ЧОРНОМОРСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ПЕТРА МОГИЛИ

Факультет політичних наук
Кафедра міжнародних відносин та зовнішньої політики

ДИПЛОМНА РОБОТА МАГІСТРА

КІБЕРБЕЗПЕКА ЯК СКЛАДОВА СУЧАСНОЇ СИСТЕМИ МІЖНАРОДНИХ ВІДНОСИН

Виконав: студент 6 курсу 691мз групи
галузі знань 29 «Міжнародні відносини
спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»
Ваколюк Олександр Сергійович

Керівник: к. політ. н., ст. викладач кафедри міжнародних відносин та зовнішньої політики
Звездова Олеся Олександрівна

Рецензент: к.і.н., доцент кафедри соціології та політології
Фесенко Артур Михайлович

Миколаїв – 2022 рік

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АС	Африканський союз
АТР	Азійсько-Тихоокеанський регіон
ГА ООН	Генеральна Асамблея ООН
ЕКОВАС	Економічне співтовариство країн Західної Африки
ЄС	Європейський Союз
ЗВО	Заклади вищої освіти
ЗМІ	Засоби масової інформації
ЗС США	Збройні сили Сполучних Штатів Америки
ЗМК	Засоби масової комунікації
ІКТ	Інформаційно-комунікаційні технології
ІТ	Інформаційні технології
КНДР	Корейська Народна Демократична Республіка
КНР	Китайська Народна Республіка
ЛАД	Ліга арабських держав
МЗС	Міністерство закордонних справ
НАТО	Організація Північноатлантичного договору
НВАК	Народно-визвольна армія КНР
НСКБ	Національна система кібербезпеки
МВФ	Міжнародний валютний фонд
ООН	Організація Об’єднаних Націй
ПАР	Південно-Африканська республіка
РБ ООН	Рада Безпеки ООН
РЄ	Рада Європи
РНБО	Рада національної безпеки та оборони
РФ	Російська Федерація
САДК	Південноафриканське співтовариство розвитку

СНД	Співдружність незалежних держав
США	Сполучені Штати Америки
ФРН	Федеративна Республіка Німеччина
ЦК КПК	Центральний комітет Комуністичної партії Китаю
ШОС	Шанхайська організація співробітництва
ENISA	Європейське агентство з мережевої та інформаційної безпеки
GDPR	Генеральний регламент про захист персональних даних
GPS	Global Positioning System – супутникова система навігації

ВСТУП

Актуальність теми. Вплив Інтернету та комп'ютерних технологій перестав бути феноменом глобальних процесів і став їх віссю, двигуном. Цифрові технології слугують кровоносною та нервовою системою людських комунікацій та взаємодій і прямо на наших очах стрімко перетворюються на глобальний мозок. При цьому будь-яка сфера діяльності у масштабі індивіда, групи чи суспільства загалом неминуче несе у собі відбиток ІКТ, трансформується з них і ними опосередковується; міжнародні відносини не є винятком.

Процеси глобалізації, бурхливий розвиток комп'ютерних технологій, загальна інтеграція спричинили за собою виникнення нової форми злочинності – злочинності в сфері високих комп'ютерних технологій – кіберзлочинності, яка, в свою чергу, перетворилася в глобальну міжнародну проблему.

Щорічно кількість кіберзлочинів зростає, причому способи їх здійснення розвиваються, стають більш професійними, внаслідок чого несуть загрози не тільки громадянам та юридичним особам, але також небезпечні для окремих держав і для світової спільноти в цілому. Сьогодні жертвою злочинів, які вчиняються у віртуальному просторі, може стати будь-який користувач. Суб'єктний склад жертв варіюється від простих громадян і організацій до низки державних органів або держав в цілому.

Труднощі боротьби з даним видом злочинної діяльності полягають в її масштабності. Найчастіше неможливо ефективно скоординувати діяльність правоохоронних органів через державні кордони, межі юрисдикцій і різноманіття законодавчих систем держав. Для протидії такому виду злочинності необхідні нові, специфічні механізми виявлення, припинення, розслідування та запобігання кіберзлочинів, які будуть ефективні тільки на основі міждержавного співробітництва.

Здається, що новітні комп'ютерні технології можуть і повинні послужити ефективним засобом боротьби з кіберзлочинами. У практику роботи правоохоронних органів необхідно впроваджувати можливості мережі Інтернет та інших високих комп'ютерних технологій не тільки по виявленню та розслідуванню злочинів, але і по координації їх діяльності.

Таким чином, кібербезпека як складова сучасної системи міжнародних відносин є досить актуальним і нагальним питанням для вивчення.

Об'єктом дослідження є явище кібербезпеки.

Предметом дослідження є кібербезпека як складова сучасної системи міжнародних відносин.

Територіальні рамки цього дослідження не обмежені.

Хронологічні рамки роботи охоплюють період з 2000 по 2022 рр. *Нижня межа* – 2000 р. – рік прийняття Окінавської Хартії глобального інформаційного суспільства. Автору інколи доводиться виходити за нжню межу та згадувати події 1990-х рр. для підсилення інформації конкретними фактами. *Верхня межа* – 2022 р. – пояснюється сучасністю.

Мета роботи полягає у аналізі кібербезпеки як складової сучасної системи міжнародних відносин.

Відповідно до мети поставлені наступні **завдання:**

- висвітлити стан наукової розробки теми та джерельну базу проблеми;
- розглянути методологічну основу та понятійно-категоріальний апарат дослідження;
- проаналізувати Стратегію національної кібербезпеки США «Про основні кіберзагрози»;
- дослідити державні програми і стратегії КНР про загрози і виклики в сфері кібербезпеки;
- надати характеристику державним стратегіям кібербезпеки держав ЄС про основні загрози в кіберпросторі;

- визначити стан та перспективи розвитку ринку послуг кібербезпеки в африканських країнах;
- проаналізувати проблеми чинного міжнародного законодавства про злочини в сфері комп'ютерної інформації та можливі шляхів їх вирішення;
- з'ясувати роль кібербезпеки в забезпеченні суверенітету України.

Наукова новизна дослідження визначається актуальністю досліджуваної проблеми і тим, що запропонована тема є недостатньо вивченою у вітчизняній історіографії та полягає у тому, що у рамках проведеного наукового дослідження:

- здійснений комплексний аналіз кібербезпеки як складової сучасної системи міжнародних відносин;
- отримала подальшої систематизації історіографія проблеми та джерельна база дослідження;
- запропоновані механізми розвитку сфери кібербезпеки як складової сучасної системи міжнародних відносин.

Практичне значення роботи полягає в тому, що магістерську роботу написано в наукових і навчальних цілях. Матеріали дипломної роботи можуть бути використані при написанні дисертаційних робіт, навчальних посібників і підручників, монографій, а також під час викладання загальних і спеціальних курсів, таких як – «Міжнародна інформація», «Міжнародні відносини та світова політика», «Сучасні тенденції міжнародних відносин», «Міжнародна та європейська безпека».

Апробація результатів дослідження. Основні положення та висновки цього дослідження були представлені на розгляд у вигляді виступів на наукових конференціях, зокрема Науково-практична конференція «Могилянські читання – 2021: Досвід та тенденції розвитку суспільства в Україні: глобальний, національний та регіональний аспекти» і XVI

Міжнародна наукова конференція «Ольвійський форум: стратегії країн Причорноморського регіону в геополітичному просторі».

Публікації. За темою дослідження було опубліковано 3 публікації з них 1 наукова стаття у збірнику, який включено до Переліку наукових фахових видань України з історичних наук (категорія Б), і 2 тез (у збірниках вищевказаних конференцій).

1. Вакалюк О.С., Звездова О.О. Стратегія забезпечення кібербезпеки в гібридній війні // Acta de Historia & Politica: Saeculum XXI. 2022. № 3. С. 82-90

2. Вакалк О.С. Звездова О. О., Боротьба з кіберзлочинністю у сучасному світі // Могилянські читання – 2021: Досвід та тенденції розвитку суспільства в Україні: глобальний, національний та регіональний аспекти. Миколаїв: Вид-во ЧНУ імені Петра Могили, 2021. С. 35-37.

3. Вакалюк О.С., Звездова О.О. Проблема забезпечення кібербезпеки України Вакалюк О.С. Ольвійський форум: стратегії країн Причорноморського регіону в геополітичному просторі. Миколаїв: Вид-во ЧНУ імені Петра Могили, 2022. (у друці)

Структура роботи відбиває поставлені перед дослідженням цілі та завдання. Загальний обсяг її становить 109 сторінок, з них основного тексту – 94 сторінки. Дипломна робота складається зі вступу, 3 розділів, 9 підрозділів, висновків, списку використаних джерел і літератури (104 найменування українською, російською, англійською мовами).

РОЗДІЛ 1.
КОНЦЕПТУАЛЬНО-ТЕОРЕТИЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ

1.1. Стан наукової розробки теми та джерельна база дослідження

Літературу, яка була використана у даній роботі автор класифікує за країнознавчим критерієм, виділяючи такі групи як праці вітчизняних дослідників, російських науковців, аналітичні доробки американських та західноєвропейських дослідників.

Важливу роль відіграють праці українських науковців Є. А. Макаренко[1], О. К. Юдіна[2], А. В. Войціховського[3], С. В. Демедюка[4], С. Ф. Джерджа[5], Є. Д. Скулиша[6], С. А. Буяджи[7], Д. В. Дубова[8], М. Ю. Яцишина[9]. Вітчизняні дослідники цікавляться досить широким колом проблем пов'язаними з кіберзлочинністю та знаходять оптимальні шляхи для всієї міжнародної спільноти у боротьбі з цим явищем.

Досить значну роль під час написання дипломної роботи відіграла стаття М. В. Копійки, у якій автор аналізує процес модернізації

---

[1] Макаренко Є. А. Міжнародна інформаційна безпека: сучасні виклики та загрози. Київ: Центр вільної преси, 2006. С. 309-310.

[2] Юдін О. К. Інформаційна безпека держави: навчальний посібник. Харків: Консум, 2005. С. 321-322.

[3] Войціховський А. В. Міжнародне співробітництво в боротьбі з кіберзлочинністю. Право і безпека. 2011. № 4 (41). С. 107-109.

[4] Демедюк С. В. Міжнародний досвід протидії кіберзлочинності. Вісник Харківського національного університету внутрішніх справ: збірник наукових праць. Харків. 2014. № 4 (67). С. 65-67.

[5] Джердж С. Ф. Інформаційна безпека як частина євроатлантичної стратегії України. Миколаїв: Вид-во ЧНУ ім.. Петра Могили, 2016. С. 16-18.

[6] Скулиш Є. Д. Міжнародно-правове співробітництво у сфері подолання кіберзлочинності // Інформація і право. 2014. № 1. С. 95-96. URL: http://nbuv.gov.ua/UJRN/Infpr_2014_1_13.

[7] Буяджи С.А. Правове регулювання боротьби з кіберзлочинністю: теоретико-правовий аспект : дис. … здоб. наук. ступ. канд. юрид. наук. 12.00.01. Київ, 2018. С. 145-146.

[8] Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва : монографія. Київ: НІСД, 2014. С. 167-169.

[9] Яцишин М. Ю. Роль міжнародних організацій у протидії кіберзлочинності // Українське право. 2019. URL: https://ukrainepravo.com/international_law/public_international_law/rol-mizhnarodnykh-organizatsiy-u-protydiyi-kiberzlochynnosti/

інформаційної безпекової політики міжнародних організацій з увахуванням появи нових гібридних загроз міжнародному миру, оскільки проблеми глобальної кібербезпеки посідають особливе місце в структурі сучасних міжнародних відносин, визначають суперечності сучасного етапу міжнародного розвитку, які досягли такого рівня, що можуть поставити під загрозу забезпечення світопорядку, навіть саме існування цивілізації[10].

Також слід згадати підручник «Міжнародна інформаційна безпека»[11] авторами якого є Є. А. Макаренко, М. М. Рижков, М. А. Ожеван, О. П. Кучмій, О. М. Фролова. У підручнику розкриваються:

1) теоретико-концептуальні положення кібербезпеки як складової сучасних міжнародних відносин;

2) визначаються теоретичні складові проблеми міжнародного співробітництва в сфері інформаційної безпеки та чинники дяльності міжнародних організацій, а також стратегії національної кібербезпеки сучасних держав світу в умовах глобальних перетворень;

3) досліджено міжнародні механізми протидії новим викликам для системи міжнародної безпеки.

Серед представників російської наукової школи активно досліджують цю проблематику В. Р. Атнашев[12], Л. П. Шматкова[13], В. В. Гафнер[14],

---

[10] Копійка М.В. Модернізація політики міжнародних організацій у сфері інформаційної безпеки // Політичні проблеми міжнародних систем та глобального розвитку. 2020. С.102.

[11] Міжнародна інформаційна безпека: теорія і практика: підручник // Макаренко Є.А., Рижков М.М., Ожеван М.А., Кучмій О.П., Фролова О.М. Київ: Центр вільної преси, 2016. 418 с.

[12] Атнашев В. Р. Международное сотрудничество в борьбе с киберпреступностью и кибертерроризмом // Евразийская интеграция: экономика, право, политика. 2019. № 3. С. 38-39.

[13] Шматкова Л. П. Международное сотрудничество в борьбе с киберпреступлениями: состояние и перспективы // Молодой ученый. 2016. № 28 (132). С. 720. URL: https://moluch.ru/archive/132/37021/

[14] Гафнер В. В. Информационная безопасность: Учебное пособие. Рн/Д: Феникс, 2010. С. 182-183.

Т. Ю. Куява[15]. Дослідники роблять акцент на тому, що міжнародне співробітництво в боротьбі з кіберзлочинністю здійснюється в рамках ООН, РЄ, Міжнародної організації експертів, Інтерполу, Європолу і на основі взаємодії вищевказаних структур приймаються нормативно-правові акти регіонального та міжнародного характеру. Ю. В. Бородакій, А. Ю. Добродєєв, І. В. Бутусов визначають кібербезпеку як основний фактор національної і міжнародної безпеки[16]. Автори статті пропонують підходи до створення адекватної сучасним загрозам системи забезпечення кібербезпеки автоматизованих систем органів військового та державного управління.

Серед авторів, що займаються розробкою даної проблеми, виділяються роботи Ю. Г. Булай і Р. І. Булай[17], які вивчали способи профілактики, а також протидії кіберзлочинності та міжнародним кіберзагрозам. Р. В. Болгова, який порушував питання акторності різних спільнот в Інтернеті, у тому числі і кіберзлочинних угруповань.

Крім цього, автор спирався на дослідження В. В. Каберника, який у своїй роботі «Проблеми класифікації кіберзброї», описав види кіберзброї та провів основні відмінності даної зброї від видів інформаційного впливу[18].

Н. І. Журавленко та Л. Є. Шведова[19], які у своїй роботі «Проблеми боротьби з кіберзлочинністю та перспективні напрямки міжнародного

---

[15] Куява Т. Ю. Киберпреступность: проблемы уголовно-правовой оценки и организации противодействия // Молодой ученый. 2016. № 29 (133). С. 255. URL: https://moluch.ru/archive/133/37306/

[16]Бородакий Ю.В. Кибербезопасность как основной фактор национальной и международной безопасности XX! века (часть 1) // Вопросы кибербезопасности. 2013. № 1. С. 3.

[17] Булай. Ю. Г. Профилактика и противодействие киберпреступности, а также международным киберугрозам // Академическая мысль. 2017. № 1. URL: https://cyberleninka.ru/article/n/profilaktika-i-protivodeystvie-kiberprestupnosti-a-takzhe-mezhdunarodnym-kiberugrozam

[18] Каберник В. В., Проблемы классификации кибероружия // Вестник МГИМО. 2013. №2 (29). URL: https://cyberleninka.ru/article/n/problemy-klassifikatsii-kiberoruzhiya

[19] Журавленко Н. И. Проблемы борьбы с киберпреступностью и перспективные направления международного сотрудничества в этой сфере // Общество и право. 2015. № 3 (53). URL: https://cyberleninka.ru/article/n/problemy-borby-s-kiberprestupnostyu-i-perspektivnye-napravleniya-mezhdunarodnogo-sotrudnichestva-v-etoy-sfere

співробітництва у цій сфері», через дослідження сучасних тенденцій кіберзлочинності та дослідження міжнародного досвіду співробітництва, визначили перспективні напрямки співпраці на міжнародній арені з цього питання.

Кібербезпеку африканських країн досліджував Є. Журенко[20], К. А. Панцерев[21], Л. Цуканов[22]. Статті Н.В. Кардави[23] та А.А. Ковальова[24] присвячені стану кіберзахищеності країн ЄС. Державні програми і стратегії КНР про загрози і виклики в сфері кібербезпеки перебувають у полі зору Є. А. Разумова[25] та А.А. Рогожина[26].

Велику роль відіграли роботи американських фахівців: М. Бреннера і С. Гудман[27], Ф. Вільямса[28], Д. Денінса[29], Дж. Льюїса[30], Б. Коліна[31], К. Браун[32],

---

[20] Журенко Е. Рынок кибербезопасности на Ближнем Востоке и в Африке // Creditplus. 2021. 10 августа. URL: https://creditplus.ua/ru/blog/kiberbezopasnost-na-vostoke-i-v-afrike

[21] Панцерев К. А. Страны Африки Южнее Сахары в цифровую эпоху: к вопросу обеспечения информационного суверенитета // Азия и Африка сегодня. 2019. № 10. С. 11-12.

[22] Цуканов Л. Кибербезопасность по-сомалийски // Российский совет по международным делам: РСМД. 2022. 17 января. URL: https://russiancouncil.ru/analytics-and-comments/columns/africa/kiberbezopasnost-po-somaliyski/

[23] Кардава Н. В. Политика обеспечения кибербезопасности в Европейском Союзе: национальный и наднациональный уровни // Каспийский регион: политика, экономика, культура, 2019. № 3(60). С. 74.

[24] Ковалев А. А. Международно-правовые аспекты политики кибербезопасности некоторых европейских стран бывшего советского блока // Вестник ПАГС. 2018. №5. С. 105-106. URL: https://cyberleninka.ru/article/n/mezhdunarodno-pravovye-aspekty-politiki-kiberbezopasnosti-nekotoryh-evropeyskih-stran-byvshego-sovetskogo-bloka

[25] Разумов Е.А. Политика КНР по обеспечению кибербезопасности // Россия и АТР. 2017. № 4 (98). С. 160-161. URL: https://cyberleninka.ru/article/n/politika-knr-po-obespecheniyu-kiberbezopasnosti

[26] Рогожин А.А. КНР – Закон о кибербезопасности принят // ИМЭМО РАН. 2017. URL: https://www.imemo.ru/news/events/text/knr-zakon-o-kiberbezopasnosti-prinyat.

[27] Marc D. Goodman and Susan W. Brenner. The emerging consensus on criminal conduct in cyberspace // Archive.org. 2018. URL: https://archive.org/details/TheEmergingConsensusOnCriminalConductInCyberspace

[28] Williams P. Organized Crime and Cybercrime: Synergies, Trends, and Responses // Crime Research. 2018. URL: http://www.crime-research.org/library/Cybercrime.htm

[29] Dennis M. A. Defenition of «Cybercrime» // Encyclopædia Britannica. 2018. URL: https://www.britannica.com/topic/cybercrime

[30] Lewis J. A. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats // Center for Strategic and International Studies, December 2002. P. 7-8.

присвячені кіберзлочинності, дають непогане уявлення про це явище, але, на жаль, ці дослідження практично ніколи не охоплюють Україну і українське законодавство, в той час, як Україна досить давно є активним учасником міжнародних зусиль з протидії кіберзлочинності. Проте, вони дають хороші теоретичні основи для вивчення кіберзлочинності в глобальному аспекті.

До дослідження питання кібербезпеки у міжнародному просторі зверталися такі європейські науковці, як М. Лібіцкі[33], Ф. Хоффман[34], Дж. Най-молодший[35], А.Себровскі[36], які розробили новітні практики використання сучасними державами світу інформаційних озброєнь у міжнародних конфліктах. Д. Вентре[37] та Дж. Р. Ліндсей[38] аналізує китайську кібербезпеку та оборону.

Отже, незважаючи на достатній науковий доробок, сучасні глобалізаційні зміни підкреслюють актуальність даного дослідження, що дозволить зробити адекватні прогнози на рахунок кібербезпеки у сучасній системі міжнародних відносин. Тому подальше дослідження обраної проблематики робить цей науковий пошук актуальним і необхідним.

Джерельна база роботи представлена офіційними документами і матеріалами, міжнародними актами, які стосуються проблеми боротьби з

---

[31] Collin B. The Future of CyberTerrorism: Where the Physical and Virtual Worlds Converge // Crime Research. URL: http://www.crime-research.org/library/Cyberter.htm

[32] Brown C. Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice // International Journal of Cyber Criminology Vol 9 Issue 1 January. June 2015. P. 32-35.

[33] Libicki M.C. Conquest in Cyberspace: National Security and Information Warfare. Cambridge: Cambridge University Press, 2007. P. 99-100.

[34] Hoffman F. Hybrid vs Compound // Small Wars Journal. 2009. October. URL: http://smallwarsjournal.com /blog/journal/docs–temp/189–hoffman.pdf.

[35] Nye J.S. Cyber Power. Cambridge: Pub. by Belfer Center for Science and International Affairs, 2010. P. 14-15.

[36] Cebrovski A. Network–Centric Warfare: Its Origin and Future // Proceedings. 1998. January. URL: http:// www. kinection.com/ncoic/ncw_origin_future.pdf

[37] Ventre D. Chinese Cybersecurity and Defense. London // Wiley-ISTE Publ., 2014. P. 221-22.

[38] Lindsay J. R. The Impact of China on Cybersecurity // International Security. 2015. Vol. 39. P. 9-10. URL: https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=2849&context=lawreview

кіберзлочинністю. Більшість англомовних документів, використаних у роботі, були взяті з офіційних сайтів державних інститутів та міжнародних організацій. Автор магістерської роботи виділяє чотири основні групи джерел, які лягли в основу розкриття обраної проблематики.

Першу групу джерел становлять офіційні міжнародні документи. Офіційні механізми міжнародного співробітництва включають в себе двосторонні, регіональні та багатосторонні договори в області боротьби з кіберзлочинністю.

Зокрема Конвенція РЄ «Про кіберзлочинність», прийнята в Будапешті в листопаді 2001 р. [39] і т.д. В Окінаві на зустрічі, що відбулася в липні 2000 р., в прийнятій хартії Глобального інформаційного суспільства[40], лідери країн Великої вісімки визнали інформаційно-комунікаційні технології в якості основного фактора, що формує суспільство XXI ст., і підтвердили свою готовність сприяти переходу до інформаційного суспільства, а також повної реалізації його переваг, виробили і включили в підсумковий документ Саміту ключові напрямки роботи для досягнення поставленої мети, зокрема, в області зміцнення політики та нормативно-правової бази по боротьбі зі зловживаннями, які підривають цілісність інформаційних мереж.

Сторони погодилися з тим, що зусилля міжнародного співтовариства, спрямовані на розвиток глобального інформаційного суспільства, повинні супроводжуватися погодженими діями по створенню безпечного і вільного від злочинності простору, здійснення ефективних заходів по боротьбі з комп'ютерною злочинністю.

---

[39] Convention on Cybercrime // Council of Europe. 2001. URL: https://rm.coe.int/1680081561

[40] Okinawa Charter on Global Information Society // Ministry of foreign affairs of Japan. 2000. URL: https://www.mofa.go.jp/policy/economy/summit/2000/documents/charter.html#:~:text=Information%20and%20Communications%20Technology%20(IT,shaping%20the%20twenty%2Dfirst%20century.&text=The%20essence%20of%20the%20IT,to%20use%20knowledge%20and%20ideas.

