ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ АГРАРНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ МЕНЕДЖМЕНТУ І ПРАВА
КАФЕДРА ПРАВОЗНАВСТВА

«Допущено до захисту»
Завідувач кафедрою
_____Н.М.Опольська
«____»_____2020 р.

МАГІСТЕРСЬКА РОБОТА
на здобуття освітньо-кваліфікаційного рівня «Магістр» зі спеціальності 8.03040101 «Правознавство»

на тему:

«Адміністративно-правові засади забезпечення кібербезпеки в Україні»

Виконав:
Студент 6-го курсу, групи ПР-19
Гоменюк Микола Павлович

Керівник:
Кандидат юридичних наук, доцент
Дзевелюк Андрій Володимирович

Вінниця – 2020

План

ВСТУП

Одним із головних напрямків розвитку України на її важкому історичному етапі є розбудова інформаційно-грамотного суспільства. Заходи із втілення даного кроку передбачають активне впровадження інформаційно-комунікаційних технологій, розвиток кібернетичного простору. Зарубіжний досвід свідчить про те, що переведення частини суспільних відносин у кібернетичний простір має низку переваг, але сприяє підвищенню відкритості та прозорості діяльності суб'єктів публічної влади, оперативності та ефективності їх взаємодії між собою та з представниками громадськості, міжнародною спільнотою. Проте одночасно швидкий розвиток інформаційних, інформаційно-телекомунікаційних засобів, технологій, систем і мереж характеризується і значними негативними моментами, зокрема появою нової сфери для процвітання злочинності. Сприятливість даної сфери для злочинної діяльності обумовлена цілим рядом факторів, наприклад: розвиток комп'ютерних та інформаційно-комунікаційних технологій випереджає розвиток законодавства, яке регулює відносини в даній сфері; необмеженість державними кордонами, що створює сприятливі умови для процвітання транснаціональної злочинності; складність виявлення безпосереднього суб'єкта злочинної діяльності та доведення його вини. Вказані та інші аспекти комп'ютеризації, кібернетизації значної частини суспільного життя змушують кожну сучасну державу особливу увагу приділяти своїй кібернетичній безпеці. Зрозуміло, що Україна в цьому питанні не є виключенням, що обумовлює необхідність суттєвого вдосконалення національного механізму забезпечення кібербезпеки. Одним із основних етапів покращення якості та ефективності організації і функціонування даного механізму є поліпшення його адміністративно-правового забезпечення, яке передбачає покращення відповідного законодавства та перегляд системи

суб'єктів, що опікуються питаннями кібербезпеки. На протязі останніх років у наукових колах все частіше мали місце думки щодо назрілої потреби зміцнення національної кібербезпеки, що є цілком зрозумілим, адже із такими кібернетичними загрозами, які є сьогодні, Україна раніше не зіштовхувалася, як результат – відсутність необхідного досвіду і нездатність ефективно протидіяти даним загрозам. Зазначене вказує на актуальність проведення комплексного вивчення адміністративно-правових засад забезпечення кібернетичної безпеки в Україні з метою виокремлення існуючих проблем у даному механізмі та визначення пріоритетів і перспективних напрямків його подальшого розвитку з урахуванням реалій і викликів сьогодення.

Також сьогодні з огляду на стрімке поширення у глобальному вимірі інформаційних та телекомунікаційних мереж , техніко- технологічного розвитку, актуальним залишається питання посилення кібербезпеки. При цьому необхідною умовою розвитку інформаційного суспільства є саме кібербезпека держави , за якою може стояти практично невичерпаний перелік проблем, починаючи від організаційно- технічних , економічних і закінчуючи правовими. Світовий досвід підвищення ефективності боротьби з кібезлочинністю демонструє потребу у створенні системи глобального обміну інформацією у захищеному форматі. Як свідчать результати оприлюднених досліджень та чисельних суспільних опитувань , питання запобігання кіберзлочинності непокоїть не тільки державу в цілому , а й кожного окремо взятого пересіченого її громадянина.

Стрімкий розвиток інформаційних технологій поступово змінює світ. Відкритий та вільний кіберпростір розширює свободу і можливості людей, збагачує суспільство , створює новий глобальний інтерактивний ринок ідей, досліджень та інновацій, стимулює відповідальну та ефективну роботу влади і активне залучення громадян до управління державою та вирішення питань

місцевого значення , забезпечує публічність та прозорість влади, сприяє запобіганню корупції.

Таким чином, необхідність удосконалення кібербезпеки в Україні, недосконаліть правового регулювання у зазначеній сфері, з одного боку, та відсутність комплексних досліджень з цієї проблематики – з іншого, обумовлюють своєчасність та актуальність комплексного дослідження адміністративно-правових засад забезпечення кібербезпеки України.

Мета і завдання дослідження. Метою магістерської роботи є визначення сутності та особливостей адміністративно-правових засад забезпечення кібербезпеки в Україні, а також шляхів їх удосконалення. Для досягнення зазначеної мети в магістерській роботі необхідно було виконати такі основні завдання: – визначити поняття та з'ясувати особливості кібербезпеки як об'єкта адміністративно-правової охорони; – здійснити історико-правовий аналіз розвитку та становлення правового інституту кібербезпеки; – встановити види об'єктів кібербезпеки та кіберзахисту; – охарактеризувати правові засади забезпечення кібербезпеки України та з'ясувати місце серед них адміністративно-правового забезпечення; – окреслити систему суб'єктів забезпечення кібербезпеки України та особливості їх адміністративно-правового статусу; – систематизувати адміністративно-правові форми та методи забезпечення кібербезпеки України; – виокремити види та особливості юридичної відповідальності за порушення законодавства у сфері кібербезпеки України; – узагальнити зарубіжний досвід забезпечення кібербезпеки та запропонувати можливості його використання в Україні; – опрацювати напрямки вдосконалення адміністративного законодавства, яке регулює забезпечення кібербезпеки в Україні; – встановити способи оптимізації системи суб'єктів забезпечення кібербезпеки України та напрямки вдосконалення взаємодії між ними.

Об'єктом дослідження є : суспільні відносини, що виникають під час забезпечення кібербезпеки в Україні.

Предметом дослідження є : адміністративно-правові засади забезпечення кібербезпеки України.

Методи дослідження. В магістерській роботі використано такі методи наукового пізнання: а) логіко-семантичний, за допомогою якого визначено поняття «кібербезпека як об'єкт адміністративно-правової охорони»), «адміністративно-правові форми забезпечення кібербезпеки України» та «адміністративно-правові методи забезпечення кібербезпеки України» , «суб'єкти забезпечення кібербезпеки України» ,б) історико-правовий – під час аналізу становлення та розвитку правового інституту кібербезпеки в) системно-структурний, за допомогою якого систематизовано види об'єктів кібербезпеки та кіберзахисту, окреслено коло суб'єктів забезпечення кібербезпеки України, особливості їх адміністративно-правового статусу та види юридичної відповідальності за порушення законодавства у сфері кібербезпеки України , г) порівняльно-правовий, що використовувався з метою з'ясування правових підстав становлення правового інституту кібербезпеки, виявлення особливостей адміністративно-правового забезпечення кібербезпеки України, опрацювання напрямків удосконалення адміністративно-правових засад забезпечення кібербезпеки в Україні (підрозділи 1.2, 3.1 – 3.3); ґ) структурного аналізу, який застосовано під час окреслення особливостей адміністративно-правового статусу суб'єктів забезпечення кібербезпеки та шляхів оптимізації їх системи (підрозділи 2.1, 3.3). В роботі використано низку інших методів наукового пізнання. Науково-теоретичне підґрунтя дипломної становлять праці вчених різної галузевої належності, які вивчали проблеми теорії та практики забезпечення кібербезпеки в Україні та світі. Нормативною основою дослідження є Конституція України, норми міжнародних нормативно-правових актів, закони та підзаконні нормативно-правові акти, які визначають адміністративно-правові засади

забезпечення кібербезпеки в Україні. Інформаційну та емпіричну основу роботи становлять узагальнення практики забезпечення кібербезпеки, довідкові видання, статистичні матеріали. Наукова новизна отриманих результатів визначається тим, що представлена магістерська робота є однією з перших спроб комплексно, з урахуванням аналізу наукових праць учених та чинного законодавства України визначити сутність та особливості адміністративно- правових засад забезпечення кібербезпеки України та запропонувати напрямки вдосконалення відповідного законодавства. У результаті проведеного дослідження сформульовано низку нових наукових положень та висновків, запропонованих особисто здобувачем. Основні з них такі:

- визначено, що адміністративно-правова охорона у сфері забезпечення кібербезпеки – це діяльність відповідних державних органів, що здійснюється на засадах імперативності та ієрархічності і направлена на підтримання та забезпечення належного стану захищеності прав, інтересів та інформації відповідних суб'єктів у кіберпросторі;

- обґрунтування того , що розмежування адміністративно-правового забезпечення кібербезпеки та адміністративно-правового забезпечення кіберзахисту є принципово важливим питанням, адже воно прямо пов'язане з процесом їх реалізації, що при неправильному підході може завдати шкоди охоронюваним законом інтересам та правам людей, які здійснюють різні операції з інформацією в кіберпросторі;

– доведена моя позиція як автора, згідно з якою суб'єкти забезпечення кібербезпеки є учасниками не інформаційних, а адміністративних правовідносин, оскільки, по-перше, відносини між ними будуються на основі влади і підпорядкування, а по-друге, останні реалізують механізм кіберзахисту шляхом використання примусу, який їм надано чинним законодавством. Крім цього, аналіз адміністративно-правового статусу суб'єктів забезпечення кібербезпеки

просто неможливо здійснювати поза межами адміністративної галузі права; удосконалено:

– розуміння того, що історія становлення та розвитку кібербезпеки як юридичного інституту прямо пов’язана з еволюцією інформаційних технологій та Інтернету, який дав людству можливість обробляти та обмінюватися колосальною кількістю даних на відстані;

– обґрунтування того, що правові засади забезпечення кібербезпеки – це весь масив керівних ідей, засад та положень, закріплених у нормативно - правових актах різної юридичної сили , які визначають механізм правового регулювання забезпечення кібербезпеки;

– характеристику основних адміністративно-правових форм забезпечення кібербезпеки України, під якими запропоновано розуміти зовнішній вираз діяльності уповноважених органів державної влади, який виявляється у вчиненні ними комплексу дій, які спрямовані на створення таких умов, за яких буде забезпечено безпеку комп’ютерних систем у всій країні в цілому; – розуміння оптимізації системи суб’єктів забезпечення кібербезпеки, яка являє собою процес, що передбачає: по-перше, створення оптимальної кількості таких суб’єктів, яких буде достатньо для виконання завдань у сфері забезпечення кібербезпеки; по-друге, належну організацію діяльності відповідних суб’єктів шляхом збільшення або зменшення кількості їх повноважень; – характеристику ознак взаємодії суб’єктів забезпечення кібербезпеки, до яких віднесено: 1) єдину мету спільної діяльності; 2) наявність декількох або більше суб’єктів; 3) обов’язковість законодавчого підґрунтя діяльності; 4) чітко визначений адміністративно-правовий статус кожного суб’єкта; 5) узгодженість заходів щодо мети, місця, часу, методів діяльності; – розуміння форм взаємодії суб’єктів забезпечення кібербезпеки в Україні, до яких запропоновано віднести: 1) проведення спільних міжвідомчих нарад; 2) обмін оперативною інформацією щодо стану забезпечення кібербезпеки, а також щодо заходів, які були вже

реалізовані кожним суб'єктом взаємодії; 3) розроблення спільних програм щодо протидії кіберправопорушенням та окреслення основних напрямків спільної діяльності; 4) спільну участь у проведенні окремих слідчих та розшукових дій; 5) утворення спільних консультативно-дорадчих та експертних органів, рад, комісій;

– визначення поняття «методи взаємодії суб'єктів забезпечення кібербезпеки», під яким запропоновано розуміти сукупність способів та прийомів, які спрямовуються на налагодження ефективної взаємодії між суб'єктами, що уповноважені забезпечувати кібербезпеку в Україні;

Дістали подальшого розвитку:

– обґрунтування того, що кібербезпека є складним правовим явищем, у рамках якого діє механізм кіберзахисту, що являє собою систему заходів організаційного, нормативно-правового, воєнного, оперативного, технічного та іншого характеру;

– розуміння того, що з прийняттям Закону України «Про основні засади забезпечення кібербезпеки України» вперше з'явилось нормативне визначення поняття «кібербезпека», що, у свою чергу, дозволило виробити стратегію захисту кібербезпеки в адміністративно-правовому порядку та закріпити засади, суб'єктний склад механізму забезпечення вказаної категорії, що, безперечно, є позитивною новацією у сфері забезпечення кіберпростору та процесу використання інноваційних технологій;

– обґрунтування того, що питання юридичної відповідальності за порушення законодавства у сфері кібербезпеки України є недостатньо врегульованим, що, безперечно, можна вважати суттєвою прогалиною, яка сприяє зростанню рівня кіберзлочинності в нашій державі. Зокрема, питання притягнення правопорушника у сфері кібербезпеки до цивільної та адміністративної відповідальності регулюється цілою низкою нормативно-правових актів, у кожному з яких містяться різні підстави притягнення особи до відповідальності.

Така розгалуженість, у свою чергу, ускладнює застосування стягнень до винних осіб органами державної влади;

– характеристика методів взаємодії суб'єктів забезпечення кібербезпеки, до яких віднесено: 1) кадровий метод, який передбачає активне навчання представників одних органів специфіці роботи інших, що, у свою чергу, сприяє налагодженню ефективної взаємодії між відомствами; 2) метод взаємного інформаційного забезпечення, який полягає в наданні суб'єктами співпраці один одному всієї необхідної інформації для більш відкритої та ефективної взаємодії; 3) метод контролю, завдяки якому сторони (суб'єкти) взаємодії мають змогу здійснювати взаємне контролювання один одного під час спільної діяльності; 4) методи планування та прогнозування; 5) економічний метод, який передбачає створення відповідної матеріальної бази для проведення спільних заходів.

Структура та обсяг магістерської роботи. Магістерська складається зі вступу, трьох розділів, що містять 9 підрозділів, висновку, списку використаних джерел. Повний обсяг дипломної становить 112 сторінок. Список використаних джерел включає 113 найменувань та розміщений на 12 сторінках.

РОЗДІЛ І

Історичні, теоретико- методологічні засади забезпечення кібербезпеки України

1.1 Історико-правовий аналіз розвитку та становлення правового інституту кібербезпеки

Становленню кібербезпеки передувала ціла низка подій, що обумовили розвиток її виразу у правовій системі держави. Тому з метою більш повного розуміння інституту кібербезпеки та його правової природи необхідно проаналізувати не тільки поточний нормативний стан кібербезпеки на основі положень чинного законодавства, але й провести історико-правове дослідження його появи та становлення**.**

Поняттям «кібербезпека» описується належний стан роботи у сфері обробки інформації шляхом використання обчислювальної техніки, іншими словами, комп’ютерів. Однак, електронні пристрої самі по собі не становлять загрози легальному статусу зазначеного вище явища. Усе змінюється в тих випадках, коли мова йде не про самостійні комп’ютерні одиниці, а про цілу систему подібних пристроїв, за допомогою яких здійснюється обмін інформацією через світову мережу. За таких умов ми можемо говорити про існування нового інформаційного простору (кіберпростору), де реально мають місце ситуації фактичного порушення прав і свобод людей. В цьому контексті кібербезпека виступає у вигляді правового механізму забезпечення захисту прав та інтересів людей у кіберпросторі. Таким чином, історія його становлення та розвитку, як юридичного інституту, прямо пов’язана з еволюцією інформаційних технологій та Інтернету, який приніс людству можливість обробляти та обмінюватися

колосальною кількістю даних. Звідси виходить, що останні аспекти також підлягають науковому висвітленню у процесі дослідження ґенези кібербезпеки.

Перші обчислювальні машини почали з'являтися вже у середині XX століття, але на той час вони являли собою великі «калькулятори», спектр функцій яких був досить вузьким. Сучасний вид та призначення комп'ютери отримали лише у кінці XX на початку XXI століття, коли їх почали випускати для персонального користування у сфері бізнесу, навчання і навіть розваг. Паралельно з комп'ютерами розвивалась «всесвітня павутина», або ж Інтернет, як його прийнято називати на сьогоднішній день. Важливий крок в історії створення Інтернету було здійснено в 1965 році такими американськими вченими як Т. Меріл та Л. Дж. Робертс. Вони вперше здійснили підключення віддалених на значну відстань один від одного комп'ютерів, коли одна машина знаходилась у штаті Массачусетс, а інша — в Каліфорнії. Експеримент було проведено з використанням низько швидкісної телефонної лінії. В результаті цього було створено першу, хоча й невелику, широкомасштабну комп'ютерну мережу. Проведений експеримент приніс розуміння того, що загальні комп'ютери можуть працювати разом, виконувати програми і за необхідності вилучати дані на видаленому комп'ютері, проте, система комутованих телефонних ліній для цього абсолютно не підходила [93].

З цього моменту починається стрімкий науковий розвиток комп'ютерних мереж, який привів до винаходу на початку 90-х років спеціального програмного забезпечення — «WorldWideWeb» («WWW» — всесвітня павутина). У квітні 1993 року було здійснено випуск вихідного коду WorldWideWeb в суспільне надбання, що означало, що кожен може його використовувати і створювати на його основі програмне забезпечення без ліцензійних відрахувань. В цьому ж році Національний центр прикладних систем для суперкомп'ютерів (National Center for Supercomputing Applications) випустив програму Mosaic, яка стала одним з перших браузерів. Спочатку вона була доступна тільки для машин під

управлінням операційної системи Unix і у формі вихідного коду, але вже в грудні 1993 Mosaic поставлявся з установниками (інсталяторами) для операційних систем Apple Macintosh і Microsoft Windows. Mosaic дуже швидко ставав популярним, а разом з ним і всесвітня павутина [93].

На сьогоднішній день Інтернет є невід'ємною частиною життєдіяльності людини, адже він використовується у багатьох сферах, зокрема: оборонній, банківській, правоохоронній, тощо. Але подібний розвиток всесвітньої павутини також призвів до появи негативних наслідків, одним з яких є кіберправопорушення. Безмежність інформаційного простору дає можливість окремим суб'єктам здійснювати всілякі маніпулювання даними з метою, наприклад, викрадення певної інформації, порушення роботи суб'єктів влади і т. ін. Саме цей аспект обумовив розвиток правового інституту кібербезпеки як механізму підтримки порядку у кіберпросторі, тобто під час використання можливостей всесвітньої павутини. Розвиток останнього відбувався паралельно еволюції інформаційних технологій. При цьому, на рівні національного законодавства інститут кібербезпеки є новелою, що обумовлено відсутністю належного нормативного закріплення. З іншого боку, історичні етапи його становлення можна дослідити на основі норм багатьох міжнародних актів, деякі з яких ратифіковано в Україні.

Найпершим в історії законодавчим актом, котрий регулював забезпечення кібербезпеки у кіберпросторі, був «The Computer Fraud and Abuse Act» (Закон про боротьбу з комп'ютерними шахрайством та комп'ютерними зловживанням), прийнятий в 1986 році у Сполучених Штатах Америки [111; 36, с. 146]. Даний акт, по суті, визнавав проблему можливості вчинення неправомірних дій у інформаційній сфері, що дало поштовх до розвитку інституту кібербезпеки. Закон закріпив відповідальність за несанкціоноване втручання у роботу комп'ютерних систем чи викрадення інформації з них. Крім цього, актом передбачено санкції для осіб, які вчиняють дії подібного характеру.

Значним внеском у розвиток інституту кібербезпеки стало прийняття Радою Європи у 1989 році Рекомендації R(89), якою було закріплено:

– по-перше, чіткий перелік дій, які набувають ознак кіберправопорушень;

– по-друге, головні аспекти розробки та побудови єдиної стратегії протидії негативним діям у кіберпросторі [108].

Положення вказаного акту фактично запустили механізм еволюції інституту безпеки у сфері використання комп'ютерних технологій з метою обміну даними. Розвиток цього явища в наступні роки до сьогоднішнього дня проходив на рівні як міжнародного права, так і національного, яке приймалося під впливом світового законодавства.

Так, в 2000 році у Відні було прийнято Віденську декларацію про злочинність та правосуддя: відповіді на виклики XXI століття (ООН). Звичайно, цей документ не визначав та не закріплював норми стосовно інституту кібербезпеки у тому вигляді, в якому він існує сьогодні. Однак, на основі положень декларації було прийнято рішення розробити орієнтовані на конкретні дії програмні рекомендації щодо попередження злочинів, пов'язаних з використанням комп'ютерів, і боротьби з ними. Тобто вже у той час порушення у сфері використання інноваційних технологій характеризувалися суспільною небезпекою, що дозволило говорити про формування кіберзлочинності. Декларація також поклала обов'язок на усіх держав–членів Організації Об'єднаних Націй (далі — ООН) працювати в напрямку зміцнення їх можливостей щодо попередження, розслідування і переслідування злочинів, пов'язаних з використанням провідних технологій і комп'ютерів [17]. У тому ж році Європейським Союзом (далі — ЄС) приймається Конвенція про взаємодопомогу в кримінальних справах між членами ЄС, в рамках якої було закріплено процесуальні особливості та нові механізми взаємодії між державами з приводу протидії кіберправопорушенням [20]. Підсумовуючи викладені вище факти, ми можемо стверджувати, що видання двох останніх міжнародних актів фактично змусило світову спільноту

поглянути на явище кібербезпеки як на самостійний юридичний осередок, а не елемент системи того чи іншого механізму протидії правопорушенням у сфері використання комп'ютерних технологій.

В подальшому кібербезпека характеризувалась як окремий правовий інститут, в рамках якого здійснюється розробка стратегії подолання анти суспільних дій у кіберпросторі. Ця теза підтверджується положеннями Резолюції Генеральної Асамблеї ООН щодо створення глобальної культури кібербезпеки, прийнятої в 2002 році. В даному акті окреслюються ключові шляхи створення глобальної культури кібербезпеки, а також пояснюються особливі моменти механізму забезпечення цього інституту, наприклад:

– необхідність визнання та охорони правового явища кібербезпеки обумовлено стрімким підвищенням числа залучених до кіберпростору країн;

– ефективна кібербезпека досягається не лише прямою діяльністю державних або правоохоронних органів, направленою на припинення відповідних протиправних діянь, але й превентивними заходами, крім цього, даний процес повинен підтримуватися суспільством;

– державні органи, в свою чергу, повинні: постійно підвищувати рівень безпеки у сфері використання інформаційних технологій та аналізувати фактори, які на нього негативно впливають [19; 44, с. 105]. Ключовою перевагою резолюції є те, що цей документ закріпив конкретні вимоги до суб'єктів кібербезпеки, які останні повинні неухильно виконувати, адже від цього залежить реальний стан правового забезпечення інституту. Відповідно до положень акту, існує дев'ять головних вимог:

а) обізнаність, тобто суб'єкти повинні бути інформовані про необхідності безпеки інформаційних систем і мереж і про те, що вони можуть зробити для підвищення безпеки;

б) відповідальність, за безпеку інформаційних систем та мереж згідно з роллю кожного з них;

в) реагування, тобто обов'язковість вживання своєчасних і спільних заходів щодо попередження інцидентів, які зачіпають безпеку, їх виявлення і реагування на них. Суб'єкти повинні обмінюватися в належних випадках інформацією про загрози та фактори уразливості і вводити процедури, що передбачають оперативну і ефективну співпрацю в справі попередження таких інцидентів, тощо;

г) етика, що значить необхідність врахування законних інтересів інших, оскільки інформаційні системи і мережі проникли в усі куточки сучасного суспільства;

г) демократія, яка проявляється у діяльності із забезпечення цінностей, які визнаються демократичним суспільством, включаючи свободу обміну думками та ідеями, вільний потік інформації, конфіденційність інформації та комунікації, належний захист інформації особистого характеру, відкритість і гласність;

д) оцінка ризику, яка: дозволяє виявляти загрози та фактори уразливості; має досить широку базу, щоб охопити такі ключові внутрішні та зовнішні аспекти як технологія, фізичні і людські фактори, застосування методики і послуги третіх осіб, що позначається на безпеці; дає можливість визначити допустимий ступінь ризику; допомагає вибрати належні інструменти контролю, що дозволяють регулювати ризик потенційного збитку інформаційним системам і мережам з урахуванням характеру та значущості інформації, що захищається;

е) проектування і впровадження засобів забезпечення безпеки;

є) управління забезпеченням безпеки, тобто здійснення комплексного підходу до управління забезпеченням безпеки, спираючись на динамічну оцінку ризику, що охоплює всі рівні діяльності учасників і всі аспекти їх операцій;

ж) переоцінка — учасники повинні піддавати питання безпеки інформаційних систем і мереж огляду і повторній оцінці та вносити належні зміни в політику,

практику, заходи і процедури забезпечення безпеки, враховуючи при цьому появу нових, зміну колишніх загроз і чинників уразливості [78].

