності у сфері захисту відомостей, що становлять державну таємницю; 6) метод сертифікації та стандартизації.

2.3. Юридична відповідальність за порушення законодавства у сфері кібербезпеки України

Сьогодні можна впевнено стверджувати, що одні із найпоширеніших правопорушень вважаються порушення у кіберпросторі. Підкреслимо, що вчиняючи такі правопорушення, можуть наступати негативні наслідки не тільки для окремих громадян, але й «підривати» безпеку всієї держави в цілому. У зв'язку з цим, вагоме значення набуває інститут юридичної відповідальності за порушення законодавства у сфері кібербезпеки України.

«Юридична відповідальність – це важливий захід захисту інтересів особистості, суспільства і держави. Вона наступає в результаті порушення приписів правових норм та виявляється у формі застосування до правопорушника заходів державного примусу. Найважливішою ознакою юридичної відповідальності є те, що вона визначається державою і застосовується її компетентними органами. Для правопорушника юридична відповідальність означає застосування до нього санкцій правових норм, вказаних в них певних заходів відповідальності», – вказує В.Н. Хропанюк [45, с. 334].

Виходячи з цієї позиції, під юридичною відповідальністю за порушення законодавства у сфері кібербезпеки України можна розуміти застосування заходів примусового характеру, які закріплені відповідно до норм чинного законодавства, до осіб, якими було вчинено правопорушення у кіберпросторі.

Відповідно до ст. 12 Закону України «Про основні засади забезпечення кібербезпеки України», випливає, що «особи, винні у порушенні законодавства у сферах національної безпеки, електронних комунікацій та захисту інформації, якщо кіберпростір є місцем та/або способом здійснення злочину, іншого винного діяння, відповідальність за яке передбачена цивільним, адміністративним, кримінальним

законодавством, несуть відповідальність згідно із законом» [11]. Тобто, із зазначеного положення є зрозумілим, що до суб'єктів, які вчинили правопорушення в зазначеній сфері, можуть застосовуватися такі види юридичної відповідальності: цивільна, адміністративна та кримінальна. Далі приділимо окрему увагу кожному із вказаних видів відповідальності.

1. Характеризуючи перший вид відповідальності, зазначимо, що цивільна відповідальність являється самостійний видом юридичної відповідальності, яка характеризується застосуванням державного примусу до правопорушника на підставі позбавлення особи певних благ або покладає обов'язки майнового характеру.

Не дивлячись на те, що на законодавчому рівні існує можливість притягнути осіб до цивільно-правової відповідальності, які порушили законодавство у сфері забезпечення кібербезпеки, однак, на сьогоднішній день механізму, який би забезпечував притягнення осіб до цього виду відповідальності, на жаль, не існує. Більш того, не визначається чіткий перелік підстав, за якими можна притягнути правопорушника до відповідальності, про них тільки опосередковано йде мова в окремих статтях Цивільного кодексу України (далі – ЦК України). Наприклад, особа може бути притягнена до цивільно-правової відповідальності, якщо порушила права інших учасників відповідних правовідносин, серед яких: «права на інформацію (ст. 302 ЦКУ); права на свободу літературної, художньої, наукової і технічної творчості (ст. 309 ЦКУ); обов'язок фізичної особи, яка поширює інформацію, переконатися в її достовірності (ст. 302 ЦКУ); майнові права інтелектуальної власності на комерційну таємницю (ст. 506 ЦКУ)» [46] тощо.

Справедливим буде відмітити, що цей вид відповідальності рідше за все застосовується в частині порушення чинного законодавства у розглядуваній сфері.

2. Перш ніж перейти до аналізу наступного виду відповідальності в зазначеній сфері, окреслимо, що за загальним розумінням, «адміністративна відповідальність – це застосування до осіб, які вчинили адміністративні проступки, адміністративних стягнень, що тягнуть для цих осіб обтяжливі наслідки майнового, морального, особистого чи іншого характеру і накладаються уповноваженими на те органами чи посадовими особами на підставах і в порядку, встановлених нормами адміністративного права» [47, с. 66].

Отже, адміністративна відповідальність за порушення законодавства у сфері кібербезпеки – це застосування до особи, яка вчинила правопорушення, санкцій, що передбачені в нормах адміністративного права. Частіше за все, такі санкції відображають матеріальний (грошовий) характер. Відмітимо, що за чинним КУпАП окремо не виділяється розділ, який присвячується правопорушенням у сфері кібербезпеки. Проте, окремі статті таку відповідальність безумовно передбачають. Як приклад, згадаємо ст. 51-2 КУпАП, за якою: «незаконне використання об'єкта права інтелектуальної власності (літературного чи художнього твору, їх виконання, фонограми, передачі організації мовлення, комп'ютерної програми, бази даних, наукового відкриття, винаходу, корисної моделі, промислового зразка, знака для товарів і послуг, топографії інтегральної мікросхеми, раціоналізаторської пропозиції, сорту рослин тощо), привласнення авторства на такий об'єкт або інше умисне порушення прав на об'єкт права інтелектуальної власності, що охороняється законом, – тягне за собою накладення штрафу від десяти до двохсот неоподатковуваних мінімумів доходів громадян з конфіскацією незаконно виготовленої продукції та обладнання і матеріалів, які призначені для її виготовлення» [48]. В свою чергу, відповідно до ст. 164-9 зазначається, що «розповсюдження примірників аудіовізуальних творів, фонограм, відеограм, комп'ютерних програм, баз даних, упаковки яких не

марковані контрольними марками або марковані контрольними марками, що мають серію чи містять інформацію, які не відповідають носію цього примірника, або номер, який не відповідає даним Єдиного реєстру одержувачів контрольних марок, – тягне за собою накладення штрафу від десяти до ста неоподатковуваних мінімумів доходів громадян з конфіскацією цих примірників аудіовізуальних творів, фонограм, відеограм, комп'ютерних програм, баз даних» [48] тощо.

Взагалі в КУпАП міститься близько сотні статей, за якими регулюються питання відповідальності щодо порушення порядку створення, збирання, одержання, зберігання, використання, поширення, охорони та захисту інформації. З цього приводу досить вдалою є думка Т.С. Перуна, який говорить про те, що «такі правопорушення можна поділити на три основні групи, а саме: а) забезпечення доступу фізичних та юридичних осіб до публічної інформації, необхідної для реалізації їх прав, свобод та законних інтересів; б) забезпечення обмеження доступу до певних відомостей, розповсюдження яких може спричинити негативний вплив правам та свободам громадян, законній діяльності юридичних осіб або національній безпеці; в) забезпечення безпеки у сфері медіа-інформації» [49].

Насамкінець відзначимо, що існує певна неоднозначність адміністративного законодавства, яке визначає засади з цього виду юридичної відповідальності в розглядуваній сфері. Враховуючи зростаючу кількість правопорушень у кіберпросторі (за 2019 рік в нашій країні було здійснено близько 5 тисяч правопорушень в зазначеній сфері), що говорить про безсумнівну потребу систематизувати положення щодо притягнення до адміністративної відповідальності осіб, які порушують законодавства про кібербезпеку.

3. Останнім, «найсуворішим» видом юридичної відповідальності у сфері кібербезпеки України є кримінальна. Кримінальна відповідальність в зазначеній сфері може наступати, якщо особа, яка

вчинила кримінальне правопорушення, тобто вчинок, здійснення якого тягне за собою куди шкідливі наслідки для іншої особи, суспільства, держави, тощо. Такий вид кримінального правопорушення в розглядуваній сфері називається «кіберзлочин», як його ще називають – комп'ютерний злочин.

Протягом останніх 10-15 років термін «комп'ютерна злочинність» було трансформовано у «кіберзлочинність» (поняття, яким охоплюється, власне кажучи, комп'ютерна злочинність та інші незаконні діяння, в яких комп'ютер виступає як предмет або спосіб для того, щоб вчинити злочин проти власності, авторських прав, громадської безпеки, тощо). Правильно буде відмітити і те, що поняття «кіберзлочин» має своє закріплення і на законодавчому рівні. Так, згідно до п. 8 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України», встановлено, що «кіберзлочин (комп'ютерний злочин) – суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України» [11].

Продовжуючи, зазначимо, що характерною особливістю кримінальної відповідальності за кіберзлочин є те, вона регулюється Конвенцією про кіберзлочинність від 2001 року, яка була ратифікована Україною від 7 вересня 2005 року [50]. Згідно до положень цієї Конвенції: «Держави–члени Ради Європи та інші держави, які підписали цю конвенцію, впевнені, що ця Конвенція є необхідною для зупинення дій, спрямованих проти конфіденційності, цілісності і доступності комп'ютерних систем, мереж і комп'ютерних даних, а також зловживання такими системами, мережами і даними, шляхом встановлення кримінальної відповідальності за таку поведінку, як це описано у Конвенції, надання повноважень, достатніх для ефективної боротьби з такими кримінальними правопорушеннями шляхом

сприяння їхньому виявленню, розслідуванню та переслідуванню, як на внутрішньодержавному, так і на міжнародному рівнях, і укладення домовленостей щодо швидкого і надійного міжнародного співробітництва» [50].

Також цим міжнародним нормативно-правовим актом передбачено чотири види злочинів, які пов’язані з використанням комп’ютерних технологій як допоміжного способу для їх вчинення. Отож, першу групу складають злочини проти конфіденційності, цілісності й доступності комп’ютерних даних і систем (протизаконний доступ, протизаконне перехоплення, вплив на дані, вплив на функціонування системи, а також протизаконне використання пристроїв і комп’ютерних програм). До другої групи входять злочини, які безпосередньо пов’язуються з використанням комп’ютерних засобів (підроблення, шахрайство). Третю групу становить злочини, які пов’язуються зі змістом даних (як приклад – дитяча порнографія). І остання, четверга група – це злочини, які мають відношення до порушення авторських та суміжних прав [51, с. 5; 50].