Даний документ був одним з перших міжнародних актів, регіонального, а потім і глобального рівня, що регламентували багатосторонні заходи з протидії кіберзлочинності, а так само сприяла стандартизації європейських кримінальних та інших видів законодавств у цій галузі.

Конвенція про кіберзлочинність[41], є єдиним документом обов'язкового застосування, який регулює правовідносини у сфері експлуатації комп'ютерної мережі[42].

Угода про співробітництво держав-учасниць СНД у боротьбі зі злочинами в сфері комп'ютерної інформації 2001 р. містить кілька статей, присвячених міжнародному співробітництву (ст. 5-7), в яких перераховані форми співпраці, які охоплюються цією угодою (а саме: обмін інформацією; надання правової допомоги відповідно до міжнародних документів; попередження, виявлення, припинення і розслідування злочинів у сфері комп'ютерної інформації тощо).[43].

Ще в січні 2015 р. учасники ШОС внесли на розгляд ГА ООН Міжнародний кодекс поведінки в області інформаційної безпеки[44], який є першим міжнародним документом, присвяченим нормам поведінки в інформаційному середовищі.

У грудні 2018 р. ГА ООН прийняла резолюцію «Досягнення у сфері інформатизації та телекомунікацій в контексті міжнародної безпеки»[45], яка

---

[41] Convention on Cybercrime // Council of Europe. 2001. URL: https://rm.coe.int/1680081561

[42] Войціховський А.В. Міжнародне співробітництво в боротьбі з кіберзлочинністю. Право і безпека. 2011. № 4 (41). С. 107-109.

[43] Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации // Верховна Рада України. 2001. URL: https://zakon.rada.gov.ua/laws/show/997_353#Text

[44] International code of conduct for information security // United Nations Organisation. URL: https://digitallibrary.un.org

[45] Генассамблея ООН проголосовала за российский проект резолюции по глобальной кибербезопасности // Экспертный центр электронного государства. 2018. URL: https://d-russia.ru/genassambleya-oon-progolosovala-za-rossijskij-proekt-rezolyutsii-po-globalnoj-kiberbezopasnosti.html

була підтримана 119 державами, 46 країн проголосували проти, 14 утрималися.

Норми матеріального права гармонізовані за допомогою цілої низки директив, зокрема, Директива про протидію сексуальній експлуатації дітей онлайн і дитячої порнографії[46], Директива щодо атак проти інформаційних систем[47], Директива про безпеку мереж та інформаційних систем[48].

Ст. 32 і 34 Конвенції ЛАД про боротьбу зі злочинами в області інформаційних технологій (2010 р.)[49] містять положення про надання взаємної допомоги, процедури співпраці та подання запитів про надання взаємної допомоги.

Ст. 28 Конвенції АС про кібербезпеку і захист персональних даних (2014 р.)[50] включає в себе положення про уніфікацію, взаємну правову допомогу у справах, пов'язаних з кіберзлочинністю, і обміну інформацією[51].

ЕКОВАС прийняв Конвенцію про взаємну правову допомогу у кримінальних справах та Конвенцію про видачу з метою сприяння співпраці у розслідуванні кіберзлочинів та видачі кіберзлочинців[52].

---

[46] Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA // EUR-Lex. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011L0093

[47] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA // EUR-Lex. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32013L0040

[48] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union // EUR-Lex. URL: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32016L1148

[49] Arab Convention on Combating Information Technology Offences // Asian School of Cyber Laws. 2010. URL: https://www.asianlaws.org/gcld/cyberlawdb/GCC/Arab%20Convention%20on%20Combating%20Information%20Technology%20Offences.pdf

[50] African Union Convention on Cyber Security and Personal Data Protection // African Union. 2014. URL: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

[51] Яцишин М.Ю. Роль міжнародних організацій у протидії кіберзлочинності // Українське право. 2019. URL: https://ukrainepravo.com/international_law/public_international_law/rol-mizhnarodnykh-organizatsiy-u-protydiyi-kiberzlochynnosti/

Другу групу джерел складають офіційні нормативно-правові акти (закони) держав у сфері кіберзлочинності (США, КНР, ФРН, Австрія, Швеція, Великобританія, Естонія, Норвегія, Україна).

Наприклад, Закон США про шахрайство і зловживання з використанням комп'ютерів, який зазначає, що особі, будучи засудженій за кіберзлочини, але яка повторно вчинила несанкціонований доступ до комп'ютера, що спричинило тяжкі наслідки, може бути призначено тюремне ув'язнення терміном до 20 років[53].

Закон про підвищення безпеки систем інформаційних технологій від 7.07.2015 р. (IT-Sicherheitsgesetz) створив в ФРН правову основу забезпечення кібербезпеки. На додаток до обов'язкового повідомлення про інциденти інформаційної безпеки, він встановлює мінімальні стандарти IT та вимоги до звітності операторів критично важливих інфраструктур (включаючи енергетику, водопостачання, охорона здоров'я, телекомунікації). Даним Законом доповнюються положення законів про телемедіа (TMG) і закону про телекомунікації (TKG) в частині захисту телемедіа- і телекомінфраструктури[54].

Разом з тим в останні кілька років активно висуваються пропозиції про перегляд названого Закону з метою посилення боротьби з кіберзлочинністю. У березні 2019 р. Міністерством внутрішніх справ опублікований проект Закону про безпеку IT 2.036 (IT-SiG 2.0). У даному проекті повноваження правоохоронних органів розширені, запропоновані зміни в кримінальному та кримінально-процесуальному законодавстві щодо посилення покарання за кіберзлочини. Сфера застосування Закону поширюється на інші сфери

---

[52] Directive C/DIR. 1/08/11 on fighting cyber crime within ECOWAS // Economic Community of West African States(ECOWAS). 2011. URL: http://www.tit.comm.ecowas.int/wp-content/uploads/2015/11/SIGNED_Cybercrime_En.pdf

[53] Computer Fraud and Abuse Act // The Free Encyclopedia Wikipedia.URL: https://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act

[54] Collin B., The Future of CyberTerrorism: Where the Physical and Virtual Worlds Converge // Crime Research. URL: http://www.crime-research.org/library/Cyberter.htm

економіки (крім критично важливих, згаданих в чинному законі про підвищення безпеки систем інформаційних технологій), зокрема сфери, які представляють суспільний інтерес, порушення в яких можуть привести до погіршення фундаментальних інтересів суспільства.

Національна стратегія кібербезпеки Австрії використовує більш широку концепцію безпеки ІКТ і розглядає кібербезпеку як захист систем ІКТ за допомогою конституційних засобів від пов'язаних із суб'єктом, технічних, організаційних та природних небезпек, що становлять ризик для безпеки кіберпростору, включаючи інфраструктуру та безпеку даних, а також безпеку в кіберпросторі[55].

У Стратегії кібербезпеки Швеції, яка була прийнята у 2016 р., під кібербезпекою розуміється комплекс заходів безпеки, спрямованих на збереження конфіденційності, достовірності та доступності інформації[56].

У квітні 2007 р. у Великобританії були змінені правила розкриття інформації про банківське шахрайство. Після прийняття в 2006 р. Закону про шахрайство банки і фінансові компанії стали першою інстанцією, куди слід було повідомляти про випадки шахрайства з пластиковими картами, чеками і системами онлайн-банкінгу. Офіційно заявленою метою цієї зміни було зменшення бюрократичної тяганини. При цьому висловлювалися побоювання, що в результаті частина інформації про подібні інциденти буде замовчуватись[57].

У Норвегії діяльність в області кібернетичної безпеки визначена урядом в Національній стратегії кібербезпеки 2018 р.. Стратегія кібербезпеки має такі цілі: 1) норвезькі компанії проходять процеси цифровізації в

---

[55] Austrian Cyber Security Strategy // ENISA: official web-site. 2013. URL:: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/austrian-cyber-security-strategy

[56] A national cyber security strategy // Government offices of Sweden: official web-site. 2016. URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/swedish-national-cyber-security-strategy

[57] Киберпреступность и закон: обзор положений законодательства Великобритании // АО Kaspersky Lab. 2009. URL: https://securelist.ru/kiberprestupnost-i-zakon-obzor-polo/1315/

безпечному і надійному форматі, а також здатні захистити себе від кіберзагроз та інцидентів; 2) критичні соціальні сервіси забезпечуються надійною цифровою інфраструктурою; 3) пріоритет розвитку компетенцій у сфері кібербезпеки; 4) суспільство підвищує навички виявлення і запобігання кібератак; 5) правоохоронні органи ефективно протидіють кіберзлочинам[58].

Закон Естонії про кібербезпеку[59] 2018 р. має на меті посилення безпеки інформаційних систем, використовуваних при наданні життєво важливих послуг. Закон встановлює вимоги до підтримання безпеки систем, процедури запобігання та вирішення кібер-інцидентів, а також регулює питання контролю, нагляду та відповідальності за порушення в сфері кібербезпеки.

Закон про кібербезпеку КНР прийнятий 06.11.2016 р. і введений в дію 01.07.2017 р.. Закон встановлює загальні положення в області кібербезпеки, підтримку і просування кібербезпеки, забезпечення функціонування інформаційно-комунікаційних мереж, забезпечення інформації в інформаційно-комунікаційних мережах, моніторинг, раннє виявлення та дії в відповідь на надзвичайні обставини, законодавчо встановлена відповідальність у сфері кібербезпеки[60].

Президент України Володимир Зеленський затвердив нову Стратегію кібербезпеки України, яку схвалила РНБО 14 травня 2021 р.. Про це повідомлялося в Указі Президента № 447/2021 від 26 серпня, яким запроваджено рішення РНБО від 14 травня 2021 року «Про Стратегію кібербезпеки України». Також у документі В. Зеленський визнав попередню Стратегію кібербезпеки (затверджено Президентом України 15 березня 2016 р..), як таку, що втратила чинність. Згідно з опублікованим текстом

---

[58] National Cyber Security Strategy for Norway // ENISA. 2018. URL: https://www.enisa.europa.eu

[59] Cybersecurity Act // Riigikantselei. 2019. URL: https://www.riigiteataja.ee/en/eli/523052018003/consolide

[60] The Cybersecurity Law of the People's Republic of China // New America. URL: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecuritylaw-peoples-republic-china/

Стратегії, забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки України та реалізація зазначеного пріоритету здійснюватиметься шляхом посилення можливостей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі[61].

Отже, стосовно до кіберзлочинності виявляються неефективними традиційні методи і способи боротьби зі злочинністю, засновані на територіальному принципі, оскільки кіберпростір має глобальний, міжнародний характер. Ця боротьба виявляється ефективнішою на регіональному рівні. Це пояснюється існуванням такого парадоксу: з одного боку, держави змушені співпрацювати для боротьби з такою транснаціональною загрозою, як кіберзлочинність, але, з іншого боку, така співпраця зачіпає суверенітет держави, обмежує його в галузі кримінального права і захисту інформації. Тому співпраця виявляється успішною в регіонах з високим рівнем політичної довіри між країнами, як це відбувається в ЄС.

Третя группа джерел включає статистичну та довідкову інформацію про стан, структуру та динаміку кіберзлочинів на сучасному етапі в умовах пандемії[62]. Важливим є матеріал, який демонструє рейтинги[63] країн за ступен кіберзагрози і кіберзахищеності протягом останніх років.

Четверта група джерел є не менш важливою і складається з матеріалів опублікованих в ЗМІ. Основний масив інформації зосереджений у офіційних

---

[61] Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України №447/2021 // Президент України: офіційне Інтернет-представництво. URL: https://www.president.gov.ua/documents/4472021-40013

[62] The COVID-19 pandemic and trends in technology // Chatham House, The Royal Institute of International Affairs. 2021. URL: https://www.chathamhouse.org/2021/02/covid-19-pandemic-and-trends-technology/03-covid-19-changing-cybercrime-landscape; Обзор киберугроз 2020: результат пандемии // TechExpert. 2020. URL: https://techexpert.ua/ru/cybersecurity-covid/

[63] Рейтинг стран мира по уровню подверженности киберугрозам 2020 (CEI – Cybersecurity Exposure Index) // 10 GUARDS. URL: https://10guards.com/ru/articles/global-cybersecurity-exposure-index-2020/; The State of Ransomware 2021 // SOPHOS: official web-site. 2021. URL: https://secure2.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf

Інтернет-представництвах газет: «Украинская правда» (https://www.pravda.com.ua/)[64]; «Хвиля.net» (http://hvylya.net/)[65]; «Deutsche Welle» (https://www.dw.com/)[66]; «УКРінформ» (https://www.ukrinform.ru/)[67]. Слід зазначити, що ця група джерел дає найбільш об'єктивне уявлення про сучасний стан кібербезпеки як складової системи міжнародних відносин.

Отже, можна зробити висновок, що перелічені джерела складають достатню базу для дослідження поставлених автором завдань та досягнення головної мети. Англомовні джерела потребували детального вивчення, адже саме вони вони акумулюють найбільший масив інформації з обраної проблематики.

1.2. Методологічна основа дослідження

У сучасній науці існує два керівні підходи у дослідженні кібербезпеки як складової сучасної системи міжнародних відносин – це технологічний та політологічний. Їхня відмінність полягає у використанні різних критеріїв безпеки. Технологічний підхід як основні критерії виділяє забезпечення конфіденційності, цілісності та доступності інформації. Політологічний підхід концентрується на захисті від інформаційних загроз, здатних призвести до руйнування традиційних духовно-моральних цінностей суспільства, розмивання ідентичності особистості, дестабілізації політичної системи та втрати державного суверенітету. Комплексне дослідження інформаційної безпеки передбачає поєднання обох підходів.

---

[64] Более полусотни кибератак на системы органов власти Украины отбили в декабре // Украинская правда. 2022. 4 января. URL: https://www.pravda.com.ua/rus/news/2022/01/4/7319426/

[65] Варшавський саміт НАТО – критичний аналіз головних рішень // «Хвиля.нет»: офіційна сторінка газети. 2016. URL: http://hvylya.net/analytics/geopolitics/varshavskiy–samit–nato–kritichniy–analiz–golovnih–rishen.html

[66] НАТО поможет Украине усилить кибербезопасность // Deutsche Welle. 2022. 15 января. URL: https://www.dw.com/ru/nato-usilit-kibersotrudnichestvo-s-ukrainoj/a-60432756

[67] Президент утвердил новую Стратегию кибербезопасности Украины // УКРінформ. 2021. 26 серпня. URL: https://www.ukrinform.ru/rubric-polytics/3304776-prezident-utverdil-novuu-strategiu-kiberbezopasnosti-ukrainy.html

У ході дослідження автор дотримувався неореалістичної парадигми теорії міжнародних відносин, виходячи з тенденції до фрагментації міжнародних зусиль у бік національних або, іноді, регіональних ініціатив, які є яскравими прикладами ефективних протидійних заходів, порівняно з міжнародними зусиллями, в той же час застосовуючи національні та регіональні заходи, держави при цьому прагнуть до збереження статусу-кво та непорушності суверенітету, у зв'язку з чим найчастіше заходи та документи загрожують самостійності держави та її винятковій ролі у самостійному прийнятті рішень, з цього питання[68].

Слід згадати про принцип комплексності – оптимальне використання різних методів, заходів та засобів захисту інформації (адміністративно-правових, організаційних, організаційно-технічних, технічних, програмних) для нейтралізації загроз інформації та підтримки заданого рівня захищеності інформації, інтеграції цих засобів в єдину технологічно пов'язану та керовану систему.

Розробкою системних ідей займається системний аналіз (спеціальна синтетична наука, у центрі якої вивчення складних систем)

Системний підхід дозволяє, по-перше, виявити ті чинники та взаємозв'язки, які можуть виявитися дуже суттєвими; подруге, видозмінювати методику спостережень та експеримент таким чином, щоб включити ці фактори до розгляду; по-третє, висвітлити слабкі місця гіпотез та припущень.

Для того щоб усвідомити необхідність системності у всіх галузях людської діяльності, слід розглянути послідовне формування трьох рівнів системності праці: механізацію, автоматизацію і кібернетизацію[69].

---

[68] Почепцов Г. Г. Інформаційна політика: навчальний посібник. С. 128-129.
[69] Макаренко Є. А. Міжнародна інформаційна безпека: сучасні виклики та загрози. С. 456-457.

1) Механізація – найпростіший спосіб підвищення ефективності праці. За допомогою механізмів та машин одна людина виконує фізичну роботу, посильну багатьом людям.

2) Автоматизація – метод підвищення продуктивності праці з допомогою автоматів, тобто технічних пристроїв (телефонний зв'язок, у промисловості функціонують автоматичні лінії, цехи та заводи, розвивається промислова та транспортна робототехніка)

3) Кібернетизація (штучний інтелект). Кібернетика першою стала претендувати на наукове вирішення проблем управління складними системами.

Потужний поштовх до системного підходу дає теорія комунікації та засоби кібернетики. У результаті їх застосування склалися уявлення про держави, нації, політичні режими як кібернетичні системи, що мають «вхід» і «вихід», що керуються за допомогою механізму зворотних зв'язків («стимул» – «реакція»).

Комплексні дослідження всіх видів безпеки доцільно здійснити на основі системного підходу та аналізу. При цьому необхідно перейти до системного дослідження об'єктів і систем, що вивчаються. Це дозволить чітко відстежити внутрішні взаємозв'язки підсистем, у тому числі підсистеми економічної безпеки, у процесі функціонування загальної системи національної кібербезпеки країни.

Системний підхід передбачає дослідження об'єкта (подання досліджуваного об'єкта як загальної системи, що з підсистем зі своїми взаємозв'язками). З цього погляду безпека країни складається з підсистем: економічної, енергетичної, продовольчої, інофрмаційної. Оскільки кожна з підсистем у своїй роботі спирається на значні обсяги інформації, що переробляється за допомогою інформаційних технологій, у внутрішній структурі кожної з підсистем має бути вирішене питання про інформаційну безпеку функціонування кожної з підсистем загальної системи. При цьому

головним питанням інформаційної безпеки є проведення заходів, що дають змогу виключити несанкціонований доступ до інформації, що циркулює в підсистемі економічної безпеки. У структурній складовій кожної підсистеми є інформаційне забезпечення, функціонування якого тісно пов'язане з підсистемою інформаційної безпеки[70].

Але найголовніше те, що у роботі використовувався принцип об'єктивності, котрий означає неупередженість, незалежність суджень дослідника, хоча при цьому він не повинен бути нейтральним і має право на обґрунтування власної позиції. Автор намагався взагалі відійти від упередженої оцінки історичних подій, бо об'єктивність полягає в правдивому зображенні суперечностей інтересів різних сторін у міжнародних відносинах і забезпечує науковість.

Порівняльний підхід був використаний виявлення відмінностей і точок дотику позицій держав у забезпеченні кібербезпеки, особливо у контексті міжнародної безпеки.

Отже, керуючись названими принципами, автор намагався викласти матеріал у послідовній і логічно завершеній формі та найбільш адекватно відобразити суть кібербезпеки. Поєднання зазначених принципів дало можливість автору уникнути суб'єктивних оцінок, залишатися на науковій точці зору і забезпечило наукову достовірність результатів дослідження. При цьому слід відзначити, що істотну роль у дослідженні відіграє принцип системності.

Метод наукового пізнання – набір інструментів і засобів для здобуття нового знання, а також його практичного використання під час вивчення тих чи інших об'єктів. Для досягнення мети дослідження та вирішення завдань, поставлених перед магістрантом, були використані загальнонаукові й спеціальні методи дослідження.

---

[70] Боднар І. Міжнародна інформація: Навчально-методичний посібник для самостійного вивчення курсу. С. 90-91.

У сучасному науковому розумінні методологія – це сукупність підходів, способів, методів, прийомів і процедур, що застосовуються в процесі наукового пізнання, це галузь теоретичних знань та уявлень про сутність і форми, закони, порядок та умови їх застосування. Вона формується як на підставі загальних принципів пізнання, так і під впливом особливостей предмета дослідження конкретної науки[71].

Методологічна основа дипломної роботи ґрунтується на загальнонаукових принципах об'єктивності та діалектичного розуміння історичного процесу.

Відповідно до поставленої мети та завдань використовуються загальнонаукові методи (аналіз, синтез), міждисциплінарні (статистичний метод), а також спеціально-історичні методи (історично-порівняльний).

В основу дослідження покладений принцип об'єктивного вивчення документів, джерел та історичних фактів. При цьому слід відзначити, що істотну роль у дослідженні відіграє принцип історизму. Метод хронології дає можливість розглянути обрану тему дослідження у часовій послідовності, тобто аналізувати усі події у хронологічному порядку.

В основі дослідження покладений принцип об'єктивного вивчення джерел, літератури, документальної бази та історичних фактів.

Структурно-функціональний метод дав можливість розкласти на складові частини складний об'єкт – кібербезпеку на дрібніші частини, продемонстрував зв'язки між ними, визначив їх роль у задоволенні потреб системи кібербезпеки у сучасному світі. Структурно-функціональний метод відповів на питання: які функції повинна виконувати кібербезпека, за допомогою яких інструментів і з якою ефективністю вона їх реалізовує.

Порівняльно-історичний метод, використаний при вивченні основних етапів розвитку та формування загального уявлення, про стан

[71] Герасимчук Т.Ф. Теоретико-концептуальні основи та методи дослідження міжнародних відносин // Український історичний журнал. 2006. № 5. С.188.

кіберзлочинності і заходів протидії їй. Історичний аналіз дозволив описати еволюцію підходів сучасних держав до забезпечення кібербезпеки та сутності кіберзагроз та кібернебезпек.

Для виявлення та аналізу нормативно-правових аспектів у сфері забезпечення безпеки у кіберпросторі використовувався інституційний підхід[72].

Порівняльно-правовий метод використовувався для аналізу існуючих угод і договорів, нормативно-правових актів, що регулюють питання кібербезпеки в провідних країнах світу, а також системний метод, який дозволяє проаналізувати структуру основних органів, що займаються питаннями попередження кіберзлочинів і їх взаємодії в процесі протидії правопорушенням. Системний метод дозволив уявити політику кібербезпеки сучасних держав у цілісному вигляді, що складається із взаємозалежних елементів та з'ясувати, що для свого сталого розвитку людство повинно знайти механізми протидії інформаційному тероризму, розробити і реалізувати комплекс заходів щодо забезпечення безпеки в інформаційному просторі. Першочерговими заходами в цій області є:

1. Об'єднання зусиль держав – членів міжнародної спільноти в галузі забезпечення інформаційної безпеки, закріплення співпадаючих інтересів і спільне проведення заходів щодо їх захисту переважно на основі двосторонніх і багатосторонніх договорів.
2. Створення базового понятійного апарату – необхідно домовитися про єдине трактування термінів, які використовуються в даній області. Необхідно прагнути до гармонізації національних законодавств у частині боротьби з інформаційним тероризмом.
3. Використання потенціалу хакерського співтовариства, тобто людей з яскраво вираженим захопленням до пізнання в області інформаційних

[72] Edgar Th. Research Methods for Cyber Security. Elsevier Science, 2017. P. 113-114.

технологій, які виходять за рамки пізнавальної та навчальної діяльності, в антитерористичних цілях.

4. Розробка системи заходів з моніторингу та контролю за поширенням знань і технологій, критичних з точки зору інформаційної безпеки. Один з основних ресурсів, які потребують моніторингу – це висококваліфіковані фахівці, що володіють знаннями в області високонадійних методів захисту інформації. Саме вони є об'єктом інтересу міжнародних терористичних організацій.
5. Сприяння кожного користувача (організації всіх секторів економіки, освітні установи, громадяни – користувачі Інтернет та ін.) забезпеченню інформаційної безпеки на тій ділянці кіберпростору, яким він володіє або користується[73].

Описовий метод використовувався для розкриття змісту кіберзагроз та кібернебезпек. Методи статистичного аналізу дозволили проаналізувати динаміку інцидентів у кіберпросторі. Статистичний, зокрема метод статистичного порівняння, який використовувався при вивченні динаміки розвитку і збільшення числа кібератак, з метою виявити основні тенденції розвитку і помітити основні причини явища кіберзлочинності[74].