Представлені вимоги увійшли до положень Женевської декларації принципів побудови інформаційного суспільства, прийнятої на Всесвітньому саміті з питань інформаційного суспільства 12 грудня 2003 року. У статті 35 частини 5 глави в декларації зазначена необхідність формування, розвитку і впровадження глобальної культури кібербезпеки у співпраці з усіма зацікавленими сторонами і компетентними міжнародними організаціями. Такі дії повинні спиратися на розширювану міжнародну співпрацю. В рамках цієї глобальної культури кібербезпеки важливо підвищувати безпеку і забезпечувати захист даних і недоторканність приватного життя, розширюючи при цьому доступ і масштаб торгових операцій. Крім того, необхідно брати до уваги рівень соціально-економічного розвитку кожної країни і враховувати пов’язані з орієнтацією на розвиток аспекти інформаційного суспільства [18].

Слід відмітити, паралельно розвитку у світовому законодавстві ґенеза правового інституту кібербезпеки також мала місце на національному рівні. Звичайно, на початковому етапі становлення України як незалежної держави самого поняття «кібербезпека» у нормативних документах країни фактично не існувало. Однак, певні основи інституту забезпечення інформаційної безпеки у різних сферах життєдіяльності населення країни вже було імплементовано у національне законодавство з урахування міжнародно-правових стандартів у цій галузі.

Розвиток правових засад організації кібербезпеки в Україні знайшов відображення в наступних нормативних актах, а саме Законах України «Про Концепцію Національної програми інформатизації» від 4 лютого 1998 року, «Про Національну програму інформатизації» від 2 жовтня 1992 року, «Про захист інформації в інформаційно-телекомунікаційних системах» від 5 липня 1994 року,

«Про науково-технічну інформацію» від 25 червня 1993 року, «Про охорону прав на топографії інтегральних мікросистем» від 5 листопада 1997 року, тощо.

Відповідні нормативні зрушення у напрямку розвитку системи забезпечення інституту кібербезпеки також простежуються на підзаконному рівні. Зокрема, протягом 2000, 2001 рр. Президентом України було видано Укази «Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України» та «Про заходи розвитку національної складової глобальної інформаційної мережі Internet та забезпечення широкого доступу до цієї мережі в Україні». Положення даних актів визначили вектор розвитку діяльності країни у сфері організації інформаційної безпеки, а також на нормативному рівні закріпили особливості використання інноваційної на той час мережі Internet та механізм її державної підтримки, яка мала прояви у :

– створенні у найкоротші строки належних економічних, правових, технічних та інших умов для забезпечення широкого доступу громадян, органів державної влади та органів місцевого самоврядування, суб'єктів підприємницької діяльності до мережі Інтернет;

– розвитку та впровадженні сучасних комп'ютерних інформаційних технологій у системі державного управління, фінансовій сфері, підприємницькій діяльності, освіті, наданні медичної та правової допомоги та інших сферах;

– вирішенні завдань щодо гарантування інформаційної безпеки держави та недопущенні поширення інформації, розповсюдження якої заборонено відповідно до законодавства, тощо [7].

Найбільшим «проривом» вітчизняного законодавства у сфері забезпечення кібербезпеки стала ратифікація в 2005 році Конвенції про кіберзлочинність, прийнятої Радою Європи. Відповідно до Преамбули, метою створення документу стала необхідність 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, 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 [16]. У конвенції також представлено список протиправних дій, поділених на групи, які, на думку міжнародної спільноти, становлять небезпеку процесу обробки та обміну інформацією у комп'ютерних системах, наприклад:

1)правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ, нелегальне перехоплення, втручання у дані, зловживання пристроями);

2)правопорушення, пов'язані з комп'ютерами (підробка, пов'язана з комп'ютерами, шахрайство);

3) правопорушення, пов'язані зі змістом (розповсюдження дитячої порнографії);

4) правопорушення, пов'язані з порушенням авторських та суміжних прав [16].

Інші положення конвенції регулюють процедурні особливості міжнародної взаємодії в процесі боротьби із кібернетичними правопорушеннями, а також містять вихідні принципи такої діяльності. Ратифікація цього документу обумовила його включення у структуру джерел правової системи України.

Останні роки характеризуються новим витком еволюції інституту кібербезпеки, який було суттєво модифіковано нормами чинного законодавства. Перейнявши досвід зарубіжних країн у сфері регулювання досліджуваного явища, наша держава створила юридичні основи його регулювання. Так, у 2016 році було видано Указ Президента, який ввів у дію рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України». Інноваційність даного акту полягає у тому, що саме в його положеннях вперше було використано термін «кібербезпека».

Згідно із загальними положеннями стратегії, стрімкий розвиток інформаційних технологій поступово трансформує світ. Відкритий та вільний кіберпростір розширює свободу і можливості людей, збагачує суспільство, створює новий глобальний інтерактивний ринок ідей, досліджень та інновацій, стимулює відповідальну та ефективну роботу влади і активне залучення громадян до управління державою та вирішення питань місцевого значення, забезпечує публічність та прозорість влади, сприяє запобіганню корупції. Водночас, переваги сучасного цифрового світу та розвиток інформаційних технологій обумовили виникнення нових загроз національній та міжнародній безпеці. Поряд із інцидентами природного (ненавмисного) походження зростає кількість та потужність кібератак, вмотивованих інтересами окремих держав, груп та осіб [15].

Отже, Стратегією [15] чітко визначається наявна проблема порушення прав і свобод громадян України у кіберпросторі, у зв'язку з чим виникає необхідність, по-перше, запровадження належного механізму правового регулювання цієї сфери, а по-друге, забезпечення охорони суспільного інтересу від протиправних посягань всередині неї. Цікавим є той факт, що даний аспекти було легалізовано на нормативному рівні, адже визначеною метою Стратегії є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави [15]. Нормативно-правовий акт також закріплює принципи, на яких ґрунтується діяльність із досягнення та забезпечення поставленої мети. В даному разі слід наголосити, що в історії розвитку кібербезпеки на національному рівні засади його ніколи не визначались. Тому Стратегія [15] певним чином посилила легальний статус інституту, надавши йому вихідні принципи, до яких віднесено такі:

– верховенство права і повага до прав та свобод людини і громадянина [15];

– забезпечення національних інтересів України [15];

– відкритість, доступність, стабільність та захищеність кіберпростору [15];

–державно-приватне партнерство, широка співпраця з громадянським суспільством у сфері забезпечення кібербезпеки та кіберзахисту [15];

– пропорційність та адекватність заходів кіберзахисту реальним та потенційним ризикам [15];

– пріоритетність запобіжних заходів [15];

– невідворотність покарання за вчинення кіберзлочинів;

– пріоритетність розвитку та підтримки вітчизняного наукового, науково-технічного та виробничого потенціалу [15];

– міжнародне співробітництво 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 протиправних та воєнних цілях [15];

– забезпечення демократичного цивільного контролю над утвореними відповідно до законів України військовими формуваннями та правоохоронними органами держави, що діють у сфері кібербезпеки [15]. Ще одним вагомими надбанням Стратегії [15] є те, що в її положеннях кібербезпека хоча і визнається правовим інститутом, однак, напрямки її забезпечення включають в себе не тільки суто юридичні елементи, а й також політичні, економічні, організаційно-технічні, тощо. Наприклад, відповідно до частини 4 Стратегії розвиток безпечного, стабільного і надійного кіберпростору має полягати насамперед у:

– виробленні і оперативній адаптації державної політики у сфері кібербезпеки, спрямованої на розвиток кіберпростору, досягненні сумісності з відповідними стандартами ЄС та НАТО;

– створенні вітчизняної нормативно-правової та термінологічної бази, гармонізації нормативних документів у сфері електронних комунікацій, захисту інформації, інформаційної та кібербезпеки відповідно до міжнародних стандартів і стандартів ЄС та НАТО;

– формуванні конкурентного середовища у сфері електронних комунікацій, наданні послуг із захисту інформації та кіберзахисту;

– розвитку технологій кіберзахисту засобів рухомого зв'язку, забезпеченні апаратної, контентної безпеки, безпеки додатків та сервісів зв'язку;

– залученні експертного потенціалу наукових установ, професійних та громадських об'єднань до підготовки проектів концептуальних документів у сфері кібербезпеки;

– підвищенні цифрової грамотності громадян та культури безпекового поводження в кіберпросторі, комплексних знань, навичок і здібностей, необхідних для підтримки цілей кібербезпеки, впровадженні державних і громадських проектів підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту;

– проведенні навчань щодо надзвичайних ситуацій та інцидентів у кіберпросторі;

– розвитку та удосконаленні системи державного контролю за станом захисту інформації, а також системи незалежного аудиту інформаційної безпеки, запровадженні кращих світових практик і міжнародних стандартів з питань кібербезпеки та кіберзахисту;

– розвитку інфраструктури електронних комунікацій, включаючи широкосмуговий доступ до мережі Інтернет, цифрове та інтерактивне телебачення;

– розвитку мережі команд реагування на комп'ютерні надзвичайні події;

– створенні системи своєчасного виявлення, запобігання та нейтралізації кіберзагроз, у тому числі із залученням волонтерських організацій;

– розвитку та вдосконаленні системи технічного і криптографічного захисту інформації;

– розвитку міжнародного співробітництва у сфері забезпечення кібербезпеки, підтримці міжнародних ініціатив у сфері кібербезпеки, які відповідають

національним інтересам України, поглибленні співпраці 50 України з ЄС та НАТО для посилення потенціалу України у сфері кібербезпеки, участі у заходах зі зміцнення довіри у кіберпросторі;

– створенні умов для впровадження в Україні сучасних технологій кіберзахисту [15]. Незважаючи на доцільність та пріоритетність прийнятої Стратегії [15], інформативність цього підзаконного нормативного акту доволі низька. Зокрема, у його положеннях досить часто терміни «кіберзахист» та «кібербезпека» ототожнюються, що не дає змогу зрозуміти аспекти унікальності даного інституту. Крім цього, вагомий недолік полягає у відсутності в положеннях Стратегії дефініцій таких понять як «кіберпростір», «кіберзлочин», «кіберзагроза», тощо. Іншими словами, нормативний акт створює механізм забезпечення інституту, сутність якого реально залишається незрозумілою.

З іншого боку, Стратегія [15] показує вінець розвитку інституту кібербезпеки, еволюція якого здійснювалась протягом великого відрізку часу. В свою чергу, недоліки вказаного нормативного акту фактично були усунені новим Законом України «Про основні засади забезпечення кібербезпеки в Україні». Його головною метою є визначення правових та організаційних засад державної політики, спрямованої на захист життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі, основні принципи та напрями забезпечення кібербезпеки України [14]. Окрім стратегічно важливої мети, даний нормативний документ характеризується рядом інших особливостей:

– по-перше, закон фактично легалізує усі поняття з префіксом «кібер», які до цього часу існували переважно у наукових роботах вчених чи положеннях міжнародних нормативно-правових актів;

– по-друге, закон на законодавчому рівні закріплює принципи, основні напрямки забезпечення та об’єкти кібербезпеки України;

– по-третє, нормативний документ уточнює поняття суб'єктів механізму забезпечення кібербезпеки, а також більш детально представляє їх повноваження у цій сфері.

Отже, провівши історико-правовий аналіз розвитку і становлення правового інституту кібербезпеки, нами було розглянуто велику кількість нормативних актів як міжнародного, так і національного права. Це дозволило виділити головну особливість ґенези досліджуваного явища — його стійкий взаємозв'язок із еволюцією комп'ютерних технологій. Питання забезпечення кібербезпеки набуло вагомості через підвищення рівня обміну інформацією між різними суб'єктами за допомогою інноваційних технологій та мережі Інтернет. Стрімкий технологічний прогрес призвів до появи осіб, які умисно використовували кіберпростір задля забезпечення власних інтересів, тим самим порушуючи інтереси звичайних користувачів, якими на сьогоднішній день є усі громадяни.

Основний розвиток кібербезпеки здійснювався у нормативній площині Європи, адже підґрунтя інституту було закладено актами ЄС. На рівні національного законодавства інститут почав розвиватися на початку XXI століття. Як ми побачили, його становленню передувало прийняття цілої низки законодавчих актів, які прямо не встановлювали правовий статус кібербезпеки, не кажучи про механізм її забезпечення. Найвизначнішим кроком до імплементації у правову систему України досліджуваного інституту стала ратифікація Конвенції Ради Європи про кіберзлочинність у 2005 році. Цей документ визначив ключові типи правопорушень, що можуть вчинятися у кіберпросторі, а також процедурні особливості міжнародної співпраці у боротьбі з ними.

В останні часи інститут кібербезпеки набув стрімкого розвитку, що пов'язано, на нашу думку, зі зміною зовнішньополітичного вектору держави. Упровадження європейських стандартів різних галузей суспільного життя в країні потребує підвищення рівня інформаційної захищеності. Тому у 2016 році

Указом Президента було введено в дію рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України», яке визначило суб'єктів, загрози і напрямки забезпечення кібербезпеки в державі, та прийнято Закон України «Про основні засади забезпечення кібербезпеки України». Крім цього, на сьогоднішній день розвиток досліджуваного інституту все ще триває, тому нам слід очікувати прийняття низки нових законодавчих актів у цій сфері.

1.2 Поняття та особливості кібербезпеки як об'єкта адміністративно-правової охорони

Починаючи з моменту надбання Україною незалежності, вектор державного розвитку було спрямовано на технологічний прогрес та імплементацію у людське життя інформаційних технологій, які на сьогоднішній день суттєво полегшують процеси пошуку та обміну інформацією. Велике значення процес «електронного» розвитку відіграє на державному рівні, адже запровадження новітніх технологій відкриває величезні можливості у сфері державо будування. Наразі практично усі органи влади, що існують в Україні, так чи інакше використовують новітні технології, що фактично спричинило перенесення процесу обміну, обробки та пошуку інформації у електронний простір. Нарівні з цим, «цифрова революція» також має низку негативних аспектів, одним з яких є низький рівень кібербезпеки. Ця проблематика неодноразово підіймалася у роботах науковців різних галузей знань. Не є виключенням правова сфера, так як саме у її рамках було розроблено головні механізми охорони кібербезпеки. Вивчення даного питання є пріоритетним напрямком роботи для правників адміністративного, кримінального, цивільного та інформаційного права, адже кібербезпека у вигляді об'єкта правової охорони безпосередньо входить в поле інтересів держави. При

цьому, механізми її забезпечення не є однорідними між собою, так як регулюються нормами різних галузей права.

Найбільш доцільним та дієвим «буфером» правової охорони зазначеного об’єкта є адміністративно-правовий, адже він походить від однойменної юридичної галузі, в рамках якої існує державний примус в його найбільш початковій формі. Іншими словами, дослідження кібербезпеки як об’єкта адміністративно-правової охорони дозволяє визначити рівень правової регламентації її захищеності.

Слід наголосити, що представлена у підрозділі проблематика є комплексною, тобто складається з декількох питань, які потребують детального аналізу таких понять як «кібербезпека» та «адміністративно-правова охорона». Адже відсутність законодавчої дефініції окремих понять перешкоджає аналізу правових інститутів, які вони окреслюють, і, як наслідок, визначенню особливостей їх практичного застосування. Таким чином, визначення поняття та особливостей кібербезпеки як об’єкта адміністративно-правової охорони має не тільки суто теоретичне значення, але і є практичним.

Тож безпосередній розгляд кібербезпеки як об’єкта адміністративно-правової охорони слід починати із визначення поняття та ключових аспектів адміністративно-правової охорони як одного з найбільш значних та функціональних механізмів забезпечення кібербезпеки. Як і будь-яке інше правове явище в державі, основні засади забезпечення кібербезпеки знаходять своє закріплення в нормах Конституції України, тому що цей нормативний акт є основним джерелом національної правової системи. Так, у статті 3 Конституції вказується, що 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. Тобто

наявність адміністративно-правового механізму охорони кібербезпеки та інших подібних об’єктів є проявом виконання державою своїх обов’язків з приводу забезпечення життєдіяльності населення країни [1].

Повертаючись безпосередньо до аналізу адміністративно-правової охорони, необхідно відмітити, що сутність цього терміну розглядається переважно у сукупності з тим благом, на яке спрямовано дію механізму. Іншими словами, в науковій літературі можна зустріти такі терміни як «адміністративно-правова охорона майнових та немайнових прав власності», «адміністративно-правова охорона прав інтелектуальної власності», «адміністративно-правова охорона надр та вод», тощо. Однак, це не свідчить про те, що термін «адміністративно-правова охорона» не розглядається самостійно у сучасному науковому середовищі. Більш того, він характеризується лінгвістичними особливостями.

Термін «адміністративно-правова охорона» складається з двох самостійних понять: «адміністративно-правовий» та «охорона», які мають окремі дефініції. Так, у загальному вигляді під категорією «охороняти» розуміють: оберігати від небезпеки кого-, що-небудь, забезпечувати від загрози нападу, замаху і т. ін.; стояти на варті біля кого-, чого-небудь; вартувати, стерегти; оберігати від руйнування, знищення, завдання шкоди і т. ін.; захищати від чого-небудь [80; 68, с. 183]. Слід наголосити, що досить часто термін «охорона» ототожнюють з терміном «захист», підтвердження чого можна знайти у словнику С. І. Ожегова, відповідно до якого єдність у розумінні «захисту» і «охорони» витікає з пояснення змісту слова «захищати», що, відповідно до С. І. Ожегова, означає охорону, спрямовану на захист від замахів, від ворожих дій та небезпеки [82; 85, с. 119]. Даний аспект нерідко викликає суперечності між вченими з приводу того, чи є інститут адміністративно-правового захисту тотожним інституту адміністративно-правової охорони. Спираючись на дослідження лінгвістів, ми можемо стверджувати, що вказані явища є абсолютно ідентичними, адже відмінність полягає лише у кінцевих термінах, суть яких є однаковою. Різниця є

лише у способі впливу, адже захист вимагає активної форми поведінки, а охорона — пасивної, при цьому мета у обох випадках є тотожною.

Що ж стосується поняття «адміністративно-правовий», то відповідно до Великого тлумачного словника сучасної української мови термін «адмініструвати» означає керувати установою, організацією, підприємством; керувати бюрократично, за допомогою наказів і розпоряджень замість конкретного керівництва [34, с. 12]. Зазначений термін, по-перше, показує приналежність певного інституту чи механізму до галузі адміністративного права, а, по-друге, дає розуміння того, що відповідні дії здійснюються у адміністративному порядку. Таким чином, в найбільш загальному вигляді адміністративно-правова охорона — це захист певних правовідносин у адміністративному порядку. Однак, як ми розуміємо, сутність цього юридичного явища є дещо глибшою, тому розкрити її повністю виключно на лінгвістичному рівні неможливо. Для цього необхідно також скористатися напрацюваннями вчених–адміністраторів.

Наразі існує велика кількість наукових поглядів на проблематику визначення поняття «адміністративно-правова охорона», що пов’язано із тим, що має місце фактична відсутність його дефініції у законодавчих актах. В. В. Галунько у своїх наукових працях визначає, що 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 [22, с. 242–247]. Дещо інший погляд на проблематику має С. О. Мосьондз, на думку якого адміністративно-правова охорона вирізняється гуманністю, спрямованістю на переконання населення в доцільності й справедливості заходів, здійснюваних державою, об’єктивній

необхідності тих або інших загальнообов'язкових правил. Вона пов'язана із масштабним використанням перевірених практикою засобів організаційної, масово-політичної та виховної роботи, активним формуванням в суспільній свідомості нетерпимого ставлення до антисоціальних проявів [78, с. 106]. Доволі цікавою є думка О. І. Харитонова, який зосереджує увагу на тому, що явище адміністративно-правової охорони являє собою окремий правовий інститут. Він 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 [102, с. 38]. Отже, підсумовуючи наукові погляди, ми можемо зробити висновок про те, що адміністративно-правова охорона — це системне явище адміністративного права, сутність якого полягає у діяльності публічних органів, спрямованій на забезпечення прав громадян або підтримання відповідного легального режиму в тій чи іншій сфері суспільного буття. Водночас, адміністративно-правова охорона, на нашу думку, трансформується у правовий інститут, коли її застосовують щодо конкретних об'єктів. Це пояснюється тим, що за подібних умов адміністративно-правова охорона перестає бути абстрактним явищем та набуває конкретного механізму реалізації, який визначається окремою групою правових норм. Тобто ми говоримо про строго внормовану, засновану на правових принципах діяльність держави в особі окремих органів влади, яку спрямовану на підтримку об'єктів права: інтелектуальної та промислової власності, надр та вод, окремих правомочностей та законних інтересів громадян, тощо. Наприклад, адміністративно-правовою охороною права власності

визнається імперативно-владна діяльність суб'єктів публічного управління із захисту прав усіх суб'єктів права власності (осіб, які здійснюють управління нею) від протиправних посягань і широкого загалу осіб від майна підвищеної небезпеки, з нормативно прописаною можливістю застосування до порушників режиму власності засобів державного впливу [73, с. 239]. Доволі лаконічно та максимально точно особливості адміністративно-правової охорони конкретного об'єкта (інтелектуальної власності) виділено Є. В. Юрковою, яка зазначила, що інститут охорони інтелектуальної власності відноситься до спеціальної юрисдикційної форми діяльності окремих суб'єктів публічного управління, зокрема: Міністерства внутрішніх справ України, Антимонопольного комітету України, тощо [105, с. 710].

Таким чином, ми визначились із тим, що адміністративно-правова охорона певного об'єкта є правовим інститутом. Незважаючи на відсутність єдиного наукового погляду на цю проблематику, вона має доволі широке нормативне підґрунтя, тобто відповідні правові джерела. Найбільше коло норм, спрямованих на охорону певних суспільних відносин, закріплено у Кодексі України про адміністративні правопорушення (далі — КУпАП). Стаття 1 вказаного нормативно-правового акту [2] закріплює, що завданнями кодексу є охорона прав і свобод громадян, власності, конституційного ладу України, прав і законних інтересів підприємств, установ і організацій, встановленого правопорядку, зміцнення законності, запобігання правопорушенням, виховання громадян у дусі точного і неухильного додержання Конституції і законів України, поваги до прав, честі і гідності інших громадян, до правил співжиття, сумлінного виконання своїх обов'язків, відповідальності перед суспільством [2]. Інші положення КУпАП спрямовані на те, щоб забезпечити охорону відповідних об'єктів, що є пріоритетом діяльності державних органів влади, тобто адміністративно-правова охорона є інститутом, який ґрунтується на принципах влади, превалюванні імперативного методу регулювання, ієрархічності, тощо. Наприклад, у статті 6

КУпАП вказується, що органи виконавчої влади та органи місцевого самоврядування, громадські організації, трудові колективи розробляють і здійснюють заходи, спрямовані на запобігання адміністративним правопорушенням, виявлення й усунення причин та умов, які сприяють їх вчиненню, на виховання громадян у дусі високої свідомості і дисципліни, суворого додержання законів України [2]. Органи місцевого самоврядування, місцеві державні адміністрації, забезпечуючи відповідно до Конституції України додержання законів, охорону державного і громадського порядку, прав громадян, координують на своїй території роботу всіх державних і громадських органів по запобіганню адміністративним правопорушенням, керують діяльністю адміністративних комісій та інших підзвітних їм органів, покликаних вести боротьбу з адміністративними правопорушеннями [2].

