ЗМІСТ

ПЕРЕДМОВА

Неодмінним атрибутом сучасних глобалізаційних процесів є стрімкий науково-технічний прогрес, цифровізація суспільних відносин, вихід людства у кіберпростір та проникнення віртуального світу в усі сфери життєдіяльності, що в сукупності формує нескінченні можливості новітнього розвитку інформаційного суспільства. Проте поряд із розвитком позитивних складових технологічний прогрес зумовлює появу нових викликів і загроз, зокрема і щодо балансу безпекових інтересів на національному та міжнародному рівнях.

За останні десятиріччя загрози порушення інтересів людей, держави й у цілому суспільства в кіберпросторі перетворилися із потенційних та гіпотетичних на цілком реальні, а протистояння їх поширенню стало пріоритетним завданням національних урядів та міжнародної спільноти.

Питання забезпечення кібербезпеки для України в період входження в новий етап суспільного розвитку є безальтернативними та обумовлені не лише загальними світовими тенденціями. Гібридна агресія проти України у формі порушення інформаційного простору, поширення негативного антидержавного та антиукраїнського наративу, утручання в діяльність критичної інфраструктури, кібертероризму, кібератак тощо примножує рівень небезпеки в кіберпросторі як щодо прав і свобод громадян, так і інтересів суспільства та держави.

Традиційним вирішенням проблем забезпечення кібербезпеки в багатьох випадках уважається врегулювання питань технічного характеру щодо телекомунікаційних систем та комп'ютерної техніки. Водночас ескалація агресором кіберзагроз, цілеспрямоване та масштабне використання кібератак зумовили необхідність розбудови ефективної системи безпеки в кіберпросторі, що базується на імплементації адекватного загрозі правового механізму та формування стійкої національної системи забезпечення кібербезпеки.

Ураховуючи зазначене, предметом даного монографічного дослідження визначено адміністративно-правове забезпечення кібербезпеки України в умовах гібридної війни. Зосереджено увагу на теоретико-методологічних засадах, які концентрують увагу не лише на адміністративно-правовій, а й на безпекознавчій системі знань, розкривають сутність кібербезпеки та акцентують увагу на її особливості в умовах гібридної війни.

Акцентовано увагу на необхідності розбудови комплексної системи забезпечення безпеки в кіберпросторі, у зв'язку із чим на основі класичного академічного підходу проаналізовано адміністративно-правові заходи, форми та методи, підходи до адміністративно-правової охорони та механізму адміністративно-правового регулювання у сфері забезпечення кібербезпеки України.

Окремої уваги заслуговують питання формування національної системи забезпечення кібербезпеки, що визначило особливий інтерес у розкритті особливостей адміністративно-правових відносин у сфері забезпечення кібербезпеки, а на основі аналізу адміністративно-правового статусу суб'єктів забезпечення кібербезпеки України здійснення їх класифікації.

У межах обґрунтування ключових напрямів розбудови вітчизняної системи забезпечення кібербезпеки проаналізовано сучасні технологічні тенденції щодо розвитку телекомунікацій, а також кіберзагрози, поширення яких є прогнозованим за таких умов. З огляду на зазначене з урахуванням світових тенденцій розвитку адміністративно-правового забезпечення кібербезпеки, а також досвіду розвинених країн ЄС і НАТО, обґрунтовуються засади формування відповідної правової регламентації ключових сучасних підходів забезпечення кібербезпеки на основі розбудови «стійкості» суспільства в протистоянні гібридним кіберзагрозам, упровадження ризик-орієнтованого підходу та підвищення спроможності суб'єктів забезпечення кібербезпеки України.

Розділ 1
КІБЕРБЕЗПЕКА: МЕТОДОЛОГІЧНІ ЗАСАДИ ПІЗНАННЯ ТА СТАНОВЛЕННЯ ПРАВОВОГО ІНСТИТУТУ ЇЇ ЗАБЕЗПЕЧЕННЯ

1.1. Гібридна війна – сучасний виклик кібербезпеці України

Зростання сучасного суспільства нерозривно пов'язане із запобіганням різноманітним загрозам, які посилюються в період реформування будь-якої сфери життєдіяльності суспільства[1]. Професор Олександр Користін зазначає, що питання протидії гібридним загрозам в інформаційній сфері, зокрема, у кіберпросторі, достатньо широко та комплексно охоплює проблеми національної безпеки. Зазначене, перш за все, потребує суттєвого аналізу ситуації, дослідження тих факторів, що спричинюють неспроможність ефективного реагування на протидію гібридним загрозам, зокрема щодо прав та свобод громадян та інтересів суспільства і держави. Поряд з цим, об'єктивність та обґрунтованість результатів дослідження потребує відповідної методологічної бази, прийнятності даних, що використовуються в аналізі, та джерел, з яких вони надходять[2].