Також у процесі написання дипломної роботи було застосовано такі методи дослідження, як теоретичний аналіз, узагальнення, порівняння, класифікування, спостереження, моделювання, а також метод прогнозування. Метод прогнозування дав змогу виявити той факт, що проблему боротьби з кібертероризмом сьогодні вже треба ставити на один рівень з тероризмом і організованою злочинністю. При цьому необхідно здійснювати комплексний підхід до вирішення цієї проблеми на міжнародному рівні. На жаль, зараз відсутні:

---

[73] Кудрявцева С. П. Міжнародна інформація. навч. посіб. для студентів вищих навч. закл.. Київ: Видавничий Дім «Слово», 2005. С. 205-206.
[74] Edgar Th. Research Methods for Cyber Security. P. 115.

1) законодавчі акти, які регулюють кримінально-процесуальні дії;

2) спеціально підготовлені кадри (оперативного і слідчого апарату, що спеціалізується на виявленні і розкритті злочинів в інформаційно-телекомунікаційній сфері);

3) немає надійної системи взаємодії з правоохоронними органами зарубіжних країн[75].

На основі методу узагальнення виявлено, що в цілому, основною проблемою в сфері боротьби з кіберзлочинністю є складність ідентифікації винних осіб і оцінки масштабу наслідків злочинного діяння. Високотехнологічні терористичні акції нової епохи здатні сьогодні продукувати системну кризу всієї світової спільноти і поставити під загрозу існування окремих регіонів світу, що не було характерно для традиційних терористичних актів. Відповідно, боротьба з комп'ютерними атаками, в тому числі що становлять загрозу кібертероризму, зводиться до однієї глобальної задачі: убезпечити кіберпростір шляхом зведення до мінімуму впливу зловмисників на інформаційні системи.

Використання емпіричних методів стало запорукою наукової об'єктивності та достовірності результатів дослідження. За допомогою нормативного методу автор зміг працювати з документальними джерелами – офіційними документами та текстами міждержавних угод. Також були використані методи аналізу та синтезу, індукції та дедукції, класифікації та ін. Зокрема, метод класифікації використовувався при аналізі джерел та літератури.

Отже, дипломна робота побудована на загальнонаукових методах пізнання, із застосуванням науково-критичного аналізу джерел.

---

[75] Denning D.E. Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy // Information Warfare Site. URL: http://www.iwar.org.uk/cyberterror/resources/denning.htm

Загальнонаукові методи дали можливість систематизувати та класифікувати сукупність наукового та прикладного знання в сфері міжнародних відносин.

1.3. Понятійно-категоріальний апарат

Сучасне розвинене суспільство, цілком ґрунтується на використанні ІКТ, комп'ютерних мереж, хмарних сховищ даних, а так само багатьох інших переваг XXI століття.

Під ІКТ слід розуміти сукупність методів, різних виробничих процесів, програмне забезпечення або лінгвістичні засоби, що об'єднуються для того, щоб накопичувати, зберігати, обробляти і передавати інформацію різного роду, в першу чергу в інтересах користувачів[76]. Більше половини населення земної кулі на сьогоднішній день є в тій чи іншій мірі активними користувачами мережі Інтернет. Щоденна робота органів державного апарату, транспортних, енергетичних систем, органів охорони здоров'я та банківських структур важко уявити без надійної і постійної роботи високих технологій і засобів ІКТ.

ІКТ – засоби, способи і методи накопичення та обміну і поширення інформації, з метою її використання, що зачіпають використання мережі Інтернет, пристроїв об'єднаних в єдиний інформаційний простір, з метою отримання і обробки максимальної кількості інформації.

Оскільки, як уже було зазначено, засоби і способи ІКТ в ході прогресу проникають в усі сфери життя людства, включаючи фінансову, освітню, державну і навіть приватне життя громадян нерідкими стають випадки порушення прав і свобод людей, організацій і навіть цілих держав, із застосуванням високих технологій, високотехнологічних пристроїв та інших втілень ІКТ.

---

[76] Почепцов Г. Г. Інформаційна політика: навчальний посібник. Київ: Знання, 2006. С. 244-245.

Об'єднання пристроїв і баз даних в єдині простір і мережі, дозволило користувачам отримувати доступ, обробляти і передавати інформацію з будь-якої точки планети, здійснювати управління власними активами, капіталами компанії або фонду, укладати угоди договору без особистого контакту. Але саме ці переваги і дозволили стати «всесвітній павутині» одночасно і місцем скоєння злочинів і метою протиправних дій зловмисників[77].

Енциклопедія «Britannica» кіберзлочинами, які, так само можуть бути названі комп'ютерними злочинами визначає використання комп'ютера, як інструмент для здійснення протиправних дій, як крадіжка, поширення порнографії або порушення прав інтелектуальної власності. Крім цього, згідно з визначенням, кіберзлочини включають в себе порушення приватного життя і крадіжку особистих даних[78]. Дане визначення, в значній мірі підходить під феномен «злочини з використанням комп'ютера», оскільки зазначає роль технічних пристроїв лише як інструменту здійснення злочинів.

Виходячи з виведеного визначення, слід і визначення кіберзлочинності в цілому, яку слід розуміти як сукупність злочинних дій, що здійснюються за допомогою технологічних засобів, які порушують законодавчо встановлені норми, з метою вилучення політичних, економічних та інших видів вигод і зазіхають на функціонування, стабільність і конфіденційність інформаційних систем.

Кіберзлочинність перетворилася в дуже вигідний бізнес, доходи від якого перевищують доходи від торгівлі зброєю або наркотиками. Кіберзлочинці відрізняються своїм професіоналізмом, скритністю, цинічністю. Головна мета таких злочинів – витяг максимального прибутку. Однією з проблем також є не повідомлення та приховування фактів, пов'язаних з кібератаками. Більшість організацій не хочуть втрачати свою

---

[77] Манойло А. В. Государственная информационная политика в особых условиях: Монография. Москва: МИФИ, 2003. С. 129-130.

[78] Dennis M. A. Defenition of «Cybercrime» // Encyclopædia Britannica. 2018. URL: https://www.britannica.com/topic/cybercrime

ділову репутацію, в зв'язку з чим намагаються приховати інформацію про вчинений злочин. Звідси і виникають проблеми виявлення та запобігання таким злочинам. Звісно ж необхідно вирішувати проблеми з кіберзлочинністю[79].

Конвенція РЄ «Про кіберзлочинність», визначає кіберзлочини, як дії, що здійснюються проти конфіденційності, цілісності, а так само доступності комп'ютерних систем, мереж та інформації, і зловживання даними системами мережами і даними в злочинних цілях[80].

Комп'ютерні злочини – це передбачені кримінальним законом суспільно небезпечні дії, в яких машинна інформація є об'єктом злочинного зазіхання. У даному випадку в якості предмета або знаряддя злочину буде виступати машинна інформація, комп'ютер, комп'ютерна система або комп'ютерна мережа. Комп'ютерні злочини умовно можна поділити на дві великі категорії: 1) злочини, пов'язані з втручанням у роботу комп'ютерів; 2) злочини, що використовують комп'ютери як необхідні технічні засоби[81].

Отже, кіберзлочин – дія, що здійснюється за допомогою використання персонального комп'ютера, мобільного пристрою або інших технічних засобів, пов'язаних між собою мережею Інтернет, що порушує права людини, а так само законодавчо встановлені норми, з метою вилучення економічних, політичних, культурних та інших вигод; порушення стабільності, конфіденційності та доступності інформаційних мереж.

Комп'ютерну інформацію як предмет злочину можна визначити наступним чином: відомості про об'єктивний світ і, що відбуваються в ньому

---

[79] Куява Т. Ю. Киберпреступность: проблемы уголовно-правовой оценки и организации противодействия // Молодой ученый. 2016. № 29 (133). С. 255. URL: https://moluch.ru/archive/133/37306/

[80] Cybercrime: The Council of Europe Convention // EveryCRSReport.com. URL: https://www.everycrsreport.com/reports/RS21208.html

[81] Макаренко С. И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI. СПб.: Наукоемкие технологии, 2017. С. 304-305.

процесах цілісність, конфіденційність і доступність яких забезпечується за допомогою комп'ютерної техніки, і які мають власника і ціну.

Розділити кіберзлочини на окремі категорії не так просто, проте в цілому можна виділити наступні види кіберзлочинів:

Фінансово-орієнтовані кіберзлочини. Не дивно, що багато кіберзлочинців використовують Інтернет з метою отримання комерційної вигоди, здійснюючи такі типи атак:

Фішинг. Кіберзлочинці люблять збирати фрукти, які низько висять, коли надається можливість заразити комп'ютери нічого жертв, які нічого не підозрюють. У подібних схемах улюбленим засобом зловмисників є електронна пошта. Суть методу полягає в примусі одержувача листа до переходу за посиланням від імені легітимної організації (банку, податкової служби, популярного інтернет магазину і т. д.). У подібних випадках метою, найчастіше, є оволодіння банківськими даними.

Кібервимагання. Ще один популярний метод фінансово-орієнтованого кіберкрімінала – вимагання. Як правило, спочатку у користувача або компанії, після завантаження шкідливого коду шифруються файли, а потім надходить пропозиція про відновлення в обмін на грошову винагороду (зазвичай у вигляді біткоїнів або іншої криптовалюти). Оскільки державні грошові знаки можна відстежити, а криптовалюту відстежити складно[82].

Фінансове шахрайство. Більшість витончених схем фінансового шахрайства пов'язано зі зломом комп'ютерних систем операторів роздрібної торгівлі з метою отримання банківських даних про покупців (так звані цільові атаки) або подальшими маніпуляціями отриманою інформацією.

[82] Marc D. Goodman and Susan W. Brenner. The emerging consensus on criminal conduct in cyberspace // Archive.org. 2018. URL: https://archive.org/details/TheEmergingConsensusOnCriminalConductInCyberspace

Деякі типи шахрайства, пов'язаного з фінансами, надзвичайно складно виявити[83].

Кіберзлочини, пов'язані з вторгненням в особисте життя. Існує кілька типів подібних кіберзлочинів, метою яких є крадіжка особистої конфіденційної інформації. Хоча найчастіше зловмисниками рухає глибша мотивація (наприклад, грошова або пов'язана зі зміною політичних настроїв), основна увага зосереджена на обході законів і пошуку проломів в технологіях, які захищають персональні конфіденційні відомості.

Крадіжка персональних даних. Крадіжка особистої інформації зазвичай відбувається з метою подальшої підміни особистості людини або групи людей. Хоча деякі зловмисники крадуть паспорта або інші посвідчення особи для фізичної підміни особистості, в основному крадіжка персональних даних відбувається виключно в Інтернеті. Наприклад, хтось, бажаючий отримати банківську позику, може вкрасти персональну інформацію людини з гарною кредитною історією[84].

Шпигунство. Метою шпигунства, починаючи від зломів персональних комп'ютерів або пристроїв і закінчуючи нелегальним масовим стеженням, є таємне відстеження особистого життя. Тут може бути як фізичнt шпигунство (наприклад, за допомогою веб-або CCTV-камер для спостереження за окремими персонами або групою людей), так і масовий моніторинг різного роду комунікацій (читання пошти, текстових повідомлень месенджерів, смс і так далі).

---

[83] Киберпреступления: понятие, виды и методы защиты // Sys-team-admin.ru. 2018. URL: https://sys-team-admin.ru/stati/bezopasnost/170-kiberprestupnost-ponyatie-vidy-i-metody-zashchity.html

[84] Williams P. Organized Crime and Cybercrime: Synergies, Trends, and Responses // Crime Research. 2018. URL: http://www.crime-research.org/library/Cybercrime.htm

Порушення авторських прав – одна з найбільш поширених форм кіберзлочинів. У першу чергу в цю категорію потрапляє оприлюднення в загальний доступ музики, фотографій, фільмів, книг і т. д. без згоди авторів[85].

Спам – надзвичайно поширений і різноманітний тип кіберзлочинів. Сюди входить масова розсилка по електронній пошті, смс, мессенджерам і іншим каналам комунікації. Будь-яку розсилку без згоди одержувачів можна віднести до спаму.

Соціальні та політично мотивовані кіберзлочини. Деякі типи кіберзлочинів спрямовані на зміни настроїв в політичному середовищі або нанесення навмисної шкоди або зниження впливу окремих особистостей або групи людей.

Злочини на ґрунті ненависті та домагання. Злочини на основі ненависті щодо особистості або групи людей зазвичай відбуваються на основі гендерної, расової, релігійної, національної приналежності сексуальної орієнтації та інших ознак. Приклади: домагання і розсилка образливих повідомлень і вкидання фальшивих новин, що стосуються певної групи осіб.

Кібербулінг. Використання комп'ютерів і підключених пристроїв для домагань, приниження і залякування осіб підпадає під категорію кібербулінгу. Кордон між кібербулінгом і деякими формами злочинів на грунті ненависті найчастіше розмитий. Деякі форми кібербулінгу (наприклад, оприлюднення оголених фотографій) можуть підпадати під незаконні дії (наприклад, експлуатація дітей)[86].

Протизаконна порнографія. Поширення порнографії через Інтернет у багатьох країнах трактується як кіберзлочини, в інших – відбувається лише заборона вмісту екстремістської спрямованості. Поширення зображень з дитячою порнографією заборонено в більшості країн.

---

[85] Гафнер В. В. Информационная безопасность: Учебное пособие. Рн/Д: Феникс, 2010. С. 182-183.

[86] Макаренко Є. А. Міжнародна інформаційна безпека: сучасні виклики та загрози. Київ: Центр вільної преси, 2006. С. 309-310.

Грумінг. Мережевий грумінг пов’язаний із сексуальними домаганнями до неповнолітніх. У процесі можуть використовуватися різні методи спілкування: смс, соціальні мережі, електронна пошта, чати (наприклад, в онлайн іграх) і форуми. У багатьох країнах грумінг підпадає під категорію кіберзлочинів.

Поширення наркотиків і зброї. Різні IT-рішення, що використовуються для поширення легітимних товарів і служб, можуть також використовуватися зловмисниками. Наприклад, ринки даркнета, існуючі у всесвітній павутині, допомагають контрабандистам продавати зброю і наркотики і в той же час залишатися поза увагою правоохоронних органів[87].

Проаналізувавши світові тенденції розвитку електронного тероризму, можна зробити висновок, що сьогодні складаються всі умови для прояву нового виду тероризму – кібертероризму.

Для того, щоб краще зрозуміти сутність цієї проблеми слід дати визначення поняттю «кібертерозм». Кібертероризм – дії спрямовані на дезорганізацію автоматизованих інформаційних систем, що створюють загрозу життю людей, заподіють значну матеріальну шкоду або призводять до інших суспільно небезпечних наслідків. Основна форма прояву – інформаційна атака на комп’ютерну інформацію, обчислювальні системи, апаратуру передачі даних; найбільш небезпечні атаки на об’єкти енергетики, телекомунікації, транспортні диспетчерські системи, фінансові та урядові інформаційні системи управління військами і стратегічною зброєю.

Слід відмітити, що екстремістські угрупування інтенсивно використовують сучасні технології для пропаганди своєї ідеології і ведення інформаційних війн. Цьому в переважній більшості випадків сприяють можливості глобальної мережі Інтернет. Всесвітня павутина приваблює терористичні групи не тільки легкістю доступу, відсутністю будь-якого

[87] Юдін О. К. Інформаційна безпека держави: навчальний посібник. Харків: Консум, 2005. С. 321-322.

урядового контролю і слабкою цензурою, але і наявністю великої потенційної аудиторії користувачів, а також анонімністю зв'язку, швидким і відносно дешевим поширенням інформації[88].

Також потрібно звернути увагу на те, що терористичні акції в кіберпросторі можуть здійснюватись не тільки окремими особами або групами, але і однією державою проти іншої. Спеціальні підрозділи для ведення мережевих атак, запровадження в комп'ютерні мережі противника комп'ютерних вірусів уже сформовані в низці держав. Кібертероризм має такі відмінні ознаки:

1) міжнародний характер, що полягає в тому, що злочинці і жертви можуть перебувати в різних державах;

2) високий рівень латентності і низький рівень розкриття;

3) відсутність великих фінансових витрат, при цьому наявність можливості нанесення величезного матеріального збитку;

4) відкритість, що виражається в залученні уваги громадськості.

Одним із напрямів удосконалення боротьби проти використання Інтернету в терористичних цілях може стати вивчення Україною досвіду інших держав по боротьбі з тероризмом в Інтернеті, як у далекому, так і в ближньому зарубіжжі[89].

Серед заходів, спрямованих на запобігання негативних наслідків, можна виділити технічні, організаційні і правові. До технічних можна віднести такі:

1) захист від несанкціонованого доступу до системи;

2) резервування особливо важливих комп'ютерних підсистем;

3) прийняття конструкційних заходів захисту від розкрадань, диверсій, вибухів;

---

[88] Боднар І. Міжнародна інформація: Навчально-методичний посібник для самостійного вивчення курсу. Львів: «Новий Світ-2000», 2005. С. 85-86.

[89] Карпенко В. О. Інформаційна політика та безпека: Підручник. Київ: Нора-Друк, 2006. С. 190-191.

4) установка резервних систем електроживлення.

Сьогодні вже розпочато роботу зі створення нового міжнародно-правового режиму, об'єктом якого повинні стати інформація, інформаційні технології і методи їх використання. Основу для міжнародного співробітництва в цій сфері заклала прийнята резолюція ГА ООН «Досягнення у сфері інформатизації та телекомунікації в контексті міжнародної безпеки»[90]. Ця резолюція переводить загальнополітичні обговорення проблем інформаційної безпеки в площину пошуку практичних рішень, запускає механізм формування Групи урядових експертів ООН з міжнародних проблем інформаційної безпеки.

Таким чином, в рамках кіберзлочинності можна виділити окремий її вид – кібертероризм. Сучасні злочинці-терористи використовують всі можливі засоби і способи, в тому числі всі інформаційні і комп'ютерні технології для досягнення злочинного результату. Крім того, з кожним роком професіоналізм використання інформаційних мереж терористами зростає. Кібербезпека стала проблемою державної ваги.

[90] Резолюция 60/45, принятая Генеральной Ассамблеей Организации Объединенных Наций, «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» // eSubscription to United Nations Documents. URL: https://undocs.org/pdf?symbol=ru/A/RES/73/27

РОЗДІЛ 2.
КІБЕРНЕБЕЗПЕКА І КІБЕРЗАГРОЗИ В СТРАТЕГІЯХ НАЦІОНАЛЬНОЇ БЕЗПЕКИ СУЧАСНИХ ДЕРЖАВ

2.1. Стратегія національної кібербезпеки США «Про основні кіберзагрози»

Законодавство низки зарубіжних країн передбачає сувору кримінальну відповідальність за кіберзлочини. Наприклад, відповідно до положень Закону США про шахрайство і зловживання з використанням комп'ютерів (Computer Fraud and Abuse Act)[91] особі, будучи засудженій за кіберзлочини, але яка повторно вчинила несанкціонований доступ до комп'ютера, що спричинило тяжкі наслідки, може бути призначено тюремне ув'язнення терміном до 20 років.

Зазначимо, що США історично стали однією з перших країн, котрі почали розглядати кібербезпеку як питання стратегічного значення. Основні положення стратегії кібербезпеки США сформовані протягом 1990-х рр. Адміністрація президента Білла Клінтона в 1995 р. оприлюднила Стратегію національної безпеки[92], в якій позначено завдання щодо досягнення інформаційної переваги шляхом наступальних та оборонних інформаційних операцій.

Директива Президента № 63 «Про захист критичної інфраструктури», подальший розвиток отримала у формі кодифікації у «Національній стратегії безпеки кіберпростору»[93] та у Директиві Президента в галузі національної безпеки №7 «Про визначення, пріоритизацію та захист критично важливих

---

[91] Computer Fraud and Abuse Act // The Free Encyclopedia Wikipedia.URL: https://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act

[92] A National Security Strategy of Engagement and Enlargement // The Historical Office of the Office of the Secretary of Defense. 1995. URL: https://history.defense.gov/Portals/70/Documents/nss/nss1995.pdf?ver=pzgo9pkDsWmIQqTYTC6O-Q%3d%3d

[93] The National Strategy to Secure Cyber Space // The White House. 2003. URL: http://georgewbush-whitehouse.archives.gov/pcipb/

елементів інфраструктури»[94]. У цих документах визначено основні принципи та завдання забезпечення кібербезпеки:

- запобігання кібератакам проти критичних інфраструктур;
- ліквідація вразливостей критичних інфраструктур;
- мінімізація потенційної шкоди у разі успішної кібератаки.

Також позначено можливість застосування США кіберзброї як оборонний захід.

У 2008 р. створено «Комплексну національну ініціативу кібербезпеки». Ця ініціатива передбачала вирішення низки завдань забезпечення кібербезпеки США: 1) захист національних баз даних від атак потенційних супротивників; 2) забезпечення поінформованості фахівців федерального уряду про наявність уразливостей та загрози безпеці в національних комп'ютерних мережах та критичних інфраструктурах; 3) розширення технічних та оперативних можливостей контррозвідувальних органів США; 4) створення системи підготовки фахівців у сфері кібербезпеки.

У 2017 р. підрозділ кіберкомандування ЗС США перетворено на підрозділ стратегічного командування[95]. Пентагон надав кіберкомандуванню США можливість застосовувати більш жорсткий підхід щодо захисту від хакерських атак, а й вторгнень у кіберпростору інших держав. Відомству надано повноваження щодо нанесення превентивних кібератак на цифрові інфраструктури супротивників. При цьому дії із захисту США від кібератак повинні переважно відбуватися в кіберпросторі супротивника. Прикладом реалізації превентивного підходу у забезпеченні кібербезпеки є ініціатива

---

[94] Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection. // U.S. Department of Homeland Security. 2003. 17 of December. URL: https://www.dhs.gov/homeland-security-presidential-directive-7

[95] Пентагон изменил стратегию киберкомандования США // News.com. 2018. URL: https://www.newsru.com/world/18jun2018/cyber.html

кіберкомандування США щодо запровадження шкідливого програмного забезпечення у кіберпростір противника[96].

У вересні 2018 р. президент Дональд Трамп підписав Національну кіберстратегію США[97]. При цьому документ 2018 р. багато в чому повторює попередні документи США в галузі кібербезпеки. Національна кіберстратегія виділяє активних противників США, які здійснюють свою діяльність у кіберпросторі. Зокрема, зазначається, що РФ, Іран, Північна Корея та КНР роблять кібератаки, які завдають збитків американській та міжнародній економіці, а також здійснюють акти економічного шпигунства за США та їх союзниками. Стратегія національної кібербезпеки складається з IV частин, кожній з яких відповідає певний напрямок політики США: I) Захист американського народу, Америки та американського способу життя; II) Забезпечення процвітання Америки; III) Збереження миру шляхом примусу; IV) Просування американського впливу.

У I частині «Захист американського народу, Америки та американського способу життя» позначена мета – забезпечення належного управління ризиками в галузі кібербезпеки, підвищення безпеки та захищеності інформаційних систем та інформації, що має державну важливість.

Реалізація мети першої частини, відбувається шляхом захисту федеральних мереж та інформації, захисту критично важливої інфраструктури, боротьби з кіберзлочинністю та поліпшення звітності про інциденти, що включає надання департаменту внутрішньої безпеки ширших повноважень контролю за цивільними зусиллями в галузі кібербезпеки, співробітництво з іншими країнами в цілях боротьби з кіберзлочинністю.