Таким чином, після того як України підписала цю Конвенцію, вона взяла зобов’язання навести «порядок» у вітчизняному законодавстві, згідно до її положень. У підсумку це знайшло своє віддзеркалення у КК України, зокрема, у Розділі XVI «Злочини у сфері використання електроннообчислювальних машин (комп’ютерів), систем комп’ютерних мереж і мереж електрозв’язку» [52].

Слушною є думка Ю.Ю. Орлова, який відмічає, що «перелік кіберзлочинів не вичерпується діяннями, визначеними в розділі XVI Особливої частини КК України. Певні злочини, що існували задовго до створення комп’ютерів, також можуть бути вчинені із застосуванням інформаційних технологій. Використання комп’ютерів спрощує вчинення злочину або уможливлює його вчинення в нових формах» [51, с. 6].

Отже, наголошує вчений, «ці злочини можна розглядати як такі, що підпадають під дію конвенції. Зокрема, ідеться про такі злочинні діяння: різні види підроблення: грошей, цінних паперів, платіжних карток, знаків поштової оплати, марок акцизного збору, контрольних марок, номерів вузлів та агрегатів транспортних засобів, документів на отримання наркотиків, інших документів (ст.ст. 199, 200, 215, 216, 224, 290, 318, 358, 366 КК України); шахрайство з різними предметами (ст.ст. 190, 192, 222, 262, 308, 312, 313, 357, 410 КК України)» [51, с. 7; 52] тощо.

Насамкінець, слід вказати, що питання юридичної відповідальності за порушення законодавства в розглядуваній сфері однозначно недостатнім чином врегульовані, що є значним недоліком, який сприяє збільшенню рівня кіберзлочинності в Україні. Зокрема, питання, які стосуються притягнення винних осіб у сфері кібербезпеки до цивільної та адміністративної відповідальності врегульовані значним масивом нормативних актів, в яких закріплено різноманітні підстави щодо притягнення особи до відповідальності. Така розгалуженість породжує тільки складність під час застосування стягнень до правопорушників державними органами. Як результат, доцільно було б внести відповідні зміни до Закону України «Про основні засади забезпечення кібербезпеки України», перш за все, в частині детального окреслення видів правопорушення та кіберзлочинів, за якими винних осіб можна притягнути до того чи іншого виду юридичної відповідальності [53, с. 189]. Означене зробить відповідне законодавство набагато урегульованим та узгодженим, а відтак, і дасть позитивний відбиток на якості забезпечення кібербезпеки в Україні.

Завершуючи розгляд даного підрозділу, констатуємо про те, що під юридичною відповідальністю за порушення законодавства у сфері кібербезпеки України можна розуміти застосування заходів примусового

характеру, які закріплені відповідно до норм чинного законодавства, до осіб, якими було вчинено правопорушення у кіберпросторі.

До суб’єктів, які вчинили правопорушення в зазначеній сфері, можуть застосовуватися такі види юридичної відповідальності: цивільна, адміністративна та кримінальна.

РОЗДІЛ 3
ШЛЯХИ УДОСКОНАЛЕННЯ ЧИННОГО ЗАКОНОДАВСТВА УКРАЇНИ В ЧАСТИНІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ: ПРОБЛЕМНІ ПИТАННЯ

3.1. Міжнародний досвід забезпечення кібербезпеки та можливості його імплементації у вітчизняне законодавство

За результатами розгляду попереднього розділу, не виникає сумнівів, що механізм забезпечення кібербезпеки, який існує сьогодні, є недосконалим та який потрібно удосконалювати. Визначити шляхи удосконалення механізм неможливо без врахування міжнародного досвіду, особливо, враховуючи прагнення України адаптувати вітчизняне законодавство відповідно до європейських та світових норм та стандартів. У зв'язку з чим, нами буде приділено увагу країнам Європейського Союзу (далі – ЄС), які являються досить розвинені в зазначеному питанні, а також окремо проаналізуємо провідні держави світу (США та Китай).

1. Аналізуючи країни ЄС, перш за все, вважаємо за необхідне приділити увагу такій країні як Великобританія, тому що в цій країні питанню кібербезпеки надають вагомого значення, яке займає одне із першочергових місць. Одразу ж відзначимо, що 31 січня 2020 року вона офіційно не є членом Європейського Союзу, однак оминути увагою її цікавий досвід не можна.

Отже, ще у 2016 році Урядом Великої Британії було оприлюднено 5-річний план реалізації Стратегії національної кібербезпеки. Ключова мета цієї Стратегії на 2021 рік в тому, щоб застосовувати всі необхідні заходи для повної безпеки Великобританії та її стійкості до кіберзагроз, яка буде процвітати та впевнено себе «відчувати» в цифровому світі.

Для цього, з позиції законодавця країни, необхідно: 1) виділяти достатню кількість коштів для того, щоб Великобританія знаходилася під захистом від можливого розвитку кіберзагроз; оперативно реагувати на інциденти та здійснювати належний захист і стійкість мереж (даних); 2) виявляти та розслідувати злочинні дії «ворогів», які наносяться проти безпеки Великобританії; 3) запроваджувати інноваційні технології та індустрії кібербезпеки; 4) розвивати кадровий потенціал. Відмітимо також те, що за цією Стратегією кіберзлочинність виступає в аспекті двох форм злочинної діяльності, які є взаємопов'язаними, а саме: 1) кіберзалежність злочинів, маються на увазі злочини, які можуть здійснювати виключно з використанням пристроїв інформаційно-комунікаційних технологій (ІКТ), де ці пристрої виступають як інструмент для того, щоб вчинити злочин і ціль такого злочину, як приклад (розробити та поширити шкідливе програмне забезпечення, щоб мати фінансову вигоду або ж зламати, щоб викрасти чи пошкодити дані/мережу; 2) злочини, які пов'язуються з використанням кібератаки. Це так звані традиційні злочини, які як правило мають тенденцію до збільшення в масштаби або охоплені за сприянням комп'ютерів (мереж) чи інших складових ІКТ [54].

Відповідно до поставлено мети Стратегії, було створено і Національний центр кібербезпеки (NCSC). NCSC дає унікальну змогу для того, щоб створювати ефективні партнерські відносини в сфері кібербезпеки між урядом, промисловістю і громадськістю, що у підсумку дає змогу реалізовувати безпеку Великобританії в мережі Інтернет.

Не можна оминути увагою і той факт, що Британським Національним агентством по боротьбі зі злочинністю (NCA), в межах Стратегії було відкрито перший в своєму роді реабілітаційний центр для людей, яких було засуджено до ув'язнення за кіберзлочини. Як писало BBC, у цьому центрі їх навчають направляти свої навички на більш

конструктивні цілі, а також готують до роботи в спецслужбах. Сьогодні, за останніми відомостями, цей центр відвідують восьмеро дорослих людей, які були затримані правоохоронцями за незаконні дії в он-лайні, ще будучи підлітками. Деякими з них було зламано сайти чи сервери, здійснювались кібератаки, вони також змушували користувачів надавати свої персональні дані, тобто, в цілому відбувалося невпинне порушення британського законодавства в частині використання комп'ютерів [55].

Загалом, якщо підвести підсумок щодо означеної Стратегії національної безпеки Великобританії на 2016–2021 роки, то можна сказати, що в ній міститься багато цікавих положень. Наприклад, із позитивного, на які, на нашу думку, необхідно звернути уваги, є наступні: 1) детально характеризуються напрями та етапи щодо реалізації інновацій у сфері забезпечення кібербезпеки; 2) досить багато приділяється уваги стосовно навчання населення в аспекті того, яким чином себе захищати від можливих порушень їх прав в зазначеній сфері [54].

2. Наступною країною є Німеччина, тому що ця країна являється одна із ключових, в якій форми державно-приватного партнерства функціонують як базовий інструмент для того, щоб система кіберзахисту країни ефективно працювала [56, с. 10]. У Німеччині, як і у Великобританії, в 2011 році було прийнято Стратегію кібербезпеки Німеччини, згідно з якою федеральним урядом застосовуються всі необхідні заходи, щоб виявляти рівні загроз за наступними стратегічними напрямами:

– захист ключових інформаційних інфраструктур. Мається на увазі, що центром уваги кібербезпеки є захист основоположних інформаційних структур, тому що безпека має вагоме значення в систематично зростаючих, провідних інфраструктурах [57, с. 112];

– посилення IT-безпеки в публічному управлінні. За цим напрямом, державні установи мають виступати як зразок стосовно

захисту даних. Базисом для електронного обміну даними і вербальної комунікації буде загальна, універсальна і надійна мережева інфраструктура Федеральної адміністрації («федеральна мережа») [57, с. 112];

– для того, щоб оптимізувати співпрацю усіх державних установ і покращити координацію відповідних заходів стосовно захисту проти ІТ-випадків, було сформовано Національний центр кіберзахисту. Центр функціонує під керівництвом Федерального відомства з інформаційної безпеки (BSI) і за безпосередньою участю Федерального відомства захисту конституції (BfV) та Федерального відомства з питань захисту населення і допомоги при стихійних лихах (BBK) [57, с. 113];

– сформовано Національну раду кібербезпеки, основним завданням якої – виявляти та усувати конструктивні причини криз, тобто це є дуже важливим превентивним інструментом у сфері кібербезпеки [57, с. 113];

– застосування безпечних і достовірних інформаційних технологій. Необхідно забезпечувати можливість для того, щоб мати доступ до безпечних ІТ-систем. Стрімке становлення інноваційних програм захисту для оновлення безпеки буде лише зростати, враховуючи суспільні та економічні аспекти [57, с. 114].