Підсумовуючи усі наведені вище відомості, ми можемо стверджувати, що адміністративно-правова охорона сама по собі є доволі цікавим явищем. Однак, метою підрозділу є розгляд інституту адміністративного забезпечення конкретного об’єкта — кібербезпеки. Останнє явище також підлягає самостійному аналізу, так як воно характеризується великою кількістю особливостей.

На сьогодні термін «кібербезпека» активно обговорюється у науковій літературі. Це дає нам змогу звернутися до напрацювань вчених, які розглядали цей об’єкт та його особливості. Кібербезпека є абстрактним поняттям, що виникло у сфері експлуатації комп’ютерної техніки з метою обміну інформацією у віртуальному просторі. Окрім цього, віртуальний простір не має меж і кордонів, в ньому будь-хто набуває широких можливостей у сфері його використання. Саме цей аспект робить віртуальний або ж кіберпростір, як його частіше називають, надзвичайно зручним середовищем для здійснення протиправної діяльності. Сюди можна віднести правопорушення і злочини в різних сферах господарювання та управління, хакерські атаки на урядові сайти та банківські

бази даних, інші дії, спрямовані на порушення суспільно-політичного ладу [60, с. 96]. За даних умов кіберпростір слід розглядати як високорозвинену модель об'єктивної реальності, в якій відомості щодо осіб, предметів, фактів, подій, явищ і процесів:

– подаються в математичному, символічному або в будь-якому іншому вигляді;

– розміщуються в пам'яті будь-якого фізичного пристрою, спеціально призначеного для зберігання, обробки й передавання інформації;

– перебувають у постійному русі по сукупності ІТ-систем і мереж [54, с. 8].

Необхідно відмітити, що визначення поняття та особливостей кіберпростору є принципово важливим аспектом нашого дослідження, адже на цьому ґрунтується бачення кібербезпеки. В даному разі цілком логічно було б зазначити, що кібербезпека — це певний стан кіберпростору, який характеризується фактичною відсутністю правопорушень, однак, представлений термін має дещо більший зміст. В. Н. Фурашев визначає кібербезпеку як стан, здібності людини, суспільства і держави щодо запобігання та уникнення спрямованого, в першу чергу — несвідомого, негативного впливу (управління) інформації [25; 202, с. 168]. 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 [45, с. 110]. Схожої думки дотримується О. А. Баранов, який зазначає, що кібербезпека — це деякий стан систем, за якого нейтралізуються загрози доступності, цілісності або конфіденційності даних, що циркулюють в інформаційних системах [25; 59, с. 38]. На нашу думку, останні погляди не зовсім точно відображають сутність досліджуваного явища, адже не зовсім зрозуміло, про які саме важливі інтереси людини і громадянина та системи йдеться мова.

Більш повним є визначення поняття «кібербезпека», яке запропоноване у підручнику В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко та С. В. Толюпа. На їх

думку, кібербезпеку можна визначити як стан захищеності кіберпростору держави в цілому або окремих об’єктів її інфраструктури від ризику стороннього кібервпливу, за якого забезпечуються їх сталий розвиток, а також своєчасне виявлення, запобігання й нейтралізація реальних і потенційних викликів, кібернетичних втручань і загроз особистим, корпоративним і/або національним інтересам [33, с. 15]. Підтримка та забезпечення подібного стану здійснюються завдяки сукупності спеціальних захисних дій, реалізаторами яких є окремі органи влади.

Найбільш змістовним ми вважаємо визначення поняття «кібербезпека» О. Г. Корченко, адже він розкриває сутність кібербезпеки через призму ключових ознак цього явища. 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 [63, с. 7] 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 [63, с. 41]. Іншою особливістю даного визначення є те, що воно подано з урахування технічної сторони явища кібербезпеки, в рамках якого здійснюється використання електронної техніки.

Вказані наукові погляди знайшли свій прояв у Законі України «Про основні засади забезпечення кібербезпеки України». У статті 1 закону зазначається, що кібербезпека — це захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [10]. Ми вважаємо, що наведене поняття хоча і є лаконічним, однак, не відображає усю

сутність явища кібербезпеки. Хоча, безперечно, нормативне визначення поняття є позитивним фактором для правової системи нашої держави

Отже, на підставі аналізу понять «адміністративно-правова охорона» та «кібербезпека» вбачається, що «адміністративно-правова охорона у сфері забезпечення кібербезпеки» — це діяльність відповідних державних органів, що здійснюється на засадах імперативності та ієрархічності і направлена на підтримання та забезпечення належного стану захищеності прав, інтересів та інформації відповідних суб'єктів у кіберпросторі. Головною особливістю адміністративно-правового забезпечення кібербезпеки є те, що воно здійснюється в адміністративному порядку, тобто в контексті адміністративно-правових відносин. При цьому, сутність даного інституту є доволі широкою і не обмежується суто захисними нормами та процедурами. Зокрема, доволі часто адміністративно-правова охорона будь-якого об'єкта сприймається як суто «каральний» інститут, що складається з положень Кодексу України про адміністративні правопорушення. Однак, норми цього закону закріплюють адміністративні стягнення для суб'єктів, які порушують легальний стан певного об'єкта, в нашому випадку — кібербезпеки.

Внаслідок здійснення ними правопорушень щодо останніх використовуються норми юридичної відповідальності, метою яких є обмеження прав і свобод. Застосування подібних юридичних механізмів є крайнім заходом, який може мати місце лише за умови вчинення правопорушень, об'єктом яких є правовідносини у сфері кібербезпеки. Інститут адміністративно-правової охорони кібербезпеки в даному разі має набагато ширшу сферу дії, адже забезпечення тих чи інших правовідносин в адміністративному порядку проявляється не тільки у покаранні винних осіб, які їх порушили, а й у діяльності органів влади з метою недопущення виникнення подібних ситуацій та інших негативних факторів.

Нормативне підґрунтя забезпечення кібербезпеки закріплено у Законі України «Про основні засади забезпечення кібербезпеки в Україні», а також в інших положеннях законодавства. Напрямки забезпечення кібербезпеки, що реалізуються у роботі різних органів державної влади, також мають певний нормативно-правовий вираз. Так, у ст. 10 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» розкривається роль державних органів у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. В законі зазначено, що спеціальний центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації має наступні повноваження:

– розробляє пропозиції щодо державної політики у сфері захисту інформації та забезпечує її реалізацію в межах своєї компетенції;

– визначає вимоги та порядок створення комплексної системи захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;

– організовує проведення державної експертизи комплексних систем захисту інформації, експертизи та підтвердження відповідності засобів технічного і криптографічного захисту інформації;

– здійснює контроль за забезпеченням захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;

– здійснює заходи щодо виявлення загрози державним інформаційним ресурсам від несанкціонованих дій в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах та дає рекомендації з питань запобігання такій загрозі [6].

Необхідно також відмітити діяльність Національного банку України (далі — НБУ) у сфері забезпечення кібербезпеки. Робота даного органу також входить до

сфери національної безпеки нашої держави, адже НБУ є центральним банком України, особливим центральним органом державного управління, юридичний статус, завдання, функції, повноваження і принципи організації якого визначаються Конституцією та іншими законами України [8]. Діяльність Нацбанку на сьогоднішній день безпосередньо пов'язана із використанням інноваційних технологій та обробкою інформації у кіберпросторі. Відповідно до цього, на НБУ покладено функцію визначення напряму розвитку сучасних електронних банківських технологій, він створює та забезпечує безперервне, надійне та ефективне функціонування, розвиток створених ним платіжних та облікових систем, контролює створення платіжних інструментів, систем автоматизації банківської діяльності та засобів захисту банківської інформації [8]. Важливість кібербезпеки у діяльності НБУ за даних умов обумовлюються тим, що усі вказані типи електронних систем несуть в собі великий об'єм даних, які за негативних обставин можуть бути використані не за їх цільовим призначенням. До того ж, головним завдання Нацбанку, відповідно до статті 8 Закону України «Про Національний банк України», є розроблення Основних засад грошово-кредитної політики та здійснення контролю за проведенням грошово-кредитної політики [8]. В даному разі робота з інформацією у кіберпросторі представляє собою невід'ємний елемент процесу реалізації подібного завдання. Цей факт дозволяє нам стверджувати, що забезпечення кібербезпеки у своїй діяльності є одним з головних обов'язків Національного банку України сьогодні.

Отже, кібербезпека як об'єкт адміністративно-правової охорони являє собою певний віртуальний інститут, охорона якого відбувається в межах норм адміністративного права та здійснюється окремими державними органами на засадах імперативності та ієрархічності.

На даний час в Україні сформовано специфічну нормативно-правову основу забезпечення кібербезпеки, однак, серед вчених немає єдності у розумінні досліджуваного інституту.

Кібербезпека характеризується великою кількістю особливостей як негативного, так і позитивного забарвлення. Головним негативним моментом кібербезпеки як об'єкта адміністративно-правової охорони є недосконалий понятійний апарат. Відсутність чіткого визначення змісту кібербезпеки фактично призводить, по-перше, до його неоднакового розуміння, а по-друге — до застосування, що в окремих випадках дозволяє правопорушнику уникнути відповідальності. Наступною особливістю досліджуваного інституту є те, що адміністративно-правова охорона кібербезпеки хоча і являє собою єдиний юридичний інститут, проте, закріплюється у нормах різних нормативно-правових актів, якими регулюється діяльність відповідних органів державної влади. Іншими словами, забезпеченням кібербезпеки займаються різні відомства в процесі виконання своїх функцій та покладених на них обов'язків. Також особливістю кібербезпеки як об'єкта адміністративно-правової охорони є те, що її забезпечення здійснюється не тільки у правовідносинах, які виникають у сфері вчинення адміністративних правопорушень. Інститут має більш широкий обсяг застосування, який передбачає не тільки припинення відповідних порушень, а й їх попередження. І останньою особливістю кібербезпеки як об'єкта адміністративно-правової охорони є те, що основні засади її забезпечення лише нещодавно знайшли своє закріплення у відповідному нормативно-правовому акті. З прийняттям цього законодавчого акту в Україні вперше з'явилось нормативне визначення поняття «кібербезпека», що, в свою чергу, дозволить виробити грамотну та надійну стратегію захисту кібербезпеки в адміністративно-правовому порядку. Крім цього, у законі детально визначаються засади та суб'єктний склад механізму забезпечення вказаної категорії, що, беззаперечно,

можна назвати юридичним проривом у сфері забезпечення кіберпростору та процесу використання інноваційних технологій.

1.3 Правові засади адміністративно-правового забезпечення кібербезпеки України

Регулювання усіх суспільних відносин в державі відбувається відповідно до вимог нормативно-правових актів, прийнятих у встановленому законом порядку. Але законодавча база є лише зовнішнім виразом права та інститутів, які входять до його структури, іншими словами, він надає правовій системі держави матеріальний вигляд. Реальною ж основою будь-якої юридичної галузі є принципи та засади, які містяться у положеннях нормативно-правових актів різної ієрархічної підпорядкованості. Не є виключенням в даному разі кібербезпека, яка з кожним днем розвивається у нашій державі. Дане явище представляє собою доволі широкий правовий інститут, об’єктом якого є правовідносини у сфері обробки інформації у кіберпросторі. Не менш цікавою є структура кібербезпеки, до складу якої входить механізм кіберзахисту. Останній являє собою систему різного типу заходів забезпечення вказаного вище правового інституту, які застосовуються задля його стабільності та дієвості. Однак, механізм забезпечення кібербезпеки є цілком правовим явищем, що, в свою чергу, обумовлює існування відповідних правових засад, на яких ґрунтується його дія. Сучасна нормативна база дає можливість виділити велику кількість правових засад забезпечення інституту, але враховуючи особливості нашого дослідження, необхідним є освітлення місця адміністративно-правового регулювання в системі принципів вказаного механізму.

Слід зауважити, що правові засади будь-якої юридичної галузі, інституту чи норми беруть свій початок у положеннях Конституції України. Тож розглядаючи адміністративно-правові засади забезпечення кібербезпеки, необхідно також враховувати особливості правової системи, принципи побудови якої у цілому закладено в нормах Конституції України. У Основному Законі держави закріплено, що Україна — суверенна і незалежна, демократична, соціальна, правова держава. Відповідно до даних особливостей наша країна функціонує та розвиває усі внутрішні галузі життєдіяльності суспільства. Велику особливість має останній термін представленої конституційної норми — правова держава. У вчених існує дискусія стосовно його ролі та сутності у правовій системі України, але в рамках цього дослідження нас цікавить принцип, дію якого було започатковано вказаним поняттям. Стаття 8 Конституції України закріплює, що в нашій державі визначається та діє засада верховенства права, яка розкривається у наступних аспектах:

– по-перше, Конституція України має найвищу юридичну силу;

– по-друге, закони та інші нормативно-правові акти приймаються на основі Конституції і повинні відповідати їй;

– по-третє, норми основного закону є нормами прямої дії [1].

Повертаючись до проблематики даного підрозділу, ми можемо стверджувати, що правові засади забезпечення кібербезпеки — це весь масив основних ідей, засад та положень, закріплених в нормах нормативно-правових актів різної юридичної сили, які визначають механізм правового регулювання забезпечення кібербезпеки.

Кібернапади – це найбільші ризики , з якими може стикнутися будь-яка організація . За даними глобального огляду проведеного об’єднанням ISACA , тільки 38 % респондентів вважають , що вони підготовлені до кібернападів , решта 83 % відносять кібернапади до однієї з найнебезпечніших загроз для організації. За наявності великого обсягу персональної та конфіденційної

інформації , яку пересилають за допомогою електронних засобів , несанкціонований доступ до неї може спричинити серйозні наслідки.

Уперше поняття « інформаційної безпеки» в Україні було визначено в Законі України « Про Основні засади розвитку інформаційного суспільства в Україні на 2007- 2015 роки» від 09. 01. 2007 р. № 537-5 , в якому інформаційна безпека визначається як стан захищеності життєво важливих інтересів людини , суспільства і держави , за якого запобігається нанесення шкоди через: неповноту , невчасність та невірогідність інформації , що використовується ; негативний інформаційний вплив ; негативні наслідки застосування інформаційних технологій ; несанкціоноване розповсюдження, використання і порушення цілісності , конфіденційності та доступності інформації.

Згідно із Законом України « Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» вирішення проблеми інформаційної безпеки має здійснюватися шляхом : створення повнофункціональної інфраструктури держави та забезпечення захисту її критичних елементів; підвищення рівня координації діяльності державних органів щодо виявлення, оцінки і прогнозування загроз інформаційній безпеці , запобігання таким загрозам та забезпечення ліквідації їх наслідків, здійснення міжнародного співробітництва із цих питань; вдосконалення нормативно- правової бази щодо забезпечення інформаційної безпеки . зокрема захисту інформаційних ресурсів , протидії комп’ютерній злочинності , захисту персональних даних , а також правоохоронної діяльності в інформаційній сфері; розгортання та розвитку Національної системи конфіденційного зв’язку як сучасної захищеної транспортної основи , здатної інтегрувати територіально розподілені інформаційні системи , в яких обробляється конфіденційна інформація. Як бачимо , поняття «інформаційна безпека» набагато ширше, ніж поняття безпеки інформації, і зовсім не зводиться до неї.

Визначальне місце в системі правових засад забезпечення кібербезпеки посідають принципи правого регулювання. Слід зазначити, що до цього часу в законодавстві не існувало сталої системи принципів забезпечення кібербезпеки. Вони були окреслені лише у доктринальній сфері правниками– теоретиками, які займалися дослідженням вказаного інституту. Однак, певні засади забезпечення кібербезпеки все ж таки містились у нормативних актах, якими регулювалися питання інформаційної безпеки в України. Їх положення на сьогоднішній день виступають правовою основою забезпечення кібербезпеки, про що говориться у новоприйнятому Законі України «Про основні засади забезпечення кібербезпеки України». Відповідно до статті 3 Закону України «Про основні засади забезпечення кібербезпеки України», 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. Крім того, якщо міжнародним договором України, згоду на обов'язковість якого надано Верховною Радою України, передбачено інші правила, ніж встановлені положеннями вищенаведеного Закону, то застосовуються положення міжнародного договору України [10]. Окрім цього, вказана норма у Законі України «Про основні засади забезпечення кібербезпеки України» не містить перелік актів, положення яких, по суті, становлять механізм забезпечення кібербезпеки. До них відносяться: Кримінальний кодекс України та Кодекс України про адміністративні правопорушення. Важливість цих офіційних документів проявляється в тому, що вони становлять «буфер» протидії правопорушенням у сфері кібербезпеки. У даних кодексах містяться норми, котрі

дозволяються застосовувати до порушників найбільш суворі заходи примусу, а також запобігати або припиняти відповідні правопорушення.

В положеннях усіх зазначених нормативних актів містяться основи, вихідні начала механізму забезпечення кібербезпеки України. Усі вони були уніфіковані у Законі України «Про основні засади забезпечення кібербезпеки України», тож на сьогодні правові засади забезпечення кібербезпеки України ґрунтується на наступних десяти принципах:

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

2) забезпечення національних інтересів України;

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

4) 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;

5) 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;

6) пріоритетності запобіжних заходів;

7) невідворотності покарання за вчинення кіберзлочинів;

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

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

10) забезпечення демократичного цивільного контролю за утвореними відповідно до законів України військовими формуваннями та правоохоронними органами, що провадять діяльність у сфері кібербезпеки.

Якщо провести паралель між принципами та правовою основою забезпечення кібербезпеки, то стає зрозумілим що практично кожна засада знаходить своє більш детальне закріплення у нормах тих або інших нормативно-правових актів. Тобто одні принципи відображають конституційність механізму забезпечення кібербезпеки, інші — особливості його застосування. Наприклад, перший принцип — верховенства права і законності — уособлює головні основи буд-якої демократичної держави та знаходить своє закріплення безпосередньо у Конституції України. Сутність верховенства права була розглянута нами вище, тож питання виникають з приводу другого елементу — законності. Досить часто ці поняття плутають або ж ототожнюють, що є серозною помилкою, хоча законність та верховенство права дійсно є пов'язаними між собою юридичними конструкціями. Наразі в юридичній науці сформувалось загальне концептуальне розуміння як поняття законності в цілому (мається на увазі законність як принцип, як правовий режим, законність як метод), так і законності як принципу організації і діяльності механізму держави. Так, законність часто характеризується як суворе і неухильне слідування державними органами та посадовими особами закону в процесі застосування права або ж як слідування праву органами держави і її громадянами [74; 16, с. 86]. У сфері забезпечення кібербезпеки законність необхідно розуміти як вимогу щодо відповідності цього механізму нормам Конституції, іншого законодавства та міжнародно-правовим актам, ратифікованим у визначеному законом порядку. Крім того, суб'єкти забезпечення кібербезпеки в процесі виконання своїх функцій не можуть діяти поза законом.

Адміністративно-правові засади забезпечення кібербезпеки нашої держави також знайшли свій прояв у переліку принципів забезпечення кібербезпеки в

Україні. Як приклад, можна навести пункт 6 статті 7 Закону України «Про основні засади забезпечення кібербезпеки України», в якому закріплено пріоритетність запобіжних заходів забезпечення кібербезпеки Сутність зазначеного принципу забезпечення кібербезпеки полягає в тому, що запобіжні заходи закріплені саме в нормах адміністративного законодавства, адже вони здійснюються державними органами та використовуються з метою попередження правопорушень у тій чи інший сфері та недопущення вчинення правопорушень в майбутньому. Крім того, в рамках механізму забезпечення кібербезпеки адміністративно-правове регулювання набуває більш широкого розуміння.

Роль адміністративно-правового регулювання у сфері забезпечення кібербезпеки полягає в тому, що саме відповідно до норм адміністративного законодавства здійснюється правове регулювання діяльності суб'єктів забезпечення кібербезпеки в Україні. Як приклад, у статті 8 Закону України «Про основні засади забезпечення кібербезпеки України» зазначається, що національна система кібербезпеки є сукупністю суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури [10]. Дана норма наглядно показує, що законодавець має на меті створення впорядкованої структури суб'єктів забезпечення кібербезпеки, тобто владних суб'єктів, які наділені відповідною компетенцією та повноваженнями, що дозволять їм регулювати правовідносини у сфері обробки інформації в кіберпросторі шляхом застосування державного примусу. Прикладом виступає Державний центр кіберзахисту, який забезпечує створення та функціонування основних складових системи захищеного доступу

державних органів до мережі Інтернет, системи антивірусного захисту національних інформаційних ресурсів, аудиту інформаційної безпеки та стану кіберзахисту об'єктів критичної інформаційної інфраструктури, системи виявлення вразливих об'єктів і реагування на кіберінциденти та кібератаки щодо об'єктів кіберзахисту, системи взаємодії команд реагування на комп'ютерні надзвичайні події, а також у взаємодії з іншими суб'єктами забезпечення кібербезпеки розробляє сценарії реагування на кіберзагрози, заходи щодо протидії таким загрозам, програмам та методикам проведення кібернавчань [10]. Адже кібербезпека сучасної держави має прямий вплив на всі складові частини її політики. Голова КНР СІ Цзіньпін зазначив , що в наші дні національна безпека неможлива без її кіберпезпеки , а модернізація країни неможлива без її інформатизації. В Україні над цим питанням також працювали і яскравим прикладом напрацювання є створення урядової команди реагування на комп'ютерні надзвичайні події України «CERT-UA». Відповідно до статті 9 Закону України «Про основні засади забезпечення кібербезпеки України», завданнями команди є:

1) накопичення та проведення аналізу даних про кіберінциденти, ведення державного реєстру кіберінцидентів;

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

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

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

5) взаємодія з правоохоронними органами, забезпечення їх своєчасного інформування про кібератаки;

6) взаємодія з іноземними та міжнародними організаціями з питань реагування на кіберінциденти;

7) взаємодія з українськими командами реагування на комп'ютерні надзвичайні події, а також іншими підприємствами, установами та організаціями незалежно від форми власності, які провадять діяльність, пов'язану із забезпеченням безпеки кіберпростору;

8) опрацювання отриманої від громадян інформації про кіберінциденти щодо об'єктів кіберзахисту;

9) сприяння державним органам, органам місцевого самоврядування, військовим формуванням, утвореним відповідно до закону, підприємствам, установам та організаціям незалежно від форми власності, а також громадянам України у вирішенні питань кіберзахисту та протидії кіберзагрозам.

Слід зауважити, що функціонування «CERT-UA» здійснюється Державною службою спеціального зв'язку та захисту інформації України [10].

Таким чином, адміністративно-правове регулювання виступає однією з головних засад забезпечення кібербезпеки України. Більш того, заходи, які складають систему управлінського регулювання, мають пріоритетний характер, так як їх дія направлена на попередження порушень прав і законних інтересів суб'єктів у сфері обробки інформації в кіберпросторі. Крім цього, адміністративно-правова складова забезпечення кібербезпеки проявляється у створенні ієрархічної структури суб'єктів його реалізації, яких наділено владними повноваженнями. Останні входять до Національної системи кібербезпеки України та відповідно до законодавства у межах своїх повноважень здійснюють підтримку належного стану вказаного інституту за допомогою спеціальних заходів, у тому числі адміністративних. Отже, адміністративно-правове регулювання є ключовою правовою засадою забезпечення кібербезпеки, так як проявляється у роботі великої кількості владних суб'єктів та процесі реалізації державної політики у сфері кібербезпеки.

РОЗДІЛ 2
АДМІНІСТРАТИВНО-ПРАВОВИЙ МЕХАНІЗМ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

2.1 Система суб'єктів забезпечення кібербезпеки України та особливості їх адміністративно-правового статусу

Правова система України складається з декількох галузей права, які, в свою чергу, включають в себе окремі підгалузі, юридичні інститути, механізми, явища, тощо. Правова система — це досить різноманітна та багатогранна структура, основою якої виступає чинне законодавство на чолі з Конституцією. Однак, будь-яке правове явище незалежно від галузевої приналежності набуває реальної юридичної сили у двох випадках: по-перше, якщо воно прописано у нормах офіційних документів, тобто має законодавче підґрунтя , по-друге, реалізовано в установленому законом порядку. Останній аспект не завжди має місце, що призводить до ситуацій, коли той чи інший інститут перебуває у стані правової інертності**.**

Впровадження норм законодавства покладається на державні органи в залежності від сфери діяльності та повноважень. Вказаний раніше негативний аспект виникає, коли подібні суб'єкти не мають відповідних прав щодо реалізації окремих правових інститутів або ж виконують свою роботу неналежним чином. Якщо звернути увагу на досліджуване явище кібербезпеки, то сьогодні воно має структурну законодавчу базу. Інститут, а також супутні йому явища, в повній мірі легалізовані на території України. Крім того, визначною перевагою законодавчої бази, котра регулює кібербезпеку, є те, що в ній детально прописані суб'єкти забезпечення інституту, а також їх повноваження. Тож враховуючи особливості

даного дослідження, ми маємо змогу детально розібрати систему суб'єктів забезпечення кібербезпеки, їх адміністративно-правовий статус, а також повноваження у сфері реалізації механізму кіберзахисту відповідних об'єктів.