---

[96] U.S. Cyber Command's Malware Inoculation: Linking Offense and Defense in Cyberspace // Council of foreign relation. 2020. URL: https://www.cfr.org/blog/us-cyber-commands-malware-inoculation-linking-offense-and-defense-cyberspace

[97] National Cyber Strategy of the United States of America // The White House. 2018. URL: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

Наведені в документі загрози кібербезпеки США можуть бути структуровані таким чином: 1) порушення функціонування мереж федеральних департаментів та агентств; 2) неналежна якість IT товарів та послуг у системі федеральної системі постачання США; 3) ненадійність федеральних підрядників, які мають доступ до державної таємниці; 4) використання державними установами застарілих IT продуктів або стандартів; 5) дестабілізація критичної інфраструктури; 6) кібератаки на виборчу інфраструктуру, транспортну, морську та космічну інфраструктуру.

II частина Національної стратегії кібербезпеки США – «Забезпечення процвітання Америки» ставить за мету зберегти вплив США у технологічній екосистемі та розвивати кіберпростір як двигун економічного зростання, інновацій та ефективності.

Реалізація мети другої частини стратегії передбачає:

1) розвиток життєздатної та ефективної цифрової економіки;

2) заохочення та захист винахідливості США;

3) створення кваліфікованого кадрового резерву;

4) співпраця з IT компаніями для тестування кібербезпеки в нових продуктах;

5) залучення та утримання висококваліфікованих кадрів з кібербезпеки. При цьому в другій частині кіберстратегії представлено низку заходів щодо забезпечення кібербезпеки США та міжнародної безпеки, серед яких:

- створення єдиних міжнародних стандартів кібербезпеки;
- створення стандартів кібербезпеки цифрової інфраструктури наступного покоління;
- економічна та політична підтримка IT продуктів у сфері кібербезпеки американського виробництва;
- посилення контррозвідувальних заходів у галузі IT технологій;
- фінансування програм шкільної та університетської IT освіти.

У III частині «Збереження миру шляхом примусу» визначено мету – виявляти, протидіяти, припиняти, послаблювати інтенсивність і стримувати дії в кіберпросторі, які дестабілізують і суперечать національним інтересам, зберігаючи при цьому перевагу США в кіберпросторі та за допомогою нього.

Здійснення цієї мети передбачається у вигляді створення норм відповідальної поведінки країн і стримування неприпустимої поведінки у кіберпросторі. У стратегії йдеться, що адміністрація використовуватиме всі інструменти національної влади для запобігання кібератакам і буде здійснювати швидкі та ефективні дії проти зловмисників.

IV частина «Просування американського впливу» має на меті зберегти довгострокову відкритість, функціональну сумісність, безпеку та надійність Інтернету, який підтримується та посилюється інтересами США.

Здійснення мети четвертої частини стратегії передбачає: просування відкритого, міжнародного, надійного та безпечного Інтернету; нарощування міжнародного кібер-потенціалу; спільну протидію загрозам, спрямованим на взаємні інтереси.

16 листопада 2018 р. президент Д. Трамп підписав закон «Про Агентство кібербезпеки та захисту інфраструктури»[98] від 2018 р. Цей закон посилює роль колишнього Національного управління захисту програм і перетворює його в агентство кібербезпеки та захисту інфраструктури. Управлінню надаються повноваження щодо створення національного потенціалу для захисту від кібератак та взаємодії з федеральним урядом щодо надання інструментів кібербезпеки, служб реагування на інциденти та можливостей оцінки для захисту державних мереж.

Військово-політичне керівництво США вважає, що різного роду кібератаки стають невід'ємною частиною сучасних збройних конфліктів, кіберпідрозділи функціонуючі в лавах збройних сил США або як окремі

[98] Cybersecurity and Infrastructure Security Agency Act of 2018 // The White House. URL: https://www.congress.gov/bill/115th-congress/house-bill/3359

відомства, володіють повноваженнями до проведення кібератак на віртуальний простір противника або до проведення заходів по всьому світу, про що свідчить витік з боку співробітника компанії-підрядника агентства національної безпеки Е. Сноудена, про діяльність агентства зі збору даних та стеження за мережевою та комунікаційною активністю не лише громадян США, а й у глобальному масштабі, включаючи особисті комунікації лідерів держав.

Таким чином, політика США в галузі кіберпростору та кібербезпеки, в першу чергу, спрямована на досягнення інформаційної переваги. Поряд із завданнями забезпечення безпеки кіберпростору, у розглянутих нормативних документах позначено політичні цілі та перераховано основні противники США у кіберпросторі – РФ, КНР, Іран, КНДР та міжнародні терористичні організації. Вказано, що перелічені актори використовують кіберпростір у військових та політичних цілях, регулярно проводять кібератаки спрямовані проти США та їх союзників, не наводячи якихось суттєвих доказів. Загалом Нові Стратегії кібербезпеки спрямовані на зміцнення могутності, посилення впливу та просування інтересів США на міжнародній арені.

2.2. Державні програми і стратегії КНР про загрози і виклики в сфері кібербезпеки

Відмінною рисою китайського Інтернету є регламентація поведінки користувачів у мережі, користувачі мають цілу низку обов’язків та обмежень, пов’язаних з використанням Інтернету. Кіберпростору, на сучасному етапі розвитку КНР, відведено особливу роль у зміцненні міжнародного становища Китаю.

Особливе місце у забезпеченні кібербезпеки належить Військовій раді ЦК КПК та Військовій раді при Держраді КНР. Структуру Держради КНР складають: профільні міністерства, зокрема Міністерство індустрії та інформаційних технологій, Міністерство науки і технологій КНР,

Міністерство державної безпеки, зокрема одинадцяте бюро міністерства державної безпеки КНР, яке відповідає за радіоелектронну розвідку та комп'ютерну безпеку; провідні малі групи, що спеціалізуються на важливих стратегічних питаннях, зокрема Центральна мала робоча група із зовнішньої політики, Ведуча мала група з питань національної безпеки та Ведуча мала група з проблем Тайваню.

У 2000 р. у КНР була спроба класифікації ймовірних правопорушень в інформаційній сфері, результатом якої стала «Постанова Всекитайських зборів народних представників із захисту Інтернет простору», де були виділені сфери, в яких можливі порушення: економічна, освітня, сфера підтримки суспільної стабільності та захисту громадян[99]. У 2002 р. була сформована та опублікована оборонна політика КНР, в якій наголошувалося на модернізації збройних сил КНР, зокрема їх інформатизації[100].

З 2004 р. в КНР розпочато реалізацію державної програми «Золотий щит», суть якої полягає у фільтрації Інтернет трафіку між китайським кіберпростором та рештою світу. Фактично, програма «Золотий щит» є спробою китайського уряду здійснити тотальний контроль за кіберпростором, з метою обмеження доступу китайських громадян до зарубіжних Інтернет-ресурсів, ЗМК та соціальних мереж[101].

У 2006 р. було прийнято «Державну стратегію розвитку інформатизації на період з 2006 по 2020 р.» У цьому документі робиться наголос на високій важливості контролю інформаційних технологій та передбачається: створити спеціальні структури регулювання процесів в інформаційному середовищі; встановити вектор розвитку інформаційних технологій та державної політики

---

[99] Разумов Е.А. Политика КНР по обеспечению кибербезопасности // Россия и АТР. 2017. № 4 (98). С. 158. URL: https://cyberleninka.ru/article/n/politika-knr-po-obespecheniyu-kiberbezopasnosti

[100] Национальная оборона Китая в 2002 году // Информационное бюро Государственного совета Народной Республики Китай. 2002. URL: http://www.scio.gov.cn/zfbps/ndhf/2002/Document/307925/307925

[101] Ventre D. Chinese Cybersecurity and Defense. London // Wiley-ISTE Publ., 2014. P. 228.

у цій галузі; створити власне програмне забезпечення, а також поєднання встановлення військової та цивільної продукції[102].

Ідея суверенної кібербезпеки подальший розвиток отримала у положеннях нового Закону про національну безпеку, прийнятого в КНР у 2015 р., наголошено на необхідності зміцнення захисту національних інформаційних систем та встановлення суверенітету кіберпростору в КНР. Ці питання докладніше розглядаються в Законі про кібербезпеку, який передбачає обов'язкову реєстрацію в Інтернет-сервісах під справжніми іменами, залучення приватних операторів до участі в урядових розслідуваннях, запровадження багатьох зобов'язань щодо зберігання персональних даних у Китаї, які повинні зберігатися тільки в країні[103].

Закон про кібербезпеку КНР прийнятий 06.11.2016 р. і введений в дію 1.07.2017 р. Закон встановлює загальні положення в області кібербезпеки, підтримку і просування кібербезпеки, забезпечення функціонування інформаційно-комунікаційних мереж, забезпечення інформації в інформаційно-комунікаційних мережах, моніторинг, раннє виявлення та дії в відповідь на надзвичайні обставини, законодавчо встановлена відповідальність у сфері кібербезпеки[104].

Частина змісту закону повторює існуючі правила, ухвалені КНР протягом багатьох років і просто поєднує окремі нормативні акти в один. Раніше існуючі правила були розкидані за різними нормативними актами. Уряд КНР, при прийнятті цього закону, багато в чому керувався положенням, що формування єдиного закону покращує ефективність правового регулювання кіберпростору, більшою мірою інформує бізнес-спільноту, а

---

[102] Разумов Е.А. Политика КНР по обеспечению кибербезопасности. С. 159. URL: https://cyberleninka.ru/article/n/politika-knr-po-obespecheniyu-kiberbezopasnosti

[103] Yan S. China's new cybersecurity law takes effect today, and many are confused // CNBC. 2017. URL: https://www.cnbc.com/2017/05/31/chinas-new-cybersecurity-law-takes-effect-today.html

[104] The Cybersecurity Law of the People's Republic of China // New America. URL: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecuritylaw-peoples-republic-china/

також широку громадськість про безпрецедентні загрози кібербезпеці в межах та за межами Китаю[105].

У Законі дається визначення низки термінів, що належать до сфери кібербезпеки. Відповідно до Ст. 76, кібербезпека належить до вжиття необхідних заходів для запобігання кібератакам, вторгненням, перешкодам, знищенню та незаконному використанню з метою забезпечення стабільного, надійного функціонування та конфіденційного функціонування мережі. Мережі розглядаються тут як системи, що складаються з комп'ютерів та інших інформаційних пристроїв або об'єктів, що використовуються для збору, збереження, передачі, обміну та обробки інформації. Особиста інформація належить до всіх видів інформації, записаної в електронному вигляді або за допомогою інших засобів, взятої поодинці або разом з іншою інформацією, достатньою для ідентифікації фізичної особи: повні імена, дати народження, національні ідентифікаційні номери, особиста біометрична інформація, адреси, номери телефонів[106].

У Ст. 31 Закону про кібербезпеку КНР йдеться, що держава має зосередитись на питаннях захисту критичної інформаційної, інфраструктури у сферах зв'язку з громадськістю, надання інформаційних послуг, енергетики, транспорту, водного господарства, фінансів, державні послуги, електронного уряду та інших ключових елементів інформаційної інфраструктури, порушення функціонування якої спричинить втрату національної безпеки, національної економіки та поставить під загрозу життю громадян[107].

Оператори критичної інформаційної інфраструктури повинні зберігати ключові дані та персональну інформацію на території КНР. У випадках, коли

---

[105] Lindsay J. R. The Impact of China on Cybersecurity // International Security. 2015. Vol. 39. P. 153. URL: https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=2849&context=lawreview

[106] Рогожин А.А. КНР – Закон о кибербезопасности принят. URL: https://www.imemo.ru/news/events/text/knr-zakon-o-kiberbezopasnosti-prinyat.

[107] Там само.

необхідно надавати інформацію зовнішнім агентам, оцінка безпеки проводиться відповідно до заходів, сформульованих національним органом управління кіберпростором спільно з відповідними департаментами Державної Ради. На операторів мереж покладаються юридичні зобов'язання у межах цього закону[108].

Закон також встановлює основний принцип заохочення та захист національного суверенітету у кіберпросторі в рамках мереж. Перелік додаткових зобов'язань для операторів мереж включає: 1) дотримання вимог багаторівневої системи захисту кібербезпеки; 2) автентифікацію реальної особи користувачів; 3) розробку стратегій дії у надзвичайних ситуаціях у галузі кібербезпеки; 4) надання допомоги та підтримки слідчим органам.

Також закон регламентує діяльність Інтернет ЗМІ та соціальних мереж. Весь вироблений у мережі контент зберігається на території КНР протягом 6 місяців. Особлива увага в законі приділяється системі ідентифікації: для здійснення будь-якої діяльності в мережі громадянам КНР необхідно підтвердити свою особу та пройти відповідну процедуру верифікації, іншими словами закон забороняє Інтернет анонімність[109].

Таким чином, Закон про кібербезпеку з одного боку захищає об'єкти критичної інформаційної інфраструктури КНР від кіберзагроз, пов'язаних з крадіжкою персональних даних та застерігає від кібершпигунства, а з іншого боку, надає спеціальним службам КНР можливість фізичного доступу до даних об'єктів критичної інформаційної інфраструктури. Незважаючи на те, що у Законі використовується поняття «загроза кібербезпеки», кіберзагрози головним чином розглядаються в рамках критичної інформаційної інфраструктури та інформаційних мереж, і представлені досить загальними

---

[108] Там само.

[109] Разумов Е.А. Политика КНР по обеспечению кибербезопасности. С. 159. URL: https://cyberleninka.ru/article/n/politika-knr-po-obespecheniyu-kiberbezopasnosti

визначеннями, такими як крадіжка персональних даних, порушення функціонування тощо.

Докладніше, кіберзагрози представлені у кримінальному законодавстві КНР. Відповідно до кримінального законодавства КНР кіберзлочини в основному розглядаються в розділі: «Злочини, пов'язані з порушенням громадського порядку». Ст. 285, 286 та 287 є основними статтями, які безпосередньо стосуються кіберзлочинів. Крадіжка або інше придбання особистої інформації громадян розглядається як «злочин порушення особистої інформації громадянина», передбачений у Ст. 253.

Відповідно до Ст. 285 Кримінального кодексу діяльність, пов’язана з вторгненням у комп’ютерну інформаційну систему в галузі державних справ, національної оборони або передової науки і техніки, кваліфікується як «злочин, який полягає у вторгненні до комп’ютерної інформаційної системи». Що ж до діяльності з вторгнення в комп’ютерну інформаційну систему, вона може бути «злочин, пов’язаний з отриманням даних із комп’ютерної інформаційної системи та управлінням комп’ютерною інформаційною системою».

Відповідно до Ст. 286 Кримінального кодексу, відмова в обслуговуванні може кваліфікуватися як «злочин, пов’язаний з підривом комп’ютерної інформаційної системи», і в особливо тяжких випадках може передбачатися позбавлення волі на строк понад п’ять років. Умисне створення та розповсюдження комп’ютерних вірусів та інших програм деструктивного характеру, що впливають на нормальне функціонування комп’ютерних систем, розглядається відповідно до частини першої Ст. 286. Незважаючи на те, що в даному документі немає спеціальної термінології, наведена класифікація кіберзлочинів досить повно відображає сутність кіберзагроз.

Окремо варто висвітлити питання місця та ролі НВАК у структурі забезпечення кібербезпеки КНР. У структурі військового апарату КНР варто

виділити третій департамент. До його повноважень входить: 1) розвідувальна діяльність; 2) пошук уразливостей інформаційних мереж; 3) розробка сценаріїв та опрацювання дій кібервійськ щодо проведення кібератак на об'єкти цифрової інфраструктури супротивника. Згідно зі звітом американських експертів, чисельність кібервійськ КНР становить 30 тис. людей. У доповіді також наголошується, що КНР регулярно проводить кібератаки на об'єкти США, переважно з розвідувальною метою. Крім того, в деяких ЗМІ було опубліковано інформацію про причетність військових хакерів з КНР до кібератак на інші країни, зокрема у 2019 р., було викрадено дані японських IT компаній[110].

Кіберпростір активно використовується НВАК для проведення кібератак на об'єкти цифрової інфраструктури супротивника, насамперед з метою завдання збитків або збору розвідданих. Також НВАК взаємодіє з комерційними та освітніми організаціями, що забезпечує доступ НВАК до передових інформаційних досліджень та технологій, у тому числі до засобів військового призначення. Варто зазначити, що кібервійська КНР на даний момент об'єктивно можуть вважатися одними з найбільш боєздатних у світі і становлять небезпеку не тільки для прямих військових супротивників КНР, але й для політичних та економічних суперників, а також технологічних компаній та організацій.

У звітах та доповідях органів різних держав КНР, як правило, з великим відривом посідає перше місце у списку країн, які здійснюють хакерські атаки та акти кібершпигунства. Керівництво Китаю побоюється у разі масштабної кібератаки втратити контроль над вузловими точками інформаційної інфраструктури, чим можуть скористатися дискредитації країни зовнішні сили.

---

[110] Китай устроил кибератаку на компании из США и Японии // РБК. 2015-2020. URL: https://quote.rbc.ru/news/article/5ae098a62ae5961b67a1c1d1

Таким чином, кіберпростір у КНР розглядається як специфічне інформаційне середовище, яке схильне до значної автономії, і в рамках якого відбувається формування сучасної КНР. При цьому уряд КНР не тільки контролює кіберпростір країни, але й підтримує та задає вектор розвитку інформаційних технологій, а також використовує кіберпростір для інформаційного впливу та контролю населення КНР. Кібербезпека в КНР забезпечується дуже жорсткими, але ефективними та багато в чому безпрецедентними заходами, при цьому розглянуті кіберзагрози в нормативно-правових актах КНР, багато в чому пов'язані з протидією інформаційному впливу іноземних держав та забезпеченню безпеки та працездатності критичної інформаційної інфраструктури.

2.3. Державні стратегії кібербезпеки держав ЄС про основні загрози в кіберпросторі

Щодо протидії кіберзагрозам серед країн ЄС можна виділити низку держав, які досягли у цій галузі значних успіхів: Австрія, Франція, Норвегія, ФРН, Швеція[111]. З огляду на транснаціональний характер кіберзлочинності з одного боку і високий рівень взаємозалежності країн ЄС з іншого, компетентні органи держав-членів ЄС дотримуються єдиних стандартів при проведенні політики кібербезпеки. Варто висвітлити основні документи та стандарти ЄС у сфері кібербезпеки[112].

У 2001 р. було підписано Конвенцію РЄ «Про кіберзлочинність»[113], яка й досі є одним із основних документів, що регулюють правовідносини у сфері глобальної інформаційної мережі щодо запобігання та контролю

---

[111] Global Cybersecurity Index (GCI) // International Telecommunication Union. 2018. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

[112] Кардава Н.В. Политика обеспечения кибербезопасности в европейском союзе: национальный и наднациональный уровни // Каспийский регион: политика, экономика, культура, 2019. № 3(60). С. 74-76.

[113] Convention on Cybercrime // Council of Europe: official web-site. 2001. URL: http:// conventions.coe.int./Treaty/en/Treaties/Html/185.htm

злочинності, пов'язаної із застосуванням комп'ютерів. У Конвенції є визначення кіберзлочинів, висвітлюються питання взаємодії країн-членів РЄ у сфері забезпечення кібербезпеки. У 2004 р. створено ENISA, яке координує діяльність країн союзу для боротьби з кіберзагрозами[114]. Стратегія кібербезпеки ЄС, прийнята у 2013 р., містить такі положення:

1. Стратегія пропонує розширення співпраці між державними органами та приватним сектором для протидії транскордонним кіберзагрозам та координування дій у надзвичайних ситуаціях.

2. Стратегія закликає держави-члени ратифікувати Будапештську конвенцію РЄ про кіберзлочинність і якнайшвидше здійснити її положення.

3. З метою підвищення стійкості кібербезпеки інформаційних систем, в галузі оборони та національної безпеки, пропонується розвиток потенціалу кібербезпеки в галузі виявлення, реагування та протидії кіберзагрозам.

4. Розробка основ політики ЄС у сфері кібербезпеки, зокрема опрацювання навчальних курсів з кібербезпеки та координація діяльності між міжнародними партнерами, включаючи НАТО[115].

Також, у 2013 р. для посилення протидії кіберзлочинності в ЄС засновано Європейський центр кіберзлочинності, основні напрямки діяльності якого:

1. Центр служить центральним вузлом інформації та розвідки.

2. Центр підтримує операції та розслідування з боку держав-членів, пропонуючи оперативний аналіз, координацію та значний досвід.

3. Центр надає різні продукти стратегічного аналізу, які дозволяють приймати обґрунтовані рішення на тактичному та стратегічному рівнях боротьби з кіберзлочинністю та її попередження.

---

[114] Кардава Н.В. Политика обеспечения кибербезопасности в европейском союзе: национальный и наднациональный уровни. С. 75.

[115] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace // European Union: official web-site. 2013. URL: http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

4. Центр забезпечує комплексну інформаційно-пропагандистську функцію, що пов'язує правоохоронні органи, які займаються боротьбою з кіберзлочинністю, приватним сектором, науковими колами та іншими партнерами, не повєязаними з правоохоронними органами.

5. Центр підтримує навчання та нарощування потенціалу, зокрема, для відповідних органів у державах-членах.

6. Центр надає вузькоспеціалізовані можливості технічної та цифрової судової підтримки розслідуванням та операціям.

7. Центр представляє правоохоронне співтовариство ЄС у галузях, що становлять спільний інтерес (вимоги до досліджень та розробок, управління Інтернетом та розробка політики)[116].

У 2016 р. було узгоджено Директиву ЄС «Про безпеку мережевих та інформаційних мереж»[117], згідно з якою держави-учасниці повинні гарантувати наявність національних систем кібербезпеки, що включають:

1. Стратегії в галузі інформаційної безпеки, а також відповідну політику та регулятивні заходи, спрямовані на підтримку високого рівня безпеки мереж та інформаційних систем.

2. Національні уповноважені органи для моніторингу реалізації директиви на території певної держави та допомоги з її послідовної реалізації.

3. Єдиного каналу взаємодії з питань безпеки мереж та інформаційних систем між державами-учасницями, групою взаємодії та мережею груп реагування на інциденти, пов'язані з комп'ютерною безпекою.

4. Однією або кількох груп, які відповідають за управління ризиками та інцидентами.

---

[116] European Cybercrime Centre – EC3 // Europol: official web-site. URL: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

[117] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union // Official Journal of the European Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

Також у ЄС прийнято загальний регламент захисту персональних даних (GDPR) – генеральний регламент про захист персональних даних, прийнятий для уніфікації та посилення персональних даних громадян держав ЄС[118]. GDPR є документом, що складається з 99 статей, де детально розглядаються різні аспекти захисту персональних даних. Регламент існує як основа для національних стратегій держав ЄС.

ЄС активно співпрацює з НАТО, тому з 2008 р. в Естонії функціонує Центр передового досвіду НАТО з кібероборони – Міжнародна військова організація, яка зосереджує свої зусилля на розширенні можливостей кібернетичної оборони НАТО та країн-партнерів. НАТО офіційно визнало кіберпростір операційним середовищем і, таким чином, прирівнювало загрози до військових загроз. А, у 2017 р. у Таллінні було створено Об'єднаний центр передових технологій з кібероборони НАТО. Центр отримав акредитацію НАТО, налічує 20 учасників – 17 членів НАТО та три держави-партнери. Основне завдання Центру – тренування фахівців з різних країн, які забезпечують безпеку у національному кіберпросторі[119].

Варто зазначити, що зважаючи на відмінності соціального, технічного та економічного рівня розвитку, не всі країни ЄС здатні повною мірою забезпечити відповідність національних кіберстратегій директивам та рекомендаціям ЄС.