Таким чином, можна сказати, що в Німеччині приділяється значно уваги питанням щодо забезпечення кібербезпеки. З-поміж іншого, в цій країні сьогодні активно залучається міжнародне співробітництво, яке підштовхує ще ефективніше та оперативніше виявляти загрози у цій сфері та оновлювати законодавство і технології у боротьбі з ними. Ще позитивним є те, що в Німеччині постійно розширюються заходи, які спрямовані на те, щоб ефективно реалізовувати державну політику у сфері забезпечення кібербезпеки.

3. У Франції, як країні, на яку також потрібно звернути увагу, основними нормативно-правовими актами, які визначають стратегічні

напрями державної політики у сфері забезпечення безпеки – слугують Біла книга оборони та національної безпеки від 2008 року і Національна стратегія цифрової безпеки 2015 року. В Білій книзі серед загроз, які можуть бути ймовірними, виділяються (тероризм, застосування балістичних ракет, організована злочинність тощо), а також названі: масштабні атаки на інформаційні системи; шпіонажі та стратегічний вплив [58, с. 202]. В свою чергу, за Стратегією вказується, що її ключовим призначенням є супровід цифрового переходу французького суспільства та адаптації до нових викликів, які пов'язуються зі зміною використання цифрових технологій і загрозами, які мають місце бути за п'ятьма цілями: 1) гарантування національного суверенітету; 2) забезпечення сильної відповіді на акти кіберзлочинності; 3) інформування громадськості; 4) забезпечення цифрової безпеки, тому що вона слугує як конкурентна перевага для підприємств Франції; 5) посилення позицій Франції на міжнародній арені.

Також відповідно до Стратегії, Франція як держава працює над тим, щоб забезпечити безпеку ІТ-систем в напрямі колективного реагування, цифрової довіри, що є необхідним для економічного і стабільного розвитку держави, а також під час захисту своїх громадян.

Отже, закріплення стратегічної стабільності і безпеки на міжнародному рівні в кіберпросторі – одна із ключових задач Франції.

4. Розглядаючи зарубіжний досвід в сфері кібербезпеки, не можна оминути увагою, країну, яка є нашим сусідом – Польща. Ця країна на сьогоднішній день дуже плідно розвиває кіберзахист на державному рівні [54].

Протягом тривалого часу, зусилля влади Польщі у боротьбі з кіберзагрозами були недостатніми. Проте, значна кількість масштабних атак на фоні того, що в Польщі був відсутній єдиний координований центр, який займається ухваленням рішень, стало стимулом для подальших дій. Так що ж, власне кажучи, зробила Польща? В першу

чергу, було прийнято відповідні зміни до законодавства, за якими влада має право вводити у країні надзвичайний стан, якщо будуть випадки атак у віртуальному просторі. А це, між іншими являється юридичною новацією, якою можуть похвалитися не так багато держав. По-друге, владою було визнано недоцільність функціонування декількох інституцій, які борються з кіберзагрозами, тобто які тільки дублювали одна одну. У зв'язку з цим, ще у 2011 році було сформовано Міністерство адміністрації і цифровізації, ключовими задачами якого стало – забезпечити кібербезпеку у військовій сфері, захищати конфіденційність громадян, розбудовувати національну освітню платформу, залучати до Інтернету людей похилого віку, а також жителів з віддалених районів. Третім напрямом було створення у 2016 Національного центру кібербезпеки в межах Міністерства цифровізації. Основне завдання цього центру – попереджати загрози, ефективно реагувати на них та координувати дії. Діяльність цього центру є вдалим прикладом державно-приватного партнерства сфери кіберзахисту. І останнім напрямом є те, що Польщею було опрацьовано нову Стратегію кібербезпеки. Нею передбачається, що до 2022 року влада виступатиме гарантом у безпеці громадян, а також щодо суб'єктів економічної діяльності і державних установ у сфері кібербезпеки [59].

5. Окремо виділимо таку країну як Сполучені Штати Америки (далі – США). На сьогоднішній день, законодавча база США у сфері забезпечення інформаційної безпеки формується з федеральних законів та законів штатів, якими була створена правова основа для реалізації єдиної державної політики у сфері захисту інформації, щоб забезпечувати інтереси національної безпеки.

Із останнього, у 2018 році у Вашингтоні оголосили про зміст статусу Кіберкомандування Збройних Сил США. По-перше, зазначену структуру в планах виключити з підпорядкування Стратегічному командуванню ЗС США та піднести її на рівень окремого

функціонального командування збройними силами. Це дасть змогу здійснити централізацію керівництва у кібернапрямі зі сторони Міністерства Оборони та Об'єднаного комітету начальників штабів США. Тепер Кіберкомандування буде мати більше повноважень стосовно розвитку можливостей у проведенні відповідних дій в кіберпросторі, під час підготовки кадрів, виконання бюджету, а також під час планування дій в кіберпросторі та їх реалізації, тощо. Водночас, продовжуються зміни на рівні видів американських збройних сил США. Як приклад, в армії США (сухопутні війська), за останні роки теж піддалось «форматуванню» в кібернапрямі. Усвідомлюючи нові загрози, а також розуміючи цінність власних операцій в кіберпросторі, ще у 2014 році з'явилися директиви, які слугували для створення фактичного нового підрозділу військ – Кіберкомандування сухопутних військ. Причина такого кроку дуже схожа с українськими реаліями, коли існує велика кількість невеликих підрозділів, за різної підпорядкованістю, однак, їх зусилля не були згуртованими та мали відношення в більшій мірі до розвідників або зв'язківців. Отже, як результат – формування нового роду військ стало підґрунтям для того, щоб інтегрувати підрозділи та об'єднувати зусилля в розширенні можливостей для активного впливу в кіберпросторі [60, с. 28].

Сьогодні та і взагалі, ні у кого немає сумнівів, що США є тою країною, в якої є всі необхідні матеріальні та технічні ресурси для того, щоб належним чином забезпечувати кібербезпеку у своїй державі та допомагати у цій сфері іншим країнам, це стосується і України. Із позитивної сторони відмітимо активну роботу спецслужб у розглядуваній сфері, досвід яких міг би бути корисним і для України.

6. Останньою країною для розгляду є Китайська Народна Республіка (далі – КНР). Особливість КНР під час здійснення діяльності у сфері забезпечення кібербезпеки пов'язується перш за все жорстким контролем щодо будь-якої інформації в Інтернеті. У 2016 році Урядом

КНР було схвалено закон про кібербезпеку, який направлено на те, щоб тільки посилювати і централізувати державний контроль над Інтернетом, це стосується і іноземних компаній, які відіграють значну роль. Цей закон ставить задачі установам і підприємствам поліпшувати їх змогу захищатися від вторгнень в мережі Інтернет, вимагаючи перевірки безпеки обладнанні і даних, які знаходяться в стратегічних секторах. В цьому законі також містяться положення, які зобов'язують інтернет-операторів надавати «технічну допомогу» владі щодо справ, які мають відношення до національної безпеки [61].

Не можна не відмітити також те, що в КНР особливо приділяється увагу кадровому забезпеченню в зазначеній сфері. Це підтверджується тим, що в країні сьогодні розпочато будівництво першого інституту, який здійснює підготовку фахівців кібербезпеки, а до 2027 року в КНР планують реалізувати 4-6 подібних навчальних заклади. В сукупності усе це є підтвердженням серйозних намірів Китаю стосовно забезпечення кібербезпеки [60, с. 29].

Отже, якщо узагальнити представлений матеріал, можна впевнено констатувати, що сьогоднішні світові тенденції розвитку інформаційного суспільства схиляють всі держави в світі приймати заходи стосовно забезпечення кібербезпеки. Україна, безумовно, не є виключенням, яка нині стоїть лише на початкових етапах розвитку зазначеного інституту.

Враховуючи досвід проаналізованих зарубіжних країн, виокремимо ключові напрями розвитку інституту забезпечення кібербезпеки, які в подальшому можливо адаптувати в нашій державі, серед яких:

– потрібно збільшувати виділення коштів на суб'єктів, діяльність яких спрямовується на те, щоб забезпечити кібербезпеку в державі;

– проводити відповідні заходи для покращення якості освіти працівників кіберполіції. Врахувавши досвід США, вважаємо, що

необхідно створити спеціальну академію при Міністерстві внутрішніх справ, яка б займалася підготовкою фахівців, які будуть протидіяти кіберзлочинам. В тому числі, державна політика повинна спрямовуватися на обмін досвідом між суб'єктами правоохоронних органів, що у підсумку дасть можливість кіберполіції переймати досвід фахівців у зазначеній сфері, а також організовано проводити висококваліфіковану підготовку, які будуть попереджати, виявляти та розкривати злочини у сфері інформаційних технологій, існуючих у кіберпросторі;

– кардинально оновити Стратегію кібербезпеки України. На нашу думку, її потрібно розширити та охопити більше коло питань у цій сфері, оскільки на даний момент вона обмежується тільки питаннями, які містять в собі базовий зміст. В цьому аспекті можна використовувати досвід Великобританії та Німеччини, тому що в цих країнах стратегії, які забезпечують кібербезпеку, охоплюють майже усі питання та являються ключовими документами у цій сфері;

– потрібно розширювати міжнародне співробітництво у сфері забезпечення кібербезпеки, тобто залучати можливості міжнародної технічної допомоги з ціллю розбудови національної системи кібербезпеки;

– розробити організаційно-технічну модель надійного захисту вітчизняного кіберпростору, а також розширити засади, щоб сформувати методи та принципи стосовно здійснення «електронної оборони»;

– необхідно збільшити контроль в Інтернеті (як приклад, тут слугує Китай). Цей напрям можна обґрунтувати тим, що сьогодні в мережу Інтернет потрапляє необмежена кількість «фейкових» новин, які в свою чергу, створюють оману для населення загалом та підривають довіру до державних органів (частіше за все це стосується правоохоронних органів), зокрема [62, с. 129-130].