Необхідно пам'ятати, що коли ми говоримо про суб'єктів забезпечення кібербезпеки, то в даному контексті маються на увазі учасники правових відносин відповідного типу. Звідси виходить, що аналізувати їх адміністративно-правовий статус необхідно крізь класичний погляд на суб'єктів правовідносин. Якщо не брати до уваги галузеві відмінності, то в цілому подібні учасники є однаковими між собою. Але, це виключає існування декількох наукових поглядів на трактування юридичного статусу суб'єктів правовідносин.

Відповідно до загальної юридичної теорії, суб'єктами правових відносин є учасники суспільних відносин, які виступають носіями юридичних прав та обов'язків [50, с. 229; 167, с. 90]. З цього приводу правильно зазначив В. М. Шаповал, який наголошував на тому, що певні особи чи органи, наділені правами та обов'язками, вступають у відношення, використовуючи свою правосуб'єктність. Це робить їх учасникам конкретних правовідносин та змінює їх правовий статус [104; 168, с. 92]. Враховуючи ці наукові погляди, доцільно було б вказати, що найбільш повно та явно особливості суб'єктів правовідносин розкриваються, якщо проводити їх дослідження в рамках тієї галузі, де відношення були започатковані. При цьому, слід пам'ятати про відмінність вказаної категорії від суміжних понять та явищ. Тому, варто відмежовувати суб'єктів правовідносин від суб'єктів права взагалі (маються на увазі суб'єкти правової системи держави, а не конкретної галузі). В цьому контексті варто згадати думку С. С. Алексєєва, який вказав на те, що суб'єкти права — це особи, що володіють «правосуб'єктністю», тобто громадяни, організації, суспільні утворення, які можуть бути носіями прав і обов'язків, брати участь у правових відношеннях [88, с. 91; 6]. Таким чином, суб'єкта правовідносин можна

визначити як учасника відносин певного характеру, на якого у зв'язку з цим покладаються спеціальні права і обов'язки.

Необхідно зазначити, що суб'єктів забезпечення кібербезпеки окремі науковці розглядають як учасників інформаційних відносин. Зокрема, подібну думку висловлює у своїх працях І. В. Діордіца. Доводячи свій погляд, він спирається на визначення учасників інформаційних відносин, подане у Словнику стратегічних комунікацій В. А. Ліпкана, де зазначено, що суб'єкт інформаційної діяльності — це юридична або фізична особа, задіяна в інформаційному процесі [46, с. 161; 106, с. 365]. Даний науковий погляд заслуговує право на життя, але, на мою думку, він є не зовсім правильним. Суб'єкти забезпечення кібербезпеки є учасниками не інформаційних, а адміністративних правовідносин, так як, по-перше, відносини між ними будуються на основі влади і підпорядкування, а, по-друге, останні реалізують механізм кіберзахисту шляхом використання примусу, який їм надано чинним законодавством. Крім цього, аналіз адміністративно-правового статусу суб'єктів забезпечення кібербезпеки просто неможливо здійснювати поза межами адміністративної галузі права.

У науковому середовищі поняття суб'єктів наведеної вище юридичної галузі визначається по різному. Наприклад, Ю. М. Старілов бачить суб'єктів адміністративного права як потенційних учасників адміністративно-правових відносин, які, мають відповідний адміністративно-правовий статус, беруть участь в організації публічного управління та управлінській діяльності, а також у процесі управління, тобто адміністративних процесах [66; 176, с. 419]. Більш стисло з цього приводу висловився Д. М. Бахрах, який відмітив , що суб'єктами адміністративного права потрібно визнати учасників управлінських відносин, які адміністративно-правовими нормами наділені правами і обов'язками, здатністю вступати в адміністративні правовідносини [27, с. 124; 201, с. 550]. Найбільш влучним є визначення суб'єктів адміністративного права, синтезоване І. С. Гриценко, Р. С. Мельником, А. А. Пухтецькою. Вони наголошують на тому, що

під суб'єктами адміністративного права слід розуміти носіїв (фізичних чи юридичних осіб) права і обов'язки яких у сфері публічного управління, передбачені адміністративно-правовими нормами, які можуть надані права реалізовувати, а покладені на них обов'язки — виконувати [51, с. 226].

Під представлену дефініцію підпадає велике коло суб'єктів, які входять до єдиної системи. Варто зазначити, що структура суб'єктів адміністративного права складається із сукупності індивідуальних та колективних осіб, але вона не закінчується їх механічною кількістю. Кожен із суб'єктів адміністративного права займає відповідне місце в системі, яке пов'язане з його адміністративно-правовим статусом, що дає можливість взаємодіяти з іншими суб'єктами. Аналіз суб'єктів адміністративного права дозволяє зробити висновок про наявність у системі двох підсистем, критерієм виокремлення яких є публічно-владні повноваження [75, с. 128]. Найбільш класичний погляд на це питання дає змогу виділити дві групи учасників правовідносин управлінського характеру:

– індивідуальні суб'єкти адміністративного права (громадяни, іноземці, особи без громадянства та посадові особи);

– колективні суб'єкти адміністративного права (органи публічної адміністрації, органи місцевого самоврядування, громадські організації).

Суб'єкти забезпечення кібербезпеки є учасниками правовідносин управлінського характеру, що обумовлюється їх правовим статусом. Отже, якщо перенести вищенаведену інформацію у сферу забезпечення кібербезпеки, то можна зробити висновок про те, що суб'єктами забезпечення кібербезпеки є державні органи та посадові особи, наділені владними повноваженнями та відповідними обов'язками щодо охорони об'єктів кібербезпеки. Дані суб'єкти знаходяться у законній підпорядкованості між собою. Звичайно, представлене авторське визначення повністю не розкриває сутність адміністративно-правового статусу учасників забезпечення кібербезпеки, проте , воно відображає теоретичне уявлення даної проблематики. З метою її більш повного та глибокого аналізу

необхідно звернутись до норм чинного законодавства, де наведений перелік суб'єктів забезпечення кібербезпеки, а також їх права та обов'язки у цій сфері.

На нормативному рівні перелік вищевказаних суб'єктів не є однорідним. Одним із перших офіційних актів, в положеннях якого говориться про систему суб'єктів забезпечення кібербезпеки, є Указ Президента України «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України». У цьому нормативному документі вперше було використано термін «національна система кібербезпеки». Саме у цю систему входять основні учасники процесу захисту прав і свобод осіб у відносинах з приводу обробки та обміну інформацією у кіберпросторі. Тож у главі 3 Стратегії вказано, що основу системи суб'єктів забезпечення кібербезпеки мають становити Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, Національний банк України, розвідувальні органи, на які мають бути покладені в установленому законом порядку спеціальні завдання [10]. Інший перелік суб'єктів закріплено у ст. 8 Закону України «Про основні засади забезпечення кібербезпеки України», відповідно до якої до основних суб'єктів забезпечення кібербезпеки віднесено: Раду національної безпеки і оборони України, Міністерство внутрішніх справ України, Міністерство оборони України, Генеральний штаб Збройних Сил України, Службу безпеки України, Державну службу спеціального зв'язку та захисту інформації України, розвідувальні органи, тощо [10]. В свою чергу, відповідно до ч. 4 статті 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 [10].

Необхідно зауважити на те , що дія Закону України «Про основні засади здійснення кібербезпеки України» не поширюється на відносини та послуги , пов'язані зі змістом інформації , що обробляється (передається , зберігається) в комунікаційних та або в технологічних системах , соціальних мережах , приватних електронних інформаційних ресурсах у мережі Інтернет (включаючи блог-платформи , відеохостинги , інші веб ресурси) , а також не стосується інформаційно-телекомунікаційних систем , у яких циркулює інформація , яка складає державну таємницю. Проте запровадження положень Закону у цій сфері може розглядатись як істотне порушення прав людини відповідно до положень Європейської конвенції про захист прав людини і основних свобод, зокрема ст. 10 Конвенції.

Національна система кібербезпеки представляє собою комплексну систему взаємодії між Державною службою спеціального зв'язку та захисту інформації України, Національною поліцією України , Службою безпеки України, Міністерством оборони України та Генеральним штабом Збройних сил України , розвідувальними органами, Національним банком України , діяльність яких

спрямована на забезпечення кібербезпеки та взаємопов'язаних заходів політичного , науково-технічного , інформаційного , освітнього характеру, організаційних , правових , оперативно-розшукових , розвідувальних , контррозвідувальних ,оборонних , інженерно-технічних заходів , а також заходів криптографічного і технічного захисту національних інформаційних ресурсів , кіберзахисту об'єктів критичної інформаційної інфраструктури.

Провідним суб'єктом національної системи кібербезпеки є Державна служба спеціального зв'язку та захисту інформації України , на яку припадає близько 80% навантаження та яка забезпечує формування та реалізацію державної політики щодо захисту в кіберпросторі державних інформаційних ресурсів та інформації , вимога щодо захисту 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 кіберінцеденти 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); координує , організовує та проводить аудит захищеності комунікаційних і технологічних систем об'єктів критичної інфраструктури на вразливість; забезпечує функціонування Державного центру кіберзахисту.

У Державному центрі кіберзахисту та протидії кіберзагрозам Держзвязку є структурований підрозділ Computer response team of Ukraine (далі – Cert- UA)-команда реагування на комп'ютерні надзвичайні події України , основною метою якого є забезпечення захисту інформаційних ресурсів та інформаційних та

телекомунікаційних систем від несанкціонованого доступу , неправомірного використання , а також порушень їх конфіденційності , цілісності та доступності. CERTA –UA періодично публікує рекомендації, які стосуються безпеки поштового сервісу, із протидії загрозі інсайдера, усунення вразливостей, пов'язаних із некоректним налаштуванням DNS-серверів , із самостійного пошуку та ліквідації веб - шеллів тощо.

Доволі специфічними є адміністративно-правовий статус Національної поліції України (далі — НПУ) та Служби безпеки України (далі — СБУ) у сфері забезпечення кібербезпеки. Дані правоохоронні органи наділенні повноваженнями щодо припинення правопорушень та притягнення винних осіб до відповідальності. Їх діяльність принципово відрізняється від роботи Державної служби спеціального зв'язку та захисту інформації України, адже ці орган створюють належні умови використання інформаційних ресурсів та інформації в цілому. При цьому, повноваження та завдання СБУ та НПУ суттєво різняться між собою, хоча сфери функціонування органів є доволі близькими. Зокрема, Національна поліція України є центральним органом виконавчої влади, який служить суспільству шляхом забезпечення охорони прав і свобод людини, протидії злочинності, підтримання публічної безпеки і порядку.

Завданнями поліції є надання поліцейських послуг у сферах:

1) забезпечення публічної безпеки і порядку;

2) охорони прав і свобод людини, а також інтересів суспільства і держави;

3) протидії злочинності;

4) надання в межах, визначених законом, послуг з допомоги особам, які з особистих, економічних, соціальних причин або внаслідок надзвичайних ситуацій потребують такої допомоги [9].

Безпосередньо у галузі забезпечення кібербезпеки НПУ наділена повноваженнями щодо забезпечення прав і свобод людини і громадянина, інтересів суспільства і держави від злочинних посягань у кіберпросторі;

запобігання, виявлення, припинення та розкриття кіберзлочинів; підвищення поінформованості громадян про безпеку в кіберпросторі [9]. Діяльність Національної поліції спрямовується та координується КМУ через підпорядковуваний орган — Міністерство внутрішніх справ (далі — МВС). Слід відзначити, що МВС як орган виконавчої влади також відіграє значну роль у процесі забезпечення кібербезпеки. До речі, відповідно до Закону України «Про основні засади забезпечення кібербезпеки України», МВС було включено до національної системи суб'єктів забезпечення кібербезпеки. У зв'язку з цим, на МВС було покладено повноваження щодо: створення і забезпечення функціонування підрозділів з протидії кіберзлочинності; розробки та реалізації комплексу організаційних і практичних заходів, спрямованих на боротьбу з кіберзлочинами; створення і забезпечення функціонування цілодобової контактної мережі для надання невідкладної допомоги у розслідуванні кіберзлочинів, тощо [9]. В положеннях Закону «Про основи забезпечення кібербезпеки України» МВС віднесено до загальних суб'єктів забезпечення інституту.

Дещо іншими повноваженнями у сфері забезпечення кібербезпеки наділена Служба безпеки України. У своїй роботі СБУ також має повноваження щодо протидії правопорушенням і припинення злочинів, однак, її можливості є дещо ширшими, враховуючи функціональну направленість відомства. Відповідно до законодавства, Служба безпеки України — це державний правоохоронний орган спеціального призначення, який забезпечує державну безпеку України. У своїй роботі СБУ підпорядковується безпосередньо Президенту України. На Службу безпеки України покладається у межах визначеної законодавством компетенції захист державного суверенітету, конституційного ладу, територіальної цілісності, економічного, науково-технічного і оборонного потенціалу України, законних інтересів держави та прав громадян від розвідувально-підривної діяльності іноземних спеціальних служб, посягань з боку окремих організацій,

груп та осіб, а також забезпечення охорони державної таємниці. До завдань Служби безпеки України також входять попередження, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, тероризму, корупції та організованої злочинної діяльності у сфері управління і економіки та інших протиправних дій, які безпосередньо створюють загрозу життєво важливим інтересам України [13]. Як ми бачимо, діяльність СБУ безпосередньо спрямовано на підтримку національної безпеки держави, що також відображається у повноваженнях органу у сфері забезпечення кібербезпеки. У Законі України «Про основні засади забезпечення кібербезпеки України» закріплено, що 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 [13].

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України», окремим суб'єктом забезпечення кібернетичної безпеки є Міністерство оборони України (далі — Міноборони) та Генеральний штаб Збройних Силу України (далі — Генеральний штаб). У галузі забезпечення кібербезпеки повноваження даних органів є цілком ідентичними. Вони 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 [13]. Але необхідно відзначити, що наведені повноваження Міноборони та Генеральний штаб реалізують у відповідності до інших повноважень кожного з них, які суттєво різняться. Зокрема, Міноборони є головним органом у системі центральних органів виконавчої влади, який забезпечує формування та реалізацію державної політики з питань національної безпеки у воєнній сфері, сфері оборони і військового будівництва у мирний час та особливий період. Міноборони є органом військового управління, у підпорядкуванні якого перебувають Збройні Сили України. Основними завданнями Міноборони є:

1) забезпечення формування та реалізація державної політики з питань національної безпеки у воєнній сфері, сфері оборони і військового будівництва у мирний час та особливий період;

2) здійснення військово-політичного та адміністративного керівництва Збройними Силами;

3) здійснення в установленому порядку координації діяльності державних органів та органів місцевого самоврядування щодо підготовки держави до оборони;

4) забезпечення в межах повноважень, передбачених законом, реалізації державної політики з оборонних питань, що пов’язані з використанням повітряного простору України та захистом суверенітету держави [5].

В свою чергу, Генеральний штаб Збройних сил України підпорядковується Міноборони та є головним військовим органом з планування оборони держави, управління застосуванням Збройних Сил України, координації та контролю за виконанням завдань у сфері оборони іншими утвореними відповідно до законів України військовими формуваннями, правоохоронними органами, тощо. Завданнями Генерального штабу є:

1) участь у формуванні та реалізації державної політики у сфері оборони, стратегії воєнної безпеки;

2) стратегічне планування застосування Збройних Сил, інших військових формувань, правоохоронних органів, координація їх підготовки до виконання завдань у сфері оборони, організація територіальної оборони та оперативного обладнання території держави;

3) безпосереднє військове керівництво Збройними Силами України;

4) організація і контроль за здійсненням заходів, спрямованих на підтримання військ (сил) Збройних Сил України та інших військових формувань і правоохоронних органів у постійній бойовій та мобілізаційній готовності.

Отже, Міноборони є координаційним політичним центром, який реалізує політику держави у сфері забезпечення кібербезпеки, у той час як Генеральний штаб є оперативним органом, діяльність якого спрямовано на подолання реальної агресії та виконання бойових завдань у випадках, передбачених законодавством.

Одне з головних місць у системі забезпечення кібербезпеки займає Національний банк України (далі — НБУ). У попередніх підрозділах дослідження я вказував, що НБУ розробляє та впроваджує у свою діяльність сучасні електронні банківські технології, новітні платіжні та облікові системи, тощо [14]. Крім того, враховуючи той факт, що основною функцією Нацбанку, відповідно до Конституції України, є забезпечення стабільності грошової одиниці України, його повноваження у галузі забезпечення кібербезпеки доволі широкі. У зв’язку з цим, НБУ:

– здійснює формування вимог щодо кіберзахисту критичної інформаційної інфраструктури у банківській сфері;

– 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, тощо [29; 200]

Використання даних повноважень, порівняно з іншими органами, здійснюється НБУ дещо простіше, адже він є центральним банком України, особливим центральним органом державного управління, головною метою якого є забезпечення фінансової стабільності у державі. Тож на основі саме цієї особливості формується його роль у механізмі підтримки інституту кібербезпеки.

Отже, всі суб'єкти забезпечення кібербезпеки наділені як комплексом специфічних, так і комплексом загальних повноважень. Серед загальних рис суб'єктів забезпечення кібербезпеки варто відзначити те, що вони: по-перше, в своїй діяльності використовують владний примус з метою реалізації передбачених законодавством функцій; по-друге, суб'єкти забезпечення кібербезпеки перебувають у системному взаємозв'язку з іншими учасниками адміністративних правовідносин, який будується на засадах ієрархічності; по-третє, діяльність суб'єктів забезпечення кібербезпеки спрямовано не тільки на припинення правопорушень у цій сфері, а й на забезпечення умов, коли такі порушення неможливі, що реалізується шляхом проведення контрольних заходів, і т.п.

На мою думку для покращення ситуації пов'язаної з кібербезпекою в Україні , необхідне налагодження взаємодії між усіма суб'єктами - державними органами , що здійснюють регулювання у сфері інформатизації та захисту інформації; органами внутрішніх справ , збройними силами , органами безпеки, розвідувальними органами України та приватним сектором.

Для виконання завдань із забезпечення координації вказаної діяльності та оптимізації функціонування національної системи кібербезпеки вважаю за доцільне створити при РНБО України Національний координаційний центр кібербезпеки.

Держава повинна залучити до національної системи кіберзахисту власників та операторів інформаційної критичної інфраструктури незалежно від сфери промисловості чи форми власності. А це в свою чергу має потягнути за собою налагодження механізму оперативного обміну інформацією між зазначеними суб'єктами.

2.2 Адміністративно-правові форми та методи забезпечення кібербезпеки України

У сучасних умовах питання забезпечення кібербезпеки не обмежується лише організацією системи захисту інформації на окремому об'єкті критичної інформаційної структури , а й передбачають створення єдиної системи захисту кібернетичного простору як складової частини інформаційної та національної безпеки будь-якої держави світу.

При цьому, виходячи із сучасних викликів та загроз , з метою забезпечення контролю за національним сегментом кіберпростору політикум будь-якої держави постійно вдосконалює організаційно-правові та техніко-економічні механізми забезпечення безпеки кіберпростору та інформаційно-телекомунікаційних мереж. Ситуація ускладнюється тим, що нині у світі здійснюється численні спецоперації у кіберпросторі , кібератаки, які супроводжуються незаконним збором інформації та особистих даних про службовців, приватний бізнес-сектор, громадян, які організовуються як спецслужбами іноземних держав, так і окремими хакерами, що фінансуються державними структурами розвинених країн та міжнародними терористичними

організаціями. Одночасно застосовуються різні методи маніпуляції людьми і технологіями з використанням Інтернет-мереж.

Обов'язком держави стає забезпечення конфіденційності, цілісності та доступності даних. Втім, доводиться констатувати, що стан реалізації заходів із забезпечення кібербезпеки в Україні залишає бажати кращого, що, в свою чергу, обумовлює необхідність комплексного дослідження та удосконалення багатьох аспектів такої діяльності, одним із яких є розгляд адміністративно-правових форм та методів забезпечення кібербезпеки України. Адже саме зазначені категорії у своїй сукупності утворюють своєрідний інструмент, за допомогою якого суб'єкти забезпечення кібербезпеки можуть вирішити складні завдання, які стоять перед ними у досліджуваній сфері.

Переходячи до розгляду поняття адміністративно-правових форм, потрібно зазначити, що в юридичній літературі не існує одного підходу щодо розуміння вказаного терміну, що, в свою чергу, обумовлює чималу кількість точок зору щодо його тлумачення. Так, Ю. П. Битяк вважає, що адміністративно-правова форма — це зовнішній вияв конкретних дій, що здійснюються органами виконавчої влади для реалізації поставлених перед ними завдань [23]. Досліджуючи адміністративно-правові форми протидії корупції, В. І. Литвиненко пропонує під вказаним терміном розуміти об'єктивне зовнішнє вираження адміністративно-правових норм і актів, а також інституційно-правову структуру органів публічної адміністрації, які виявляються в повноваженнях суб'єктів публічної адміністрації та здійснюваних на їхній основі діях щодо запобігання, виявлення й боротьби з корупцією, спрямованих на створення потенційно несприятливих умов для здійснення корупційних діянь, обмеження можливості розвитку корупції, виявлення наявної корумпованості в суспільстві, сприяння подоланню та викоріненню корупції з державно-владного апарату й інших сфер суспільного життя шляхом усунення наслідків корупції, притягнення винних у корупційних правопорушеннях до юридичної відповідальності,

поновлення прав та інтересів осіб, що були порушені корупційним діянням [67, с. 50]. В свою чергу, Т. А. Кобзєва під адміністративно-правовими формами управління фінансовою системою України розуміє спрямовану ззовні й засновану на приписах норм адміністративного права діяльність уповноважених державою на здійснення управління фінансовою системою суб'єктів, що спричиняє юридично значимі наслідки для правовідносин в межах фінансової системи [58]

В першу чергу необхідно вказати таку адміністративно-правову форму забезпечення кібербезпеки України як нормо творчість (тобто прийняття нормативно-правових актів у сфері забезпечення кібербезпеки). О. Ф. Скакун вважає, що під нормо творчістю слід розуміти офіційну діяльність уповноважених суб'єктів держави та громадянського суспільства щодо встановлення, зміни, призупинення і скасування правових норм, їх систематизації [90, с. 342]. Досить розгорнуте визначення нормо творчості надає О. В. Петришин, який зазначає, що це діяльність уповноважених на це суб'єктів з розроблення, розгляду, прийняття та офіційного оприлюднення нормативно-правових актів, яка здійснюється за визначеною процедурою [96]. Науковець сформулював наступні характерні ознаки вказаного поняття: 1) нормо творчість є етапом право утворення. Під час нормо творчості в нормативно-правових актах мають закріплюватися норми права, які є результатом узагальнення найбільш важливих повторювальних суспільних відносин, а також засобом витіснення шкідливої суспільної практики; 2) нормо творчість є правовою формою діяльності публічної влади поряд із правозастосуванням, тлумаченням права, контрольно-наглядовою та установчою діяльністю. Тому нормотворча діяльність урегульована правом і є юридично значущою, тобто породжує правові наслідки. Основна відмінність нормо творчості від інших правових форм діяльності полягає в тому, що її метою є створення, зміна або скасування норм права; 3) результатом нормотворчої діяльності є нормативно-правові акти, за допомогою

яких формально закріплюються норми права. Загальним результатом нормо творчості є законодавство як джерело права; 4) нормо творчість здійснюється уповноваженими на це суб'єктами — органами і носіями публічної впади: органами державної влади та органами місцевого самоврядування, їх посадовими особами, народом та територіальними громадами; 5) нормо творчість здійснюється за певною процедурою, яка регламентується законодавством. Процедурний характер нормотворчої діяльності (тобто її здійснення в установленому порядку) зменшує вірогідність свавілля та помилкових рішень, забезпечує створення справедливих та ефективних норм права. Суттєві порушення процедури нормо творчості можуть призвести до визнання нормативно-правового акту недійсним у судовому порядку [96].