Стратегію кібербезпеки ФРН[120] прийнято у 2011 р., основну увагу у Стратегії ФРН приділено запобіганню кібератакам, кримінальному переслідуванню кіберзлочинів, а також попередженню виходу з ладу

---

[118] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 // Official Journal of the European Union. URL: http://data.europa.eu/eli/reg/2016/679/oj

[119] Ковалев А. А. Международно-правовые аспекты политики кибербезопасности некоторых европейских стран бывшего советского блока // Вестник ПАГС. 2018. №5. С. 108. URL: https://cyberleninka.ru/article/n/mezhdunarodno-pravovye-aspekty-politiki-kiberbezopasnosti-nekotoryh-evropeyskih-stran-byvshego-sovetskogo-bloka

[120] Cyber Security Strategy for Germany // Federal Ministry of the Interior. 2011. URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-for-germany

фізичної складової інформаційних систем. Відповідно до стратегії ФРН, кібербезпека – це бажаний стан кібербезпеки, при якій ризики, що виходять з кіберпростору, зведені до прийнятного мінімуму. Кібербезпека у ФРН поділяється на цивільну та військову, де перша фокусується на всіх ІТ системах для цивільного використання у кіберпросторі ФРН, а друга фокусується на всіх ІТ системах для військового використання у німецькому кіберпросторі. Незважаючи на поділ кібербезпеки на військову та цивільну в документі наведено лише основні загрози та виклики, що виходять з кіберпростору, без поділу на військові та цивільні, це: 1) атаки на критичну інформаційну інфраструктуру; 2) кібертероризм; 3) кібершпигунство; 4) використання кіберпростору у військових цілях; 5) вразливість нових інформаційних технологій; 6) атаки на промислові інфраструктури, що не належать до критичних.

Також, у Стратегії кібербезпеки ФРН наголошується на важливості підтримки державою стабільності та доступності кіберпростору для громадян ФРН, особливо для економічного сектора, при цьому перешкода використанню кіберпростору, визнається неприпустимою. У розділі, що регламентує кримінальне покарання осіб, які вчиняють злочини в кіберпросторі, зазначено, що транснаціональний характер кіберзлочинності вимагає тісної співпраці між правоохоронними органами різних країн, а також дотримання міжнародних норм, правил та стандартів.

У 2016 р. парламентом ФРН було прийнято Закон про кібербезпеку, який доповнює видану раніше стратегію кібербезпеки. Закон торкається питань забезпечення безпеки критичної інформаційної інфраструктури, зокрема, згідно із законом, постачальники інформаційних послуг зобов’язані протягом 2-х років запровадити нові стандарти безпеки у кіберпросторі. Розглядається можливість впровадження в критичні інформаційні інфраструктури нових технологій кібербезпеки, зокрема, нові стандарти шифрування та ідентифікації користувачів.

У 2016-2017 у ФРН було створено командування кібер та інформаційного простору, що є окремим компонентом Бундесверу. Відмінною особливістю німецького кіберкомандування є його широкий функціонал, крім проведення кібероперацій, воно займається захистом інформації, радіоелектронною боротьбою, картографією, розвідкою та зв'язком[121].

Національна стратегія кібербезпеки Австрії використовує більш широку концепцію безпеки ІКТ і розглядає кібербезпеку як захист систем ІКТ за допомогою конституційних засобів від пов'язаних із суб'єктом, технічних, організаційних та природних небезпек, що становлять ризик для безпеки кіберпростору, включаючи інфраструктуру та безпеку даних, а також безпеку в кіберпросторі[122]. Стратегія безпеки ІКТ є ініціативною концепцією, спрямованою на захист кіберпростору та людей у цьому віртуальному просторі з урахуванням їх основних прав та свобод. Конкретний підхід країни до кібербезпеки тісно пов'язаний з існуючими в ній найбільш зацікавленими сторонами та структурами – різними організаціями, установами чи окремими особами[123].

У порівнянні з розглянутими раніше стратегіями кібербезпеки, в Австрійській стратегії наведено одну з найповніших класифікацій кіберзагроз. Відповідно до матриці кібер-ризиків, кіберзагрози умовно можна розділити на IV групи: малоймовірні та безпечні; малоймовірні та небезпечні; можливі та безпечні; можливі та небезпечні[124].

---

[121] Кибервойска Европы и НАТО // РСДМ. URL: https://russiancouncil.ru/analytics-and-comments/analytics/kibervoyska-evropy-i-nato/

[122] Austrian Cyber Security Strategy // ENISA: official web-site. 2013. URL:: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/austrian-cyber-security-strategy

[123] Кардава Н.В. Политика обеспечения кибербезопасности в европейском союзе: национальный и наднациональный уровни //Каспийский регион: политика, экономика, культура. 2019. № 3(60). С. 74.

[124] Там само.

До малоймовірних і безпечних належить маніпуляція сигналом часу GPS, оскільки, з одного боку на громадському рівні дана кіберзагроза з великою ймовірністю не спричинить фатальних наслідків, а з іншого боку, на рівні критичної інформаційної інфраструктури, дані системи дублюються.

Малоймовірні та небезпечні кіберзагрози: 1) технічний збій або злом системи цифрового підпису; 2) використання даних персональної ідентифікації громадян, розподілені атаки на кшталт «відмова в обслуговуванні»; 3) неправомірний доступ до системи контролю водопостачання; 4) неправомірний доступ до системи контролю подачі електроенергії та постачання ІТ – послуг; 5) непрофесійні та недбалі дії співробітників критичної інформаційної інфраструктури; 6) отримання неправомірного доступу до супутникового та цифрового зв'язку; 7) отримання неправомірного доступу до фінансових операцій; 8) захоплення контролю за критичною інформаційною інфраструктурою. Найбільш ймовірними джерелами даного типу кіберзагроз, є: техногенні катастрофи, природні вразливості інформаційних інфраструктур (наприклад, людський фактор), кібертероризм та кібервійна[125].

Імовірні та безпечні кіберзагрози: систематична крадіжка персональних даних, соціальна інженерія, відсутність або старіння правової основи регулювання кіберзлочинів, непоінформованість громадян про стандарти безпеки, відсутність або неповне управління безперервністю бізнесу, маніпуляція та шантаж громадян через соціальні мережі, відсутність аудиту. Найбільш ймовірними джерелами даного типу кіберзагроз є: кіберзлочинність і технічні дефекти або вразливості ІТ систем[126].

Імовірні та небезпечні кіберзагрози: неправомірний доступ до промислових автоматичних систем управління, неправомірний доступ до

---

[125] Austrian Cyber Security Strategy. URL:: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/austrian-cyber-security-strategy

[126] Там само.

хмарних сховищ даних, неправомірний фізичний доступ до ІТ систем при їх транспортуванні, недостатність фінансування сфери кібербезпеки, відсутність фахівців кібербезпеки, відсутність або неясність відповідальності або низькоякісні ІТ продукти, кібершпигунство, невідомі ІТ загрози. Найбільш ймовірними джерелами даного типу кіберзагроз, є: кіберзлочинність, кібертероризм та кібервійна.

Ще однією країною ЄС, що займає лідируючі позиції у глобальному індексі кібербезпеки, є Швеція. Високий рівень кібербезпеки у Швеції багато в чому зумовлений високим рівнем економічного та соціального розвитку країни. У Стратегії кібербезпеки Швеції[127], яка була прийнята у 2016 р., під кібербезпекою розуміється комплекс заходів безпеки, спрямованих на збереження конфіденційності, достовірності та доступності інформації[128].

Кіберзагрози у Стратегії кібербезпеки Швеції, представлені у більш загальному вигляді, порівняно з Австрійською стратегією. Умовно, представлені кіберзагрози можна розділити за такими категоріями:

1. Загрози, пов’язані з персональними даними та інформацією: кібератаки в ході яких викрадаються важливі дані з метою подальшого використання або продажу; шантаж громадян під час незаконного отримання персональної інформації; крадіжка даних, що становлять державну або комерційну таємницю.

2. Загрози, пов’язані з критичною інформаційною інфраструктурою: 1) порушення функціонування системи управління країною в критичних ситуаціях; 2) отримання доступу або порушення діяльності цифрових систем інформації та контролю, що постійно обробляють велику кількість конфіденційної інформації з метою контролю, наприклад: розподіл

[127] Global Cybersecurity Index (GCI) // International Telecommunication Union. 2018. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

[128] A national cyber security strategy // Government offices of Sweden: official web-site. 2016. URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/swedish-national-cyber-security-strategy

електроенергії, водопостачання, транспорту, транспортної інфраструктури або лікарняного обладнання; 3) атаки на промислові об'єкти, які використовують IT-системи; 4) інциденти та атаки, що стосуються шведської торгівлі та промисловості.

3. Кіберзагрози, що мають політичні цілі: 1) кібершпигунство; 2) кібератаки з боку ворожих держав та спонсорованих ними суб'єктів; 3) диверсії проти критично важливих об'єктів інформаційної інфраструктури; 4) неправомірний доступ до незалежних ЗМІ та інформаційних агенцій; 5) дезінформація через кіберпростір.

Отже, підхід ФРН у забезпеченні кібербезпеки не можна назвати «стандартним» у порівнянні з іншими країнами ЄС, у яких основна увага приділяється мінімізації економічних втрат, пов'язаних із кіберзагрозами. Підхід ФРН заснований на поділі військової та цивільної кібербезпеки, будучи, таким чином, свого роду збалансованим підходом. Політика кібербезпеки Австрії передбачає тотожність категорій інформаційна безпека та кібербезпека і приділяє значну увагу кіберзагрозам, що створюють ризики для економічного, варто сказати, що такий підхід характерний для більшості країн ЄС. При цьому, у Стратегії кібербезпеки Австрії представлена одна з найдокладніших класифікацій кіберзагроз серед держав, розглянутих у дипломній роботі. Структура Стратегії кібербезпеки Швеції схожа, з розглянутими раніше стратегіями країн ЄС, проте, відмінністю шведської стратегії, є докладний розгляд кіберзагроз, пов'язаних із захистом суверенітету Швеції від зовнішнього зазіхання.

2.4. Ринок послуг кібербезпеки в африканських країнах: стан та перспективи розвитку

Поряд з АТР, в Африці найбільша кількість країн з високим рівнем схильності до кіберзагроз – на її частку припадає 36,67% усіх країн з високим рівнем вразливості. В Африці найвищий показник схильності до кіберзагроз

на країну. 75% африканських країн належать до груп з високим та дуже високим рівнем уразливості. Маврикій – найменш уразлива до кібератаків країна, за нею йдуть ПАР, Єгипет, Кенія та Нігерія. Ефіопія є найбільш уразливою до кібератаків країною, за нею слідують Лівія, Марокко, Замбія та Танзанія[129].

У Ст. 28 Конвенції АС про кібербезпеку і захист персональних даних (2014 р.)[130] включає в себе положення про уніфікацію, взаємну правову допомогу у справах, пов'язаних з кіберзлочинністю, і обміну інформацією[131]. Ця конвенція містить, серед інших положень, заклик до держав АС приймати національні закони та/або вносити поправки до чинних національних законів з метою ефективної боротьби з кіберзлочинністю, уніфікувати національні законодавства, укладати договори про взаємну правову допомогу, якщо вони ще не укладені, сприяти обміну інформацією між державами, сприяти регіональному, міжурядовому та міжнародному співробітництву та використовувати наявні засоби для співпраці з іншими державами та навіть приватним сектором[132].

Фінансові вкладення, які можуть дозволити Африці уникнути фінансових шляхів, пов'язаних з Інтернетом: відсутність кібербезпеки в Африці коштує континенту кілька млрд дол.. щорічно. Згідно зі звітом кенійської компанії "Serianu", у 2017 р. Африка втратила 3,5 млрд. дол.. «Загроза, яку представляють комп'ютерні атаки, наразі добре відома в Африці, але уряди та приватний сектор ще не інвестували у відповідні засоби

---

[129] Рейтинг стран мира по уровню подверженности киберугрозам 2020 (CEI – Cybersecurity Exposure Index) // 10 GUARDS. URL: https://10guards.com/ru/articles/global-cybersecurity-exposure-index-2020/

[130] African Union Convention on Cyber Security and Personal Data Protection // African Union. 2014. URL: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

[131] Яцишин М.Ю. Роль міжнародних організацій у протидії кіберзлочинності // Українське право. 2019. URL: https://ukrainepravo.com/international_law/public_international_law/rol-mizhnarodnykh-organizatsiy-u-protydiyi-kiberzlochynnosti/

[132] African Union Convention on Cyber Security and Personal Data Protection. URL: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

захисту, щоб обмежити поширення», – сказав Вільям Макатіані, генеральний директор “Serianu”, який оцінив, що «безпека комп’ютерних даних має стати пріоритетом для державних та приватних установ»[133].

Крім захисту від кіберзлочинності держави можуть запропонувати майбутнє сотням тисяч молодих африканців. Однак, за винятком кількох навчальних закладів, таких як Дакарська школа кібербезпеки, континент ще не вжив заходів кібербезпеки.

29 листопада 2018 р. “Orange Cyberdefense” оголосила про відкриття в Марокко центру безпеки, покликаного розширити міжнародну присутність компанії. Кібербезпека – стратегічно важливий напрямок діяльності групи Orange. Станом на листопад 2018 р. “Orange Cyberdefense” була представлена у 20 країнах Африки та Близького Сходу. Африка активно інвестує кошти в кібербезпеку – за прогнозами експертів, до 2020 р. цей ринок зріс на 74%, з 1,33 млрд. дол. у 2017 р. до 2,32 млрд. дол. у 2020 р.. Планується, що центр “Orange Cyberdefense” у Касабланці залучить найкращих місцевих фахівців та співпрацюватиме з французьким центром компетенцій Orange у сфері кібербезпеки. Мета – сформувати до 2020 р. в Марокко штат приблизно з п’ятдесяти співробітників. Щоб прискорити розвиток, центр навчатиме молодих спеціалістів з кібербезпеки в рамках партнерських програм із провідними інженерними навчальними закладами Франції.

Пропоновані рішення будуть аналогічні тим, що вже надаються у Франції: від консультаційних послуг та тестування на проникнення загроз до захисту та спостереження спеціалістами центру кібербезпеки (CyberSOC) та команди реагування на надзвичайні ситуації у сфері комп’ютерної безпеки (CERT). Експерти в Марокко отримають доступ до передового досвіду та

[133] Африка упускает из виду свою кибербезопасность? // Le journal de l'Afrique: official web-site. URL: https://lejournaldelafrique.com/ru/lafrique-dapres/lafrique-est-elle-en-train-de-passer-a-cote-de-sa-cybersecurite/?amp=1

методології “Orange Cyberdefense” та тісно співпрацюватимуть з марокканським підрозділом Orange[134].

В Африці зростання обсягу безготівкових розрахунків призведе до зростання попиту на кібербезпеку. З’являться нові види мобільних грошей та цифрових платежів. При цьому Кенія стане регіональним лідером із запровадження та розповсюдження рішень для мобільних платежів, таких як M-Pesa. Незважаючи на те, що дослідження показують загальне зниження кількості шкідливих програм в Африці в першому півріччі 2020 р., «Лабораторія Касперського» попереджає, що кіберзагрози, як і раніше, широко поширені. Африка не застрахована від методів Advanced Persistent Threats, а також можливості стати майбутньою метою груп зловмисників[135].

Положення Сомалі у системі світової кібербезпеки справедливо можна охарактеризувати як хитке. Через відкладений старт країна має низький рівень цифровізації, а частка активних Інтернет-користувачів не перевищує 3% від загальної кількості мешканців. Водночас є значна хакерська активність. Так, за даними моніторингових агенцій, понад 90% атак, вчинених на цифрову інфраструктуру (насамперед, на урядові установи) Сомалі завершилися вдало. Дуже примітно, що напади часто велися з використанням простих засобів (заражені листи та ін.), що завдавало державі додаткових іміджевих збитків. Постійно зростаюча загроза з кіберпростору змушує Могадішо включати цифрові виклики до порядку денного поряд із традиційними для регіону загрозами[136].

У 2017 р. у країні було ухвалено Закон про комунікації. Серед іншого Закон вніс істотні зміни до порядку регулювання сектору зв’язку (включаючи

---

[134] Orange Cyberdefense // TADVISER. 2022. URL: https://www.tadviser.ru/index.php/%D0%9A%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F:Orange_Cyberdefense

[135] Журенко Е. Рынок кибербезопасности на Ближнем Востоке и в Африке // Creditplus. 2021. 10 августа. URL: https://creditplus.ua/ru/blog/kiberbezopasnost-na-vostoke-i-v-afrike

[136] Цуканов Л. Кибербезопасность по-сомалийски // Российский совет по международным делам: РСМД. 2022. 17 января. URL: https://russiancouncil.ru/analytics-and-comments/columns/africa/kiberbezopasnost-po-somaliyski/

Інтернет та телекомунікації), сприявши деякій лібералізації цієї галузі (зокрема, було спрощено регулювання електронних операцій із фінансами). У наступні роки влада Сомалі прийняла низку додаткових регламентів, покликаних проілюструвати окремі нормотворчі ініціативи, проте Закон 2017 р. як і раніше залишається основним у питаннях регулювання відносин у кіберпросторі. Проте, незважаючи на зрушення, положення Закону регулюють переважно сектор телекомунікацій та частково (на основі додаткових регламентів) банківський сектор, тоді як у суміжних галузях (наприклад, охорона здоров'я) цифрове регулювання відсутнє.

Головний показник підвищення технічних можливостей Сомалі в галузі кібербезпеки – створення національної Комп'ютерної групи реагування на надзвичайні ситуації (SomCERT) у 2019 р., а також започаткування при ньому координаційного центру захисту дітей в онлайн-середовищі (COP) у 2020 р. для протидії кібератакам. Обидві ініціативи свідчать про прагнення керівництва Сомалі до розвитку національної цифрової екосистеми, що базується на принципах співпраці та відкритості. Проте на цьому етапі діяльність сомалійського CERT обмежується захистом цифрової інфраструктури від кіберзагроз, а також наданням технічної підтримки державним органам. При цьому практика проведення кібер-навчань (як і сертифікації національних фахівців у галузі кібербезпеки) не налагоджена. Питання створення галузевих CERT (з метою зміцнення безпеки телекомунікаційного чи енергетичного сектора) на порядок денний також не виноситься[137].

ПАР на регулярній основі приймає різні міжнародні форуми на найвищому рівні, присвячені розвитку IT та забезпеченню міжнародної інформаційної безпеки. Так, у ПАР регулярно, починаючи з 2007 р., проходить Міжнародний саміт у сфері інформаційної безпеки (ITWeb

[137] Там само. URL: https://russiancouncil.ru/analytics-and-comments/columns/africa/kiberbezopasnost-po-somaliyski/

Security Summit). У роботі цього саміту щорічно бере участь понад 500 учасників із різних країн світу. Форум дає унікальну можливість як топ-менеджерам великих IT-компаній, так і главам держав та урядів поділитись важливою інформацією у сфері забезпечення інформаційної безпеки. Ця обставина переконливо свідчить про те, що цей саміт є найбільшим форумом у сфері кібербезпеки в Африці[138].

У 2020 р. в африканські стартапи було вкладено близько 2,4 млрд. дол., а до 2025 р. обсяг продажів електронної комерції в Африці, за прогнозами, досягне 75 млрд. дол.. Тут проживає половина з 40 найбільш швидко зростаючих країн з ринком, що формується, і країн, що розвиваються, і в даний час він є найбільш підприємливим. Ця тенденція лише посилюватиметься, оскільки ініціативи зі скорочення цифрового розриву до 2030 р. підключать 78% населення, що залишилося, до Інтернету[139].

Порівняно низький ступінь інфраструктурного та технологічного розвитку країн континенту дозволяє впроваджувати та масштабувати передові рішення по цілій низці напрямків: від заходів з розробки та контролю міського простору, що динамічно зростає, до цифровізації документів, що засвідчують особу. Лише державний сектор ринку з адаптації цифрових технологій у країнах Африки на південь від Сахари оцінюється в десятки мільярдів доларів і вважається одним із головних «інвестиційних клондайків» найближчого десятиліття. На даний момент лише 18 країн

---

[138] Панцерев К. А. Страны Африки Южнее Сахары в цифровую эпоху: к вопросу обеспечения информационного суверенитета // Азия и Африка сегодня. 2019. № 10. С. 10-11.

[139] Перестройка кибербезопасности для создания более безопасной сети для всех – TechCrunch // Hitech Glitz. URL: https://hitechglitz.com/russia/%D0%BF%D0%B5%D1%80%D0%B5%D1%81%D1%82%D1%80%D0%BE%D0%B9%D0%BA%D0%B0-%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D0%B8-%D0%B4%D0%BB%D1%8F-%D1%81/

Африки на південь від Сахари запровадили електронні системи подання податкових декларацій, а можливість дистанційної оплати є не в кожній з них[140].

Згідно з нещодавнім звітом Африканського центру стратегічних досліджень[141], лише 18 африканських держав створили національні групи реагування на кіберінциденти. Як одну з причин, автори виділяють нестачу понад ста тисяч співробітників служби кібербезпеки по всьому континенту. Таким чином, ще однією точкою входу на африканські ринки для зарубіжних ІТ-компаній може стати сфера підготовки кадрів та підвищення кваліфікації фахівців.

Проблема забезпечення кібербезпеки в Африці не вичерпується вразливістю державних відомств та інфраструктури, окремий інтерес становить комерційний сегмент. Автори звіту марокканської компанії "Dataprotect" за 2020 р. проаналізували становище 148 банків із Західноафриканського валютно-економічного союзу та трьох країн Центральної Африки: 85% повідомляли про неодноразові кібератаки, що призвели до фінансових втрат. При цьому кінцева вартість відновлення фінансових компаній після кібератак буде підвищуватися зі збільшенням кількості онлайн-транзакцій.

Ще однією особливістю недержавного сектора у контексті кібербезпеки є високий попит у країнах – флагманах африканської цифровізації. Згідно з останнім опублікованим дослідженням[142] компанії "Sophos", що займається програмним забезпеченням та безпекою, майже кожна четверта комерційна організація в ПАР постраждала від атак кібер-

[140] Тарасенко Д. Зачем России Африка и с чем «ходить гулять»? // Российский совет по международным делам: РСМД. 2021. 20 августа. URL: https://russiancouncil.ru/analytics-and-comments/analytics/zachem-rossii-afrika-i-s-chem-khodit-gulyat/

[141] Africa's Evolving Cyber Threats // Africa Center for Strategic Studies: official web-site. 2021. 19 of January. URL: https://africacenter.org/spotlight/africa-evolving-cyber-threats/

[142] The State of Ransomware 2021 // SOPHOS: official web-site. 2021. URL: https://secure2.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf

вимагачів у 2020 р. У цьому ж зізналося 22% опитаних у Нігерії. Середня вартість відновлення після кібератаки у Південній Африці оцінюється “Kaspersky” у 447 097 дол., що більш ніж удвічі перевищує середній світовий показник (170 404 дол.)[143].

Таким чином, африканським країнам слід не лише приділяти увагу безпосередньо розвитку на своїй території інформаційних технологій, але й забезпеченню свого інформаційного суверенітету через зменшення своєї технологічної залежності від США та інших західних країн. Рішення цього насущного завдання є можливим за допомогою послідовної реалізації наступних заходів:

1. Побудова альтернативної оптоволоконної кабельної системи, яка йшла б в обхід території США та інших західних країн.

2. Створення регіональних дата-центрів, які акумулювали б регіональний Інтернет-трафік і не були б підконтрольні американським спецслужбам. Подібні дата-центри можуть бути побудовані в ПАР, Нігерії, Гані, Кенії та на Маврикії.

3. Розробка місцевого програмного забезпечення, як і створення регіональних інноваційних комплексів, технопарків, які б орієнтовані реалізацію потреб місцевого населення і виробляли б технології, максимально адаптовані до місцевих умов, навіть якщо у тому основі лежать західні технологічні рішення.

[143] Ransomware recovery cost more than doubles // IT-online. 2021. 29 of April. URL: https://it-online.co.za/2021/04/29/ransomware-recovery-cost-more-than-doubles/

РОЗДІЛ 3.
МЕХАНІЗМИ РОЗВИТКУ СФЕРИ КІБЕРБЕЗПЕКИ ЯК СКЛАДОВОЇ СУЧАСНОЇ СИСТЕМИ МІЖНАРОДНИХ ВІДНОСИН

3.1. Аналіз проблем чинного міжнародного законодавства про злочини в сфері комп'ютерної інформації та можливих шляхів їх вирішення

Офіційні механізми міжнародного співробітництва включають в себе двосторонні, регіональні та багатосторонні договори в області боротьби з кіберзлочинністю.