Отже, роблячи висновок з викладеного, зазначимо, що сьогоднішні світові тенденції розвитку інформаційного суспільства схиляють всі держави в світі приймати заходи стосовно забезпечення кібербезпеки. Протягом останніх десяти років, в багатьох Європейських країнах поширюються плани заходів та Стратегії, які слугують для вирішення задач щодо забезпечення кібербезпеки, не є виключенням і Україна.

3.2. Недоліки законодавства щодо забезпечення кібербезпеки в Україні, шляхи їх вирішення та можливі напрями удосконалення

В процесі дослідження неодноразово наголошувалося, що законодавство, яке регулює забезпечення кібербезпеки в Україні, є недосконалим та потребує удосконалення, що, в свою чергу, обумовлює необхідність дослідити зазначенні питання.

В контексті забезпечення кібербезпеки потрібно говорити про недоліки в законодавстві як про явище, яке є негативним. Адже їх наявність апріорі загрожує безпеці кожного окремого громадянина, державним органам та державі в цілому. Саме тому, законодавці повинні здійснювати всі необхідні заходи для подолання та усунення недоліків в нормативній базі, яка регулює забезпечення кібербезпеки в Україні.

Визначаючи напрями удосконалення законодавства у сфері забезпечення кібербезпеки, перш за все, звернемо увагу на вже знайомий Закон України «Про основні засади забезпечення кібербезпеки України» [11]. Першим недоліком можна вважати те, що в цьому законі представлено досить широке коло суб’єктів, які забезпечують кібербезпеку в Україні, однак, при цьому, в ньому не визначається той єдиний (ключовий) орган, повноваження якого повинні відноситись до оперативного командування всіх інших суб’єктів в розглядуваній сфері. Нагадаємо, що нами вже наголошувалось в попередньому розділі про те, що КМУ не тільки повинен входити до національної системи

забезпечення кібербезпеки, а й фактично очолювати її. Проте, положеннями чинної нормативної бази, КМУ до цієї системи не відноситься, а просто слугує як суб'єкт із загальним статусом, що підтримує цей інститут. Тож, сподіваємось, що у найближчому майбутньому цей нормативний недолік буде виправлено.

Ще один недолік полягає в термінологічній недосконалості означеного закону, оскільки деякі терміни відображені досить «просто» та не характеризують усю специфіку окремих категорій. Як приклад, законодавцем визначено, що «кібертероризм – терористична діяльність, що здійснюється у кіберпросторі або з його використанням» [11]. Вважаємо більш вдалою думку Б.В. Кузьменко, який визначає його «як один з напрямків тероризму, в якому об'єктом деструктивної дії для досягнення цілей використовують інформаційно-обчислювальну техніку, комплекси та мережеві сегменти, які підтримують критично важливі, з точки зору національної безпеки, системи» [63, с. 22].

Позитивним моментом виділимо те, що в Законі України «Про основні засади забезпечення кібербезпеки України» було законодавчо встановлено, що «кіберзагроза – наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів» [11]. Однак, законодавцем чомусь не було виділено, які є види кіберзагроз. У зв'язку з цим, можна розділити позицію І.В. Діордіці та виділити наступні види кіберзагроз: 1) націлені атаки (advanced persistent threat), які може бути здійснено: а) застосовуючи програмне забезпечення (віруси, трояни тощо), мета яких компрометувати якомога більше систем; б) компрометувати комп'ютери конкретних установ чи користувачів; 2) кібервійни, які являються прообразом кіберзброї для того, щоб здійснювати диверсії чи відключати системи (як приклад, комплекси протиповітряної або

протиракетної оборони); 3) хактивізм – злочини, за якими зловживається інформація у соціальних мережах (впливає на суспільство); 4) атаки на електронний уряд [64, с. 207], тощо. Отже, закріпивши види кіберзагроз на рівні закону, це матиме вагоме значення не тільки з теоретичної, але й з практичної сторони, тому що: 1) унеможливлює неоднозначність тлумачення деяких правових норм; 2) дає змогу якісніше формулювати положення інших нормативно-правових актів в розглядуваній сфері.

Наостанок відмітимо, що в законі не існує таких понять, як «кіберправопорушення» та «кіберпроступок», що являється недопустимим, бо чинним законодавством передбачається цивільна та адміністративна відповідальність. Пропонується внести відповідні зміни до Закону України «Про основні засади забезпечення кібербезпеки України», додавши зазначені терміни.

Наступний недолік нормативно-правового акта, який слід розглядати, стосується деяких положень закону, щодо яких законодавцем було використано принцип «від зворотного» та недвозначно вказавши, що в ч. 1 ст. 2 Закону України «Про основні засади забезпечення кібербезпеки України» – «цей Закон не поширюється на: 1) відносини та послуги, пов’язані із змістом інформації, що обробляється (передається, зберігається) в комунікаційних та/або в технологічних системах; 2) діяльність, пов’язану із захистом інформації, що становить державну таємницю, комунікаційні та технологічні системи, призначені для її оброблення; 3) соціальні мережі, приватні електронні інформаційні ресурси в мережі Інтернет (включаючи блог-платформи, відеохостинги, інші веб-ресурси), якщо такі інформаційні ресурси не містять інформацію, необхідність захисту якої встановлена законом, відносини та послуги, пов’язані з функціонуванням таких мереж і ресурсів; 4) комунікаційні системи, які не взаємодіють з публічними мережами електронних комунікацій (електронними мережами загального користування), не підключені до

мережі Інтернет та/або інших глобальних мереж передачі даних (крім технологічних систем)» [11].

Якщо аналізувати тільки цю норму, то неможливо відповісти на питання, чи має поширення закон на приватні мережі суб'єктів господарювання, оскільки вони також є підключеними до Інтернету. Однак, якщо ж характеризувати цю норму в сукупності з іншою, яка зазначена в ч. 2 ст. 4 Закону України «Про основні засади забезпечення кібербезпеки України» (об'єкти кіберзахисту, про які йшла мова в першому розділі, відмічаючи конкретно об'єкти критичної інформаційної інфраструктури), то цілком логічно можна дійти висновку, що цей Закон все ж таки поширює свою дію на приватні мережі суб'єктів господарювання у разі, коли той чи інший господарюючий суб'єкт буде відноситись до об'єктів критичної інфраструктури [65]. Тому, на нашу думку, зазначене вище необхідно уточнити та внести відповідні зміни, що дозволить також уникнути неоднозначність тлумачення цих норм та буде сприяти більш якісно покращувати механізм забезпечення кібербезпеки в Україні.

Ще одним суттєвим недоліком Закону України «Про основні засади забезпечення кібербезпеки України», можна вважати те, що в ньому відсутні норми, які б детально регламентували організаційні та процедурні засади щодо забезпечення кібербезпеки в Україні. Серед іншого, як нами вже було визначено в попередньому розділі, форми та методи забезпечення кібербезпеки також не закріплені на законодавчому рівні. У зв'язку з чим, на сьогоднішній день, в цьому аспекті також необхідно внести відповідні зміни, що в результаті надасть сприятливе поле для того, щоб уповноважені суб'єкти, які забезпечують кібербезпеку ефективно виконували свою діяльність.

Таким чином, не дивлячись на те, що Закон України «Про основні засади забезпечення кібербезпеки України» було прийнято не так вже і давно, а на його обговорення та розробку було витрачено декілька років,

в ньому по сей день залишається безліч проблемних та невирішених питань, яким необхідно приділяти увагу як зі сторони законодавця, так зі сторони правознавців. Звісно, запропоновані зміни до цього Закону не претендують на вичерпний перелік, однак, в чому можна бути переконаним, так це в тому, що ці зміни сприятимуть тому, щоб покращити практичну діяльність суб'єктів, які забезпечують кібербезпеку в Україні, а як наслідок – позитивно вплинуть на стан кіберзахисту.

Продовжуючи розгляд щодо можливих напрямів удосконалення адміністративного законодавства, яке здійснює регулювання забезпечення кібербезпеки в Україні, виокремимо і інший нормативно-правовий акт, про який обов'язково потрібно вказати – це новий закон України «Про національну безпеку України» від 21 червня 2018 року [66], в якому містяться цікаві та нові положення про кібербезпеку та і який в принципі є значно прогресивнішим аніж попередній Закон України від 2003 року «Про основи національної безпеки України». Зокрема, важливий аспект відображено в ст. 31, за якою визначено, що «Стратегія кібербезпеки України є документом довгострокового планування, в якому визначаються пріоритети національних інтересів України у сфері кібербезпеки, наявні та потенційно можливі кіберзагрози життєво важливим інтересам людини і громадянина, суспільства та держави в кіберпросторі, пріоритетні напрями, концептуальні підходи до формування та реалізації державної політики щодо безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави, підвищення ефективності основних суб'єктів забезпечення кібербезпеки, насамперед суб'єктів сектору безпеки і оборони, щодо виконання завдань у кіберпросторі, а також потреби бюджетного фінансування, достатні для досягнення визначених цілей і виконання передбачених завдань, та основні напрями використання фінансових ресурсів» [66].

Однак, означений закон також має певні недоліки. Наприклад, не дуже зрозуміло виключення (у порівнянні з тим же попереднім Законом України «Про основи національної безпеки України») статті, за якою визначались основоположні реальні та потенційні загрози внутрішньо- та зовнішньополітичній національній безпеці України, а також стабільності в суспільстві. Попри це, в законі як загрози національній безпеці закріплено деякі негативні фактори розвитку суспільства та держави, незважаючи на те, що їх усунення не може бути забезпечене роботою органів сектору безпеки. Перелік загроз національної безпеки України, який закріплено на рівні закону, а також заходів реагування на них, в практичному плані не відповідає державам ЄС та НАТО, цим самим ускладнюючи встановлення пріоритетів державної політики у сфері національної безпеки та своєчасну реакцію на можливі зміни безпекової ситуації.