Узагальнюючи все вказане вище, можна із впевненістю стверджувати, що нормо творчість є однією з ключових форм забезпечення кібербезпеки в Україні, оскільки за її допомогою вбачається можливим створити таке правове поле, яке буде виключати будь-які можливості для суб'єктів відповідних правовідносин вчинити правопорушення у досліджуваній сфері. А відтак, нормо творчість, через процес створення правового припису, дозволяє досягти певної поведінки людей у конкретній сфері суспільних правовідносин, що, в свою чергу, має важливий соціальний, економічний та політичний ефект. Якісна та своєчасна нормотворча діяльність дозволяє не лише забезпечити необхідний стан якоїсь сфери суспільних відносин, вона також сприяє підвищенню рівня довіри до суб'єкта нормо творчості (держави), а також підвищує відчуття захищеності громадян у власній країні [39].

Наступною формою забезпечення кібербезпеки, на яку хотілося б звернути увагу, є прийняття індивідуальних актів у сфері забезпечення кібербезпеки. Так, на переконання С. С. Алєксєєва, індивідуальний акт — це припис, який розрахований на конкретний, чітко визначений, одиничний випадок і, виходячи з цього, являє собою акт «одноразової дії»; такі акти здебільшого персоніфіковані

і їх дія завершується із настанням відповідних наслідків або фактів, що безпосередньо ними передбачені [24, с. 208;]. У своєму дисертаційному дослідженні О.О . Мандюк дійшов висновку, що індивідуальний акт — це одностороннє волевиявлення адміністративного органу зовнішньої дії, що безпосередньо впливає на права, свободи чи інтереси конкретних осіб або стосується конкретної ситуації. До основних ознак вказаного поняття автор відносить такі: односторонність, індивідуальність (конкретність), зовнішня дія, породження правових наслідків, приймається адміністративним органом [71, с. 6–7]. Інший науковець — К. І. Бриль — доводить, що під індивідуальним актом слід розуміти вольову дію суб'єктів права, яка здійснюється ними в передбачених законом випадках, закріплюється в установленій законом формі (у формі акту–документа) та спрямована на реалізацію вимог правових норм в конкретних суспільних відносинах і конкретних ситуаціях. Автор підкреслює, що індивідуальні акти належать до різних частин механізму правового регулювання. Разом з тим, всіх їх об'єднує те, що кожний акт поширюється на конкретний випадок. Оскільки всі індивідуальні акти є дуже різноманітними і критеріїв їх класифікації можна виділити досить багато, то ми виберемо найбільш загальний і важливий критерій — за місцем в механізмі правового регулювання [30].

Таким чином, індивідуальні акти у сфері забезпечення кібербезпеки дозволяють оперативно вирішити нагальні проблеми, що з'являються у даній сфері суспільних відносин. Їх перевага полягає у тому, що вони направлені на конкретного суб'єкта, а тому за їх допомогою можливо вирішити більш конкретні проблемні питання. В якості прикладу таких документів В. В. Марков слушно наводить такі: 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 [72, с. 44].

На наступному етапі мого дослідження приділю увагу адміністративно-правовим методам забезпечення кібербезпеки в Україні. У загальному розумінні метод — це шлях до мети, спосіб її досягнення [101, с. 241]. З точки зору філософії, як зазначає В. Л. Петрушенко, поняття методу, як правило, застосовують для пояснення пізнання, наукового пошуку або ж для окреслення таких інтелектуальних та практичних дій, які передбачають високий рівень усвідомлення того, що ми робимо, чому це робимо саме так і чому результат повинен мати саме такі очікувані характеристики. Сам термін «метод» сходить до давньогрецького виразу «мета — одоїс», що можна перекласти як «через вистежений (або підготовлений) шлях» [86, с. 223]. В. С. Зеленецький під методами розуміє сукупність взаємопов'язаних правил, технологічних прийомів і наукових положень, які визначають оптимальні шляхи та способи реалізації пізнання й перетворення дійсності. На його думку, відповідні методи можуть бути реалізовані лише за допомогою конкретних дій, тобто тактичних прийомів їх реалізації [52, с. 213; 24]. Поняття методу активно використовується у багатьох сферах суспільного життя, втім, найбільш дослідженим воно є саме в галузі права, а в залежності від галузі права воно набуває своїх характерних особливостей.

Адміністративно-правові методи, як зазначає В. О. Бурбика, — це сукупність прийомів впливу, що містяться в адміністративно-правових нормах, за допомогою яких встановлюється юридичне владне і юридичне підвладне становище сторін у правовідносинах [31]. На нашу думку, слід погодитись із точкою зору В. К. Колпакова та О. В. Кузьменко, які доводять, що адміністративно-правові методи — це способи та прийоми безпосереднього і цілеспрямованого впливу органів державного управління (посадових осіб) на підпорядковані їм об'єкти управління [62, с. 36]. Методи, підкреслюють вчені, є

досить різноманітними, однак, вони мають загальні риси, а саме: способи впливу органів державного управління на підпорядковані їм об’єкти управління; вираження державного публічного інтересу; засоби досягнення мети; способи організації, прийоми здійснення функцій, що виникають в процесі спільної діяльності; способи реалізації компетенції [57, с. 36].

Необхідно вказати на той факт, що в науковій літературі не існує єдиного підходу щодо визначення конкретних адміністративно-правових методів забезпечення кібербезпеки в Україні. А тому на основі аналізу норм чинного законодавства та наукових поглядів вчених мною були визначені такі методи забезпечення кібербезпеки:

– адміністративний примус. У найбільш загальному розумінні це метод психічного чи фізичного впливу державних органів (посадових осіб) на свідомість і поведінку певних осіб з метою спонукати, примусити їх виконувати правові норми [21, с. 151]. Р. С. Мельник відзначає, що адміністративний примус — це «застосування до право зобов’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» [76, с. 5; 165]. Таким чином, ключове значення вказаного методу полягає у тому, що він спрямований на попередження виникнення правопорушень у досліджуваній сфері. Проте, справедливо буде також підкреслити, що застосування методу адміністративного примусу не лише спрямоване на попередження виникнення протиправної поведінки, а й покликане забезпечити захист інформаційних, приватних, комп’ютерних ресурсів, тощо;

– метод позитивного зобов’язання. Позитивне зобов’язання — це категорія, що включає та доповнює інше поняття — моральне зобов’язання. Позитивне в юриспруденції означає встановлення (правила) волею чи силою панівного,

господарюючого суб'єкта; зобов'язання, відповідно, означає дію чи бездіяльність (що рідше), обов'язковість якої випливає внаслідок вольового акту чи внутрішнього переконання, що відповідає: перше — державному закону, друге — моральному закону [42];

– метод дозволу та заборон. В контексті даної дипломної роботи метод дозволу означає надання суб'єктам відповідних правовідносин можливості (права) здійснювати активні дії та/або бездіяльність, тобто мати свободу вибору напрямку (варіанта) поведінки. Однак, при цьому не слід забувати, що така поведінка все одно не повинна виходи за межі, визначені чинним законодавством. Щодо методу заборон, то він передбачає покладання на суб'єкта обов'язку певної пасивної поведінки, утримання від вчинення якихось дій під загрозою настання відповідальності [90];

– метод адміністративного контролю. В. М. Кудрявцев визначає 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 [64, с. 140]. Таким чином, застосування вказаного методу є важливим з точки зору забезпечення ефективного функціонування суб'єктів забезпечення кібербезпеки в Україні, що, в свою чергу, прямо впливає на вказану сферу суспільних відносин;

– 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» [81, с. 32]. А відтак, ліцензування, беззаперечно, можна

вважати одним із найважливіших методів забезпечення інформаційної безпеки, оскільки воно дозволяє: по-перше, контролювати осіб, що мають доступ до конкретної інформації; по-друге, забезпечити захист інформації, яка не повинна буди доступною для загалу;

– метод сертифікації та стандартизації. Стандартизація та сертифікація — це необхідні заходи, які пов’язані із встановленням мінімальних вимог до певних небезпечних засобів. Стандартизація — діяльність, що полягає в установленні положень для загального та неодноразового використання щодо наявних чи потенційних завдань і спрямована на досягнення оптимального ступеня впорядкованості в певній сфері [14]. А відтак, зазначений метод зазвичай використовується з метою стандартизації та сертифікації системи телекомунікаційного обладнання й програмного забезпечення автоматизованих систем обробки інформації згідно з вимогами інформаційної безпеки;

– реєстраційний метод, який ґрунтується на використанні інформації, яку отримують шляхом підрахунку кількості процесів, предметів або витрат на створення, споживання продукції [92].

Таким чином, завершуючи представлений підрозділ магістерської роботи , слід констатувати, що вказаний мною перелік форм та методів забезпечення кібербезпеки в Україні не є вичерпним, однак, на мою думку, саме вони найбільш якісно та всебічно характеризують зміст такої діяльності. Разом із тим, потрібно буде відмітити, що для забезпечення кібербезпеки в нашій державі необхідним є комплексне використання таких форм і методів. Як недолік слід визнати те, що жодна із вказаних категорій не дістала законодавчого відображення у законі , що, беззаперечно, потребує негайного вирішення шляхом внесення змін до відповідних нормативно-правових актів [38].

2.3 Види та особливості юридичної відповідальності за порушення законодавства у сфері кібербезпеки України

В умовах сьогодення можна беззаперечно констатувати, що одними із найпоширеніших правопорушень є порушення у кіберпросторі. Варто підкреслити, що вчинення таких правопорушень може не тільки мати негативні наслідки для кожного окремого громадянина, а й нести небезпеку для всієї держави взагалі. Саме тому важливого значення набуває інститут юридичної відповідальності за вчинення злочинів у сфері кібербезпеки України. Взагалі ж «відповідальність» у науковій літературі в більшості випадків трактується лише як підзвітність (accountability) і усвідомлення осудності (immutability). У юридичній ж науці феномен відповідальності вивчається головним чином у плані покарання (punishability). Цікаво також відзначити той факт, що термін «відповідальність» вперше ввів у науковий обіг Альфред Бен, який тлумачив її саме в значенні «покарання» [26]. Тривалий час проблема відповідальності була в основному предметом уваги правознавців, що, в свою чергу, обумовило чималу кількість підходів до його розуміння.

Так, відповідно до точки зору В. Н. Хропанюка, 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 визначена державою і впроваджується її компетентними органами. Для злочинця юридична відповідальність означає застосування до нього санкцій правових норм, вказаних в них певних заходів відповідальності [103, с. 334; 40]. На переконання Д. М. Лук'янця, юридична відповідальність — це регламентована правовими нормами реакція з боку уповноважених суб'єктів на діяння фізичних або юридичних осіб

(колективних суб'єктів), що проявляються в недотриманні встановлених законом заборон, невиконанні встановлених законом обов'язків, порушенні цивільно-правових зобов'язань, нанесенні шкоди або завданні збитків, і виражена в застосуванні до осіб, які вчинили такі діяння, засобів впливу, що тягнуть за собою позбавлення особистого, майнового або організаційного характеру [68, с. 15].

Розкриваючи поняття «юридична відповідальність», не можна не звернути увагу на характерні ознаки вказаної категорії. В цьому контексті я поділяю точку зору О. В. Зайчука та Н. М. Оніщенко, які цілком слушно зазначають, що для всіх різновидів юридичної відповідальності спільними є такі ознаки [95]: 1. Підставою відповідальності є правопорушення як конкретний факт поведінки, юридична кваліфікація якого вміщена у законі. Ознаки правопорушення та санкції, що визначають засоби примусу за його вчинення, не підлягають звужувальному чи розширювальному тлумаченню. У процесі застосування відповідальності повинно бути доведено, що особа, яка притягнута до відповідальності, вчинила правопорушення, ознаки якого вміщені у законі. Цей вид відповідальності не може бути застосований за наміри, вислови, погрози чи вчинення моральних проступків. Чіткість підстав відповідальності у правовій сфері забезпечує її реальність, справедливість та законність. Правопорушення не завдає шкоди нормам закону, які продовжують діяти, поширюючись на всіх суб'єктів. Воно завдає шкоди охоронюваним державою правам, свободам та законним інтересам суб'єктів суспільних відносин. 2. Наявність правової основи, яку складають правові норми. Саме вони характеризують поведінку як протиправну та у санкціях включають вичерпний перелік видів відповідальності та засобів, що можуть бути застосовані до порушника. Вказана норма права вміщається у документі, який має форму нормативно-правового акту, що видається органом публічної влади. 3. Наявність індивідуально визначеного суб'єкта — фізичної чи юридичної особи, що за своїм віковим та психічним станом може самостійно відповідати за вчинене. Тому такий суб'єкт повинен

володіти певними ознаками, а вчинене правопорушення має пов’язуватись із наявністю вини, тобто психологічним ставленням особи до скоєного. Саме це і визначає можливість покладення відповідальності та впливає на її види і форму. 4. Юридична відповідальність опирається на державний примус та пов’язана із досягненням певної мети — перевиховання, покарання правопорушника та поновлення порушених прав. Державний примус є специфічним впливом на поведінку людей, заснованим на організованій силі. Особливістю такого примусу є спрямованість на примусове виконання норм права, нормативна регламентованість його законом, наявність чітко встановлених меж та здійснення лише компетентними державними органами. Проте, потрібно пам’ятати, що державний примус є більш широким поняттям, ніж юридична відповідальність, оскільки він може здійснюватися різними способами, не пов’язаними з відповідальністю (наприклад, митний огляд багажу, стягнення аліментів і.т.д). 5. Метою відповідальності є охорона правопорядку, що здійснюється шляхом примусового поновлення порушених прав, припинення протиправного стану чи покарання правопорушника. Дієвість цього інституту забезпечує реальну можливість безперешкодного здійснення суб’єктивних прав та можливість досягнення правового результату правомірною поведінкою суб’єктів суспільних відносин. Своєчасне застосування відповідальності забезпечує можливість перевиховання правопорушника та реалізацію виховної функції у суспільстві. 6. Відображається у настанні певних негативних наслідків для злочинця , що мають особистий, майновий, організаційний характер. Юридична відповідальність є підставою виникнення у суб’єкта, винного у скоєнні правопорушення, додаткового обов’язку зазнати певних обмежень відповідно до санкції норми права та рішення правозастосовного органу держави. 7. Наявність особливої процесуальної форми покладення та реалізації відповідальності. Вона має нормативне закріплення та виявляється у наявності певних стадій відповідальності, кожна з яких має певне значення, межі та відповідає певним

вимогам. Основними з них є виникнення юридичної відповідальності, вияв правопорушення; офіційне визнання правопорушення як підстави відповідальності актом компетентного органу; реалізація юридичної відповідальності [95]. Стосовно вказаних вище характерних ознак О. В. Зайчук та Н. М. Оніщенко наголошують, що їх наявність є обов'язковою, а відсутність хоча б однієї з них свідчить про відсутність юридичної відповідальності та можливість застосування певного різновиду неправової соціальної відповідальності [95].

Отже, під юридичною відповідальністю за порушення закону у сфері кібербезпеки України варто розуміти застосування заходів примусового характеру, які визначені нормами чинного законодавства, до осіб, що вчинили правопорушення у кіберпросторі. Заходи юридичної відповідальності застосовуються лише у випадку винного діяння відповідного суб'єкта, а санкції повинні пропорційно відповідати рівню шкоди вчиненого діяння. Відповідно до нещодавно прийнятого Закону України «Про основні засади забезпечення кібербезпеки України» [10], 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 [10]. Виходячи із вказаного положення, до суб'єктів, що вчинили правопорушення у досліджуваній сфері, можуть бути застосовані такі види юридичної відповідальності: цивільна, адміністративна та кримінальна. Далі приділимо окрему увагу кожному із вказаних видів відповідальності.

Розглядаючи цивільну відповідальність, зазначу , що дана відповідальність — це самостійний вид юридичної відповідальності, який полягає у застосуванні державного примусу до правопорушника шляхом позбавлення особи певних матеріальних благ чи покладення обов'язків майнового характеру. До

правопорушника застосовуються санкції майнового характеру, які спрямовані на відновлення порушених прав та полягають у відшкодуванні збитків, стягненні неустойки чи пені. Особливості даного виду юридичної відповідальності, на думку Р. О. Стефанчука, є: 1) майновий характер; 2) стягується на користь потерпілої сторони; 3) компенсаційна природа, тобто спрямованість на відновлення майнового стану потерпілого [94]. Цивільна відповідальність, як підкреслює Н. В. Іванчук, — це насамперед компенсаційна відповідальність, яка означає, що одна із сторін компенсує завдані нею втрати, тому її називають майновою. Одночасно вона є і відновлювальною відповідальністю, тому що завдяки їй часто відновлюються порушені раніше певні права громадян, правове становище суб'єктів (повернення боргів, недійсні окремі види угод, тощо). Особливістю цивільної відповідальності є її чітко виражена позитивна, добровільна форма юридичної відповідальності, що передбачає можливість і належність добровільного виконання взятих на себе обов'язків, без використання примусу з боку держави. Сторона, що порушила взяті на себе обов'язки чи завдала збитків, може самостійно відшкодувати ці збитки, якщо потерпіла сторона на це погодиться [53, с. 47– 48].

Відзначу, що не беручи до уваги законодавче закріплення можливості притягнення осіб до цивільно-правової відповідальності за порушення законодавства у сфері забезпечення кібербезпеки, сьогодні відсутній механізм притягнення осіб до вказаного виду відповідальності. Крім того, не визначено чіткого переліку підстав притягнення правопорушника до вказаного виду відповідальності, про них лише окремо говориться в статтях Цивільного кодексу України. Так, особу може бути притягнено до цивільно-правової відповідальності за порушення прав інших учасників відповідних правовідносин, зокрема: 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);

обов’язок право володільця передавати інформацію користувачеві для здійснення прав, наданих йому за договором комерційної концесії (ст. 1120 ЦКУ); право на таємницю особистого життя (ст. 301 ЦКУ); майнові права інтелектуальної власності на комерційну таємницю (ст. 506 ЦКУ); обов’язки виконавця за договором на виконання науково-дослідних або дослідно-конструкторських та технологічних робіт утримуватися від публікації без згоди замовника науково-технічних результатів, одержаних при виконанні робіт (ст. 897 ЦКУ); тощо [3].

Варто зазначити, що цивільна відповідальність найрідше застосовується за порушення законодавства у площині кібербезпеки. Найбільш поширеними є санкції, передбачені адміністративним та кримінальним законодавством. Переходячи до наступного виду відповідальності за порушення законодавства у сфері кібербезпеки України, в першу чергу зазначу, що у найбільш загальному розумінні адміністративна відповідальність — це застосування до осіб, які вчинили адміністративні проступки, адміністративних стягнень, що обтяжують цих осіб у майновому, моральному, особистому чи іншому плані і накладаються уповноваженими на те державними органами чи посадовими особами на підставах і в порядку, встановлених нормами адміністративного права [84]. І. О. Галаган доводить, що адміністративна відповідальність — це застосування у встановленому порядку уповноваженими на це органами і службовими особами адміністративних стягнень, зазначених у санкціях адміністративно-правових норм, до винних осіб у вчиненні адміністративних проступків, що містять державний і громадський осуд, засудження їх особи і протиправного діяння, що виявляється у негативних для них наслідках, які вони зобов`язані виконати, і переслідують цілі їх покарання, виправлення і перевиховання, а також охорони суспільних відносин у сфері державного управління [41, с. 41].

Більш вичерпний перелік ознак адміністративної відповідальності, на мою думку, надає С. Т. Гочарук. Автор вказує, що для вказаного виду юридичної

відповідальності є характерними такі властивості: 1) це один із самостійних видів правової відповідальності (поряд з кримінальною, дисциплінарною та цивільно-правовою); 2) це форма правового регулювання з боку держави в особі її компетентних органів на категорію протиправних діянь; 3) це державно репресивний захід як результат протиправної поведінки особи; 4) це один із видів державного примусу, зокрема, адміністративний його різновид (одна із ланок заходів адміністративного примусу); 5) це водночас правовий обов'язок правопорушника дати відповідь перед повноважним державним органом щодо своїх неправомірних дій і понести за це певне покарання; 6) юридичною підставою для настання адміністративної відповідальності, є окремий вид правопорушень — адміністративні проступки; 7) засобами реалізації адміністративної відповідальності є самостійні юридично-імперативні (примусові) заходи — адміністративні стягнення; 8) адміністративна відповідальність — це правовідносини між органами (посадовими особами), що її застосовують, та правопорушниками, причому в таких правовідносинах відсутні елементи службового підпорядкування; 9) певними правами щодо встановлення та застосування адміністративної відповідальності наділене значне коло державних органів (посадових осіб); 10) це один із важливих адміністративно-правових інститутів, нормами якого значною мірою охороняється велика кількість суспільних відносин, урегульованих як адміністративно-правовими нормами, так і нормами інших галузей права; 11) адміністративна відповідальність реалізується в установлених законом формах та порядку, чітко визначених адміністративно-процесуальними нормами; 12) суб'єктами адміністративно-правової відповідальності можуть бути як фізичні, так і юридичні особи [43, с. 20–21; 102].

Тож, адміністративна відповідальність за порушення законодавства у сфері кібербезпеки — це застосування до особи, що вчинила правопорушення, санкцій, передбачених нормами адміністративного права. У більшості випадків санкції за

вчинення адміністративного проступку носять матеріальний (виражений у грошовому еквіваленті) характер. Відзначу, що у чинному Кодексі України про адміністративні правопорушення не виокремлено окремий розділ, який було б присвячено адміністративним проступкам за порушення законодавства у сфері кібербезпеки. Однак, в окремих статтях така відповідальність все ж таки передбачена. Наприклад, стаття 51-2 КУпАП встановила, що незаконне використання об'єкта права інтелектуальної власності, зокрема: комп'ютерної програми, бази даних, наукового відкриття, винаходу, корисної моделі, промислового зразка, знаку для товарів і послуг, топографії інтегральної мікросхеми, 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; стаття 1649 — 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; тощо [85].

Справедливо буде зазначити, що КУпАП містить більше ста статей, якими врегульовані питання відповідальності за порушення порядку створення, збирання, одержання, зберігання, використання, поширення, охорони та захисту інформації [85, с. 81]. Такі правопорушення, на слушну думку Т. С. Перуна, можна поділити на три основні групи :

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 [85].

Підсумовуючи огляд адміністративної відповідальності за порушення законодавства у сфері забезпечення кібербезпеки в Україні, варто відзначити неоднозначність законодавства, яке визначає засади даного виду юридичної відповідальності у даній сфері. Враховуючи зростання кількості правопорушень у кіберпросторі (зокрема, за 2019 рік в Україні було вчинено понад 3 тисячі правопорушень у цій сфері), сьогодні не викликає сумнівів необхідність систематизації положень про притягнення до адміністративної відповідальності осіб, що порушили законодавство про кібербезпеку. А отже, пропоную у чинному КУпАП створити окремий розділ, присвячений адміністративним проступкам у кіберпросторі.

Останній вид юридичної відповідальності за порушення законодавства у сфері кібербезпеки України — кримінальна. На думку А. В. Наумова, кримінальна відповідальність — це особливий правовий інститут, у межах якого здійснюється офіційна оцінка поведінки особи як злочинної. Кримінальна відповідальність закріплюється в обвинувальному вироку суду і зазвичай включає засудження особи за вчинений злочин, призначення їй покарання, його відбування, судимість, тощо [79, с. 17]. П. М. Давидов вказує, що кримінальна відповідальність — це така, що реалізується, покладається на винну у вчинені злочину особу, обов`язок якої полягає у відбуванні засудження, оскільки в законі кримінальна відповідальність не прирівнюється до покарання, обов`язковим і основним компонентом кримінальної відповідальності є засудження, яке визнається в теорії права елементом не лише кримінальної, але і будь-якої іншої

юридичної відповідальності, а основним кримінально-процесуальним актом, в якому виражається засудження, є вирок [44, с. 35]. Таким чином, кримінальна відповідальність за порушення законодавства у сфері кібербезпеки України настає у випадку вчинення особою злочину, здійснення якого мало найбільш шкідливі наслідки для іншої особи, суспільства, держави, тощо. Такий злочин у досліджуваній сфері має назву «кіберзлочин».