Міжнародне законодавство про злочини в сфері комп'ютерної інформації включає такі нормативно-правові акти: Конвенція РЄ про кіберзлочинність 2001 р.; Угода про співробітництво в боротьбі зі злочинами в сфері комп'ютерної інформації, підписана країнами-членами СНД у 2001 р.; Конвенція ЛАД про боротьбу зі злочинами в області інформаційних технологій, прийнята ЛАД у 2010 р.; Угода про співробітництво в галузі забезпечення міжнародної інформаційної безпеки, прийнята ШОС в 2010 р.; Конвенція АС про кібербезпеку і захист персональних даних 2014 р. Необхідно підвищувати ефективність способів боротьби.

Одним з найбільш важливих етапів у розвитку міжнародного підходу до питань боротьби з кіберзлочинністю, є Конвенція РЄ «Про кіберзлочинність», прийнята в Будапешті в листопаді 2001 р.. Даний документ був одним з перших міжнародних актів, регіонального, а потім і глобального рівня, що регламентували багатосторонні заходи з протидії кіберзлочинності, а так само сприяла стандартизації європейських кримінальних та інших видів законодавств у цій галузі

Конвенція про кіберзлочинність[144], є єдиним документом обов'язкового застосування, який регулює правовідносини у сфері експлуатації комп'ютерної мережі. Дана Конвенція досить значима не лише в рамках РЄ, а й на глобальному рівні. Вона є одним з основоположних документів у сфері протидії кіберзлочинності. Конвенцію підписали не тільки країни Європи, але також Аргентина, Австралія, Ізраїль, Японія, США, в цілому більше 50 держав.

Однак ця Конвенція в деякій мірі є застарілою і не відповідає життєвій ситуації у зв'язку зі стрімкими темпами освоєння цифрового простору і впровадження нових технологій. Оскільки Конвенція розроблялася в 1997-2001 рр., багато загроз в області кіберпростору на той момент не були відомі або їм не приділялося належної уваги. Дуже складним є ефективне ведення боротьби з новими проявами тероризму в інформаційному просторі без його юридичного визначення і, відповідно, криміналізації як самого поняття, так і його складових[145].

Позитивні аспекти, що знайшли своє відображення в Конвенції РЄ від 2001 р.:

1) у рамках даної Конвенції, була поставлена мета її прийняття і дотримання, а саме вироблення всеосяжної і гармонійної політики кримінального права, що стосується питань злочинів у сфері інформаційних технологій, яка б захищала суспільство від кіберзлочинності, як на внутрішньодержавному, так і регіональному рівні;

2) так само в Конвенції класифікуються основні види правопорушень в кіберпросторі, а додаткові протоколи, прийняті в Страсбурзі у 2003 р., доповнюють класифікацію деякими видами правопорушень, зокрема

[144] Convention on Cybercrime // Council of Europe. 2001. URL: https://rm.coe.int/1680081561
[145] Войціховський А.В. Міжнародне співробітництво в боротьбі з кіберзлочинністю. Право і безпека. 2011. № 4 (41). С. 107-109.

дискримінацію, поширення расистських поглядів, ксенофобію і виправдання геноциду і расизму в кіберпросторі;

3) особлива увага в рамках цієї Конвенції приділяється сфері міжнародного співробітництва.

Мета стратегії кібербезпеки ЄС («Стратегія кібербезпеки ЄС: відкритий, надійний та безпечний кіберпростір»)[146] – підвищення стійкості і нарощування потенціалу в області кібербезпеки держав-членів ЄС (посилення боротьби з кіберзлочинністю, формування ефективної інфраструктури забезпечення безпеки, розробка принципів міжнародної політики в області кібербезпеки). Слід зазначити, що сьогодні практично неможливо домогтися єдиного рішення з проблем кібербезпеки, прийнятого на загальноєвропейському рівні. Не всі країни ЄС сьогодні готові сформулювати на національному рівні відповідь на інциденти в сфері комп'ютерної безпеки. Немає єдиного органу, здатного приймати загальноєвропейські рішення в цій сфері.

Аналіз культури і практики роботи європейських Комп'ютерних груп реагування на надзвичайні ситуації Комп'ютерної команди реагування на надзвичайні ситуації показує, що навіть там, де вони мають міцну правову основу, CERT регулярно працюють ізольовано і відчувають серйозні проблеми не тільки під час транскордонної передачі інформації, але і при спробі міжвідомчого інформаційного обміну. Тому найважливіший аспект стратегії – гармонізація можливостей забезпечення інформаційної безпеки європейських держав, і уніфікація інфраструктури забезпечення кібербезпеки за допомогою:

1) змін в національних законодавствах, створення національних групам реагування на комп'ютерні інциденти;

---

[146] Europe 2020. A European strategy for smart, sustainable and inclusive growth // European Union official web-site. URL: https://ec.europa.eu/eu2020/pdf/COMPLET%20EN%20BARROSO%20%20%20007%20-%20Europe%202020%20-%20EN%20version.pdf

2) формування компетентних національних органів, забезпечених професійними і матеріальними ресурсами, які будуть відслідковувати ситуацію в своїх країнах і управляти кібер-ризиками, а також підтримувати взаємодію з ЄК.

Стратегія передбачає зміцнення співпраці між державним і приватним секторами, а також розробку концептуальних документів, що забезпечують єдині поняття та підходи, для формування єдиного загальноєвропейського погляду на організацію і проведення інформаційних операцій в рамках розроблюваної стратегічної концепції «Спільної оборони і політики безпеки».

3 квітня 2014 р. в Брюсселі, на зустрічі представників Координаційної групи з кібербезпеки з віце-президентом ЄК Нелі Крус, відбулося обговорення ролі стандартів в зміцненні безпеки в мережі Інтернет та захисту персональних даних в рамках реалізації стратегії кібербезпеки ЄС. Експерти Групи звертали увагу на значення гармонізованих стандартів кібербезпеки для формування єдиного європейського ринку. В якості основи для узгодженої роботи був запропонований Регламент Європейського Парламенту та Ради 025/2012 від 25 жовтня 2012 р. про європейську стандартизацію[147].

Рекомендації 10 вересня 2014 р. представляють собою докладний виклад пропозицій Координаційної групи з кібербезпеки, систематизовані за трьома критеріями: управління, узгодження і глобальний вимір. При цьому Агентство рекомендує «узгодити використання ключових термінів кібербезпека», «безпека мереж та інформації» і «кіберзлочинність» в ЄС на основі існуючих визначень.

[147] Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardization // EUR-Lex. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32012R1025

У 2018 р. ЄС вирішив оновити і посилити стратегію спільноти з кібербезпеки прийняту у 2013 р. в зв'язку з останніми кібератаками. Одним із пріоритетів нової стратегії ЄС має стати створення Європейського агентства з кібербезпеки на базі існуючого агентства мережевої та інформаційної безпеки, яке отримає постійний мандат для допомоги країнам-членам у запобіганні кібератак і реагуванні на них. Агентство буде проводити щорічні навчання з кіберзахисту у всьому ЄС. Агентство поліпшить готовність ЄС реагувати (на атаки), організовуючи щорічні пан'європейські навчання з кібербезпеки і забезпечуючи найкращий обмін даними про погрози та інформацію за допомогою створення центрів обміну і аналізу інформації.

Міжнародне співробітництво в боротьбі з кіберзлочинністю ускладнюється розбіжністю позицій різних держав світу, обумовленим базовими відмінностями в підходах до визначення понять, відсутністю чіткого розуміння меж між різними явищами, які вимагають різних мехнізмів співпраці, відмінністю в підходах до забезпечення безпеки персональних даних, загальним рівнем взаємної недовіри, що унеможливлює співпрацю з питань транскордонного процесуального партнерства. У силу цього в ООН був відхилений запропонований РФ і КНР проект глобальної Конвенції з кіберзлочинності в 2010 р..

Сьогодні відкритість кіберпростору означає практично загальний доступ до будь-якого контенту. Нагальною вимогою є міжнародне співробітництво в сфері подолання низки негативних наслідків такої повної відкритості, перш за все у сфері протидії найбільш серйозним транснаціональним злочинам. Можливо, і в кіберпросторі має бути створено «простір свободи, безпеки та правосуддя» за аналогією з невіртуальним простором ЄС (ст. 3 Договору про ЄС)[148]. Для того, щоб міжнародне

[148] The Treaty on European Union and the Treaty on the Functioning of the European Union // EUR-Lex. URL: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT

співробітництво країн у боротьбі з кіберзлочинністю було ефективним, необхідно уніфікувати правові норми різних держав при регламентації дій сторін у процесі використання коштів в боротьбі з кіберзлочинами.

Стратегічна концепція НАТО[149] 2010 р., прийнята на саміті в Лісабоні, приділяє основну увагу загрозам можливих кібератак. По суті, у ній йдеться про прирівнювання кібератаки до традиційного військового нападу. Інформаційна безпека має першорядне значення для Альянсу. Політика НАТО з питань кіберзахисту розглядає міжнародне партнерство у сфері кібербезпеки як один із ключових елементів стратегії НАТО у цій сфері.

Ця заява була підтверджена в Декларації саміту НАТО в Чикаго, прийнятої главами країн та урядів на засіданні Північноатлантичної ради в травні 2012 р. Зокрема, Ст. 49 підтверджує готовність співпрацювати із закордонними партнерами та організаціями з питань кіберзахисту та наголошує на необхідності зміцнення захисту кіберпростору.

Наприклад, Центр передового досвіду НАТО в області комп'ютерної безпеки випустив збірник рекомендацій «Таллінське керівництво по застосуванню міжнародного права в кібервійні»[150]. В якості основних завдань вказані «адаптація існуючих правових норм щодо збройних конфліктів під специфіку ворожої діяльності на віртуальному просторі» і спроба розробити дефініції основних понять в сфері комп'ютерної безпеки.

Угода про співробітництво держав-учасниць СНД у боротьбі зі злочинами в сфері комп'ютерної інформації 2001 р. містить кілька статей, присвячених міжнародному співробітництву (ст. 5-7), в яких перераховані форми співпраці, які охоплюються цією угодою (а саме: обмін інформацією; надання правової допомоги відповідно до міжнародних документів;

---

[149] Strategic Concept 2010 // NATO: official we-site. 2010. URL: https://www.nato.int/cps/en/natohq/topics_82705.htm

[150] Tallinn Manual on the International Law Applicable to Cyber Warfare // Cambridge University Press 2021. 2013. URL: https://www.cambridge.org/core/books/tallinn-manual-on-the-international-law-applicable-to-cyber-warfare/50C5BFF166A7FED75B4EA643AC677DAE

попередження, виявлення, припинення і розслідування злочинів у сфері комп'ютерної інформації тощо), а також способи, за допомогою яких держави-члени можуть робити запити, і керівні вказівки для держав-членів щодо виконання запитів. У Ст. 8 цієї Угоди вказані обставини, за яких в проханні про надання допомоги може бути відмовлено (а саме: коли виконання запиту суперечить національному законодавству запитуваної Держави), і вимога, відповідно до якої держава, яка відмовляється виконувати запит, зобов'язана письмово повідомити державу, яка подає запит про відмову із зазначенням причин відмови[151].

Ще в січні 2015 р. учасники ШОС внесли на розгляд ГА ООН Міжнародний кодекс поведінки в області інформаційної безпеки[152], який є першим міжнародним документом, присвяченим нормам поведінки в інформаційному середовищі. Документ має наступні цілі:

- визначити права і обов'язки держав в інформаційному просторі;
- стимулювати конструктивну і відповідальну поведінку держави;
- зміцнювати співпрацю проти загроз і викликів в інформаційному просторі.

Нарешті, в грудні 2018 р. ГА ООН прийняла Резолюцію «Досягнення у сфері інформатизації та телекомунікацій в контексті міжнародної безпеки»[153], яка була підтримана 119 державами, 46 країн проголосували проти, 14 утрималися. Оскільки кодекс поведінки держав в Інтернеті, що міститься в Резолюції має рекомендаційний характер, ведеться робота по розробці конвенції ООН з міжнародної інформаційної безпеки.

---

[151] Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации // Верховна Рада України. 2001. URL: https://zakon.rada.gov.ua/laws/show/997_353#Text

[152] International code of conduct for information security // United Nations Organisation. URL: https://digitallibrary.un.org

[153] Генассамблея ООН проголосовала за российский проект резолюции по глобальной кибербезопасности // Экспертный центр электронного государства. 2018. URL: https://d-russia.ru/genassambleya-oon-progolosovala-za-rossijskij-proekt-rezolyutsii-po-globalnoj-kiberbezopasnosti.html

Надалі країни-члени ЄС максимально поглибили співпрацю в області кібербезпеки через інструменти європейського права. Норми матеріального права гармонізовані за допомогою цілої низки директив, зокрема, Директива про протидію сексуальній експлуатації дітей онлайн і дитячої порнографії[154], Директива щодо атак проти інформаційних систем[155], Директива про безпеку мереж та інформаційних систем[156].

Успішний приклад співпраці країн ЄС є прикладом фрагментації міжнародно-правового співробітництва та несе в собі загрози для можливостей широкого консенсусу держав. Незважаючи на те, що Управління ООН з наркотиків і злочинності надає підтримку національним органам для зміцнення потенціалу у сфері боротьби з кіберзлочинністю, в тому числі технічну, а також збір даних, проведення досліджень і аналітичної роботи з проблеми кіберзлочинності, ні правові основи, ні завдання, ні масштаби його діяльності не можна порівняти з прикладом співпраці в європейському регіоні. Подібна ситуація може привести до ослаблення ролі ООН у співпраці в галузі боротьби з кіберзлочинністю, беручи до уваги той факт, що перспективи прийняття універсальних правових інструментів співробітництва в рамках ООН виглядають досить туманно[157].

---

[154] Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA // EUR-Lex. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011L0093

[155] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA // EUR-Lex. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32013L0040

[156] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union // EUR-Lex. URL: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32016L1148

[157] Демедюк С.В. Міжнародний досвід протидії кіберзлочинності. Вісник Харківського національного університету внутрішніх справ: збірник наукових праць. Харків. 2014. № 4 (67). С. 65-67.

Крім того, Ст. 32 і 34 Конвенції ЛАД про боротьбу зі злочинами в області інформаційних технологій (2010 р.)[158] містять положення про надання взаємної допомоги, процедури співпраці та подання запитів про надання взаємної допомоги.

Більш того, Ст. 28 Конвенції АС про кібербезпеку і захист персональних даних (2014 р.)[159] включає в себе положення про уніфікацію, взаємну правову допомогу у справах, пов'язаних з кіберзлочинністю, і обміну інформацією. У положенні про обмін інформацією міститься заклик до держав створювати установи, які можуть сприяти обміну інформацією про загрози кібербезпеки і вразливості, такі як групи реагування на комп'ютерні інциденти (CERT) або групи реагування на інциденти в сфері комп'ютерної безпеки (CSIRT). Відповідно до ст. 28 (4) державам наказано «використовувати існуючі механізми міжнародного співробітництва», які можуть включати в себе «міжнародні, міжурядові, регіональні або ... державно-приватні партнерства», для вжиття заходів реагування на кіберзлочини[160].

Регіональними організаціями та/або регіональними міжурядовими організаціями були також розроблені та імплементовані закони та директиви у сфері боротьби з кіберзлочинністю.

---

[158] Arab Convention on Combating Information Technology Offences // Asian School of Cyber Laws. 2010. URL: https://www.asianlaws.org/gcld/cyberlawdb/GCC/Arab%20Convention%20on%20Combating%20Information%20Technology%20Offences.pdf

[159] African Union Convention on Cyber Security and Personal Data Protection // African Union. 2014. URL: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

[160] Яцишин М.Ю. Роль міжнародних організацій у протидії кіберзлочинності // Українське право. 2019. URL: https://ukrainepravo.com/international_law/public_international_law/rol-mizhnarodnykh-organizatsiy-u-protydiyi-kiberzlochynnosti/

Типовий закон[161] про комп'ютерні злочини та кіберзлочинність САДК 2012 р.. Цей закон є керівництвом для держав-учасниць САДК для розробки норм матеріального та процесуального права у сфері боротьби з кіберзлочинністю. Оскільки цей закон є типовим, він не накладає на держави будь-яких юридичних зобов'язань щодо здійснення співробітництва. Держави, які не мають та/або не розробляють закони про кіберзлочинність, можуть використовувати Протокол САДК про взаємну правову допомогу у кримінальних справах та Протокол САДК про видачу для сприяння співпраці та координації при здійсненні міжнародних розслідувань кіберзлочинів.

Директива про боротьбу з кіберзлочинністю[162] ЕКОВАС 2011 р. Ця директива вимагає від держав-учасниць криміналізації кіберзлочинності в національному законодавстві та сприяє взаємній правовій допомозі, співпраці та видачі злочинців у справах, пов'язаних із кіберзлочинністю та кібербезпекою. ЕКОВАС прийняв Конвенцію про взаємну правову допомогу у кримінальних справах та Конвенцію про видачу з метою сприяння співпраці у розслідуванні кіберзлочинів та видачі кіберзлочинців.

Проте, континент, схоже, не хоче оцінювати небезпеку. З одного боку, багато країн досі не ратифікували Конвенцію Африканського союзу про кібербезпеку та захист особистих даних, відому як «Конвенція Малабо», яка могла б забезпечити основу для реагування на ці загрози. Іншими словами, відсутність правової бази з кібербезпеки та незнання цифрового сектора є проблематичною. З іншого боку, оскільки кібербезпека є пріоритетом для урядів африканських країн, задіяні ресурси не відповідають завданням[163].

---

[161] Computer Crime and Cybercrime: Southern African Development Community (SADC) Model Law // ITU. 2012. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/SADC%20Model%20Law%20Cybercrime.pdf

[162] Directive C/DIR. 1/08/11 on fighting cyber crime within ECOWAS // Economic Community of West African States(ECOWAS). 2011. URL: http://www.tit.comm.ecowas.int/wp-content/uploads/2015/11/SIGNED_Cybercrime_En.pdf

[163] Африка упускает из виду свою кибербезопасность? URL: https://lejournaldelafrique.com/ru/lafrique-dapres/lafrique-est-elle-en-train-de-passer-a-cote-de-sa-cybersecurite/?amp=1

Лише 29 країн в Африці мають закони про кібербезпеку і лише 19 мають групи реагування на кіберінциденти та надзвичайні ситуації. У результаті економіка африканських країн виявляється незахищеною, а глави африканських держав та урядів опиняються поза органами, що визначають глобальну політику кібербезпеки.

Лише вісім країн ратифікували Конвенцію Малабо про кібербезпеку та захист особистих даних, і лише шість країн ратифікували Будапештську конвенцію. Ці договори були розроблені, щоб допомогти державам обмінюватися інформацією, встановлювати стандарти та отримувати вигоду з міжнародної технічної допомоги та співробітництва. На даний момент менше половини держав Африканського союзу мають будь-яке правове регулювання цифрового середовища. Серед країн без спеціального законодавства щодо безпеки особистих даних Камерун, Республіка Конго, Ефіопія, Ліберія, Сьєрра-Леоне, Південний Судан, Судан та Сомалі. Ще низка країн перебуває у стадії розробки власних законопроектів – Ботсвана, Намібія, Уганда, Танзанія та Зімбабве[164].

Отже, створення системи органів і агентств для протидії кіберзагрозам на загальноєвропейському рівні продовжиться. Разом з тим рівень обізнаності та свідомості європейських громадян і компаній про проблеми кібербезпеки залишається низьким, починаючи з базових основ пошуку інформації та закінчуючи поведінкою в разі кібер-інцидентів. На рівні держави-членів ЄС знадобиться вести більш активну інформаційно-освітню роботу.

3.2. Роль кібербезпеки в забезпеченні суверенітету України

[164] Тарасенко Д. Зачем России Африка и с чем «ходить гулять»? URL: https://russiancouncil.ru/analytics-and-comments/analytics/zachem-rossii-afrika-i-s-chem-khodit-gulyat/

Проблема кібертероризму є актуальною і для України. Це обумовлено тим, що з одного боку, країна не настільки багата, щоб переобладнати сучасними засобами управління свої підприємства та атомні електростанції, що зробить їх невразливими для нападів інтелектуальних диверсантів. З іншого боку, відкриті мережі сьогодні – це засоби інформаційного протиборства в руках політиків, бізнесменів, релігійних організацій, терористичних груп і злочинних угруповань. Небезпека інформаційного тероризму для України полягає в тому, що він не має національних кордонів і терористичні акції можуть здійснюватися з будь-якої точки світу. Дії терористів можуть бути спрямовані як на громадські, так і на військові об'єкти. Найбільш уразливими точками української інфраструктури є енергетика, телекомунікації, авіаційні та диспетчерські системи, фінансові електронні системи, урядові інформаційні системи, а також автоматизовані системи управління військами і зброєю[165].

Часто кібератаки спрямовані проти інформаційних систем державних органів, секторів охорони здоров'я, фінансів та транспорту та призводять до небезпечних та непередбачуваних наслідків. Крім того, конфлікт на сході України підтверджує тезу про те, що багато в чому гібридна війна підтримується широким спектром інструментів кібервійни. Один цікавий аспект полягає в тому, що найчастіше метою є урядові інформаційні ресурси та бази даних, які терористи розглядають як засоби створення та реалізації можливостей щодо встановлення контролю над певною територією та населенням для забезпечення підтримки економічних заходів та псевдоуправління.

Для вітчизняного законодавства однією з проблем є сам понятійно-категоріальний апарат, який використовується для опису кіберзлочинів. Такі терміни, як «кіберзлочинність», «кібератака», «кіберзлочинець»,

[165] Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва : монографія. Київ: НІСД, 2014. С. 178-179.

«віртуальний простір», безумовно, вимагають законодавчого закріплення для правильного розуміння і застосування кримінально-правових норм.

Позитивними є прагнення Міністерства інформаційної політики України використати ресурси Інтернет у вигляді проекту «Інформаційні війська», метою якого є розвиток мережі українських Інтернет-користувачів, які будуть протистояти російській пропаганді. Здійснення цієї мети базуватиметься на основі власної інформаційної платформи задля заповнення прогалин щодо реальних подій, зокрема, в середині самої країни[166].

Виходячи, що НАТО вперше відкриває та фінансує подібний центр поза межами власне країн-членів НАТО. А це є визнанням як надзвичайної актуальності проблеми, так і належною оцінкою досвіду України в цій сфері. Є підстави сподіватись, що саме українці, які більше ніж будь-хто сьогодні знають про інформаційну та гібридну війну, завдяки підтримці НАТО і спільно з НАТО зможуть ефективно протидіяти ворожій пропаганді та кібератакам. Це зрештою сприятиме захисту українців і європейців від згубної пропаганди РФ і відповідно від деструктивного впливу на свідомість та психіку наших громадян.

У 2015 р. Кабінет міністрів України розробив проект закону з кібербезпеки, який запровадив термін «кібербезпека» та інші терміни із приставкою «кібер» до національного законодавства. Стратегія національної безпеки України, прийнята 2016 р. РНБО та затверджена Президентом, як головна загроза національній безпеці визначає «уразливість критично важливої інформаційної інфраструктури та урядових інформаційних ресурсів перед кібератаками». Ця загроза завжди потребувала адекватної протидії. На жаль, Україна все ще перебувала у процесі розгортання своєї НСКБ, передбаченої попередньою редакцією Стратегії національної безпеки від 2012 р. Вперше ідея організувати НСКБ виникла у 2010 р. У рішенні Ради

[166] Буяджи С.А. Правове регулювання боротьби з кіберзлочинністю: теоретико-правовий аспект : дис. … здоб. наук. ступ. канд. юрид. наук. 12.00.01. Київ, 2018. С. 145-146.