Ще одним нормативно-правовим актом, на який слід звернути увагу, – Указ Президента України «Про Доктрину інформаційної безпеки України» від 25 лютого 2017 року [67]. «Метою Доктрини є уточнення засад формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу Російської Федерації в умовах розв'язаної нею гібридної війни» [67]. Але, як вказує Н. Тарасенко, «така мета більше підходить для іншого документа, який має визначати основні засади державної інформаційної політики, особливо її структуру і зміст. Поки що такого документа на державному рівні в Україні не існує» [68]. З-поміж іншого, експертом вважаються «відкритими питання щодо методології підходів до проблематики забезпечення інформаційної безпеки, які закріплені в Доктрині» [68]. В свою чергу, Т. Попова «вбачає за необхідне поставити на перше місце співвідношення понять «інформаційна безпека» та «кібербезпека». Вона констатує, що українська наука чітко обґрунтувала необхідність розгляду національного сегмента кіберпростору як

складової частини інформаційного простору держави, з чого випливає і логічність розгляду питань кібербезпеки в контексті інформаційної безпеки» [68].

Останнім нормативно-правовий актом, який вже неодноразово аналізувався є Стратегія кібербезпеки України [12]. Пропонуємо виділити важливі аспекті, які, на нашу думку, потребують удосконалення:

1. Перший недолік полягає у відсутності конкретних строків, на які приймається Стратегія. З нашої позиції, оптимальний є строк прийняття такої Стратегії в нашій державі на 3-5 років. Аргументуємо цю позицію наступним чином: а) в провідних країнах світу подібні Стратегії приймаються на 3-5 років; б) кіберпростір є тією сферою, яка систематично розвивається, в ній постійно з'являються нові виклики та проблеми, які мають відношення до кібербезпеки. А відтак, і законодавча база в цьому плані повинна оновлюватись досить часто, щоб уникнути недоліків.

2. В Стратегії обов'язково повинна бути визначена сума грошових коштів, які необхідно витратити на її реалізацію, мається на увазі – бюджет. Як приклад, у таких країнах як (Великобританія, Польща тощо), перед тим як затвердити Стратегію, формується бюджет, за яким законодавець відштовхується під час створення плану для реалізації Стратегії. Справедливим буде відмітити, що згідно до ст. 13 Закону України «Про основні засади забезпечення кібербезпеки України» вказується наступне: «Джерелами фінансування робіт і заходів із забезпечення кібербезпеки та кіберзахисту є кошти державного і місцевих бюджетів, власні кошти суб'єктів господарювання, кредити банків, кошти міжнародної технічної допомоги та інші джерела, не заборонені законодавством» [11]. Але, все ж таки, вважаємо, що в Стратегії треба чітко окреслити, куда саме повинні використовуватись

кошти державних та місцевих бюджетів, мається на увазі – цільове призначення.

3. У Стратегії забезпечення кібербезпеки в Україні, порівняно з більшою частиною держав в світі, чомусь не приділяється увага кадровому питанню щодо суб'єктів, які уповноважені займатися забезпеченням кібербезпеки в Україні. Кадрове забезпечення являється як невід'ємна складова в процесі управління, тому що воно відноситься до структури управління, а його стан безпосередньо має вплив на ефективність такого управління. Отже, кадрове забезпечення обов'язково має бути складовою Стратегії забезпечення кібербезпеки і включати в собі такі аспекти:

– кількість фахівців, яких необхідно підготувати, щоб здійснювати діяльність в зазначеній сфері;

– напрямки підготовки фахівців;

– відповідальні особи, які представлені державними органами, обов'язок яких – відповідати за формування програм щодо підготовки та перепідготовки кадрів.

4. Ще в Стратегії недостатнім чином розкривається питання взаємодії суб'єктів забезпечення кібербезпеки як між собою, так і з громадськістю, а також суб'єктами, які здійснюють господарську діяльність [69, с. 53-56].

Отже, проаналізувавши все наведене вище, можна сказати, що Стратегія забезпечення кібербезпеки в Україні сьогодні є дещо «проста» та практично не відповідає тим викликам, які існують перед Україною як сучасної держави щодо забезпечення кібербезпеки [70, с. 12].

Узагальнюючи, нами було визначено найбільш важливі недоліки законодавства у сфері забезпечення кібербезпеки, серед яких можна виділити наступні: 1) в Законі України «Про основні засади забезпечення кібербезпеки України» представлено досить широке коло суб'єктів, які забезпечують кібербезпеку в Україні, однак, при цьому, в

ньому не визначається той єдиний (ключовий) орган, повноваження якого повинні відноситись до оперативного командування всіх інших суб'єктів в розглядуваній сфері; 2) термінологічна недосконаліть Закону України «Про основні засади забезпечення кібербезпеки України», оскільки деякі терміни відображені досить «просто» та не характеризують усю специфіку окремих категорій; 3) законодавцем не виділено, які є види кіберзагроз та кіберзлочинів; 4) в Законі України «Про основні засади забезпечення кібербезпеки України» не існує таких понять, як «кіберправопорушення» та «кіберпроступок», що являється недопустимим, бо чинним законодавством передбачається цивільна та адміністративна відповідальність; 5) в Законі України «Про основні засади забезпечення кібербезпеки України» відсутні норми, які б детально регламентували організаційні та процедурні засади щодо забезпечення кібербезпеки в Україні. Серед іншого, це стосується форм та методів забезпечення кібербезпеки, які також не закріплені на законодавчому рівні; 6) недолік у вигляді виключення з нового Закону України «Про національну безпеку України» від 2018 року (у порівнянні з попереднім Законом України «Про основи національної безпеки України» від 2003 року) статті, за якою визначались основоположні реальні та потенційні загрози внутрішньо- та зовнішньополітичній національній безпеці України, а також стабільності в суспільстві; 7) спрямованість Доктрини інформаційної безпеки виключно на Російську Федерацію; 8) відсутні конкретні строки, на які приймається Стратегія кібербезпеки України, не вирішено питання щодо цільового призначення грошових коштів, не приділено уваги кадровому питанню щодо суб'єктів, які уповноважені займатися забезпеченням кібербезпеки в Україні, а також недостатнім чином розкривається питання взаємодії суб'єктів забезпечення кібербезпеки як між собою, так і з громадськістю, в тому числі між суб'єктами, які здійснюють господарську діяльність.

В свою чергу, в аспекті означених недоліків, запропоновано визначити наступні напрями удосконалення адміністративного законодавства, яке здійснює регулювання забезпечення кібербезпеки в Україні: 1) закріпивши види кіберзагроз на рівні закону, це матиме вагоме значення не тільки з теоретичної, але й з практичної сторони, тому що: а) унеможливлює неоднозначність тлумачення деяких правових норм; б) дає змогу якісніше формулювати положення інших нормативно-правових актів в розглядуваній сфері; 2) пропонується внести відповідні зміни до Закону України «Про основні засади забезпечення кібербезпеки України», додавши такі терміни як «кіберправопорушення» та «кіберпроступок», які будуть чітко відображати можливість притягнення винних до адміністративної та цивільної відповідальності; 3) у Стратегії кібербезпеки України: а) закріпити конкретні строки реалізації стратегії; б) приділити увагу кадровому питанню щодо суб'єктів, які уповноважені займатися забезпеченням кібербезпеки в Україні.

Таким чином, як підсумок, зазначимо, що протягом останніх років фахівцями та політиками наголошувалось на тому, щоб суттєво покращити вітчизняне законодавство у сфері забезпечення кібербезпеки в Україні. З цим не можна не погодитись, проте, зазвичай ними відмічається поліпшення законодавчої бази, якщо порівнювати те, що було в Україні до 2013 року. На нашу думку, це не дуже справедливо, тому що відправною точкою у цій сфері повинно слугувати не законодавство, яке є застарілим, а позитивний досвід зарубіжних країн, які виступають як взірець під час забезпечення кібербезпеки. А тому не викликає сумнівів, що зміни, які було запропоновано, сприятимуть тому, щоб покращити практичну діяльність суб'єктів, які забезпечують кібербезпеку в Україні, а як наслідок – позитивно вплинуть на стан кіберзахисту.

ВИСНОВКИ

У кваліфікаційній роботі було здійснено теоретичне обґрунтування адміністративно-правових засад щодо забезпечення кібербезпеки в Україні, встановлено проблемні питання, визначено шляхи їх вирішення, а також сформульовано можливі напрями удосконалення зазначеної сфери, враховуючи міжнародний досвід.

У результаті дослідження виокремлено низку висновків, спрямованих на вирішення окреслених завдань. До основних із них можна віднести такі:

1. Після прийняття Закону України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року вперше було закріплено поняття кібербезпеки, яке означає «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».

Встановлено, що адміністративно-правова охорона у сфері забезпечення кібербезпеки – це діяльність відповідних органів державної влади, яка виконується відповідно до засад імперативності та ієрархічності та направлена на те, щоб підтримувати та забезпечувати належний стан захищеності прав, інтересів та інформації конкретних суб’єктів у кіберпросторі.

Ключовими особливостями кібербезпеки як об’єкта адміністративно-правової охорони є наступні:

1) відсутність чіткого визначення змісту кібербезпеки, що говорить про неоднозначність його розуміння, а також про те, що її

застосування дає змогу в окремо взятих випадках правопорушнику уникати відповідальності;

2) адміністративно-правова охорона кібербезпеки хоч і виконується в аспекті адміністративно-правових відносин, однак, суть зазначеного інституту є досить широкою і не обмежується виключно нормами захисту та спеціальними процедурами.