За останніх 15 років поняття «комп'ютерна злочинність» перетворилось у термін «кіберзлочинність» — поняття, яке охоплює власне комп'ютерну злочинність та інші протиправні діяння, де комп'ютер є знаряддям або способом вчинення злочину проти власності, авторських прав, громадської безпеки, моралі, тощо. Але, кіберзлочин — це будь-який злочин, який може вчинятися за допомогою комп'ютерної системи або мережі, в рамках комп'ютерної системи або мережі чи проти інформації в комп'ютерній системі або мережі. В принципі, цей термін охоплює будь-який злочин, який може бути скоєно в електронному середовищі [86]. Варто буде відзначити, що сьогодні поняття «кіберзлочин» має законодавче закріплення, зокрема, у Законі України «Про основні засади забезпечення кібербезпеки України». Відповідно до вказаного нормативно-правового акту, 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 [10**].**

Одною з найбільш характерних особливостей кримінальної відповідальності за кіберзлочини є те, що вона як у вузькому, так і широкому розумінні врегульовується Конвенцією про кіберзлочинність від 2001 року. При цьому, слід зазначити, що кримінальний закон окремо взятих країн світу визначає відповідальність за кіберзлочини лише у вузькому розумінні, не є виключенням і Україна [49, с. 129]. Держави–члени Ради Європи та інші держави, які підписали цю конвенцію, обґрунтовують, що вона 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 [47]. Вказаний вище міжнародний нормативно-правовий акт передбачає чотири групи злочинів, пов'язаних з використанням комп'ютерних технологій як інструменту їх учинення. До першої групи віднесено 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 — злочини, пов'язані з використанням комп'ютерних засобів (підроблення, шахрайство). До третьої групи віднесено злочини, пов'язані зі змістом даних (дитяча порнографія). До четвертої — злочини, пов'язані з порушенням авторського права та суміжних прав [83, с. 5; 92].

Підписуючи Конвенцію про кіберзлочинність, Україна взяла на себе обов'язок привести вітчизняне законодавство у відповідність до її положень. Все це відобразилось у Кримінальному кодексі України, наприклад, Розділі XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем комп'ютерних мереж і мереж електрозв'язку». Тож до положень вказаного розділу, передбачаються наступні санкції за вчинення кіберзлочинів: «Стаття 361. Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до

порушення встановленого порядку її маршрутизації, — карається штрафом від шестисот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк від двох до п’яти років, або позбавленням волі на строк до трьох років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до двох років або без такого. Стаття 361-1. Створення з метою використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку, — караються штрафом від п’ятисот до тисячі неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або позбавленням волі на той самий строк. Стаття 361-2. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп’ютерах), автоматизованих системах, комп’ютерних мережах або на носіях такої інформації, створеної та захищеної відповідно до чинного законодавства, — караються штрафом від п’ятисот до тисячі неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк до двох років. Стаття 362. Несанкціоновані зміна, знищення або блокування інформації, яка оброблюється в електронно-обчислювальних машинах (комп’ютерах), автоматизованих системах чи комп’ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї, — караються штрафом від шестисот до тисячі неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років. Стаття 363-1. Умисне масове розповсюдження повідомлень електрозв’язку, здійснене без попередньої згоди адресатів, що призвело до порушення або припинення роботи електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку, — карається штрафом від п’ятисот до тисячі неоподатковуваних

мінімумів доходів громадян або обмеженням волі на строк до трьох років; тощо» [4]

Проте, як зазначив Ю. Ю. Орлов, список кіберзлочинів не вичерпується діяннями, визначеними в розділі XVI Особливої частини КК України. Окремі злочини, що існували раніше до повномасштабного використання комп'ютерів, також можуть бути вчинені із застосуванням інформаційних технологій. Використання комп'ютерів спрощує вчинення злочину або уможливлює його вчинення в нових формах. 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, тощо (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); увезення, виготовлення, збут і розповсюдження порнографічних предметів (ст. 301 КК України); порушення авторського права й суміжних прав (ст. 176 КК України) [83, с. 5; 97].

Підсумовуючи даний підрозділ магістерської роботи, варто сказати, що питання юридичної відповідальності за порушення законодавства у сфері кібербезпеки України є недостатньо вирішеним, що беззаперечно можна вважати суттєвою прогалиною, яка сприяє зростанню рівня кіберзлочинності в нашій державі. Наприклад, питання притягнення правопорушника у сфері кібербезпеки до цивільної та адміністративної відповідальності регулюється цілою низкою законодавчих актів, в кожному із яких містяться різні підстави притягнення особи до відповідальності. Така розкиданість ускладнює застосування стягнень до винних осіб органами державної влади. Таким чином, з огляду на все зазначене вище, вважаю що необхідно внести зміни до Закону України «Про основні засади забезпечення кібербезпеки України», зокрема, більш детально окреслити види

правопорушень та кіберзлочинів, через які особу може бути притягнено до того чи іншого виду юридичної відповідальності [83]. Все вказане зробить відповідне законодавство більш кодифікованим та узгодженим, а отже, і позитивно вплине на якість забезпечення кібербезпеки в державі.

РОЗДІЛ 3
УДОСКОНАЛЕННЯ АДМІНІСТРАТИВНО-ПРАВОВИХ ЗАСАД ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

3.1 Зарубіжний досвід забезпечення кібербезпеки та можливості його використання в Україні

Сьогодні вже ніхто не сумнівається, що існуючий в Україні механізм забезпечення кібербезпеки є недосконалим та потребує доопрацювання. В цьому аспекті відмітю, що для розуміння шляхів покращення даного механізму є неможливим без опрацювання зарубіжного досвіду, що особливо є актуальним у прагненні України адаптувати вітчизняне законодавство до європейських та світових стандартів. Тому в аспекті представленої дипломної роботи я не лише приділяю увагу досвіду найпотужніших країн Європи, а й розглядаю інші успішні держави світу, наприклад, США, Японію, Китай, тощо. Розглядаючи країни Європи, в першу чергу приділимо увагу досвіду Великобританії, адже сьогодні в цій країні питання кібербезпеки виходить на першочергові місця, що підтверджується тим, що у листопаді 2016 року Уряд Великої Британії оприлюднив 5-річний план реалізації Стратегії національної кібербезпеки і виділив на це рекордні 1,9 млрд. фунтів**.**

Однак перед тим як ми розглянемо досвід провідних країн світу , хотів би описати досить оригінальний вихід із ситуації такої країни як Уганда. Так , з 1 липня 2018 року в цій країні набув чинності закон , яким запроваджено податок на користування соціальними мережами «Facebook» , «Whats App» , «Viber» «Twitter». Користувачі забовязані платити 200 угандійських шилінгів на день ($

0,05). Кошти , одержані від податку , повинні використовуватися для посилення захисту кіберпростору та розширення життєзабезпечення мереж електропостачання , щоб громадяни могли частіше користуватися соціальними мережами.

Таким чином , у кожній країні існує власне національне тлумачення поняття « кібербезпека». Як наслідок , відрізняється і підходи до формування стратегій кібербезпеки. Проте керівні документи , що хоплюють питання кібербезпеки , як правило, передбачають:

1. побудову державної системи управління у сфері забезпечення кібербезпеки;
2. визначення відповідного механізму (в основному суспільно - державного партнерства) , що дає змогу приватним і державним зацікавленим сторонам обговорювати проблеми забезпечення безпеки національних інформаційних інфраструктур;
3. регламентацію стратегічних засад політики безпеки та регулюючих механізмів, чіткий розподіл завдань , прав і відповідальності для приватного і державного секторів (наприклад, обовязкове інформування про кіберінциденти , оцінка загроз , розробка критеріїв віднесення обєктів до критичної інформаційної інфраструктури тощо).

Нині більшість держав світу успішно проводять політику посилення кібербезпеки та її складників. У міжнародному форматі можна виділити три основні моделі правового врегулювання поширення інформації в мережі Інтернет:

- перша модель передбачає тотальний , жорсткий контроль держави над мережею Інтернет. Такої моделі дотримується , наприклад , КНР, де практично весь інтернет перебуває під повним державним контролем. Окремі елементи китайського досвіду сьогодні впроваджуються в практичну площину в країні-агресорі РФ.

- друга модель передбачає відповідальність провайдера за будь-які дії користувача. Наприклад у Франції провайдери забовязані надавати відомості про авторів сайтів на вимогу третіх осіб. Крім того , у Франції ще з 1978 року існує спеціальний орган (Національна комісія інформатики і свобод) , який забовязаний контролювати , щоб інформація в мережі не порушувала права і свободи людини.
- третя модель регулювання безпеки в мережі Інтернет передбачає звільнення провайдера від відповідальності в тому разі, якщо він виконує певні умови умови, повязані з характером надання послуг і взаємодії із субєктами інформаційного обміну. Так , у Німеччині відповідальність провайдерів за розміщення нелегального контенту на Інтернет- ресурсах, що знаходиться в їх мережі, настає у разі , якщо вони самі є власником інформації або свідомо поширювали її з посиланням на інші джерела. Така модель також активно використовується в Японії.

За таких умов можна констатувати , що кожна країна світу вибирає власну модель розбудови національної системи кібербезпеки . Наприклад , Казахстан у цьому сенсі не є винятком, і так як це є пострадянська країна , вона на мою думку близька до України.

Розглянемо досвід цієї країни у сфері організаційно-правового забезпечення кібербезпеки. Так, у своєму посланні до народу Казахстану від 31 січня 2017 року Презедент Н. А. назарбаєв доручив Комітету національної безпеки і Уряду країни створити систему « Кіберщит Казахстану» . Концепція заснована на оцінці поточної ситуації у сфері інформатизації державних органів , автоматизації державних послуг , перспектив розвитку « цифрової» економіки і технологічної модернізації виробничих процесів у промисловості , розкомунікаційних послуг. Концепція визначає основні напрямки у сфері захисту електронних інформаційних , інформаційних ресурсів, інформаційних систем та мереж

телекомунікацій , забезпечення сталого й безпечного використання інформаційно-комунікаційних технологій.

Законодавство Казахтану декларує необхідність формування єдиного підходу до моніторингу забезпечення інформаційної безпеки державних органів , фізичних і юридичних осіб, а також вироблення механізмів попередження й оперативного реагування на кіберінциденти у тому числі в умовах надвичайних ситуацій соціального , природного і техногенного характеру, введення надзвичайного або воєнного стану.

Під час розроблення концепції враховувася міжнародний досвід у галузі формування підходів до захисту національної інформаційно-комунікаційної інфраструктури як держав лідерів у сфері розробки та використання інформаційно-телекомунікаційних технологій , так і країн , що прагнуть розширити сферу їх застосування для досягнення цілей соціально-економічного розвитку. При цьому в положеннях зазначеного програмного документа акцент зроблений на тому, що транснаціональна кіберзлочинність використовує IT-продукцію іноземного виробництва у своїх цілях з метою вчинення протиправних дій стосовно користувачів і операторів ІКГ – послуг і власників Інтернет- ресурсів, розміщених у національному сегменті, а також інформаційних систем , що взаємодіють із мережею Інтернет.

У положеннях Концепції анонсовано , що висока латентність і часто міжнародний характер кіберзлочинів підвищують їх суспільну небезпеку. Ситуація ускладнюється сформованим в суспільстві стереотипами про безкарність так званої « кібезлочинності» , неефективність вжитих державою заходів щодо зміцнення сфери безпечного використання ІКГ, обмеженні можливості органів правопорядку щодо притягнення до відповідальності винних у скоєнні високотехнологічних злочинів , незважаючи на розвинені кримінально-правові інститути інформаційної безпеки. У глобальному мвсшабі здійснюється активна мілітаризація сфери ІКГ.

Законодавством Казахстану встановлено, що кібербезпека має реагувати на такі потужні загрози, як:

- низька правова грамотність населення , працівників ІКГ та керівників організацій з питань інформаційної безпеки;
- порушення державними і недержавними субєктами інформатизації та користувачами послуг у сфері ІКГ встановлених вимог , технічних стандартів і регламентів збору, обробки , зберігання та передачі інформації в електронній формі;
- ненавмисні помилки персоналу і технологічні збої . що чинять негативний вплив на інформаційні ресурси та системи , програмне забезпечення й інші елементи інформаційно-телекомунікаційної інфраструктури;
- діяльність міжнародних злочинних організацій, спільнот і окремих осіб щодо здійснення розкрадань у фінансово-банківській сфері , а також шкідливий вплив з метою порушення штатної роботи автоматизованих систем управління технологічними процесами промисловості, транспорту , енергетики , звязку та у сфері інформаційно-комунікаційних послуг;
- діяльність терористичних чтруктур , розвідувальних і спеціальних служб іноземних держав. Спрямована на підрив економічного потенціалу Республіки Казахстан шляхом здійснення розвідувального та підривного впливу на інформаційно-телекомунікаційну інфраструктуру.

Загалом очікується , що практичне впровадження положень Конвенції дасть змогу забезпечити підтримку максимального рівня захищеності електронних інформаційних ресурсів , інформаційних систем та обєктів інформаційно-комунікаційної інфраструктури від зовнішніх і внутрішніх загроз, сприятиме сталому розвитку країни в умовах глобальної економічної та інформаційної конкуренції.

Повертаючись до провідних країн світу таких як Англія , варто розказати про те чим вони керуються у власному захисті проти кібератак. Основним же

документом, що спрямований на забезпечення кібербезпеки у Великобританії, є Стратегія національної кібербезпеки 2016– 2021 рр., яку було прийнято замість аналогічної стратегії 2011–2015 рр. Основна мета Стратегії на 2021 рік полягає в тому, щоб зробити Великобританію безпечною і стійкою до кіберзагроз, процвітаючою і впевненою в цифровому світі. Для цього, на думку законодавців країни, є необхідним: 1) виділяти достатньо коштів для захисту Великобританії від розвитку кіберзагроз; ефективно реагування на інциденти і забезпечувати захист і стійкість мереж і даних у Великобританії; 2) виявляти, розуміти, розслідувати ворожі дії, що вживаються проти Британії; 3) розробляти та сприяти розвитку інноваційних технологій та індустрії кібербезпеки; 4) сприяти розвитку кадрового потенціалу. Слід також відмітити, що ця Стратегія стосується кіберзлочинності в контексті двох взаємопов’язаних форм злочинної діяльності: 1) кіберзалежність злочинів, тобто злочинів, які можуть бути здійснені тільки з використанням пристроїв інформаційнокомунікаційних технологій (ІКТ), де ці пристрої є інструментом для вчинення злочину і метою злочину (наприклад, розробка та поширення шкідливого програмного забезпечення для фінансової вигоди, зламати, щоб вкрасти, пошкодити, спотворити або знищити дані та/або мережу або діяльність); а також 2) злочини, пов’язані з використанням кібератаки, — традиційні злочини, які можуть бути збільшені в масштабі або охоплені за допомогою комп’ютерів, комп’ютерних мереж або інших видів ІКТ (таких як шахрайство з використанням кібертехнологій і крадіжка даних).

Відповідно до положень чинного законодавства, основний обов'язок уряду Великобританії полягає в тому, щоб захистити країну від нападів інших держав, захистити громадян і економіку від шкоди і встановити внутрішні і міжнародні рамки для захисту інтересів країни. Будучи власником значних даних і постачальником послуг, уряд приймає суворі заходи для забезпечення гарантій для своїх інформаційних активів. Уряд також несе відповідальність за консультування та інформування громадян про стан виконання Національної

стратегії кібербезпеки 2016 року. Крім того, уряд повинен інформувати громадян про те, що потрібно зробити, щоб захистити себе в Інтернеті, а за необхідності встановити стандарти, дотримання яких Великобританія очікує від ключових компаній і організацій. В Стратегії підкреслюється, що хоча ключові сектори економіки країни знаходяться в приватних руках, уряд в кінцевому рахунку несе відповідальність за забезпечення національної безпеки.

Слід звернути увагу на те, що з метою реалізації Стратегії 1 жовтня 2016 року було створено Національний центр кібербезпеки (NCSC). NCSC надає можливість для створення ефективних партнерських відносин в області кібербезпеки між урядом, промисловістю і громадськістю, щоб у результаті забезпечити безпеку Великобританії в Інтернеті. Вперше ключові сектори зможуть безпосередньо взаємодіяти з Центром для отримання найкращих можливих рекомендацій і підтримки щодо захисту мереж і систем від кіберзагроз. NCSC забезпечує: 1) єдине джерело консультацій для попередження загрози кібербезпеки і забезпечення інформації; 2) ефективну та прозору роботу уряду по боротьбі з кіберзагрозами, працюючи рука об руку з промисловістю, науковими колами та міжнародними партнерами, щоб захистити Великобританію від кібератаки. В процесі виконання Стратегії буде встановлено поетапний підхід до побудови можливостей NCSC.

Цікавим є той факт, що Британське Національне агентство по боротьбі зі злочинністю (NCA), в рамках Стратегії національної кібербезпеки 2016 року, відкрило перший реабілітаційний центр для людей, які були засуджені до ув'язнення за кіберзлочини. Як пише BBC, у ньому їх навчають використовувати свої уміння та навички у більш конструктивних та легальних цілях та готують до роботи в спецслужбах. Нині центр відвідують вісім молодих людей, які потрапили в поле зору правоохоронців за нелегальні дії ще у підлітковому віці. Деякі з них ламали сайти чи сервери, здійснювали кібератаки, змушували користувачів розкривати свої персональні дані, зламували шкільні мережі або ж

іншим чином порушували британське законодавство про використання комп'ютерів [89]. Серед слухачів центру є й ті, хто в грудні 2016 року брав участь в атаці на британського провайдера TalkTalk. Тоді було пошкоджено майже 5 мільйонів роутерів. За словами самих хлопців, вони здебільшого робили подібні дії «для розваг». Більшість учасників центру отримали умовні терміни, але їх також зобов'язали ходити на реабілітацію кожні вихідні. Вони відвідують лекції про судово-медичний аналіз та захист мереж компаній від атак. Також їх вчать шукати лазівки в системах безпеки і повідомляти про них керівництву за винагороду. Крім того, хакерам розповідають про вакансії в службі кібербезпеки [98].

Тож аналіз Стратегії національної кібербезпеки Англії на 2016–2021 роки дає нам змогу стверджувати те, що вона містить низку інноваційних та цікавих положень та взагалі потребує окремого наукового дослідження. Позитивними моментами вказаної Стратегії є те, що в ній: 1) визначено та закріплено офіційне тлумачення низки понять у сфері забезпечення кібербезпеки (наприклад, кібернетична оборона, активна кібернетична оборона, тощо); 2) детально окреслено напрямки та етапи запровадження інновацій у сфері забезпечення кібербезпеки; 3) суттєва увага приділена навчанню населення щодо того, як захистити себе від можливих порушень їх прав у досліджуваній сфері; 4) виокремлено напрямки навчання персоналу, адже забезпечення кібербезпеки є неможливим без відповідного кадрового забезпечення.

Ще одна провідна країна досвід якої знадобиться нам в пригоді — Німеччина, адже саме ця держава є прикладом того як ефективно боротись із кіберзлочинністю. Проте, в останні декілька років у Німеччині спостерігається різке зростання кіберзлочинності. 2016 року кількість скоєних кримінальних діянь з використанням Інтернеттехнологій сягнула 82649 випадків, у той час як в 2015 році поліція зареєструвала 45793 кіберзлочини. Але із впевненістю можна сказати що дані про розкриття подібних злочинів також збільшуються у

статистичному відображенні .У цілому кількість розкритих правопорушень такого типу зросла на 5,9%, досягнувши рівня в 38,7%. І така тенденція в державі продовжується й досі [97]. В силу цього А. Меркель наголосила, що кібербезпека має «надзвичайно важливе значення». Вона зазначила, що уряд Німеччини актуалізував стратегію кібербезпеки. Крім того, федеральний уряд готовий співпрацювати з містами та громадами. Вона також закликала представників органів місцевої влади та підприємств звертатися до Федеральної служби безпеки в сфері інформаційних технологій у разі виявлення підозрілих випадків [77].

Як і у Англії , у 2011 р. в Німеччині було прийнято Стратегію кібербезпеки Німеччини, відповідно до якої федеральний уряд впроваджує заходи на основі вже створених структур до відповідних рівнів загроз за наступними стратегічними напрямками [47, с. 113–115]:

1. Захист найважливіших інформаційних інфраструктур. В центрі уваги кібербезпеки лежить захист найважливіших інформаційних структур, адже безпека має важливе значення в постійно зростаючих майже всіх найважливіших інфраструктурах [93; 63, с. 114].

2. Посилення ІТ-безпеки в публічному управлінні. Публічне управління ще сильніше захистить свої ІТ-системи. Державні установи повинні бути зразком щодо захисту даних. Основою електронного обміну даними і вербальної комунікації буде загальна, універсальна і надійна мережева інфраструктура Федеральної адміністрації («федеральна мережа») [93; 63, с. 114].

3. Для оптимізації оперативної співпраці усіх державних установ і покращення координації заходів щодо захисту проти ІТ-випадків було створено Національний центр кіберзахисту. Він працює під керівництвом Федерального відомства з інформаційної безпеки (BSI) і за безпосередньою участю Федерального відомства захисту конституції (BfV), а також Федерального відомства з питань захисту населення і допомоги при стихійних лихах (BBK) [112; 63, с. 113].

4. Ефективна боротьба зі злочинністю у кіберпросторі. Посилюються повноваження правоохоронних органів, Федеральної служби безпеки в сфері ІТ і економіки в контексті подолання ІКТ-злочинності (стосовно захисту від шпіонажу і диверсій).

5. Ефективна співпраця у кібербезпеці в Європі та у світі. Безпека в глобальному кіберпросторі досягається лише за допомогою сукупності узгоджених засобів та методів на національному і міжнародному рівнях.

6. Використання надійних і достовірних інформаційних технологій. Необхідно забезпечувати можливість доступу до перевірених ІТ-систем і ІТкомпонентів. Модернізаціія інноваційних програм захисту для покращення безпеки буде прискорюватись, враховуючи суспільні та економічні аспекти. Тому ФРН буде продовжувати розвивати відповідні дослідження в ІТ-безпеці і найважливіших інфраструктурах [47, с. 113–115].

У липні 2015 р. у Німеччині був прийнятий Закон «Про інформаційну безпеку» для запобігання атакам на важливі інформаційні системи. Закон зазначає мінімальні стандарти кібербезпеки для більш ніж 2 тисяч компаній — операторів критичної інфраструктури. Відповідно до закону, ці мінімальні вимоги до безпеки мають забезпечуватися шляхом вдосконалення доступності, автентичності, конфіденційності та цілісності ІТ-безпеки у всій Німеччині; підвищення безпеки Інтернету для громадян; кращого захисту критично важливої інфраструктури національного значення [113; с. 21].

Тож, в Німеччині досить багато уваги приділяється питанню забезпечення кібербезпеки, про що говорить розгалужена система органів державної влади у досліджуваній сфері. Крім того, в державі активно застосовується міжнародне співробітництво, що, в свою чергу, дозволяє більш ефективно та оперативно виявляти загрози у досліджуваній сфері та розвивати вітчизняне законодавство і технології. Із позитивного також варто вказати те, що в країні постійно

відбувається розширення заходів, спрямованих на реалізацію державної політики у сфері забезпечення кібербезпеки.