національної безпеки та оборони говорилося про «проблеми та національної безпеки України у 2011 р.» та необхідності «загальної національної системи протидії кіберзлочинності».

При виконанні цього завдання стало зрозуміло, що для забезпечення національної безпеки в інформаційній сфері необхідний комплексний підхід, що враховує не тільки кримінальні загрози, а й увесь спектр загроз, що варіюються залежно від їхнього походження, інструментів, цілей і, зрозуміло, кінцевої мети. Внаслідок цього з'явилася концепція національної системи кібербезпеки. НСКБ є поєднанням комплексів заходів адміністративного, правового та технічного характеру, що належать до інформаційної безпеки та захисту даних від потенційних ризиків в оборонному, правоохоронному та розвідувальному секторах.

Кіберзагрози поділяються на такі групи: кібервійна, кібертероризм, кібершпигунство і кіберзлочинність. Така класифікація вимагає, щоб НСКБ включала кілька допоміжних систем: систему оборонної кібербезпеки, правоохоронну систему і систему національної безпеки (з упором на кібертероризм і шпигунство)[167].

За оцінками аналітиків DX Agent, у 2020 р. обсяг українського ринку рішень інформаційної безпеки зменшився на 22% і становив орієнтовно 68 млн. дол. у цінах замовників (для порівняння: у 2019 р. він зріс на 52% та досяг 86 млн. дол.).

Як зазначається, у структурі продажів, як і раніше, переважає ПЗ з часткою 57% (38,8 млн. дол.), чверть припадає на апаратно-програмні рішення (16,8 млн. дол.), причому саме їх продажі впали на 49%, а ось частка послуг виросла на два пункти – до 18% (12 млн. дол.).

---

[167] Петров В. Международные угрозы вынуждают Киев создать национальную систему кибербезопасности // per Concordiam. 2016. 7 января.URL: https://perconcordiam.com/ru/%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C-%D0%BD%D0%B0-%D1%83%D0%BA%D1%80%D0%B0%D0%B8%D0%BD%D0%B5/

22 липня 2020 р. стало відомо про те, що США нададуть Україні фінансову підтримку у розмірі 38 млн. дол. на розвиток кібербезпеки в країні.

У березні 2020 р. Держдепартамент оголосив, що США виділяє Україні ще 8 млн. дол. на забезпечення кібербезпеки на додаток до 10 млн. дол., які були обіцяні у 2017 р.. Частину цього фінансування планувалося направити на підтримку нового проекту Агентства США з міжнародного розвитку в галузі кібербезпеки[168].

Президент України Володимир Зеленський затвердив нову Стратегію кібербезпеки України, яку схвалила РНБО 14 травня 2021 р.. Про це повідомлялося в Указі Президента № 447/2021 від 26 серпня, яким запроваджено рішення РНБО від 14 травня 2021 року «Про Стратегію кібербезпеки України». Також у документі В. Зеленський визнав попередню Стратегію кібербезпеки (затверджено Президентом України 15 березня 2016 р..), як таку, що втратила чинність. Згідно з опублікованим текстом Стратегії, забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки України та реалізація зазначеного пріоритету здійснюватиметься шляхом посилення можливостей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі[169].

«Російська Федерація залишається одним з основних джерел загроз національній та міжнародній кібербезпеці, активно реалізує концепцію інформаційного протиборства, засновану на поєднанні деструктивних дій у кіберпросторі та інформаційно-психологічних операцій, механізми якої активно застосовуються в гібридній війні проти України. Така деструктивна активність створює реальну загрозу актів кібертероризму та кібердиверсій

---

[168] Информационная безопасность на Украине // TAdviser.com. 2021. 4 октября. URL: https://www.tadviser.ru/

[169] Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України №447/2021 // Президент України: офіційне Інтернет-представництво. URL: https://www.president.gov.ua/documents/4472021-40013

щодо національної інформаційної інфраструктури», – наголошується у стратегії[170].

У Стратегії серед іншого визначено, що пріоритетами забезпечення кібербезпеки України є:

1) забезпечення безпеки кіберпростору для захисту суверенітету держави та розвитку суспільства;

2) захист прав, свобод та законних інтересів громадян України у кіберпросторі;

3) європейська та євроатлантична інтеграція у сфері кібербезпеки.

Відповідно до Стратегії, Україна:

1) забезпечить посилення національної кіберготовності та кіберзахисту у співпраці із суб'єктами приватного сектору, академічною спільнотою та громадськістю;

2) проведе наукові дослідження у сфері кібербезпеки, реформує систему підготовки та підвищення кваліфікації кадрів, розробить навчальні програми, курси, тренінги з кібернавчання;

3) спрямує зусилля на забезпечення посилення надійності та безпеки цифрових послуг[171].

1 вересня 2021 р. Президент США Джо Байден та Президент України В. Зеленський провели переговори у очному форматі. Вони тривали в Білому домі близько двох годин. За підсумками зустрічі було підписано кілька угод, одна з яких передбачає співпрацю Державної служби спеціального зв'язку та захисту інформації України та американського Державного департаменту. Також Держспецзв'язку домовилася про спільну роботу з Агентством з кібербезпеки та безпеки інфраструктури Держдепу США.

---

[170] Там само. URL: https://www.president.gov.ua/documents/4472021-40013

[171] Президент утвердил новую Стратегию кибербезопасности Украины // УКРінформ. 2021. 26 серпня. URL: https://www.ukrinform.ru/rubric-polytics/3304776-prezident-utverdil-novuu-strategiu-kiberbezopasnosti-ukrainy.html

Було укладено договір про встановлення лінії захищеного зв'язку. Як зазначив голова Держспецзв'язку Юрій Щегол, підписання угоди, а також створення національних центрів обміну інформацією у столицях двох країн є важливим кроком для України та США.

Крім того, за результатами зустрічі Дж. Байдена та В. Зеленського до кінця 2021 р. планувалося підписати угоду, яка передбачає обмін досвідом та інформацією щодо протидії «агресії РФ у кіберпросторі», а також розробку спільних протоколів дій. Інші умови цієї угоди такі:

1) побудова платформи обміну інформацією про кіберінциденти;
2) спільні дії щодо захисту об'єктів критичної інформаційної інфраструктури та надання інформації для покращення системи реагування на кіберінциденти;
3) обмін досвідом у межах системи управління ризиками (Risk Management).

У середині травня 2021 р. стало відомо про створення в Україні національних кібервійськ. Цю ініціативу одноголосно підтримали усі 21 член РНБО України[172]. У травні 2021 р. відбулося офіційне відкриття державного центру для захисту держструктур та бізнесу від кібератак. Він отримав назву «Кіберцентр UA30».

Фахівці Ситуаційного центру забезпечення кібербезпеки СБУ у грудні 2021 р. припинили та нейтралізували 59 кібератак на інформаційні системи органів державної влади. Це сталося шляхом безпосереднього аналізу понад 28 тис. критичних подій інформаційної безпеки, виявлених за місяць. Основними типами виявлених кіберзагроз (хакерських атак) були:

1) з'єднання з командно-контрольними серверами (C&C Server);
2) спроби отримання несанкціонованого доступу (Brute Force Attack);
3) атаки на веб-програми (Web App Attack);

[172] Информационная безопасность на Украине. URL: https://www.tadviser.ru/

4) шкідливе програмне забезпечення (Malware)[173].

У ніч на 15 січня 2022 р. невідомі зловмисники атакували сайти МОН України, Мінагрполітики та МЗС України та розмістили там звернення до громадян країни з погрозами українською, російською та польською мовами. Хоча ця атака відбулася в умовах напруженості між РФ та Україною, Київ поки не став звинувачувати Москву. Водночас у Польщі чиновники вказали на РФ як можливе джерело нападу.

НАТО після масштабної атаки хакерів на урядові сайти в Україні пообіцяла Києву посилити співпрацю в галузі кібернетичної безпеки. Тим самим Північноатлантичний альянс, як підкреслив генеральний секретар НАТО Єнс Столтенберг вирішив відреагувати на інцидент.

«Найближчими днями НАТО та Україна підпишуть угоду про посилену кіберспівпрацю, яка, крім іншого, передбачає доступ України до платформи НАТО для обміну інформацією про шкідливі програми», – заявив Є. Столтенберг. Він нагадав, що Північноатлантичний альянс уже багато років співпрацює з Україною для зміцнення її кібербезпеки.

ЄС та уряд ФРН також оголосили, що підтримають Україну у цій сфері. Верховний представник ЄС із закордонних справ та безпекової політики Жозеп Боррель на зустрічі глав зовнішньополітичних відомств країн ЄС у французькому Бресті заявив, що ЄС мобілізує всі засоби для підтримки Києва. Окрім технічної допомоги для України було заплановано екстрене засідання Комітету ЄС з політики та безпеки[174].

Державна служба спеціального зв'язку та захисту інформації внесла невідкладні законодавчі зміни для узаконення процедури BugBounty. Про це повідомив голова Держспецзв'язку Юрій Щиголь. За його словами, це

[173] Более полусотни кибератак на системы органов власти Украины отбили в декабре // Украинская правда. 2022. 4 января. URL: https://www.pravda.com.ua/rus/news/2022/01/4/7319426/

[174] НАТО поможет Украине усилить кибербезопасность // Deutsche Welle. 2022. 15 января. URL: https://www.dw.com/ru/nato-usilit-kibersotrudnichestvo-s-ukrainoj/a-60432756

зроблено для покращення стану кібербезпеки України та запобігання інцидентам, подібним до того, що стався 14 січня 2022 р..

«Такий підхід дозволяє залучити зовнішніх фахівців до пошуку помилок та вразливостей програмних продуктів, інформаційно-комунікаційних систем тощо і оперативно усувати всі недоліки та прогалини у безпеці», – йдеться у повідомленні прес-служби Держспецзв'язку. За інформацією відомства, для цього буде внесено зміни до Ст. 361 та 361-1 Кримінального кодексу України.

Зокрема, перша стосується несанкціонованого втручання у роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, друга – створення шкідливих програмних чи технічних засобів, а також їх поширення чи збут.

Крім цього, законодавчі новації передбачають запровадження в органах державної влади та на об'єктах критичної інформаційної інфраструктури посад офіцерів із кіберзахисту. Їм підпорядковуватимуться служби захисту інформації.

Також серед новацій:

1. Створення інструментів фінансового стимулювання співробітників державних органів, що виконують завдання з адміністрування ІТ-систем.
2. Посилення відповідальності посадових осіб за невиконання вимог щодо кіберзахисту в органах державної влади та на об'єктах критичної інформаційної інфраструктури.
3. Закріплення комплексу заходів щодо виявлення вразливостей та недоліків у налаштуванні інформаційних систем, в яких обробляються державні інформаційні ресурси.
4. Надання повноважень запроваджувати вимоги щодо кібербезпеки до підрядних організацій, які працюють з органами державної влади;

5. Надання повноважень від органів державної влади та об’єктів критичної інфраструктури вимагати усунення критичних уразливостей з подальшою звітністю, а також встановлення відповідальності за порушення чи невиконання зазначених вимо[175]г.

Сьогодні в Україні по суті три центри підготовки фахівців з кібербезпеки: Київський політехнічний університет, Харківський університет радіоелектроніки та Національний університет «Львівська політехніка». При цьому інтерес абітурієнтів до професії зростає. Щоб захоплені школярі за кілька років стартували свою кар’єру впевненими молодими фахівцями, необхідно вкладати у вищу освіту чималі ресурси. Тенденція така сама, як і в ІТ-сфері загалом: ЗВО варто поєднувати зусилля з бізнесом, щоб студенти отримували оптимальний мікс фундаментальних знань та навичок у роботі із сучасними технологіями.

Наразі в Україні працює одна урядова команда реагування на комп’ютерні надзвичайні події CERT-UA, яка контролює цей напрямок. Проте Держспецзв’язку та представники міської та обласної влади порушують питання про розміщення таких підрозділів у регіонах. Це масштабний державний проект, розроблений та запропонований Держспецзв’язку. Державна служба готова надати обладнання та поділитися знаннями, здійснювати координацію роботи регіонів як однієї великої команди[176].

Отже, аналіз національної безпеки України підтверджує високий рівень загрози, пов’язаної з транснаціональною кіберзлочинністю та спробами іноземних урядів, організацій та приватних осіб використати сучасні

---

[175] Нарожный Д. Госспецсвязи планирует существенно усилить кибербезопасность Украины // Delo.ua. 2022. 25 января. URL: https://delo.ua/telecom/gosspecsvyazi-planiruet-sushhestvenno-usilit-kiberbezopasnost-ukrainy-391811/

[176] Балашов В. В государстве – как в бизнесе. Какие подходы из мира предпринимателей могут усилить кибербезопасность в Украине // Dsnews.ua. 2021. 1 ноября. URL: https://www.dsnews.ua/spec/v-gosudarstve-kak-v-biznese-kakie-podhody-iz-mira-predprinimateley-mogut-usilit-kiberbezopasnost-v-ukraine-01112021-441499

інформаційні технології проти країни. Таким чином, розвиток національної системи кібербезпеки є життєво важливим для гарантування національної безпеки України. Для України можна запропонувати такі рекомендації щодо покращення стану забезпечення інформаційної безпеки: 1) чітко визначити рамки дії, цілі стратегії і саме тлумачення терміна «кібербезпека»; 2) співпрацювати з іншими країнами, що входять в ЄС, а також з комісією ЄС, щоб гарантувати узгоджений характер кібербезпеки.

ВИСНОВКИ

Під час написання магістерської роботи автор дійшов до таких *висновків*:

1. Комплекс проблем пов’язаних з кібербезпекою займає особливе місце серед найактуальніших питань сучасних міжнародних відносин. Для повної характеристики проблеми автор роботи дослідив джерела вітчизняної та зарубіжної історіографії. У своїх роботах представники вітчизняної та зарубіжної шкіл приходять до висновків, що очікується зростання кіберзлочинності і кількості атак, в тому числі на критичні інфраструктури. У таких умовах особливо важливо використовувати захисні продукти і рішення, що відповідають вимогам часу, впроваджувати автоматизацію забезпечення інформаційної безпеки, посилювати аутентифікацію віддалених користувачів. На думку науковців, рівень обізнаності та свідомості громадян і провідних світових компаній про проблеми кібербезпеки залишається низьким, починаючи з базових основ пошуку інформації та закінчуючи поведінкою в разі кібер-інцидентів, що вимагає проводити більш активну інформаційно-освітню роботу. Автору вдалося зібрати і опрацювати досить значну кількість доробок, систематизувати історіографію дослідження і, таким чином, узагальнити теоретико-методологічні аспекти кібербезпеки як складової сучасної системи міжнародних відносин. Однак, в жодній праці не було висвітлено чіткого механізму покращення стану інформаційної безпеки країн, які формують сучасну систему міжнародних відносин, що ще раз підкреслює актуальність обраної проблематики і вимагає детального її розкриття.

Проаналізувавши джерельну базу дослідження, яка складається з чотирьох груп джерел автор дипломної роботи прийшов до висновку, що договірно-правове співробітництво реалізується шляхом: 1) універсальних міжнародних договорів (Конвенція ООН проти транснаціональної

організованої злочинності); 2) багатосторонніх угод щодо боротьби з окремими злочинами (Європейська конвенція про кіберзлочинність); 3) регіональних багатосторонніх угод (Угода СНД в боротьбі зі злочинами в сфері комп'ютерної інформації); 4) рішень ООН і інших міжурядових органів; 5) двосторонніх угод держав. Міжнародне законодавство про злочини в сфері комп'ютерної інформації включає такі нормативно-правові акти: Конвенція РЄ про кіберзлочинність 2001 р.; Угода про співробітництво в боротьбі зі злочинами в сфері комп'ютерної інформації, підписана країнами-членами СНД у 2001 р.; Конвенція ЛАД про боротьбу зі злочинами в області інформаційних технологій, прийнята ЛАД у 2010 р.; Угода про співробітництво в галузі забезпечення міжнародної інформаційної безпеки, прийнята ШОС в 2010 р.; Конвенція АС про кібербезпеку і захист персональних даних 2014 р. Проаналізувавши національне законодавство різних країн світу у сфері боротьби з кіберзлочинністю, автор дипломної роботи, прийшов до висновку, що зараз: а) прискорюється тенденція до фрагментації міжнародних підходів в рамках окремо взятих регіональних об'єднань, які приймають і реалізують власні специфічні підходи до даної проблеми; б) протиріччя між національними державами з питань основних законодавчих ініціатив і принципів багатосторонньої співпраці, які, як наприклад у випадку з відмовою РФ від підписання Конвенції РЄ від 2001 р., можуть поставити під удар національний суверенітет країни; в) наявність правового відставання від процесів розвитку інформаційних технологій, коли, юридичні норми не встигають врегулювати поведінку з використанням конкретних технологій, а в найближчому часі з'являються вже інші, поведінка в яких так само вимагає регулювання. Третя (статистична та довідкова інформація) і четверта група джерел (публікації зі ЗМІ) відіграли одну з найважливіших ролей під час написання дипломної роботи, адже саме за їх допомогою автор проаналізував сучасний стан та перспективи розвитку кібербезпеки як складової системи міжнародних відносин.

2. Надзвичайно високий динамізм розвитку та реструктуризація всієї системи міжнародних відносин зумовили необхідність переосмислення традиційних і розробки нових підходів до вивчення кібербезпеки. Виникла необхідність переосмислення основних категорій науки. Це стосується насамперед такого базового поняття, як «інформаційна безпека». Під час дослідження обраної проблематики автор використав технологічний, політологічний та системний підходи. Значну роль відіграли принципи комплексності та об'єктивності, а також порівняльний та історичний підходи.

Автором були використані такі методи: аналізу та синтезу, індукції та дедукції, класифікації, хронології, структурно-функціональний метод, порівняльно-історичний метод, порівняльно-правовий метод, описовий метод, методи статистичного аналізу, метод узагальнення та нормативний метод. Також у процесі написання дипломної роботи було застосовано такі методи дослідження, як теоретичний аналіз, узагальнення, порівняння, класифікування, спостереження, моделювання, а також метод прогнозування.

Аналіз понятійно-категоріального апарату дослідження передбачає розкриття таких термінів: *кіберзлочинність* – будь-яка злочинна активність у віртуальному просторі (кіберпросторі); *кіберзлочини* – дії, що здійснюються проти конфіденційності, цілісності, а так само доступності комп'ютерних систем, мереж та інформації, і зловживання даними системами мережами і даними в злочинних цілях; *кібертероризм* – дії спрямовані на дезорганізацію автоматизованих інформаційних систем, що створюють загрозу життю людей, заподіюють значну матеріальну шкоду або призводять до інших суспільно небезпечних наслідків; к*омп'ютерні злочини* – це передбачені кримінальним законом суспільно небезпечні дії, в яких машинна інформація є об'єктом злочинного зазіхання; *інформаційна війна* – широкомасштабна інформаційна боротьба із застосуванням способів і засобів інформаційного впливу на супротивника в інтересах досягнення цілей впливаючої сторони. Можна виділити такі види кіберзлочинів: 1) фінансово-орієнтовані

кіберзлочини (фішинг, кібервимагання, фінансове шахрайство); 2) кіберзлочини, пов’язані з вторгненням в особисте життя (крадіжка персональних даних, шпигунство, порушення авторських прав, спам, соціальні та політично мотивовані кіберзлочини, злочини на ґрунті ненависті та домагання, кібербулінг, протизаконна порнографія, грумінг, поширення наркотиків і зброї).

3. Підвищена увага у Національній кіберстратегії США (2018 р.) приділяється покращенню кібербезпеки на транспортній та морській інфраструктурі, а також у космосі. У міру модернізації цих секторів вони стають більш вразливими для кібератак. Значний акцент у Стратегії зроблено на дії, що мають сприяти розширенню американського впливу у світі. Одним із таких напрямків є розвиток можливостей країн-партнерів щодо протидії кіберзлочинності. Важливим елементом політики США щодо розширення свого впливу є просування нових технологій та надання консультацій з питань розгортання інфраструктури, управління ризиками, вироблення політики та стандартів для розширення охоплення глобального Інтернету та забезпечення його сумісності, безпеки та стабільності. Впровадження зарубіжних ноу-хау та стандартів кібербезпеки у національні технічні розробки може призвести не тільки до втрати технологічного суверенітету в цій важливій галузі, але й до появи недокументованих програмно-апаратних функцій. У Стратегії не окреслено планів щодо створення міжнародних правових механізмів, які могли б незалежно, об’єктивно та з належною компетенцією провести легітимне розслідування та винести судове рішення щодо зловмисних актів у ІКТ-середовищі.

4. У державній стратегічній програмі інноваційного розвитку КНР закріплені важливі положення про розвиток кіберпростору та забезпечення його безпеки. Інформаційна безпека для КНР – це насамперед безпека його інновацій, і в цьому важлива особливість підходу країни до інформаційної та кібербезпеки. У КНР відсутня єдина стратегія розвитку кіберпростору та

забезпечення безпеки інформаційних систем, але це зовсім не означає, що немає концептуального обґрунтування значущості проблеми. Основним документом, в якому наголошується на значній ролі ІКТ у житті китайського суспільства, є Всеосяжна концепція національної безпеки Китаю. У концепції зазначено, що сучасний світ як відкриває багато можливостей, так і створює загрози політичної, економічної, військової безпеки КНР. Велику увагу в документі приділено Інтернету як найбільш значущому, але найменш керованому сегменту глобального інформаційного простору.

5. Стратегії кібербезпеки країн ЄС значною мірою відрізняються від стратегій США та КНР. Враховуючи взаємозв'язок між станом кібербезпеки країни та рівнем економічного розвитку, кіберпростір для європейських держав є інструментом досягнення певних економічних цілей. Кіберзагрози, що згадуються в стратегіях, представлені в основному, у вигляді різних варіантів кібератак і у вигляді інших можливостей неправомірного використання кіберпростору, що говорить про практичну спрямованість стратегій кібербезпеки. Питання використання кіберпростору для досягнення глобальних геополітичних чи військових цілей у національних стратегіях зазвичай не висвітлюються, за винятком стратегії ФРН, проте це питання регламентується на наднаціональному рівні. Держави-члени активно співпрацюють з НАТО в галузі забезпечення кібербезпеки, крім того проводять спільні навчання, спрямовані не тільки на попередження кіберзагроз, але й на опрацювання наступальних дій у кіберпросторі.

6. Незважаючи на помітний прогрес у поширенні цифрових рішень для африканських проблем та наявність передових країн-флагманів ІТ-індустрії, сьогодні лише 28% африканців мають доступ до Інтернету. Проте не варто розраховувати, що дві третини ринку, що залишилися, довго чекатимуть інвесторів і підрядників. Автором з'ясовано, що темпи скорочення відриву Африки на південь від Сахари від інших регіонів світу у питанні Інтернет-доступності на душу населення надзвичайно високі. Коронавірусна пандемія

виступила каталізатором процесу цифровізації, прискоривши приплив капіталу в область африканських ІКТ. Так, Лагос, Найробі та Йоганнесбург претендують на статус цифрової столиці Африки, вкладаючись у мережеву інфраструктуру та колекціонуючи представництва найбільших міжнародних ІТ-компаній від “Twitter” та “MasterCard” до “Amazon” та “Microsoft”, що відкривають для себе бездонні африканські ринки. Проблема забезпечення кібербезпеки в Африці не вичерпується вразливістю державних відомств та інфраструктури, окремий інтерес становить комерційний сегмент.