2. Кібербезпека являється складним правовим явищем, в межах якого діє механізм кіберзахисту, який представлено у вигляді засобів різного характеру (організаційного, нормативно-правового, воєнного, технічного тощо), що забезпечують підтримку інституту кібербезпеки та який є невід'ємною складовою частиною під час визначення об'єктного складу в зазначеній сфері.

Встановлено, що об'єктний склад кібербезпеки представлений у вигляді суспільних відносин щодо використання кіберпростору та організації безпечного пошуку, обробки та передачі інформації в розглядуваній сфері, серед яких визначено наступні:

1) правовідносини у сфері розвитку державної інформаційної інфраструктури;

2) правовідносини у сфері знаходження міжнародних зв'язків з ціллю обмінюватися необхідним досвідом при розбудові сфери кібербезпеки;

3) правовідносини щодо регулювання, координування та контролю діяльності правоохоронних органів та інших суб'єктів, які забезпечують кібербезпеку під час виконання своїх обов'язків;

4) правовідносини, які стосуються сфери запровадження інформаційних технологій в ключових галузях життєдіяльності суспільства та приведення в належний стан процес під час їх безпечного використання;

5) правовідносини, які стосуються сфери розвитку науки та техніки з ціллю побудувати предметну основу інституту кібербезпеки,

мається на увазі розробити новітні технології, які допоможуть підвищити безпеку під час роботи у кіберпросторі;

6) правовідносини, які стосуються сфери адаптації у чинне законодавство України правових механізмів, які дозволять забезпечити кібербезпеку, враховуючи міжнародний досвід у цій галузі;

7) правовідносини, які стосуються сфери підвищення інформаційної освіченості суспільства під час роботи з відповідною інформацією у кіберпросторі, тощо.

Окрім цього переліку існують ще об'єкти, які закріплені у Законі України «Про основні засади забезпечення кібербезпеки України», за яким встановлено: «1) конституційні права і свободи людини і громадянина; 2) суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища; 3) держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність; 4) національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави; 5) об'єкти критичної інфраструктури».

В свою чергу, об'єктами механізму кіберзахисту є матеріальні та нематеріальні блага, на які спрямовуються заходи щодо забезпечення кібербезпеки, які складають цей механізм. Ці об'єкти представлені наступним чином:

1) інформаційно-телекомунікаційні системи, відповідно до яких обробляється інформація, яка охороняється законом, тобто це такі відомості, які не призначаються для загального користування;

2) об'єкти критичної інформаційної інфраструктури;

3) інформаційно-телекомунікаційні системи, за якими відбувається обробка державних інформаційних ресурсів.

3. Під правовими засадами забезпечення кібербезпеки слід розуміти керівні ідеї, засади та положення, які закріплені за нормами нормативно-правових актів, що мають різну юридичну силу та

визначають механізм правового регулювання щодо забезпечення кібербезпеки.

На сьогоднішній день правові засади, які забезпечують механізм кібербезпеки України, ґрунтуються на основних принципах, які закріплені у Законі України «Про основні засади забезпечення кібербезпеки України».

Також було встановлено, що адміністративно-правове регулювання можна вважати як одну із ключових засад в зазначеній сфері. Тобто, роль адміністративно-правового регулювання проявляється в тому, що згідно до діючих норм адміністративного законодавства відбувається правове регулювання діяльності суб'єктів, які забезпечують кібербезпеку в Україні.

4. Суб'єкти, які забезпечують кібербезпеку являються учасниками не інформаційних, а адміністративних правовідносин, тому що: 1) їх відносини базуються на засадах влади і підпорядкування; 2) реалізація механізму кіберзахисту здійснюється за рахунок використання примусу, який надається їм згідно до чинного законодавства; 3) їх діяльність спрямовується на те, щоб припиняти правопорушення у цій сфері. Необхідно також додати, що для того, щоб аналізувати адміністративно-правовий статус зазначеної категорії, апріорі неможливо виходити за межі адміністративної галузі права.

Суб'єктів, які забезпечують кібербезпеку, потрібно поділяти на дві групи: загальну та спеціальну.

До суб'єктів загальної групи слід відносити: «міністерства та інші центральні органи виконавчої влади; місцеві державні адміністрації; органи місцевого самоврядування; правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності; Збройні Сили України, інші військові формування, утворені відповідно до закону; Національний банк України; підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури; суб'єкти

господарювання, громадяни України та об'єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом».

За кожним учасником правовідносин в зазначеній групі закріплюються повноваження, які дають змогу йому реалізувати напрями діяльності та забезпечувати необхідні заходи з ціллю підтримувати належний стан зазначеного інституту.

В свою чергу, спеціальну групу суб'єктів складають: 1) Державна служба спеціального зв'язку та захисту інформації України; 2) Національна поліція України; 3) Служба безпеки України; 4) Міністерство оборони України; 5) Генеральний штаб Збройних Сил України; 6) розвідувальні органи; 7) Національний банк України.

Роль перелічених суб'єктів, які забезпечують кібербезпеку, характеризується особливими напрямками їх діяльності та змогою використовувати спеціальні заходи стосовно підтримки законного та належного рівня кібербезпеки, які фактично інші органи в своєму розпорядженні не мають.

5. В юридичній літературі не визначається єдиний підхід стосовно конкретних форм та методів в зазначеній сфері, а тому, акцентуючи увагу на наукову літературу та норми чинного законодавства України, було запропоновано власний погляд стосовно переліку відповідних форм та методів.

Надано характеристику наступним формам забезпечення кібербезпеки України: 1) нормотворчість; 2) прийняття індивідуальних актів; 3) адміністративний договір; 4) правореалізація.

В свою чергу, серед основних методів було виділено та охарактеризовано наступні: 1) адміністративний примус; 2) метод дозволу та заборон; 3) метод адміністративного контролю; 4) метод

контролю доступу; 5) метод ліцензування діяльності у сфері захисту відомостей, що становлять державну таємницю; 6) метод сертифікації та стандартизації.

Загалом, слід відзначити, що форми і методи в сукупності створюють так званий інструмент, завдяки якому суб'єкти, що забезпечують кібербезпеку мають можливість вирішувати складні завдання, які стоять перед ними в зазначеній сфері.

6. Під юридичною відповідальністю за порушення законодавства у сфері кібербезпеки України можна розуміти застосування заходів примусового характеру, які закріплені відповідно до норм чинного законодавства, до осіб, якими було вчинено правопорушення у кіберпросторі.

До суб'єктів, які вчинили правопорушення в зазначеній сфері, можуть застосовуватися такі види юридичної відповідальності: цивільна, адміністративна та кримінальна.

Характерними особливостями юридичної відповідальності за порушення законодавства в зазначеній сфері є наступні:

1) специфічність предмету правопорушення чи кіберзлочину, яким виступає інформація, що міститься в Інтернеті;

2) складність в тому, щоб виявити суб'єкта правопорушення у зв'язку з відсутністю належного матеріально-технічного та кадрового забезпечення;

3) найрозповсюдженіший вид юридичної відповідальності – кримінальна, оскільки вона зумовлена значним рівнем шкоди у результаті вчинення кіберзлочину;

4) шкода, яка завдається, в більшій мірі носить матеріальний характер та не наносить ніякої шкоди фізичному здоров'ю особи.

Питання юридичної відповідальності за порушення законодавства в розглядуваній сфері однозначно недостатнім чином врегульовані, що є значним недоліком, який сприяє збільшенню рівня кіберзлочинності в

Україні. Зокрема, питання, які стосуються притягнення винних осіб у сфері кібербезпеки до цивільної та адміністративної відповідальності врегульовані значним масивом нормативних актів, в яких закріплено різноманітні підстави щодо притягнення особи до відповідальності. Така розгалуженість породжує тільки складність під час застосування стягнень до правопорушників державними органами. Як результат, доцільно було б внести відповідні зміни до Закону України «Про основні засади забезпечення кібербезпеки України», перш за все, в частині детального окреслення видів правопорушення та кіберзлочинів, за якими винних осіб можна притягнути до того чи іншого виду юридичної відповідальності. Означене зробить відповідне законодавство набагато урегульованим та узгодженим, а відтак, і дасть позитивний відбиток на якості забезпечення кібербезпеки в Україні.

7. Сьогоднішні світові тенденції розвитку інформаційного суспільства схиляють всі держави в світі приймати заходи стосовно забезпечення кібербезпеки. Україна, безумовно, не є виключенням, яка нині стоїть лише на початкових етапах розвитку зазначеного інституту.

Враховуючи досвід проаналізованих зарубіжних країн (Великобританії, Німеччини, Франції, Польщі, США та Китаю), виокремлено ключові напрями розвитку інституту забезпечення кібербезпеки, які можна адаптувати в нашій державі, серед яких:

– потрібно збільшувати виділення коштів на суб’єктів, діяльність яких спрямовується на те, щоб забезпечити кібербезпеку в державі;

– проводити відповідні заходи для покращення якості освіти працівників кіберполіції. Врахувавши досвід США, вважаємо, що необхідно створити спеціальну академію при Міністерстві внутрішніх справ, яка б займалася підготовкою фахівців, які будуть протидіяти кіберзлочинам. В тому числі, державна політика повина спрямовуватися на обмін досвідом між суб’єктами правоохоронних органів, що у підсумку дасть можливість кіберполіції переймати досвід фахівців у

зазначеній сфері, а також організовано проводити висококваліфіковану підготовку, які будуть попереджати, виявляти та розкривати злочини у сфері інформаційних технологій, існуючих у кіберпросторі;

– кардинально оновити Стратегію кібербезпеки України. На нашу думку, її потрібно розширити та охопити більше коло питань у цій сфері, оскільки на даний момент вона обмежується тільки питаннями, які містять в собі базовий зміст. В цьому аспекті можна використовувати досвід Великобританії та Німеччини, тому що в цих країнах стратегії, які забезпечують кібербезпеку, охоплюють майже усі питання та являються ключовими документами у цій сфері;

– потрібно розширювати міжнародне співробітництво у сфері забезпечення кібербезпеки, тобто залучати можливості міжнародної технічної допомоги з ціллю розбудови національної системи кібербезпеки;

– розробити організаційно-технічну модель надійного захисту вітчизняного кіберпростору, а також розширити засади, щоб сформувати методи та принципи стосовно здійснення «електронної оборони»;

– необхідно збільшити контроль в Інтернеті (як приклад, тут слугує Китай). Цей напрям можна обґрунтувати тим, що сьогодні в мережу Інтернет потрапляє необмежена кількість «фейкових» новин, які в свою чергу створюють оману для населення загалом та підривають довіру до державних органів (частіше за все це стосується правоохоронних органів), зокрема.