Досліджуючи дану тему , не можна не звернути увагу на країну–сусіда Польщу, яка сьогодні активно займається розвитком кіберзахисту на державному рівні [56]. За прогнозами аналітиків, через два-три роки Польща буде лідером в IT-галузі в країнах Центрально-Східної Європи. А вже нині півмільйона осіб працює в польському секторі високих технологій, а вартість ринку IT-послуг у Польщі сягнула майже 3,5 мільярда доларів і продовжує зростати. Стрімкий розвиток цього сектору приваблює в країну закордонних інвесторів та програмістів–іноземців, зокрема, українців. Якщо тенденції розвитку польського ITсектору зберігатимуться, то в 2021 році його вартість досягне 4 мільярдів доларів, тоді як ринок IT-послуг усієї Центрально-Східної Європи коштуватиме 11 мільярдів доларів. Такі дані оприлюднила дослідницька фірма IDC. Через позитивну динаміку багато фірм з різних країн світу вирішують розмістити свої підприємства саме у Польщі [89]. Що ж надало Польші такий стрімкий стрибок? По-перше, уряд ухвалив зміни до законодавства, які дозволяють запроваджувати у країні надзвичайний стан в разі атаки у віртуальному просторі. Такими юридичними змінами можуть похвалитися небагато держав. По-друге, влада погодилася з недоцільністю функціонування кількох інституцій по боротьбі із кіберзагрозами, які лише дублювали одна одну. У 2011 році було створене Міністерство адміністрації і цифровізації, завданнями якого стали забезпечення кібербезпеки у військовій сфері, захист конфіденційності громадян, побудова національної освітньої платформи, залучення до Інтернету людей похилого віку і жителів віддалених районів країни. По-третє, в рамках Міністерства цифровізації у 2016 році створили Національний центр кібербезпеки. Його ключовим завданням стало попередження загроз, реакція на них та координація дій. Робота центру — приклад державно-приватного партнерства у сфері кіберзахисту. Працює центр цілодобово. По-четверте, Польща опрацювала нову

стратегію кібербезпеки. Вона передбачає, що до 2022 року влада гарантуватиме безпеку громадян, суб'єктів економічної діяльності і державних установ у галузі кібербезпеки [106]. Більш конкретними цілями вказаної стратегії є: 1) досягти здатності координувати дії на національному рівні, спрямовані на запобігання, виявлення, боротьбу та мінімізацію наслідків та/або інцидентів, що порушують безпеку систем ІКТ, необхідних для функціонування держави; 2) посилення здатності протистояти кіберзагрозам; 3) підвищення національного потенціалу та компетенції в галузі безпеки в кіберпросторі; 4) формування сильної міжнародної позиції Республіки Польща у сфері кібербезпеки.

Окрему увагу хотів би звернути на Міністерство адміністрації і цифровізації, до завдань якого віднесено: розробка та реалізація стратегічних документів і правових актів в області кібербезпеки, проведення національного і міжнародного співробітництва, розробка керівних принципів для створення відповідних заходів щодо захисту інформаційних систем, підготовка аналізу щодо стану кібербезпеки на національному рівні, а також розробка центральних навчальних планів, вправ та випробувань. Міністерство активно співпрацює з іншими відомствами, університетами, інститутами, неурядовими організаціями та приватним сектором при виконанні завдань. Міністерство у співпраці з іншими організаціями є вкрай важливими суб'єктами для забезпечення безпеки кіберпростору, зокрема, підготовлено два документи для вдосконалення та розвитку національної системи кібербезпеки. 27 квітня 2017 р. Рада міністрів прийняла стратегічний документ — Національні рамки політики кібербезпеки Республіки Польща на 2017– 2022 роки. 31 жовтня минулого року політика була спрямована на громадські консультації та міжміністерські консультації щодо проекту закону про національну систему кібербезпеки [109].

Найбільш прискіпливої уваги заслуговує наступна країна – Сполучені Штати Америки .На сьогоднішній день законодавство США у сфері забезпечення інформаційної безпеки складається з федеральних законів та законів штатів, які

створили юридичну основу для формування єдиної державної політики в галузі захисту інформації для забезпечення інтересів національної безпеки. Це, такі Закони: «Про інформаційну безпеку», «Про удосконалення інформаційної безпеки» (1997 р.), «Про комп'ютерне шахрайство та зловживання» (1986 р.), «Про свободу інформації» (1967 р.), «Про висвітлення діяльності уряду», «Про охорону особистих таємниць», «Про таємницю» (1974 р.), «Про право на фінансову таємницю» (1978 р.), «Про доступ до інформації про діяльність ЦРУ» (1984 р.), «Про безпеку комп'ютерних систем» (1987 р.) [35].

Також хотілося б звернути увагу на те, що у Конгресі представлений законопроект, що передбачає створення посади посла США по кіберпростору, а також впровадження американської міжнародної кібердипломатії. У разі прийняття закону Держдепартамент США буде зобов'язаний включати в щорічні доповіді про дотримання прав людини в світі оцінки про свободу Інтернету. Останнім часом відносини Росії, Китаю і США помітно погіршилися, особливо стосовно кіберпростору. США звинувачують російську владу у втручанні у вибори Президента, що виразилося у зломі пошти штабу кандидата в Президенти Хілларі Клінтон, а також створенні фейкових акаунтів в соціальних мережах і спробах впливати на думку виборців через рекламу на Facebook [107, с. 31]. Якщо ж вказаний законопроект буде запроваджено у життя, то це в кінцевому результаті суттєво вплине на забезпечення кібербезпеки не лише в США, а й в усьому світі.

Ні для кого не є секретом що Солучені Штати Америки володіють достатнім матеріальним потенціалом для впровадження достатнбого захисту проти кібератак на всіх рівнях. Крім того, у розпорядженні Кіберкомандування і спецслужб США сьогодні є достатній арсенал засобів протидії, які розроблені за попередні роки. Слід також відмітити, що в Сполучених Штатах особлива увага приділяється навчанню населення того, як захистити себе від правопорушень у досліджуваній сфері, що, в свою чергу, беззаперечно впливає на загальний стан

забезпечення кібербезпеки у державі. З позитивного боку хотілося б відмітити активну діяльність спецслужб у сфері забезпечення кібербезпеки, досвід роботи яких, беззаперечно, був би корисним і для нашої держави.

І остання країна, якій я приділив увагу, — Китайська Народна Республіка, діяльність якої у сфері забезпечення кібербезпеки пов'язана в першу чергу із жорстким контролем над будь-якою інформацією у мережі Інтернет. Сьомого листопада 2016 року Уряд Китаю схвалив новий закон щодо кібербезпеки, спрямований на подальше посилення і централізацію державного контролю над Інтернетом, в тому числі над роллю, яку відіграють іноземні компанії в китайському кіберпросторі. Закон, прийнятий в постійному комітеті законодавчого органу Китаю, дає завдання установам і підприємствам поліпшити їх здатність захищатися від мережевих вторгнень, вимагаючи перевірки безпеки обладнання і даних в стратегічних секторах. Закон, зокрема, містить положення, що зобов'язує інтернет-операторів надавати «технічну допомогу» владі в справах, пов'язаних з національною кібербезпекою . Він вимагає перевірки безпеки устаткування для «критичної інфраструктури», яка визначається як така, що стосується інформаційних послуг, енергетики, транспорту, фінансів та інших важливих секторів [55]. Під час розробки закон критикували іноземні бізнес-групи і технічні експерти, називаючи його основою для подальшого відгородження вже ізольованого Інтернету у Китаї. Китайські законодавці описали закон як необхідність для зміцнення безпеки в Інтернеті у часи поширення великої кількості загроз [55]

Слід звернути увагу на те, що в Китаї особлива увага приділяється кадровому підбору. Даний факт підтверджується тим, що в країні розпочато будівництво першого інституту з підготовки фахівців кібербезпеки, на який буде витрачено близько 800 млн дол. США, а до 2027 року в КНР планується побудувати 4–6 таких навчальних закладів. Все це, беззаперечно, підтверджує серйозність намірів країні щодо забезпечення кібербезпеки. А відтак,

незважаючи на те, що в більшості країн світу політика Китаю вбачається не вірною та такою, що суперечить міжнародним нормативно-правовим актам, але, не можна не погодитись, що така політика країни є доволі ефективною, що в тому числі підтверджує статистика вчинення кіберзлочинів у державі [36]

Тож, підсумовуючи весь наведений матеріал у даному підрозділі магістерської роботи, можу із впевненістю сказати, що сьогодні світові тенденції розвитку інформаційного суспільства спонукають всі держави для прийняття заходів щодо забезпечення кібербезпеки. Не є виключенням і Україна, яка нині знаходиться лише на перших етапах розвитку цього інституту. Аналіз досвіду вказаних вище країн дає змогу виокремити наступні напрямки розвитку інституту забезпечення кібербезпеки в Україні:

– по-перше, необхідно збільшити фінансування суб'єктів, діяльність яких спрямована на забезпечення кібербезпеки ;

– по-друге, слід покращити якість освіти працівників кіберполіції;

– по-третє, кардинального оновлення потребує Стратегія кібербезпеки України.

– по-четверте, необхідно розширювати міжнародне співробітництво у сфері забезпечення кібербезпеки, не обмежуючись співпрацею з однією конкретною країною (в нашому випадку — США);

– по-п'яте, необхідно посилити контроль у мережі Інтернет (на прикладі Китаю).

3.2 Напрямки удосконалення адміністративного законодавства, яке регулює забезпечення кібербезпеки в Україні

В ході написання магістерської роботи я неодноразово наголошував, що законодавство, яке врегульовує забезпечення кібербезпеки в Україні, є

недосконалим та потребує кодифікації, що, в свою чергу, обумовлює необхідність проведення ґрунтовних наукових досліджень, присвячених вказаній проблемі.

Визначаючи шляхи вдосконалення законодавства у галузі забезпечення кібербезпеки, в першу чергу слід звернути увагу на прийнятий Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року. І в першу чергу відмітю досить широке коло суб'єктів забезпечення кібербезпеки в Україні, однак, при цьому у вказаному вище нормативно-правовому акті не визначено єдиного органу, до повноважень якого повинно бути віднесене оперативне командування всіма іншими суб'єктами у цій сфері. Взагалі питання оптимізації суб'єктів забезпечення кібербезпеки в Україні є дуже актуальним, а тому йому буде приділено окрему увагу у наступному підрозділі дипломної роботи.

Ще можна звернути увагу на один недолік, , — це термінологічна недосконаліть вказаного вище закону, так як деякі терміни вбачаються занадто «простими» та не відображають всю специфіку та ясність окремих категорій. Законодавець визначає кібертероризм як «терористичну діяльність, що здійснюється у кіберпросторі або з його використанням». На мою думку, більш вдале трактування «кібертероризму» надає Б. В. Кузьменко, який зазначає, що цей термін слід розуміти 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 [65, с. 22].

Хотів би зауважити на те, що в законі відсутнє тлумачення таких понять як, «кіберправопорушення» та «кіберпроступок», що є досить незрозумілим, тому що законодавством передбачено такі види відповідальності як цивільна та адміністративна.Тому пропоную до Закону України «Про основні засади

забезпечення кібербезпеки України» включити вказані терміни і надати їм ґрунтовні визначення.

Зважаючи на ситуацію в країні слід вказати позицію керівництва СБУ, яке підтримує прийняття Верховною Радою України проекту Закону «Про внесення змін до деяких законодавчих актів України щодо протидії загрозам національній безпеці в інформаційній сфері». Служба Безпеки України стверджує, що внесення змін у чинне законодавство в частині забезпечення інформаційної безпеки та кібербезпеки забезпечить впровадження правового механізму блокування інформаційного ресурсу (сервісу) на підставі рішення слідчого судді та суду у кримінальному провадженні. Блокування можливе за рішенням РНБО України, прийнятим відповідно до Закону України «Про санкції». Застосування РФ під час гібридної війни новітніх технологій проти України перетворило інформаційну сферу та кіберпростір на одну з ключових арен протиборства з агресором. Починаючи з 2014 року, відбулися численні кібератаки з використанням шкідливого програмного забезпечення на об’єкти інформаційної критичної інфраструктури та державні установи. Ініційовані спецслужбами РФ кібератаки викликали тимчасове припинення енергопостачання, що створило реальні передумови для надзвичайних ситуацій техногенного характеру, вивели з ладу десятки серверів й електронних систем, блокували систему бюджетних виплат та надання банківських і адміністративних послуг. Передбачене проектом закону унормоване ведення відкритого у загальному доступі Єдиного реєстру виконання судових рішень і застосування санкцій у сфері телекомунікацій, наявність прозорої процедури прийняття процесуальних рішень про тимчасове блокування доступу до інформаційних ресурсів (сервісів) забезпечать демократичний цивільний контроль над діями СБУ для зміцнення національної безпеки України. Крім того, відповідно до прийнятого Закону України «Про національну безпеку України» також здійснюватиметься парламентський контроль за діяльністю органів сектору безпеки і оборони [99]

Також хотів би звернути увагу на Стратегію кібербезпеки України від 15 березня 2016 року [12].Попередньо я вже зазначав що дана стратегія є досить не досконалою , і в ній містяться певні розбіжності , на яких я хотів би сконцентруватись більш детально :

1. Перший недолік, на який я хотів би звернути увагу, — це відсутність конкретних термінів (строків) під час яких має настати реальний результат , на які приймається Стратегія. Я вважаю, що найбільш оптимальним строком прийняття Стратегії кібербезпеки в Україні є 4–5 років. Така моя пропозиція обґрунтовується кількома фактами: по-перше, у всіх найбільш успішних країнах (у сфері забезпечення кібербезпеки) такі стратегії приймаються щонайменше на 3-4 роки, а найбільше — на 5; по-друге, кіберпростір — це така сфера, яка постійно трансформується та розвивається, в ній виникають нові виклики та проблемні питання, які стосуються кібербезпеки. А відтак, і нормативно-правові акти у цьому напрямку повинні оновлюватись частіше, щоб уникати прогалин в ньому.

2. В Стратегії повинна зазначатись сума грошових коштів, яка має бути витрачена на її реалізацію, тобто повинен визначатись кошторис. Так, наприклад, у Великобританії, Франції, Польщі та інших країнах, перш ніж затвердити стратегію, визначається бюджет, від якого законодавець відштовхується при формуванні плану реалізації останньої.В Законі України «Про основні засади забезпечення кібербезпеки України» вказується, що 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 [10]. Однак, при цьому, на мою думку, в Стратегії має бути чітко визначено, куди повинні бути використані кошти державних та місцевих бюджетів, тобто окреслено їх цільове призначення.

3. Найбільшою проблематикою на мою думку є те що, у Стратегії забезпечення кібербезпеки в Україні не приділена достатня увага кадровому питанню суб'єктів, що уповноважені забезпечувати кібербезпеку в Україні. Кадрове забезпечення — це система підготовки, що має на меті навчання та виховання фахівців, які здатні розв'язувати складні завдання у сфері забезпечення кібербезпеки [28]. Кадрове забезпечення характеризується низкою ознак, серед яких варто особливо відмітити такі: 1) являє собою триваючий в часі динамічний процес, який має неоднорідну структуру; 2) здійснюється на постійній основі, починається з професійної підготовки (період до призначення) та закінчується звільненням із подальшим призначенням пенсії або переведенням до іншого місця роботи (період після звільнення); 3) основний період кадрового забезпечення починається після призначення; здійснюється кадровими службами відповідної управлінської структури; 4) його організація на конкретному підприємстві, установі, організації регламентується законодавством, підвідомчими нормативно-правовими актами, а також локальними актами; 5) метою кадрового забезпечення є укомплектування підприємства, установи або організації кваліфікованими кадрами, постійна робота з кадрами, що включає підвищення кваліфікації, перепідготовку, забезпечення службової або трудової дисципліни, тощо [100]. Так як це діє у США , на сьогоднішній день структура кіберкомандування США охоплює понад 50 тис. осіб і представляє собою складну багаторівневу структуру, що об'єднує зусилля Міністерства оборони США , АНБ та Кіберкомандування США і нараховує 133 бойові команди чисельністю понад 6,2 тис осіб. У Кіберстратегії має бути чітко відмічено кількість фахівців яку планується підготувати, напрями підготовки фахівців , установи які будуть навчати відповідні кадри (як це передбачено у стратегії Казахстану) .Має бути чіткий план , який необхідно закріпити достатньою кількістю матеріальних активів , з якими у нашій країні проблема.

4. Не можна також не звернути увагу на те, що в Стратегії не в повній мірі розкрито питання взаємодії суб'єктів забезпечення кібербезпеки як один з одним, так і з громадськістю та суб'єктами господарської діяльності [37].Потрібно працювати над взаємодією між силовими структурами і тими комерційними організаціями , які можуть забезпечити цей сервіс із подолання проблем при атаках і.т.д.

Тож із вищезазначеного можна сказати що дана Кіберстратегія є занадто простою та не відповідає тим загрозам та викликам які сьогодні стоять перед Україною.

3.3 Оптимізація системи суб'єктів забезпечення кібербезпеки України та удосконалення взаємодії між ними

Перспективним напрямком покращення впровадження кібербезпеки в Україні є оптимізація системи суб'єктів, що мають здійснювати діяльність у цій сфері, а також налагодження ефективної взаємодії між ними. Практика зарубіжних країн та українські реалії свідчать, що врегулювання основних завдань кібербезпеки неможливе без створення [32, с. 8–9; 60]: 1) міжвідомчого структурного органу, який постійно має забезпечувати координацію діяльності певних відомств, правоохоронних і силових структур України з питань реалізації кібербезпеки .Атака 27 червня 2017 року на Україну довела неспроможність на практиці Національним координаційним центром кібербезпеки забезпечити належний захист критичної інфраструктури. І тим самим дала привід для роздумів про практичне впровадження ідей які є в Стратегії кібербезпеки

України. А саме створення 1) центральних органів у структурі певних відомств, правоохоронних і силових структур України з функціями виявлення та оцінювання рівня (визначення ступеня) критичності стороннього кібервпливу, розроблення концептуальних засад та надання рекомендацій щодо протидії його проявам, а також активної протидії кібератакам та впливу на їх ІТС; 2) органи власної інформаційної і кібербезпеки — державних установ (відомств) та комерційних структур повинні тісно взаємодіяти із зазначеними центральними органами з питань вироблення єдиної стратегії щодо захисту як власного, так і спільного національного інформаційного і кіберпростору [32, с. 8–9; 62]. Із вищезазначеного можна зрозуміти, що система вказаних органів повинна бути якомога оптимальнішою.

Перше, що необхідно зробити , — це створення єдиного державного органу, який має бути наділений повноваженнями щодо координації діяльності всіх суб'єктів забезпечення кібербезпеки України. Наголошую, що РНБО здійснює лише координацію та стратегічне управління. Генштаб — оперативне управління в «особливий період». Але як свідчить практика кібервійну ніхто ніколи не об'являє. А тому, на мою думку, цікавим є досвід Польщі, яка створила Міністерство цифровізації, завданням якого є координація діяльності всіх без винятку суб'єктів забезпечення кібербезпеки в державі.

Реалізація положень Стратегії кібербезпеки України та Закону України «Про основні засади забезпечення кібербезпеки України» передбачає розроблення та застосування якісно нового законодавства у сфері кібербезпеки , що засноване на напрацьованому за п'ять років гібридної війни досвіді , усвідомленні та імплементації досвіду та нормативних документів ЄС та НАТО. Зокрема , підлягають розробленню такі нормативно-правові акти: Закон України « Про критичну інфраструктуру та її захист» , постанови Кабінету Міністрів України , зокрема: « Порядок формування переліку об'єктів критичної інформаційної інфраструктури», « Загальні вимоги з кіберзахисту об'єктів критичної

інфраструктури» (прийняті 19 червня 2019 р. № 518), «Про затвердження Протоколу спільних дій основних субєктів забезпечення кібербезпеки , суб'єктів кіберзахисту та власників (розпорядників) об'єктів критичної інформаційної інфраструктури під час попередження, виявлення , припинення кібератак та кіберінцидентів , а також під час усунення їхніх наслідків» , «Вимоги щодо проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури та Порядку проведення незалежного аудиту інформаційної безпеки». Має бути створений: реєстр об'єктів критичної інформаційної інфраструктури , реєстр аудиторів інформаційної безпеки. Результатом впровадження зазначених нормативних актів має стати Комплексний огляд сектору безпеки і оборони, частиною якого має стати огляд стану кіберзахисту критичної інформаційної інфраструктури , державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом.

Під взаємодією суб'єктів забезпечення кібербезпеки варто розуміти їх спільну взаємоузгоджену діяльність, яка спрямована на досягнення єдиної мети — забезпечення належного стану кібернетичної безпеки в Україні. До основних ознак такої взаємодії варто віднести: 1) єдину мету спільної діяльності; 2) наявність двох або більше суб'єктів; 3) обов'язковим є законодавче підґрунтя діяльності, (про яке я говорив у попередньому абзаці); 4) чітко визначений адміністративно-правовий статус кожного суб'єкта; 5) узгодженість заходів щодо цілі, місця, часу, методів. Питанню взаємодії у сфері забезпечення кібербезпеки приділяється особлива увагу, оскільки і науковці, і законодавець усвідомлюють, що без взаємодії досягнення кінцевого результату у цій сфері просто неможливе.

Так, відповідно до Стратегії кібербезпеки України, Національна система кібербезпеки має насамперед забезпечити взаємодію з питань кібербезпеки державних органів, органів місцевого самоврядування, військових формувань, правоохоронних органів, наукових установ, навчальних закладів, громадських

об’єднань, а також підприємств, установ та організацій незалежно від форми власності, які провадять діяльність у сфері електронних комунікацій, захисту інформації та/або є власниками (розпорядниками) об’єктів критичної інформаційної інфраструктури [12]. Однак, на жаль, доводиться констатувати, що на цьому увага законодавця до питання взаємодії суб’єктів забезпечення кібербезпеки в Україні і обмежується.

Необхідно звернути увагу на статтю 7 Закону України «Про основні засади забезпечення кібербезпеки України» від 2017 року, в якій зазначено, що однією з основних засад забезпечення кібербезпеки в Україні є насамперед державно-приватна взаємодія, тобто широка співпраця з громадянським суспільством у сфері кібербезпеки та кіберзахисту. Наприклад шляхом обміну інформацією про випадки кібербезпеки, реалізації спільних наукових та дослідницьких проектів, навчання та підвищення кваліфікації кадрів у даній сфері [10]. В статті 10 цього закону уточнюється, що державно-приватна взаємодія у сфері кібербезпеки здійснюється шляхом: 1) запровадження системи своєчасного виявлення, запобігання та нейтралізації кіберзагроз, у тому числі із залученням громадських організацій; 2) підвищення цифрової освідченості громадян та культури безпечного поводження в кіберпросторі, загальних знань, навичок і вмінь, необхідних для підтримки цілей кібербезпеки, реалізації державних і громадських проектів з підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту; 3) обміну інформацією між державними органами, приватним сектором і громадськістю щодо кіберзагроз об’єктам критичної інфраструктури, інших кіберзагроз, кібератак та кіберінцидентів; 4) партнерства та координації команд реагування на комп’ютерні надзвичайні події; 5) залучення науковців з профільних установ, професійних об’єднань та громадських організацій до підготовки ключових галузевих проектів та нормативних документів у сфері кібербезпеки; 6) запровадження консультативної та практичної допомоги з питань реагування на кібератаки; 7)

формування ініціатив та створення авторитетних консультаційних пунктів для громадян, представників промисловості та бізнесу з метою забезпечення безпеки в мережі Інтернет; 8) запровадження механізму громадського контролю ефективності заходів із забезпечення кібербезпеки; 9) періодичного проведення національного саміту з професійними постачальниками бізнес-послуг, включаючи страховиків, аудиторів, юристів, визначення їхньої ролі у сприянні кращому управлінню ризиками у сфері кібербезпеки; 10) створення системи підготовки кадрів та підвищення компетентності фахівців різних сфер діяльності з питань кібербезпеки; 11) тісної взаємодії з фізичними особами, громадськими та волонтерськими організаціями, IT-компаніями з метою виконання заходів кібероборони в кіберпросторі [10].

На законодавчому рівні мало уваги приділяється взаємодії конкретних суб'єктів забезпечення кібербезпеки. Зокрема, не має розробленого механізму такої взаємодії, який включає: 1) визначання взаємних прав та обов'язків суб'єктів під час здійснення їхньої діяльності; 2) визначення напрямків взаємодії; 3) окреслення форм та методів взаємодії; 4) визначення повноважень суб'єкта, який буде координувати спільну діяльність суб'єктів забезпечення кібербезпеки в Україні. Тож, беручи до уваги постійну динаміку розвитку кіберпростору, сьогодні є нагальна необхідність прийняття окремого положення «Про порядок взаємодії суб'єктів забезпечення кібербезпеки в Україні», в якому потрібно передбачити всі вказані параметри такої взаємодії.