Глобалізація суспільних відносин та прискорення технологічного прогресу визначають чітке усвідомлення того, що сучасне

[1] Протидія відмиванню коштів: міжнародні стандарти, зарубіжний досвід, адміністративно-правові, кримінологічні, кримінально-правові, криміналістичні засади та система фінансового моніторингу в Україні : підручник / за ред. Користіна О.Є. Київ : Скіф, 2015. 984 с.

[2] Ковальчук Т.І., Користін О.Є., Свиридюк Н.П. Гібридні загрози у секторі цивільної безпеки в Україні. *Наука і правоохоронна*. 2019. № 3(45). С. 69–79. DOI: https://doi.org/10.36486/np.2019.3; Kovalchuk T.I., Korystin O.Y., Sviridyuk N.P. Hybrid threats in the civil security sector in Ukraine. *Проблеми законності.* 2019. Вип. 147. С. 163–175.

інформаційне суспільство охоплює всі сфери життєдіяльності людини і держави, а кіберсфера стала важливим економічним, політичним і соціальним ресурсом[3]. Технологічний розвиток інформаційних відносин сформував нові можливості соціального прогресу, проте паралельно також створив нові можливості для зловживань, а з розвитком Інтернет технологій виникла надзвичайно специфічна група загроз системі національної безпеки. Професор Баранов О.А. зазначає, що широких масштабів проблема кібербезпеки набула тоді, коли можлива шкода від реалізації загроз у сферах, де використовувались комп'ютерні системи та телекомунікаційні мережі, стала досягати великих обсягів[4]. Саме тому глобалізаційні інформаційні процеси об'єктивно супроводжуються поширенням кіберзагроз зі специфікою сучасного технологічного розвитку.

Зростання залежності людини, суспільства та національних інфраструктур (енергетичної, транспортної, телекомунікаційної) від належної роботи інформаційно-телекомунікаційних систем зумовлює їхню вразливість від кіберзагроз, що, у свою чергу, підвищує ризик виникнення надзвичайних ситуацій, створює реальні загрози життєдіяльності людини, суспільства, держави, подальшому соціально-економічному розвитку та національній безпеці України[5].

Стратегія забезпечення кібербезпеки України визначає, що побудова інформаційного суспільства в різних країнах світу, глобалізація інформаційних процесів, суттєве зростання ролі інформаційної інфраструктури в різних сферах суспільного життя з одного боку створюють підґрунтя для ефективного соціально-економічного розвитку держав, задоволення конституційного права особи на інформацію, побудови ефективної системи державного управління.

---

[3] Данильчук Л.О. Сутність дефініції «інформація». *Педагогіка і психологія професійної освіти*. 2012. № 5. С. 28.

[4] Баранов О.А. Про тлумачення та визначення поняття «кібербезпека». *Правова інформатика*. 2014. № 2 (42). С. 133.

[5] Шеломенцев В.П. Сутність організаційного забезпечення системи кібербезпеки України та напрями його удосконалення. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2012. № 2(28). С. 299.

З іншого, – сучасні інформаційні технології, перетворюють інформаційні системи урядового, оборонного, виробничого, кредитно-банківського, комунального та інших секторів на надзвичайно вразливі для реалізації кіберзагроз об'єкти[6].

Проте лише декілька злочинців можуть суттєво вплинути на безпеку тисячі користувачів. Технологічні можливості формують низку якостей, що спрощують, забезпечують анонімність та доступність для людей, але, у той же час, приваблюють злочинців для вчинення протиправних дій. Наслідком зростаючого використання інформаційних технологій є одночасне зростання та поширення кіберзагроз, зокрема, і у форму кіберзлочинів.