8. Визначено найбільш важливі недоліки законодавства у сфері забезпечення кібербезпеки, серед яких можна виділити наступні:

1) в Законі України «Про основні засади забезпечення кібербезпеки України» представлено досить широке коло суб’єктів, які забезпечують кібербезпеку в Україні, однак, при цьому, в ньому не визначається той єдиний (ключовий) орган, повноваження якого повинні

відноситись до оперативного командування всіх інших суб'єктів в розглядуваній сфері;

2) термінологічна недосконаліть Закону України «Про основні засади забезпечення кібербезпеки України», оскільки деякі терміни відображені досить «просто» та не характеризують усю специфіку окремих категорій;

3) законодавцем не виділено, які є види кіберзагроз та кіберзлочинів;

4) в Законі України «Про основні засади забезпечення кібербезпеки України» не існує таких понять, як «кіберправопорушення» та «кіберпроступок», що являється недопустимим, бо чинним законодавством передбачається цивільна та адміністративна відповідальність;

5) в Законі України «Про основні засади забезпечення кібербезпеки України» відсутні норми, які б детально регламентували організаційні та процедурні засади щодо забезпечення кібербезпеки в Україні. Серед іншого, це стосується форм та методів забезпечення кібербезпеки, які також не закріплені на законодавчому рівні;

6) недолік у вигляді виключення з нового Закону України «Про національну безпеку України» від 2018 року (у порівнянні з попереднім Законом України «Про основи національної безпеки України» від 2003 року) статті, за якою визначались основоположні реальні та потенційні загрози внутрішньо- та зовнішньополітичній національній безпеці України, а також стабільності в суспільстві;

7) спрямованість Доктрини інформаційної безпеки виключно на Російську Федерацію;

8) відсутні конкретні строки, на які приймається Стратегія кібербезпеки України, не вирішено питання щодо цільового призначення грошових коштів, не приділено уваги кадровому питанню щодо суб'єктів, які уповноважені займатися забезпеченням кібербезпеки

в Україні, а також недостатнім чином розкривається питання взаємодії суб'єктів забезпечення кібербезпеки як між собою, так і з громадськістю, в тому числі між суб'єктами, які здійснюють господарську діяльність.

В свою чергу, в аспекті означених недоліків, запропоновано визначити наступні напрями удосконалення адміністративного законодавства, яке здійснює регулювання забезпечення кібербезпеки в Україні:

1) закріпивши види кіберзагроз на рівні закону, це матиме вагоме значення не тільки з теоретичної, але й з практичної сторони, тому що: а) унеможливлює неоднозначність тлумачення деяких правових норм; б) дає змогу якісніше формулювати положення інших нормативно-правових актів в розглядуваній сфері;

2) пропонується внести відповідні зміни до Закону України «Про основні засади забезпечення кібербезпеки України», додавши такі терміни як «кіберправопорушення» та «кіберпроступок», які будуть чітко відображати можливість притягнення винних до адміністративної та цивільної відповідальності;

3) у Стратегії кібербезпеки України: а) закріпити конкретні строки реалізації стратегії; б) приділити увагу кадровому питанню щодо суб'єктів, які уповноважені займатися забезпеченням кібербезпеки в Україні.

В цілому, слід також зазначити, що протягом останніх років фахівцями та політиками наголошувалось на тому, щоб суттєво покращити вітчизняне законодавство у сфері забезпечення кібербезпеки в Україні. З цим не можна не погодитись, проте, зазвичай ними відмічається поліпшення законодавчої бази, якщо порівнювати те, що було в Україні до 2013 року. На нашу думку, це не дуже справедливо, тому що відправною точкою у цій сфері повинно слугувати не законодавство, яке є застарілим, а позитивний досвід зарубіжних країн,

які виступають як взірець під час забезпечення кібербезпеки. А тому не викликає сумнівів, що зміни, які було запропоновано, сприятимуть тому, щоб покращити практичну діяльність суб’єктів, які забезпечують кібербезпеку в Україні, а як наслідок – позитивно вплинуть на стан кіберзахисту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Конституція України: Закон України від 28 червня 1996 року № 254к/96 – ВР (останні зміни: 01.01.2020) / Верховна Рада України. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141.

2. Адміністративне право України: навчальний посібник у 4-х томах / В.В. Галунько. Херсон: ХМТ, 2011. Т. 1. 334 с.

3. Харитонова О.І. Адміністративно-правові відносини: концептуальні засади та правова природа. Одеса, 2004. 328 с.

4. Єрьоміна Л.В. Удосконалення законодавства України у сфері кібербезпеки: термінологічний аспект. *Інформ. безпека людини, сусп-ва, держави*. 2013. № 2. С. 129–135.

5. Коваленко Н.В. Про правовий режим кібербезпеки в Україні. *Актуальні проблеми вітчизняної юриспруденції*. 2016. № 3. С. 96–100.

6. Дубов Д.В. Кіберпростір як новий вимір геополітичного суперництва: монографія / Д.В. Дубов. Київ: НІСД, 2014. 321 с.

7. Тонконогов А.В. Кибернетическая безопасность: понятие и сущность феномена. *Право и кибербезопасность*. 2013. № 2. С. 36–43.

8. Діордіца І.В. Система забезпечення кібербезпеки: сутність та призначення. *Інформаційне право*. 2017. № 7. С. 109–110.

9. Баранов О.А. Про тлумачення та визначення поняття «кібербезпека». *Правова інформатика*. 2014. № 2 (42). С. 1–9.

10. Корченко О.Г., Бурячок В.Л., Гнатюк С.О. Кібернетична безпека держави: характерні ознаки та проблемні аспекти. *Ukrainian Scientific Journal of Information Security*. 2013. № 19. С. 40–44.

11. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII (останні зміни: 08.07.2018) / Верховна Рада України. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403.

12. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»: Указ Президента України 15 березня 2016 року № 96/2016 / Президент України. *Офіційний вісник Президента України*. 2016. № 96/2016.

13. Про рішення Ради національної безпеки і оборони України «Про нову редакцію Воєнної доктрини України»: Указ Президента України 2 вересня 2015 року № 555/2015 / Президент України. *Офіційний вісник Президента України*. 2015. № 555/2015.

14. Коломієць О.В. Проблеми національного законодавства в сфері боротьби з кіберзлочинністю та шляхи їх вирішення. *Гілея*. 2012. Вип. 57 (№ 2). С. 546–551.

15. Шеломенцев В.П. Кримінологічна безпека у кіберпросторі: система понять. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2010. № 23. С. 342–348.

16. Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації: Рішення Ради національної безпеки і оборони України від 29 грудня 2016 року / Рада національної безпеки і оборони України. *Офіційний вісник Верховної Ради України*. 2016.

17. Про державну таємницю: Закон України від 21 січня 1994 року № 2163-VIII (останні зміни: 13.02.2020) / Верховна Рада України. *Відомості Верховної Ради України*. 1994. № 16. Ст. 93.

18. Науково-практичний коментар Кримінального процесуального кодексу України / В.М. Тертишник. Київ: Правова Єдність, 2017. 824 с.

19. Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави: Постанова Кабінету Міністрів України від 23 серпня 2016 року № 563 / Кабінет Міністрів України. *Офіційний вісник Верховної Ради України*. 2016. № 563.

20. Довгань О.Д. Інформаційні ресурси: національні та державні, зміст, поняття. *Інформація і право*. 2015. № 3 (15). С. 85–91.

21. Про Стратегію сталого розвитку «Україна – 2020»: Указ Президента України 12 січня 2015 року № 5/2015 / Президент України. *Офіційний вісник Президента України*. 2015. № 5/2015.

22. Колодій А.М. Принципи права: генеза, поняття, класифікація та реалізація. *Альманах права*. 2012. Вип. 3. С. 42–46.

23. Дубов Д.В. Стратегічні аспекти кібербезпеки України. Стратегічні пріоритети: [наук.-аналіт. щокварт. зб.] / Нац. ін-т стратег. дослідж. Київ: НІСД, 2013. № 4 (29). С. 119–126.

24. Бурячок В.Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби: підручник / В.Л. Бурячок, Г.М. Гулак, В.Б. Толубко. Київ : ТОВ «СІК ГРУП Україна», 2015. 449 с.

25. Гіда О.Ф. Соціальні мережі як засіб деструктивних впливів через інформаційний простір. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2013. № 3. С. 268–278.

26. Про схвалення Концепції Державної цільової програми реформування та розвитку оборонно-промислового комплексу на період до 2020 року: Розпорядження Кабінету Міністрів України від 20 січня 2016 року № 19-р / Кабінет Міністрів України. *Офіційний вісник Верховної Ради України*. 2016. № 19-р.

27. Котелянець О.О. Шляхи підвищення ефективності демократичного цивільного контролю над сектором безпеки. *Стратег. пріоритети*. 2011. № 4 (21). С. 118–123.

28. Загальна теорія держави і права: підручник / М.В. Цвік, О.В. Петришин, Л.В. Авраменко. Харків: Право. 2011. 584 с.