Ще один момент, на який варто звернути увагу, — це створення органу, який би координував спільні дії суб'єктів забезпечення кібербезпеки в Україні. Так як, координація — це діяльність щодо організації взаємодії, поняттям «координація» охоплюється поняття «взаємодія» [70, с. 105]. О. Є. Луньов зазначав, що координація означає погодження та об'єднання дій з метою найбільш швидкого і найбільш правильного вирішення завдань із найменшими витратами сил, коштів та матеріальних цінностей. Науковець виділяв два типи координації: вертикальну

і горизонтальну. Вертикальна координація — це управлінські відносини, які виникають між вищим і нижчим органами виконавчої влади. При цьому, суб'єкти зв'язку можуть перебувати в організаційній залежності (один із них має бути підпорядкований іншому), а можуть і не перебувати в ній. Горизонтальна координація виникає між двома або більше органами, що перебувають на одному організаційному рівні системи органів: наприклад, вищезазначене Міністерство юстиції координує діяльність центральних органів виконавчої влади щодо правової освіти населення [69, с. 148; 1]. В контексті представленого наукового дослідження цікавою є позиція В. П. Пивненка, який справедливо підкреслює, що координація — це функція одного із суб'єктів системи, а взаємодія — принцип діяльності, засіб їх контактів із суб'єктами інших служб і підрозділів [87, с. 157–159].

Тому, все вказане в попередніх абзацах підтверджує необхідність прийняття єдиного «Порядку взаємодії суб'єктів забезпечення кібербезпеки в Україні» з урахуванням всіх вказаних мною пропозицій, які, здатні суттєво покращити взаємодію між суб'єктами забезпечення кібербезпеки в Україні, а як результат — створити всі необхідні умови для розвитку безпечного кіберпростору в державі та захистити її від зовнішніх та внутрішніх кіберзагроз.

ВИСНОВКИ

В процесі написання магістерської роботи мною , було з’ясовано , що найбільш перспективними напрямками розвитку національної системи кіберзахисту , є : вдосконалення правової основи кіберзахисту об’єктів критичної інфраструктури

; впровадження системи незалежного аудиту інформаційної безпеки на обєктах критичної інфраструктури; створення галузевих центрів реагування на кіберінциденти ; розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки; розвиток системи підготовки кадрів у сфері кібербезпеки; підвищення цифрової грамотності (правил кібергігієни) громадян та культури безпекового поводження в кіберпросторі , впровадження систем інформаційного комплексу та, насамперед , створення довірчих відносин між державою та суспільством , для якого держава повинна грати сервісну роль.

Так як це діє у більшості держав світу , де проблематика забезпечення кібербезпеки перебуває у фокусі уваги політикуму та включає розробку та реалізацію організаційно-правових заходів, спрямованих на протидію та запобігання кіберзагрозам. Так , у вже попередньо розглянутому Казахстані державна програма « Кіберщит» передбачає посилення заходів, спрямованих на забезпечення кібербезпеки та інформаційної безпеки державних електронних ресурсів. При цьому концепція цієї програми передбачає тільки державний тільки державний захист інформаційних систем , а безпосереднім захистом приватних ІТ- ресурсів повинен займатися виключно кожен власник. Очікується , що у повному форматі система інформаційної безпеки « Кіберщит» запрацює у 2019 – 2020 році, що дасть змогу значно мінімізувати наслідки кіберзагроз та максимально убезпечити об’єкти критичної інфраструктури від нападів та інцидентів , здійснювати постійний моніторинг кіберпростору з превентивною метою, захищати державні органи від аварійного та позаштатного витоку даних.

Концепція « Кіберщит» перший стратегічний документ у Казахстані , який ретельно описує проблематику кібербезпеки та визначає заходи , практичне впровадження яких дасть можливість посилити безпеку в національному сегменті кіберпростору , гарантовано захистити державні інформаційні ресурси , забезпечити функціонування дієвого механізму адекватного реагування на загрози та виклики в сучасному цифровому світі. Даний досвід Казахстану міг би допомогти Україні в її слабких місцях , для впровадження схожого проекту необхідне достатнє фінансування та бажання діяти , незважаючи на окремі інтереси окремих бізнес груп та осіб.

У 21-му столітті все більше зростає роль інформаційної безпеки, а мережева архітектура є новими кровоносними судинами нової економіки – економіки даних. Про це заявив Анатолій Амелін, співзасновник Українського інституту майбутнього та керівник економічних програм під час дискусії «Кібербезпека. Новий підхід в Україні», яка відбулась у приміщенні Українського інституту майбутнього. На жаль, в Україні дуже низький рівень кібербезпеки, і саме тому під час написання даної магістерської роботи по даній темі я намагався донести найбільш вразливі сторони нашої держави.

Але опираючись на матеріали дослідників та інші джерела необхідні для пізнання даної теми , я не брав до уваги корективи які внесла епідомологічна ситуація повязана з (COVID-19) в Україні та світі. Карантин не тільки змінив формат роботи багатьох компаній, комунікацій, формату ведення бізнесу, а і прискорив процес технологізації бізнесу, а разом з тим і збільшив ризики кіберзагроз. Після COVID-19 ФБР США повідомило про зростання на 300% числа зареєстрованих кіберзлочинів; до 2021 року на кібербезпеку у світі буде витрачено близько 6 трильйонів доларів; за оцінками Університету Меріленд, кожні 39 секунд у світі відбуваються кібератаки; 43% кібератак націлені на малий бізнес; 64% компаній стикалися з атаками через інтернет, а 62% зазнали фішингові і соціальні атаки; 59% компаній стикалися зі шкідливим кодом і

ботнетами, а 51% – з відмовами в обслуговуванні; понад 93% організацій охорони здоров'я зіткнулися з витоком даних за останні три роки; 95% порушень кібербезпеки відбуваються через людську помилку; до 2025 року кількість підключених IoT-пристроїв досягне 75 мільярдів; до 2021 року незаповнені вакансії кібербезпеки перевищать 4 мільйони осіб; інженери з кібербезпеки є одними з найбільш високооплачуваних посад, що починаються в середньому від 140 тис. дол на рік; понад 77% організацій не мають плану реагування на інциденти кібербезпеки; більшості компаній потрібно майже 6 місяців для виявлення витоку даних; для публічних компаній кібератаки призводять до падіння вартості акцій в середньому на 7%».Дані статистичні дані взяті з матеріалів Українського інституту майбутнього , який проводив в цьому році семінар за участю бізнесу по-розгляді даної проблеми.

Тому не потрібно багато говорити про важливість , та актуальність даної теми в наш час . Коли наша країна активно переходить на електронний документообіг , так звану діджиталізацію , під час якої в обіг електронної мережі потраляє велика кількість персональних даних наших громадян беззаперечно необхідно розвивати та продовжувати досліджувати дану тему . Але беззаперечним фактом залишається одне , що скільки б ми не досліджували проблематику та шляхи покращення кібербезпеки , нам необхідні величезні вливання коштів для того шоб реалізовувати дані положення не тільки на папері , але і в реальних діях.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Конституція України: закон від 28.06.1996 № 254к/96-ВР. Відомості Верховної Ради України. 1996. № 30. Ст. 141.
2. Кодекс України про адміністративні правопорушення: кодекс від 07.12.1984 № 8073 X. Відомості Верховної Ради України. 1984. № 51.Ст. 1122. URL: http://zakon2.rada.gov.ua/laws/show/80731-10/conv. (дата доступу – 14.01.2018).
3. Цивільний кодекс України від 16 січня 2003 р. № 435-IV. Відомості Верховної Ради України. 2003. № 40–44. Ст. 356.
4. Кримінальний кодекс України: кодекс,законвід05.04.2001№2341III.Відомості Верховної Ради України. 2001. № 25. Ст. 131. URL: http://zakon3.rada.gov.ua/laws/show/2341-14/conv. (дата доступу – 11.07.2017)
5. Про затвердження Положення про Міністерство оборони України: постанова від 26.11.2014 № 671. Офіційний вісник України. 2014. № 97. Ст. 51.
6. Про захист інформації в інформаційно-телекомунікаційних системах: закон від 05.07.1994 № 80/94 ВР. Відомості Верховної Ради України. 1994. № 31. Ст. 286.
7. Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України: указ від 06.12.2001 № 1193/2001. Офіційний вісник України. 2001. № 50. Ст. 25.
8. Про Національний банк України: закон від 11.10.2017 № 679 XIV. Відомості Верховної Ради України. 1999. № 29. Ст. 238.
9. Про Національну поліцію: закон від 02.07.2015 № 580-VII. Офіційний вісник України. 2015. № 63. Ст. 33.
10. Про основні засади забезпечення кібербезпеки України: закон України від 05.10.2017 №2163-VIII. Голос України. 2017. № 208. URL: http://zakon2.rada.gov.ua/laws/show/2163-19. (дата доступу – 24.07.2018).
11. Про основні засади забезпечення кібербезпеки України: закон України від 05.10.2017 №2163-VIII. Голос України. 2017. № 208. URL: http://zakon2.rada.gov.ua/laws/show/2163-19. (дата доступу – 24.07.2018).
12. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України», затверджена Указом Президента України від 15.03.2016 № 96/2016. URL: http://zakon5.rada.gov.ua/laws/show/96/2016. (дата доступу – 29.07.2017).

13. Про Службу безпеки України: закон від 25.03.1992 №2229-XI. Відомості Верховної ради України. 1992. № 27. Ст. 382.

14. Про стандартизацію: Закон України від 05.06.2014. URL: http://zakon2.rada.gov.ua/laws/show/1315-18. (дата доступу – 12.08.2018).

15. Про Стратегію кібербезпеки України: указ від 15.03.2016 № 96/2016. Офіційний вісник України. 2016. № 23. Ст. 69.

16. Конвенція про кіберзлочинність: міжнародний документ, конвенція від 23.11.2001. Офіційний вісник України. 2007. № 65. Ст. 107. URL: http://zakon3.rada.gov.ua/laws/show/994_575/conv. (дата доступу – 22.11.2017).

17. Віденська декларація про злочинність та правосуддя: відповіді на виклики XXI століття: міжнародний документ, декларація від 17.04.2000. URL: http://zakon3.rada.gov.ua/laws/show/995_443. (дата доступу –31.03.2016).

18. Декларація принципів «Побудова інформаційного суспільства глобальне завдання у новому тисячолітті»: міжнародний документ, декларація від 12.12.2003. URL: http://zakon3.rada.gov.ua/laws/show/995_c57. (дата доступу – 21.05.2016).

19. Створення глобальної культури кібербезпеки: резолюція Генеральної Асамблеї ООН від 20.12.2002 №57/239. URL: https://documentsdds-ny.un.org/doc/UNDOC/GEN/N02/555/24/PDF/N0255524.pdf?OpenElement. (дата доступу – 13.03.2018).

20. Конвенція про взаємодопомогу в кримінальних справах між державами-членами Європейського Союзу: міжнародний документ, конвенція від 29.05.2000. URL: http://zakon5.rada.gov.ua/laws/show/994_238/page. (дата доступу – 23.01.2018).

21. Административная деятельность органов внутренних дел. Часть Общая: учебное пособие 3-е изд. / под ред. А. П. Коренева. Москва, 2000. 367 с.

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

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

24. Алексеев С. С. Проблемы теории права: курс лекций в двух томах. Свердловск, 1972. Т. I. 396 с.

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

26. Баранова Н. М. Етика: навч, посіб. Ніжин: НДУ ім. М. Гоголя, 2015. 323 с.

27. Бахрах Д. Н., Россинский Б. В., Старилов Ю. Н. Административное право: учебник для вузов. 3-е изд., пересмотр, и доп. Москва: Норма. 2007. 816 с.

28. Берлач А. І. Біржове право України: [навч. посіб.]. Київ: Універси-тет «Україна», 2008. 316 с.

29. Бистрик Г. М. Принцип законності і засоби його правового забезпечення у функціонуванні механізму держави. Наукові праці МАУП. 2014. Вип. 1. С.85–90.

30. Бриль К. І. Правозастосовний акт як особливий вид індивідуальних правових актів: дис ... канд. юрид. наук: 12.00.01. Київ: Б.в., 2008. 214 с.

31. Бурбика В. О. Адміністративно-правові засади взаємодії органів місцевого самоврядування з правоохоронними органами: дисертація ... канд. юрид. наук, спец.: 12.00.07 адміністративне право і процес; фінансове право; інформаційне право. Суми: СумДУ, 2017. 251 с.

32. Бурячок В. Л., Гнатюк С. О., Корченко О. Г. Характерні ознаки та проблемні аспекти забезпечення кібернетичної безпеки. Інформаційна безпе-ка: виклики і загрози сучасності: зб. матеріалів наук.-практ. конф. (5 квітня 2013 року, м. Київ). Київ: Наук.-вид. центр НА СБ України, 2013. 416 с.

33. Бурячок В. Л., Корченко О. Г., Хорошко В. О., Кудінов В. А. Стратегія оцінювання рівня захищеності держави від ризику стороннього кібернетичного впливу. Захист інформації. 2013. Том 15, № 1. С. 5–12.

34. Бусел В. Т. Великий тлумачний словник сучасної української мови. Київ; Ірпінь: ВТФ «Перун», 2005. 1728 с.

35. Бусол О. Інформаційна безпека США: законодавче регулювання та перспективи співпраці для України: офіційний web-сайт Центру досліджень соціальних комунікацій НБУВ. URL: http://www.nbuviap.gov.ua/index.php?option=com_content&view=article&id=2988:informatsijna-bezpeka-ssha-zakonodavche-regulyuvannya-ta-perspektivispivpratsi-dlya-ukrajini&catid=8&Itemid=350. (дата доступу – 13.03.2017).

36. Бухарєв 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.

37. Бухарєв В. В. Напрямки вдосконалення адміністративного законодавства, яке регулює забезпечення кібербезпеки в Україні. Наше право. 2018. № 2. С. 52–57.

38. Бухарєв В. В. 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.

39. 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.

40. Волеводз А. Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. Москва: ООО Издательство «Юрлитинформ», 2002. 86 с.

41. Галаган И. А. Административная ответственность в СССР. Изд. Воронежского ун-та, 1970, 251 с.

42. Гетьман-П'ятковська І. А. Право та мораль: теоретико правові проблеми співвідношення та взаємодії: дис ... канд. юрид. наук. Київ: б. в., 2007. 210 с.

43. Гончарук С. Т. Адміністративна відповідальність за законодавством України. Київ: КМУЦА, 1995. 78 с.

44. Давыдов П. М. Обвинительный приговор основная форма реализации уголовной ответственности. Свердловск: СЮИ, 1979. 142 с.

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

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

47. 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.

48. 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.

49. Європіна І. В. Види протиправних діянь у сфері новітніх інформаційних технологій. Вісник Академії адвокатури України. 2010. № 3. С. 129–136.

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

51. Загальне адміністративне право: підручник / І. С. Гриценко, Р. С. Мельник, А. А. Пухтецька Київ: Юринком Інтер. 2015. 568 с.

52. Зеленецкий В. С. Общая теория борьбы с преступностью: ч. 1 Концептуальные основы. Харків: Основа, 1994. 375 с.

53. Іванчук Н. В. Взаємна відповідальність особи і держави в контексті розбудови сучасної української держави: дис... канд. юрид. наук: 12.00.01 / Київський національний ун-т внутрішніх справ. Київ, 2007. 185 арк.

54. Інформаційна кібербезпека: соціотехнічний аспект: підручник / В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа. Київ: ДУТ, 2015. 288с.

55. Китай схвалив новий закон про кібербезпеку. Українські націона- льні новини «інформаційне агентство UNN». URL: http://www.unn.com.ua/uk/news/1616273-kitay-skhvaliv-noviy-zakon-prokiberbezpeku. (дата доступу – 23.11.2017).

56. Кібербезпека: віртуальна зброя держави. URL: https://biz.nv.ua/ukr/experts/kutsenko1/kiberbezpeka-zbroja-derzhavi-u-virtualnijploshchini-2014774.html. (дата доступу – 10.01.2018).

57. Ківалов С. В., Біла Л. Р. Адміністративне право України: навчальнометодичний посібник. Вид. друге, перероб. і доп. Одеса: Юридична література, 2002. 312 с.

58. Кобзєва Т. А. Адміністративно-правове забезпечення управління фінансовою системою України: монографія. Суми: СумДУ, 2018. 433 с.

59. Кобзєва Т. А. Адміністративно-правове забезпечення управління фінансовою системою України: монографія. Суми: СумДУ, 2018. 433 с.

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

61. Колпаков В. К. Адміністративне право України. Київ: ЮрінкомІнтер, 2004. 724 с.

62. Колпаков В. К., Кузьменко О. В. Адміністративне право України: підручник. Київ: Юрінком Інтер, 2003. 544 с.

63. 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.

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

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

66. Литвин І. Сутність системи суб'єктів адміністративно-правових відносин у сфері надання освітніх послуг. Підприємництво, господарство і право. 2016. № 5. С. 63–66.

67. Литвиненко В. І. Адміністративно-правові форми протидії корупції в Україні. Наук. вісн. Херсон. держ. ун-ту. Вип. 2 (№ 3-2). С. 50–55.

68. Лук'янець Д. М. Інститут адміністративної відповідальності: проблеми розвітку: монографія. Київ: Інститут держави і права ім. В. М. Корецького НАН України, 2001. 136 с.

69. Лунев А. Е. Теоретические проблемы государственного управления. Москва: Наука, 1974. 247 с.

70. Мангутов И. С., Уманский Л. И. Организатор и организаторская деятельность. Л.: ЛГУ, 1975. С. 103–127.

71. Мандюк О. О. Індивідуальні адміністративні акти: теорія та практика застосування: дисертація на здобуття наукового ступеня кандидата юридичних наук: 12.00.07 адміністративне право і процес; фінансове право; інформаційне право / Міністерство освіти і науки України, Національний університет «Львівська політехніка». Львів, 2017. 213 с.

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

73. Марущак Ю. В. Адміністративно-правова охорона майнових та немайнових прав власності в Україні. Науковий вісник Національного університету біоресурсів і природокористування України. 2014. Вип. 197, ч. 2. С. 238–242.

74. Марченко М. Н. Проблемы теории государства и права. Москва: Проспект. 2001. 687 с.

75. Мацелик Т. О. Суб'єкти адміністративного права: поняття та система (монографія). Ірпінь.: Видавництво Національного університету податкової служби України. 2013. 342 с.

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

77. Меркель: уряд Німеччини актуалізував стратегію кібербезпеки. URL:http://vgolos.com.ua/news/merkel_uryad_nimechchyny_aktualizuvav_strategiyu_k iberbezpeky_256173.html. (дата доступу – 13.02.2018).

78. Мосьондз С. О. Адміністративно-правова охорона сфери науки в Україні: концептуальне бачення. Науково-аналітичний журнал «Митна справа». 2012. № 5 (83), частина 2, книга 2. С. 102–107.

79. Наумов А. В. Реализация уголовного права и деятельность следователя. Волгоград: ВСШ, 1987. 83 с.

80. Новий тлумачний словник української мови: у 3 т. / В. Яременко, О. Сліпушко. Київ: Аконіт, 2003. Т. 3: ОБЕ-РОБ. 927 с.

81. Новоселов В. И. Правовое положение граждан в отраслях советского государственного управления. Саратов: Изд-во Сарат. ун-та, 1977. 166 с.

82. Ожегов С. И. Словарь русского языка. Москва: Русский язык, 1984. 797 с.

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

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

85. Перун Т. С. Адміністративна відповідальність в системі заходів забезпечення інформаційної безпеки. URL: http://aphd.ua/publication-229/. (дата доступу – 14.02.2018).

86. Петрушенко В. Л. Філософія: навчальний посібник, 2-е видання, виправлене і доповнене. Київ: Каравела, 2002. 544 с.

87. Пивненко В. П. Проблеми підвищення ефективності роботи правоохоронних органів в Україні у боротьбі з організованою злочинністю. Вісник Академії правових наук. 1997. Вип. 1. С. 157–159.

88. Ронжин В. Н. О понятии и системе принципов социалистического права. Вестник МГУ. Сер.11. Право. 1977. № 2. С. 34.

89. Савицькиій Ю. Досвід Польщі для України: чому варто робити ставку на високі технології? URL: https://www.radiosvoboda.org/a/27631224.html. (дата доступу – 24.08.2017).

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

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

92. Сокольська Т. В. Якісна складова конкурентоспроможності продукції агросфери: дис ... канд. екон. наук. Біла Церква: б. в., 2009. 210 с.

93. Спасибо І. А. Щодо історії виникнення глобальної мережі інтернет. Право та інновації. 2014. № 3 (7). С. 15–25.

94. Стефанчук Р. О. Цивільне право України: навчальний посібник. Київ: Наукова думка, 2004. 361 с.

95. Теорія держави і права: Академ. Курс: підручн. / За ред. О. В. Зайчука, Н. М. Оніщенко. Київ: Юринком-Інтер, 2006. 688 с.

96. Теорія держави і права: підруч. для студ. юрид. вищ. навч. закл. / О. В. Петришин, С. П. Погребняк, В. С. Смородинський та ін.; за ред. О. В. Петришина. Харків: Право, 2014. 368 с.

97. У Німеччині різко зросла кіберзлочинність. URL: https://www.dw.com/uk/y-німеччині-різко-зросла-кіберзлочинність/a38555191. (дата доступу – 29.09.2017).

98. У Великобританії створили реабілітаційний центр для кіберзлочинців. URL http://ms.detector.media/web/cybersecurity/u_velicobritanii_stvorili_reabilitatsiyniy_tsentr_dlya_kiberzlochintsiv/. (дата доступу – 28.08.2018).

99. Удосконалення законодавства щодо протидії загрозам національній безпеці в інформаційній сфері необхідне для блокування російських кібератак СБУ. Офіційний WEB-сайт Служби безпеки України. URL: https://ssu.gov.ua/ua/news/1/category/2/view/5025#.1BtQx74C.dpbs. (дата дос-тупу – 12.08.2018).

100. Фелик В. І. Адміністративно-правове забезпечення профілактичної діяльності Національної поліції України: монографія. Харків, 2016. 511 с.

101. Философский словарь / Под ред. М. М. Розенталя. Москва: Политиздат, 1972. 496 с.

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

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

104. Шаповал В. Суб'єкти конституційного права України: Постановка проблем теоретичного визначення. Право України. 2000. № 8. С. 21.

105. Юркова Є. В. Межі адміністративно-правової охорони права інтелектуальної власності в Україні. Форум права. 2009. № 3. С. 710–714.

106. Як це робила Польща: досвід боротьби з кіберзагрозами. Електронне видання «Економічна правда». URL: https://www.epravda.com.ua/columns/2017/10/12/630044/. (дата доступу – 19.09.2017).

107. Якість і безпека: сучасні реалії: матеріали наук.-практ. конф., 02- 03 берез. 2017 р. / Вінниц. нац. техн. ун-т, Вінниц. нац. аграр. ун-т, Вінниц. мед. коледж ім. Данили Заболотного. Вінниця: ВНТУ, 2017. 91 с.

108. Computer-related crime. Recommendation no. R. (89) 9 on computerrelated crime and final report of the European Committee on Crime Problems / Strasbourg. Council of Europe, Pub. And Documentation Service. Croton N.Y.: Manhattan Pub. Co. 1990. 114 p.

109. Cyberbezpieczeństwo / Ministerstwo Cyfryzacji Official website. URL: https://www.gov.pl/cyfryzacja/cyberbezpieczenstwo.

110. Februar 2011. URL: http://www.bmi.bund.de/SharedDocs/Downloads/De/Themen/OED_Verwaitung/Informationsgesellschaft/cyber/pdf?_blob=publicatio nFile/

111. Marshall J. H. Office of Legal Education Executive Office for United States Attorneys / J. H. Marshall, M. W. Balle. 2010. 213 p.

112. Rosenbach Markel. Nationales Cyber–Abwehrzentrum. Spiegel OnlineNetzwelt, 21 März 2011. URL: http://www.spiegel.de/netzwelt/netzpolitik/0,1518,747140,00.html.

113. Watson Farley & Williams, "Briefing: The New German IT Security Act," February 2016, http://www.wfw.com/wpcontent/ uploads/2016/02/WFWBriefing-GermanyIT-Security-Feb-2016-EN-15-Feb.pdf