7. Проблеми чинного міжнародного законодавства про злочини в сфері комп’ютерної інформації демонструють той факт, що кіберзлочинність не зникне, оскільки є побічним продуктом епохи Інтернету, який, стає основою існування сучасного суспільства. Необхідно сформувати ефективну систему боротьби з кіберзлочинами, яка буде спрямована, перш за все, на їх попередження та запобігання. У зв’язку з цим, для вирішення зазначених проблем, а також протидії кіберзлочинності, автор дипломної роботи вважає за необхідне законодавцю спільно з правоохоронними органами розробити міжнародну концепцію кримінально-правової політики в області захисту суспільства і держави від злочинів у сфері високих інформаційних технологій, а також забезпечення безпеки інформаційних процесів.

8. Питання забезпечення кібербезпеки надзвичайно актуальні для України, а заходи щодо протидії викликам та загрозам у зазначеній сфері знаходяться на початковому етапі та не мають комплексного характеру. Досліджуючи дане питання, автор дипломної роботи також хотів би акцентувати увагу на тому, що даний момент є досить актуальним сьогодні й для нашої країни, особливо враховуючи той факт, що нажаль, інформаційна політика України має багато недоліків, а головне несвоєчасність реагування на ті чи інші події, що досить негативно впливає на подальше прийняття рішень. Питання інформаційної безпеки держави повинні забезпечуватись системно і стосуватися таких сфер, як: а) внутрішня політика України –

захист внутрішнього інформаційного простору – Міністерство внутрішніх справ і Служба безпеки України; б) міжнародна сфера – забезпечення суверенітету країни, зміцнення державних позицій України, перешкоджання зовнішньої інформаційної експансії – МЗС України, Служба зовнішньої розвідки України; в) військова сфера – захист суверенітету, державної та територіальної цілісності – Міністерство оборони України; г) соціальна і духовна сфера – забезпечення інформаційного та культурного впливу за кордоном, використання «м'якої сили» – Міністерство культури, Міністерство соціальної політики, МЗС України; д) інформаційна сфера – пошук та надання інформаційних каналів для інформування громадськості, а також захист державних інформаційних ресурсів – Міністерство транспорту і зв'язку, Національна рада України з питань телебачення та радіомовлення. Тому, враховуючи досвід вище розглянутих країн, наша держава повинна сформувати власну інформаційну політику стосовно кіберзлочинності, застосовуючи метод «міксування», беручи за основу найкращі складові інших країн у даній галузі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ТА ЛІТЕРАТУРИ

ДЖЕРЕЛА

Міжнародні договори та угоди

1. Резолюция 60/45, принятая Генеральной Ассамблеей Организации Объединенных Наций, «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» // eSubscription to United Nations Documents. URL: https://undocs.org/pdf?symbol=ru/A/RES/73/27
2. Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации // Верховна Рада України. 2001. URL: https://zakon.rada.gov.ua/laws/show/997_353#Text
3. African Union Convention on Cyber Security and Personal Data Protection // African Union. 2014. URL: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection
4. Arab Convention on Combating Information Technology Offences // Asian School of Cyber Laws. 2010. URL: https://www.asianlaws.org/gcld/cyberlawdb/GCC/Arab%20Convention%20on%20Combating%20Information%20Technology%20Offences.pdf
5. Computer Crime and Cybercrime: Southern African Development Community (SADC) Model Law // ITU. 2012. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/SADC%20Model%20Law%20Cybercrime.pdf
6. Convention on Cybercrime // Council of Europe. 2001. URL: https://rm.coe.int/1680081561
7. Cybercrime: The Council of Europe Convention // EveryCRSReport.com. URL: https://www.everycrsreport.com/reports/RS21208.html

8. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace // European Union: official web-site. 2013. URL: http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf
9. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union // EUR-Lex. URL: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32016L1148
10. Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA // EUR-Lex. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011L0093
11. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA // EUR-Lex. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32013L0040
12. Directive C/DIR. 1/08/11 on fighting cyber crime within ECOWAS // Economic Community of West African States(ECOWAS). 2011. URL: http://www.tit.comm.ecowas.int/wp-content/uploads/2015/11/SIGNED_Cybercrime_En.pdf
13. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union // Official Journal of the European Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

14. Europe 2020. A European strategy for smart, sustainable and inclusive growth // European Union official web-site. URL: https://ec.europa.eu/eu2020/pdf/COMPLET%20EN%20BARROSO%20%20%20007%20-%20Europe%202020%20-%20EN%20version.pdf
15. International code of conduct for information security // United Nations Organisation. URL: https://digitallibrary.un.org
16. Okinawa Charter on Global Information Society // Ministry of foreign affairs of Japan. 2000. URL: https://www.mofa.go.jp/policy/economy/summit/2000/documents/charter.html#:~:text=Information%20and%20Communications%20Technology%20(IT,shaping%20the%20twenty%2Dfirst%20century.&text=The%20essence%20of%20the%20IT,to%20use%20knowledge%20and%20ideas.
17. Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardization // EUR-Lex. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32012R1025
18. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 // Official Journal of the European Union. URL: http://data.europa.eu/eli/reg/2016/679/oj
19. Strategic Concept 2010 // NATO: official we-site. 2010. URL: https://www.nato.int/cps/en/natohq/topics_82705.htm
20. Tallinn Manual on the International Law Applicable to Cyber Warfare // Cambridge University Press 2021. 2013. URL: https://www.cambridge.org/core/books/tallinn-manual-on-the-international-law-applicable-to-cyber-warfare/50C5BFF166A7FED75B4EA643AC677DAE
21. The Treaty on European Union and the Treaty on the Functioning of the European Union // EUR-Lex. URL: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT

Офіційні нормативно-правові акти держав

22. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України №447/2021 // Президент України: офіційне Інтернет-представництво. URL: https://www.president.gov.ua/documents/4472021-40013
23. A National Security Strategy of Engagement and Enlargement // The Historical Office of the Office of the Secretary of Defense. 1995. URL: https://history.defense.gov/Portals/70/Documents/nss/nss1995.pdf?ver=pzgo9pkDsWmIQqTYTC6O-Q%3d%3d
24. A national cyber security strategy // Government offices of Sweden: official web-site. 2016. URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/swedish-national-cyber-security-strategy
25. Austrian Cyber Security Strategy // ENISA: official web-site. 2013. URL:: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/austrian-cyber-security-strategy
26. Computer Fraud and Abuse Act // The Free Encyclopedia Wikipedia.URL: https://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act
27. Cybersecurity Act // Riigikantselei. 2019. URL: https://www.riigiteataja.ee/en/eli/523052018003/consolide
28. Cyber Security Strategy for Germany // Federal Ministry of the Interior. 2011. URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-for-germany
29. Cybersecurity and Infrastructure Security Agency Act of 2018 // The White House. URL: https://www.congress.gov/bill/115th-congress/house-bill/3359
30. Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection. // U.S. Department of

Homeland Security. 2003. 17 of December. URL: https://www.dhs.gov/homeland-security-presidential-directive-7

31. National Cyber Security Strategy for Norway // ENISA. 2018. URL: https://www.enisa.europa.eu
32. National Cyber Strategy of the United States of America // The White House. 2018. URL: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf
33. The Cybersecurity Law of the People's Republic of China // New America. URL: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecuritylaw-peoples-republic-china/
34. The National Strategy to Secure Cyber Space // The White House. 2003. URL: http://georgewbush-whitehouse.archives.gov/pcipb/
35. U.S. Cyber Command's Malware Inoculation: Linking Offense and Defense in Cyberspace // Council of foreign relation. 2020. URL: https://www.cfr.org/blog/us-cyber-commands-malware-inoculation-linking-offense-and-defense-cyberspace

Статистична та довідкова інформація

21. Обзор киберугроз 2020: результат пандемии // TechExpert. 2020. URL: https://techexpert.ua/ru/cybersecurity-covid/
22. Рейтинг стран мира по уровню подверженности киберугрозам 2020 (CEI – Cybersecurity Exposure Index) // 10 GUARDS. URL: https://10guards.com/ru/articles/global-cybersecurity-exposure-index-2020/
23. Убытки от киберпреступности в мире выросли за два года на 50% до $945 млрд. // Фориншурер. 2020. URL: https://forinsurer.com/news/20/12/10/38866
24. Cybercrime Industry 2021 // Reportlinker.com. 2021. URL: https://www.reportlinker.com/market-report/Cybersecurity/517797/Cybercrime?gclid=Cj0KCQjwwLKFBhDPAR

IsAPzPi-JyjmGL1ahfKru6oLq3xDVnNViF9zWpUMnZJMsucuwNLukX0KZDiHEaAnn9EALw_wcB

25. Global Cybersecurity Index (GCI) // International Telecommunication Union. 2018. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf
26. The COVID-19 pandemic and trends in technology // Chatham House, The Royal Institute of International Affairs. 2021. URL: https://www.chathamhouse.org/2021/02/covid-19-pandemic-and-trends-technology/03-covid-19-changing-cybercrime-landscape
27. The State of Ransomware 2021 // SOPHOS: official web-site. 2021. URL: https://secure2.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf
28. Why cybercrime is increasing – and how to stay secure // RSM network. URL: https://www.rsmuk.com/ideas-and-insights/why-cybercrime-is-increasing-and-how-to-stay-secure

Публікації зі ЗМІ

29. Африка упускает из виду свою кибербезопасность? // Le journal de l'Afrique: official web-site. URL: https://lejournaldelafrique.com/ru/lafrique-dapres/lafrique-est-elle-en-train-de-passer-a-cote-de-sa-cybersecurite/?amp=1
30. Более полусотни кибератак на системы органов власти Украины отбили в декабре // Украинская правда. 2022. 4 января. URL: https://www.pravda.com.ua/rus/news/2022/01/4/7319426/
31. Варшавський саміт НАТО – критичний аналіз головних рішень // «Хвиля.нет»: офіційна сторінка газети. 2016. URL: http://hvylya.net/analytics/geopolitics/varshavskiy–samit–nato–kritichniy–analiz–golovnih–rishen.html

32. Генассамблея ООН проголосовала за российский проект резолюции по глобальной кибербезопасности // Экспертный центр электронного государства. 2018. URL: https://d-russia.ru/genassambleya-oon-progolosovala-za-rossijskij-proekt-rezolyutsii-po-globalnoj-kiberbezopasnosti.html
33. Генеральний секретар НАТО Єнс Столтенберг розповів про збільшення кібератак на НАТО // «Deutsche Welle»: офіційна сторінка газети. 2016. URL: http://bit.ly/2luWZKb
34. Китай устроил кибератаку на компании из США и Японии // РБК. 2015-2020. URL: https://quote.rbc.ru/news/article/5ae098a62ae5961b67a1c1d1
35. НАТО поможет Украине усилить кибербезопасность // Deutsche Welle. 2022. 15 января. URL: https://www.dw.com/ru/nato-usilit-kibersotrudnichestvo-s-ukrainoj/a-60432756
36. Пентагон изменил стратегию киберкомандования США // News.com. 2018. URL: https://www.newsru.com/world/18jun2018/cyber.html
37. Перестройка кибербезопасности для создания более безопасной сети для всех – TechCrunch // Hitech Glitz. URL: https://hitechglitz.com/russia/%D0%BF%D0%B5%D1%80%D0%B5%D1%81%D1%82%D1%80%D0%BE%D0%B9%D0%BA%D0%B0-%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D0%B8-%D0%B4%D0%BB%D1%8F-%D1%81/
38. Президент утвердил новую Стратегию кибербезопасности Украины // УКРінформ. 2021. 26 серпня. URL: https://www.ukrinform.ru/rubric-polytics/3304776-prezident-utverdil-novuu-strategiu-kiberbezopasnosti-ukrainy.html
39. Трамп визнав кібервтручання Росії у вибори в США // «Deutsche Welle»: офіційна сторінка газети. 2016.URL: http://bit.ly/2lzDtup

40. Africa’s Evolving Cyber Threats // Africa Center for Strategic Studies: official web-site. 2021. 19 of January. URL: https://africacenter.org/spotlight/africa-evolving-cyber-threats/
41. Ransomware recovery cost more than doubles // IT-online. 2021. 29 of April. URL: https://it-online.co.za/2021/04/29/ransomware-recovery-cost-more-than-doubles/

ЛІТЕРАТУРА

Монографії, підручники, посібники

42. Боднар І. Міжнародна інформація: Навчально-методичний посібник для самостійного вивчення курсу. Львів: «Новий Світ-2000», 2005. 216 с.
43. Гафнер В. В. Информационная безопасность: Учебное пособие. Рн/Д: Феникс, 2010. 324 с.
44. Громов Ю. Ю. Информационная безопасность и защита информации: Учебное пособие. Ст. Оскол: ТНТ, 2010. 384 с.
45. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва : монографія. Київ: НІСД, 2014. 328 с.
46. Карпенко В. О. Інформаційна політика та безпека: Підручник. Київ: Нора-Друк, 2006. 320 с.
47. Кудрявцева С. П. Міжнародна інформація. навч. посіб. для студентів вищих навч. закл. Київ: Видавничий Дім «Слово», 2005. 400 с.
48. Макаренко Є. А. Міжнародні інформаційні відносини: монографія. Київ: Наша культура і наука, 2002. 452 с.
49. Макаренко Є. А. Міжнародна інформаційна безпека: сучасні виклики та загрози. Київ: Центр вільної преси, 2006. 916 с.
50. Макаренко С. И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI. СПб.: Наукоемкие технологии, 2017. 546 с.
51. Манойло А. В. Государственная информационная политика в особых

условиях: Монография. Москва: МИФИ, 2003. 388 с.

52. Міжнародна інформаційна безпека: теорія і практика: підручник // Макаренко Є.А., Рижков М.М., Ожеван М.А., Кучмій О.П., Фролова О.М. Київ: Центр вільної преси, 2016. 418 с.
53. Почепцов Г. Г. Інформаційна політика: навчальний посібник. Київ: Знання, 2006. 663 с.
54. Юдін О. К. Інформаційна безпека держави: навчальний посібник. Харків: Консум, 2005. 576 с.
55. Brown C. Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice // International Journal of Cyber Criminology Vol 9 Issue 1 January. June 2015. 65 p.
56. Edgar Th. Research Methods for Cyber Security. Elsevier Science, 2017. 428 p.
57. Goldman J. Intelligence and Information Policy for National Security: Key Terms and Concepts. Rowman & Littlefield. 2016. 654 p.
58. Libicki M.C. Conquest in Cyberspace: National Security and Information Warfare. Cambridge: Cambridge University Press, 2007. 336 p.
59. Ventre D. Chinese Cybersecurity and Defense. London // Wiley-ISTE Publ., 2014. 301 p.

Статті

60. Атнашев В. Р. Международное сотрудничество в борьбе с киберпреступностью и кибертерроризмом // ЕВРАЗИЙСКАЯ ИНТЕГРАЦИЯ: экономика, право, политика. 2019. № 3. С. 37-42.
61. Балашов В. В государстве – как в бизнесе. Какие подходы из мира предпринимателей могут усилить кибербезопасность в Украине // Dsnews.ua. 2021. 1 ноября. URL: https://www.dsnews.ua/spec/v-gosudarstve-kak-v-biznese-kakie-podhody-iz-mira-predprinimateley-mogut-usilit-kiberbezopasnost-v-ukraine-01112021-441499

62. Бородакий Ю.В. Кибербезопасность как основной фактор национальной и международной безопасности XX! века (часть 1) // Вопросы кибербезопасности. 2013. № 1. С. 2-9.
63. Булай. Ю. Г. Профилактика и противодействие киберпреступности, а также международным киберугрозам // Академическая мысль. 2017. № 1. URL: https://cyberleninka.ru/article/n/profilaktika-i-protivodeystvie-kiberprestupnosti-a-takzhe-mezhdunarodnym-kiberugrozam
64. Войціховський А. В. Міжнародне співробітництво в боротьбі з кіберзлочинністю. Право і безпека. 2011. № 4 (41). С. 107-112.
65. Герасимчук Т.Ф. Теоретико-концептуальні основи та методи дослідження міжнародних відносин // Український історичний журнал. 2006. № 5. С.188-199.
66. Демедюк С. В. Міжнародний досвід протидії кіберзлочинності. Вісник Харківського національного університету внутрішніх справ: збірник наукових праць. Харків. 2014. № 4 (67). С. 65-75.
67. Джердж С. Ф. Інформаційна безпека як частина євроатлантичної стратегії України. Миколаїв: Вид-во ЧНУ ім. Петра Могили, 2016. С. 16-21.
68. Джердж С. Ф. Інформаційна війна Росії проти України. Асиметрична відповідь // Науково-практичне видання «Мас-медіа. Демократія. Інформаційна війна». Київ: СПД Матвієнко. 2014. С. 4-7.
69. Журавленко Н. И. Проблемы борьбы с киберпреступностью и перспективные направления международного сотрудничества в этой сфере // Общество и право. 2015. № 3 (53). URL: https://cyberleninka.ru/article/n/problemy-borby-s-kiberprestupnostyu-i-perspektivnye-napravleniya-mezhdunarodnogo-sotrudnichestva-v-etoy-sfere
70. Журенко Е. Рынок кибербезопасности на Ближнем Востоке и в Африке // Creditplus. 2021. 10 августа. URL: https://creditplus.ua/ru/blog/kiberbezopasnost-na-vostoke-i-v-afrike

71. Информационная безопасность на Украине // TAdviser.com. 2021. 4 октября. URL: https://www.tadviser.ru/
72. Каберник В. В. Проблемы классификации кибероружия // Вестник МГИМО. 2013. №2 (29). URL: https://cyberleninka.ru/article/n/problemy-klassifikatsii-kiberoruzhiya
73. Кардава Н. В. Политика обеспечения кибербезопасности в Европейском Союзе: национальный и наднациональный уровни // Каспийский регион: политика, экономика, культура, 2019. № 3(60). С. 74-76.
74. Киберпреступления: понятие, виды и методы защиты // Sys-team-admin.ru. 2018. URL: https://sys-team-admin.ru/stati/bezopasnost/170-kiberprestupnost-ponyatie-vidy-i-metody-zashchity.html
75. Киберпреступность и закон: обзор положений законодательства Великобритании // АО Kaspersky Lab. 2009. URL: https://securelist.ru/kiberprestupnost-i-zakon-obzor-polo/1315/
76. Кибервойска Европы и НАТО // РСДМ. URL: https://russiancouncil.ru/analytics-and-comments/analytics/kibervoyska-evropy-i-nato/
77. Ковалев А. А. Международно-правовые аспекты политики кибербезопасности некоторых европейских стран бывшего советского блока // Вестник ПАГС. 2018. №5. С. 105-114. URL: https://cyberleninka.ru/article/n/mezhdunarodno-pravovye-aspekty-politiki-kiberbezopasnosti-nekotoryh-evropeyskih-stran-byvshego-sovetskogo-bloka
78. Копійка М.В. Модернізація політики міжнародних організацій у сфері інформаційної безпеки // Політичні проблеми міжнародних систем та глобального розвитку. 2020. С. 102-109.
79. Куява Т. Ю. Киберпреступность: проблемы уголовно-правовой оценки и организации противодействия // Молодой ученый. 2016. № 29 (133). С. 255-257. URL: https://moluch.ru/archive/133/37306/

80. Нарожный Д. Госспецсвязи планирует существенно усилить кибербезопасность Украины // Delo.ua. 2022. 25 января. URL: https://delo.ua/telecom/gosspecsvyazi-planiruet-sushhestvenno-usilit-kiberbezopasnost-ukrainy-391811/
81. Национальная оборона Китая в 2002 году // Информационное бюро Государственного совета Народной Республики Китай. 2002. URL: http://www.scio.gov.cn/zfbps/ndhf/2002/Document/307925/307925
82. Панцерев К. А. Страны Африки Южнее Сахары в цифровую эпоху: к вопросу обеспечения информационного суверенитета // Азия и Африка сегодня. 2019. № 10. С. 10-16.
83. Петров В. Международные угрозы вынуждают Киев создать национальную систему кибербезопасности // per Concordiam. 2016. 7 января.URL: https://perconcordiam.com/ru/%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C-%D0%BD%D0%B0-%D1%83%D0%BA%D1%80%D0%B0%D0%B8%D0%BD%D0%B5/
84. Разумов Е.А. Политика КНР по обеспечению кибербезопасности // Россия и АТР. 2017. № 4 (98). С. 156-170. URL: https://cyberleninka.ru/article/n/politika-knr-po-obespecheniyu-kiberbezopasnosti
85. Рогожин А.А. КНР – Закон о кибербезопасности принят // ИМЭМО РАН. 2017. URL: https://www.imemo.ru/news/events/text/knr-zakon-o-kiberbezopasnosti-prinyat.
86. Скулиш Є. Д. Міжнародно-правове співробітництво у сфері подолання кіберзлочинності // Інформація і право. 2014. № 1. С. 93-100. URL: http://nbuv.gov.ua/UJRN/Infpr_2014_1_13.
87. Тарасенко Д. Зачем России Африка и с чем «ходить гулять»? // Российский совет по международным делам: РСМД. 2021. 20 августа.

URL: https://russiancouncil.ru/analytics-and-comments/analytics/zachem-rossii-afrika-i-s-chem-khodit-gulyat/

88. Цуканов Л. Кибербезопасность по-сомалийски // Российский совет по международным делам: РСМД. 2022. 17 января. URL: https://russiancouncil.ru/analytics-and-comments/columns/africa/kiberbezopasnost-po-somaliyski/
89. Шматкова Л. П. Международное сотрудничество в борьбе с киберпреступлениями: состояние и перспективы // Молодой ученый. 2016. № 28 (132). С. 720-723. URL: https://moluch.ru/archive/132/37021/
90. Яцишин М. Ю. Роль міжнародних організацій у протидії кіберзлочинності // Українське право. 2019. URL: https://ukrainepravo.com/international_law/public_international_law/rol-mizhnarodnykh-organizatsiy-u-protydiyi-kiberzlochynnosti/
91. Cebrovski A. Network–Centric Warfare: Its Origin and Future // Proceedings. 1998. January. URL: http:// www. kinection.com/ncoic/ncw_origin_future.pdf
92. Collin B. The Future of CyberTerrorism: Where the Physical and Virtual Worlds Converge // Crime Research. URL: http://www.crime-research.org/library/Cyberter.htm
93. Denning D. E. Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy // Information Warfare Site. URL: http://www.iwar.org.uk/cyberterror/resources/denning.htm
94. Dennis M. A. Defenition of «Cybercrime» // Encyclopædia Britannica. 2018. URL: https://www.britannica.com/topic/cybercrime
95. European Cybercrime Centre – EC3 // Europol: official web-site. URL: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

96. Hoffman F. Hybrid vs Compound // Small Wars Journal. 2009. October. URL: http://smallwarsjournal.com /blog/journal/docs–temp/189–hoffman.pdf.
97. Lewis J. A. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats // Center for Strategic and International Studies, December 2002. 12 p.
98. Lindsay J. R. The Impact of China on Cybersecurity // International Security. 2015. Vol. 39. P. 7-47. URL: https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=2849&context=lawreview
99. Marc D. Goodman and Susan W. Brenner. The emerging consensus on criminal conduct in cyberspace // Archive.org. 2018. URL: https://archive.org/details/TheEmergingConsensusOnCriminalConductInCyberspace
100. Nye J.S. Cyber Power. Cambridge: Pub. by Belfer Center for Science and International Affairs, 2010. 26 p.
101. Orange Cyberdefense // TADVISER. 2022. URL: https://www.tadviser.ru/index.php/%D0%9A%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F:Orange_Cyberdefense
102. Yan S. China’s new cybersecurity law takes effect today, and many are confused // CNBC. 2017. URL: https://www.cnbc.com/2017/05/31/chinas-new-cybersecurity-law-takes-effect-today.html
103. Williams P. Organized Crime and Cybercrime: Synergies, Trends, and Responses // Crime Research. 2018. URL: http://www.crime-research.org/library/Cybercrime.htm

Автореферати дисертацій:

104. Буяджи С.А. Правове регулювання боротьби з кіберзлочинністю: теоретико-правовий аспект: дис. … здоб. наук. ступ. канд. юрид. наук. 12.00.01. Київ, 2018. 203 с.