29. Діордіца І.В. Суб’єкти забезпечення кібербезпеки. *Науковий вісник Ужгородського національного університету*. 2017. Вип. 45. Том 1. С. 160–165.

30. Про Кабінет Міністрів України: Закон України від 27 лютого 2014 року № 794-VII (останні зміни: 20.03.2020) / Верховна Рада України. *Відомості Верховної Ради України*. 2014. № 13. Ст. 222.

31. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 23 лютого 2006 року № 3475-IV (останні зміни: 20.03.2020) / Верховна Рада України. *Відомості Верховної Ради України*. 2006. № 30. Ст. 258.

32. Про розвідувальні органи: Закон України від 22 березня 2001 року № 2331-III (останні зміни: 09.05.2018) / Верховна Рада України. *Відомості Верховної Ради України*. 2001. № 19. Ст. 94.

33. Великий тлумачний словник сучасної української мови / [уклад. і голов. ред. В.Т. Бусел]. Ірпінь: ВТФ «Перун», 2004. 1440 с.

34. Адміністративне право України: підручник / за заг. ред. проф. Ю.П. Битяка. Харків: Право, 2000. 526 с.

35. Логінов О.В. Адміністративно-правове забезпечення інформаційної безпеки органів виконавчої влади: дис. … канд. юрид. наук: спец. 12.00.07. Київ, 2005. 201 с.

36. Бухарєв В.В. Нормотворчість як адміністративно-правова форма забезпечення кібербезпеки в Україні. *Розвиток сучасного права в умовах глобальної нестабільності*: Матеріали міжнародної науково-практичної конференції (м. Одеса, Україна, 9-10 вересня 2016 р.). Одеса: ГО «Причорноморська фундація права», 2016. С. 78–79.

37. Марков В.В. Поняття та види форм адміністративно-правової протидії кіберзлочинності в Україні. *Європейські перспективи*. 2015. Вип. 7. С. 43–47.

38. Стефанюк В. С. Судовий адміністративний процес. Харків: Консум, 2003. 473 с.

39. Бухарєв В.В. Адміністративний договір як важлива адміністративно-правова форма забезпечення кібербезпеки в Україні. *Розвиток державності та права в Україні: реалії та перспективи*: Матеріали міжнародної науково-практичної конференції, м. Львів, 14–15 вересня 2018 р. Львів: Західноукраїнська організація «Центр правничих ініціатив», 2018. С. 61–64.

40. Бурбика В.О. Адміністративно-правові засади взаємодії органів місцевого самоврядування з правоохоронними органами: дисертація ... канд. юрид. наук, спец.: 12.00.07. Суми, 2017. 251 с.

41. Мельник Р.С. Забезпечення законності застосування заходів адміністративного примусу, не пов'язаних з відповідальністю: автореф. дис... канд. юрид. наук. Харків, 2002. 19 с.

42. Скакун О.Ф. Теорія права і держави: підручник. 3-те видання. Київ: Алерта; ЦУП, 2011. 524 с.

43. Кудрявцев В.Н. Правовое поведение: норма и патология. Москва, 1997. 223 с.

44. Клюєв О.М. Адміністративно-правові методи забезпечення кібербезпеки в Україні. *Сучасні правові системи світу в умовах глобалізації: реалії та перспективи*: Міжнародна науково-практична конференція, м. Київ, 13-14 березня 2015 р. К.: Центр правових наукових досліджень, 2015. С. 59–62.

45. Хропанюк В.Н. Теория государства и права / Под ред. В.Г. Стрекозова. Москва: Интерстиль, 2000. 377 с.

46. Цивільний кодекс України: Закон України від 16 січня 2003 року № 435-IV (останні зміни: 23.05.2020) / Верховна Рада України. *Відомості Верховної Ради України*. 2003. № 40(44). Ст. 356.

47. Педешко А.І. Адміністративна відповідальність за порушення митних правил: дис... канд. юрид. наук: 12.00.07 / Університет внутрішніх справ. Харків, 2000. 176 с.

48. Кодекс України про адміністративні правопорушення: Закон УРСР від 7 грудня 1984 року № 2755-VI (останні зміни: 11.06.2020) / Верховна Рада України. *Відомості Верховної Ради України*. 1984. додаток до № 51. Ст. 1122.

49. Перун Т.С. Адміністративна відповідальність в системі заходів забезпечення інформаційної безпеки / [Електронний ресурс]. URL: http://aphd.ua/publication-229/ (дата звернення: 10.10.2020).

50. Конвенція про кіберзлочинність від 23 листопада 2001 року, ратифікована Україною від 7 вересня 2005 року / [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 10.10.2020).

51. Орлов Ю.Ю. Реалізація вимог Міжнародної конвенції про кіберзлочинність у законодавстві України. *Наук. вісн. Нац. акад. внутріш. справ*. 2011. № 6. С. 3–9.

52. Кримінальний кодекс України: Закон України від 5 квітня 2001 року № 2341-III (останні зміни: 11.06.2020) / Верховна Рада України. *Відомості Верховної Ради України*. 2001. № 25(26). Ст. 131.

53. Мовчан А.В. Види юридичної відповідальності за порушення законодавства у сфері кібербезпеки України. *Науковий вісник Херсонського державного університету. Серія «Юридичні науки»*. 2018. Вип. 6-2. Т. 2. С. 188–192.

54. Законодавство та стратегії у сфері кібербезпеки країн Європейського союзу США, Канади та інших / [Електронний ресурс]. URL:https://parlament.org.ua/wp-content/uploads/2016/11/INFODOVIDKA-ZAKONODAVSTVO-TA-STRATEGIYI-KIBERBEZPEKA.pdf (дата звернення: 10.10.2020).

55. У Великобританії створили реабілітаційний центр для кіберзлочинців / [Електронний ресурс]. URL: http://prportal.com.ua/Fakty/u-velikobritaniyi-stvorili-reabilitaciyniy-centr-dlya-kiberzlochinciv (дата звернення: 10.10.2020).

56. Бойко В.О. Державно-приватне партнерство у сфері кібербезпеки: кейс Німеччина: аналітична записка. Київ: Національний інститут стратегічних досліджень, Відділ інформаційної безпеки та розвитку інформаційного суспільства Національного інституту стратегічних досліджень 2018. 18 с.

57. Добржанська О.Л., Демцов А.А. Кібербезпека як феномен міжнародних відносин на прикладі Федеративної Республіки Німеччини.

Актуальні проблеми міжнародних відносин. 2011. Вип. 102 (1). С. 111–116.

58. Петрик В.М. Забезпечення інформаційної безпеки держави: підручник / за заг. ред. О.А. Семченка та В.М. Петрика. Київ: ДНУ «Книжкова палата України», 2015. 672 с.

59. Як це робила Польща: досвід боротьби з кіберзагрозами. Електронне видання «Економічна правда» / [Електронний ресурс]. URL: https://www.epravda.com.ua/columns/2017/10/12/630044/ (дата звернення: 10.10.2020).

60. Булавін А.В. Про підходи США та Китаю щодо забезпечення кібербезпеки. *Суспільство: політика, економіка, право*. 2018. № 1. С. 27–31.

61. Китай схвалив новий закон про кібербезпеку / [Електронний ресурс]. URL: https://www.unn.com.ua/uk/news/1616273-kitay-skhvaliv-noviy-zakon-pro-kiberbezpeku (дата звернення: 10.10.2020).

62. Сухонос В.В. Зарубіжний досвід забезпечення кібербезпеки та можливості його використання в Україні. *Науковий вісник Ужгородського національного університету. Серія «Право»*. 2017. Вип. 43. Т. 3. С. 128–133.

63. Кузьменко Б.В. Інформаційна диверсія та інформаційний саботаж інструменти кібертероризму. *Роль правоохоронних органів у формуванні правової держави в умовах євроінтеграції України*: матеріали Всеукр. підсумк. наук.-практ. конф. (м. Київ, 12 березня 2015 р.). Київ: Нац. акад. внутр. справ, 2015. Ч. 1. С. 20–22.

64. Діордіца І.В. Класифікація кіберзагроз та їх легітимізація у нормативно-правових актах України. *Підприємництво, госп-во і право*. 2017. № 10. С. 206–211.

65. Щодо Закону України «Про основні засади забезпечення кібербезпеки України» / [Електронний ресурс]. URL: http://kmp.ua/uk/analytics/infoletters/regarding-the-law-of-ukraine-on-the-

basic-principles-of-cybersecurity-protection-of-ukraine/ (дата звернення: 10.10.2020).

66. Про національну безпеку: Закон України від 21 червня 2018 року № 2469-VIII (останні зміни: 15.03.2020) / Верховна Рада України. *Відомості Верховної Ради України*. 2018. № 31. Ст. 241.

67. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України 25 лютого 2017 року № 47/2017 / Президент України. *Офіційний вісник Президента України*. 2017. № 47/2017.

68. Тарасенко Н., Попова Т. Доктрина інформаційної безпеки України в оцінках експертів / [Електронний ресурс]. URL: http://nbuviap.gov.ua/index.php?option=com_content&view=article&id=2760:doktrina-informatsijnoji-bezpeki-yak-zasib-protidiji-informatsijnim-zagrozam-2&catid=63&Itemid=393 (дата звернення: 10.10.2020).

69. Величко Д.М. Напрямки вдосконалення адміністративного законодавства, яке регулює забезпечення кібербезпеки в Україні. *Наше право*. 2018. № 2. С. 52–57.

70. Грайворонський М.В. Сучасні підходи до забезпечення кібернетичної безпеки. Матеріали XIII Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених *«Теоретичні і прикладні проблеми фізики, математики та інформатики»* (м. Київ, 21–23 травня 2018). Київ: НТУУ «КПІ», 2018. С. 10–17.