Орлов О.В. та Онищенко Ю.М. зазначають, що кіберзлочинність є неминучим наслідком глобалізації інформаційних процесів. Жертвами кіберзлочинців, можуть стати не лише окремі особи або підприємства, але й цілі держави, що безперечно є загрозою національній безпеці[7]. Семенов В.М. та Гиркіна О.О. звертають увагу на те, що сучасні інформаційні технології перетворюють інформаційні системи урядового, оборонного, виробничого, кредитно-банківського, комунального та інших секторів на надзвичайно вразливі для реалізації кіберзагроз об'єкти[8].

У сучасному світі прогрес неможливий без цифрового інфраструктурного базису – ключового компоненту економічного розвитку. Реальною є сучасна залежність людини та суспільства в цілому від кіберпростору, що охоплює прилади, обладнання, програмне забезпечення, комп'ютерну техніку, телефонію, які є невід'ємною складовою сучасної повсякденної життєдіяльності. Це телекомунікаційні мережі урядової, виробничої та соціальної сфер, секретні військові та розвідувальні мережі, відкритий Інтернет, локальні мережі окремих суб'єктів інші масові мережі, які пов'язали людей,

[6] Стратегія забезпечення кібербезпеки України. Офіційний текст: проект Закону України. URL: w1.c1.rada.gov.ua/pls/.../webproc34?id

[7] Орлов О.В. Попередження кіберзлочинності – складова частина державної політики в Україні. *Теорія та практика державного управління*. Вип. 1 (44). URL: www.irbis-nbuv.gov.ua/.../cgiirbis_64.exe?

[8] Семенов В.М., Гиркіна О.О. Сучасні аспекти забезпечення інформаційної безпеки України. *Науковий вісник Херсонського державного університету: Серія: Юридичні науки*. Вип. 5., Т. 2. С. 235.

громади, підприємства та суспільства. Саме реальність кіберпростору і робить реальними ризики, які виникли разом із ним[9].

Потрібно зазначити, що США, як одна з найбільш інформаційно розвинених країн, одна з перших зіткнулися з проблемою забезпечення недоторканості приватного життя та економічної безпеки держави й громадян. За даними дослідження, тільки за два роки кіберзлочинність вартувала американцям 8 млрд доларів[10]. У серпні-жовтні 2008 р. хакери отримали доступ до електронної пошти і низки файлів передвиборної кампанії Барака Обами, включаючи документи, що розкривають політичні позиції та плани поїздок[11]. За оцінками фахівців, лише упродовж року, у глобальному вимірі, кіберзлочини завдають збитків на суму до $1 трлн власникам інтелектуальної власності[12]. Зрозумілим стає, що економічне зростання будь-якого суспільства в XXI ст. залежатиме від кібербезпеки.

Але не лише США, а й більшість країн Заходу, зіткнулися з необхідністю забезпечення інформаційної безпеки особи, суспільства та держави, зокрема, і за допомогою адміністративно-правових засобів, що спричинено технічним прогресом у сфері телекомунікацій та інформаційних технологій, який призвів до виникнення низки абсолютно нових неврегульованих правом суспільних відносин.

З метою інституційного забезпечення, у травні 2009 р. при федеральному уряді США була створена Єдина Рада з національної безпеки, однією з основних функцій якої є моніторинг реалізації політики кібербезпеки. У Білому Домі створено також новий відділ, яким керує Координатор з кібербезпеки[13], який підпорядковується безпосередньо Президенту. У межах своїх повноважень Координатор є відповідальним за інтеграцію і злагоджену роботу усіх складових державного управління у сфері кібербезпеки, за співпрацю офісу

[9] Березовська І.Р. Адміністративно-правові засоби забезпечення інформаційної безпеки в Україні : дис. ... канд. юрид. наук: 12.00.07. Київ. 2012. С. 61.

[10] AIG Technology Report 2007–2008: Readiness for the Networked World Center for International Development at Harvard University. March 2009. P. 16.

[11] Там само.

[12] WIPO 2008 Report. WIPO Site. URL: http://www.wipo.int/meetings/en/archive.jsp

[13] Barack Obama Speech, March, 13, 2009. Barack Obama Site. URL: http://my.barackobama. com/page/content/ofasplashbsignon/

адміністрації Президента та за координацію дій у випадку настання надзвичайної події, або кібератаки.

Виступаючи 29 травня 2009 р., Президент Обама визначив п'ять головних напрямів діяльності, зокрема[14]:

– розроблення нової стратегії забезпечення безпеки інформаційно-телекомунікаційних мереж Америки;

– налагодження взаємодії державних та місцевих органів влади з метою забезпечення організованої відповіді на кібератаки;

– зміцнення співробітництва державного та приватного секторів, оскільки переважна кількість найважливіших інформаційних інфраструктур у США перебуває у власності або управляються приватним сектором;

– запровадження національної пропагандистської кампанії з метою поширення серед населення інформованості і грамотності у сфері цифрових технологій.

У січні 2010 р. під час Всесвітнього економічного форуму в Давосі глава компанії-розробника антивірусних програм McAfee Дейв ді Велт сповістив учасників про початок епохи «гонки озброєнь» у кіберпросторі. За його словами, останнім часом спостерігається рух державних комп'ютерних структур від традиційних оборонних стратегій до наступальних. Інтернет стає полем міжнародних бойових дій. Півтора-два десятки країн, серед яких Росія, США та Китай, готуються до можливих операцій в Інтернеті. Експерти вже закликають до активного публічного обговорення проблеми віртуальних воєн[15].

Восени 2009 р. фахівці McAfee представили «Звіт про віртуальну злочинність» та зазначили, що виявили ознаки застосування «кіберзброї» в п'яти країнах – США, Китай, Росія, Ізраїль та Франція[16]. Спостерігається різке збільшення кількості хакерських атак в усьому світі. За підрахунками McAfee, за рік кількість нових шкідливих

[14] Remarks by the President on Securing our Nation's Cyber Infrastructure. White House Official Site. URL: http://www.whitehouse.gov/the_pressoffice/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure

[15] Тумарец В. Новые угрозы для информационного общества. Москва : ЭКСМО, 2008. С. 58 с.

[16] United Nations «Global E-Government Survey-2008». UN PAN Site. URL: http://www.unpan.org/egovkb/ global_reports/08report.htm

програм зросла на 500 %. Спостерігається підвищена увага світової громадськості до кіберсфери. Це наочно демонструє, на думку ді Велта, недавній випадок із компанією Google, яка після хакерської атаки на поштовий сервіс заявила про намір припинити роботу в Китаї. Але це був лише один із багатьох подібних нападів за останні роки, більшість же з них були непомічені. Тим часом експерти попереджають, що в майбутньому кібератаки проти ключових об'єктів життєзабезпечення, які в більшості розвинених країн недостатньо захищені, можуть обернутися величезним збитком. Уже зараз, як показало дослідження McAfee, атаки хакерів обходяться в середньому в $6,3 млн на добу, тобто в $1,75 млрд на рік у всьому світу[17]. Найдорожчі – напади на мережеву інфраструктуру нафтогазового сектора. Антивірусна компанія McAfee спільно з Центром стратегічних і міжнародних досліджень (CSIS) представила на Всесвітньому економічному форумі в Давосі звіт про результати дослідження, проведеного серед шестисот керівників нафтових і газових об'єктів, електростанцій та іншої критично важливої інфраструктури[18].

Зазначене підтверджується і іншими дослідженнями. У межах експертного опитування 54 % респондентів, які займають вищі ланки менеджменту підприємств, сповістили про наявні збитки від великомасштабних кібератак, що мали місце у минулому. Окрім того, 37 % респондентів повідомили про те, що через скорочення корпоративних бюджетів ситуація з кібербезпекою погіршилася. А 40 % опитаних очікують великого інциденту у сфері кібербезпеки. Середня величина збитків, спровокованих втручанням у роботу IT-систем, прогнозується в межах 6,3 мільйона доларів на день. Відповідальність за запобігання таким атакам 45 % опитаних покладають на регіональні або місцеві органи влади[19].

Дослідницькі установи ООН також активно займаються оцінюванням інформаційної безпеки в глобальному світі. Зокрема,

[17] Прохожев А.А., Турко Н.И. Основы информационной войны. Анализ систем на пороге XXI века: теория и практика. Москва, 1996. С. 45.

[18] Березовська І.Р. Адміністративно-правові засоби забезпечення інформаційної безпеки в Україні : дис. ... канд. юрид. наук: 12.00.07. Київ. 2012. С. 63–64.

[19] Даниелова А. Основные направления информатизации американского общества. США–Канада. 2009. № 5. С. 27.